Slobodan Vujošević

MATEMATIČKA LOGIKA

O MOGUĆNOSTIMA FORMALNOG METODA

CID

PODGORICA
1996

Slobodan Vujošević,
Matematička logika: o mogućnostima formalnog metoda
ISBN 86-495-0019-6

Elektronsko izdanje
Matematički fakultet

BEOGRAD
2013

Metod formalizacije

Jezik se menja, obogaćuje se novim rečima, menja se upotreba ili značenje postojećih reči i u krajnjem, menja se njegova struktura. Međutim, postoje nepromenljivi fragmenti jezika, otporni na njegovu svakodnevnu upotrebu, na prevođenje sa jednog na drugi jezik, na promene gramatičkih pravila ili na uvođenje novih reči. Značenje takvih fragmenata je konstantno i oni se nužno javljaju u svim prirodnim jezicima. U odnosu na *rečenicu* kao osnovnu gramatičku kategoriju, svaki jezik sadrži *veznike* "i, ili, ne, ako onda, za svaki i ineki." Struktura koju veznici ovog tipa određuju u klasi svih rečenica prirodnog jezika je nepromenljiva i nazivaćemo je *logikom*.

Globalna struktura jezika je znatno složenija i sigurno sadrži i oblike koji nisu obuhvaćeni ovom definicijom. Razlozi zbog kojih smo se opredelili da se na ovom nivou bavimo logikom prevashodno su matematički. Sa filosofskog ili lingvističkog stanovišta definicija konstantne strukture jezika bi mogla izgledati i nešto drugačije. Ovako postavljena, ona odgovara potrebama matematike iz dva razloga: prvo, ovaj fragment jezika sadrži sva matematička tvrđenja i drugo, on sam može se izučavati matematičkim sredstvima.

Kako je matematika inkorporirana u konstantnu strukturu jezika, kada istražuje takvu strukturu ona se na određen način bavi i sama sobom. Ali za razliku od filosofije ili književne kritike, koje su prosto opsednute takvim pitanjima, razlozi zbog kojih se matematika bavi sama sobom, tj. fragmentima prirodnog jezika, koje ona sama koristi i u kojima se izražavaju njena tvrđenja, mnogo su dublji. Za matematiku jeste značajan i jedan krug pitanja filosofskog karaktera koji se javlja u logičkoj analizi matematičkih argumenata, ali potreba za takvom analizom prevashodno postoji zbog konkretnih matematičkih problema – matematika se nužno bavi i sama sobom zato što jedan broj njenih problema nije moguće drugačije rešiti.

Iako se u okviru našeg izlaganja nećemo baviti istorijom, napominjemo da su se prva sistematska istraživanja logike matematičkim sredstvima javila u okviru Fregeovih nastojanja da matematiku zasnuje na logičkim i skupovno-teorijskim principima i u okviru Hilbertovih ambicija da dokaže "da opšte prihvaćeni matematički principi uzeti u svojoj ukupnosti ne dovode do kontradikcije". Značaj Gotloba Fregea je u tome što je izmislio formalni metod u savremenom smislu, a Davida Hilberta što je implicitno postavio grupu pitanja koja i danas čine centralni sadržaj *logike*. Uprošćeno rečeno, Frege je definisao sredstva, a Hilbert ciljeve logike kao posebne grane matematike.

Sa stanovišta njenih ciljeva, za logiku je značajna sledeća grupa pitanja:

– ukoliko uopšte imaju bilo kakav smisao, kakav je stvarni sadržaj matematičkih tvrđenja,

– šta su to matematički dokazi, kakvim sredstvima se mogu ostvarivati i kako se može proveriti njihova korektnost,

– da li postoje ograničenja dokazivosti matematičkih tvrđenja i ako uopšte postoje, kakva je priroda tih ograničenja,

– do kog stepena se matematički dokazi mogu mehanički reprodukovati, tj. da li postoji jednostavna lista pravila zaključivanja dovoljna da automatski reprodukuje sva matematička tvrđenja?

Sa stanovišta njenih sredstava, logika je nezaobilazan metod za rešavanje jedne grupe matematičkih problema. Postoje problemi koji se ne mogu rešiti, a često ni dobro razumeti, bez odgovarajuće logičke analize. Ovo naglašavamo zato što se logika često razume kao kontekst u kome se postojeće teorije mogu rigorozno izložiti, ali koji sa stanovišta konkretnih rezultata ne donosi praktično ništa novo. Istina, u ovom veku bilo je nekoliko pokušaja da se matematika celovito shvati kao jedinstven sistem zasnovan u teoriji skupova i logici, ali su takve ambicije danas uglavnom napuštene. Logika predstavlja samo jednu od matematičkih teorija u čijem okviru je razvijen jedan broj matematičkih metoda koji se po prirodi bitno ne razlikuju od metoda algebre, analize ili topologije, tj. koji su po svojoj prirodi matematički i služe za rešavanje matematičkih problema.

Na primer, na sadašnjem nivou razvoja matematike, problem hipoteze kontinuuma možemo razumeti jedino kao činjenicu da u skupu svih dokaza teorije skupova ne postoji dokaz hipoteze kontinuuma. Isto važi i za problem neprotivrečnosti aritmetike. U takvim slučajevima, logičke ideje kao što su teorija, dokaz ili neprotivrečnost moraju imati jasan matematički smisao. Bez prethodne formalizacije ovih ideja, problem kontinuuma ili problem neprotivrečnosti aritmetike uopšte i nije matematički problem. Svaki matematički problem može svesti na problem oblika: da li u nekoj klasi matematičkih objekata postoji objekt koji zadovoljava određene uslove. U slučaju problema kontinuuma, treba proveriti da li u klasi svih dokaza teorije skupova postoji dokaz hipoteze kontinuuma. To je moguće ako se sama matematička tvrđenja, jezik u kome su formulisana i njihovi dokazi, definišu kao i svi drugi matematički pojmovi.

Matematička tvrđenja izražavamo u *prirodnom jeziku*, poput srpskog ili ruskog, eventualno proširenom matematičkom terminologijom engleskog korena i specifičnom matematičkom simbolikom. Međutim, prirodni jezik dopušta određene nepreciznosti i neregularnosti, pa je logička analiza njegovih argumenata teško izvodljiva. On nije zaštićen od strukturnih protivrečnosti, pa je u izučavanju matematičkih tvrđenja neophodan *formalni jezik*, tj. jezik čija je struktura potpuno regularna. Sa jedne strane, on omogućava logička istraživanja matematičkog zaključivanja, a sa druge, matematičku analizu logičkih principa.

Iz tih razloga, prvi korak u izučavanju matematičke logike jeste izgradnja formalnog jezika. Takav jezik sadrži dve vrste simbola: jednu grupu čine simboli koji odgovaraju logičkim veznicima, kao što su konjunkcija, implikacija, negacija ili kvantifikatori, koji imaju fiksno značenje, a druga grupa sadrži simbole čije se značenje može menjati u zavisnosti od konkretnog konteksta koji nastojimo da formalno izrazimo i analiziramo.

U izučavanju svojstava formalnog jezika prirodno se javlja jasna razlika između formalnih problema i problema značenja. Prvi se odnose na strukturu izraza i u jeziku se javljaju nezavisno od interpretacije, a drugi na značenje izraza formalnog jezika kada se njegovi simboli interpretiraju na određeni način. Formalnu strukturu jezika nazivaćemo *sintaksom*, a strukturu njegovog značenja *semantikom*.

Kada je jezik predmet našeg izučavanja, treba voditi računa da se u tom slučaju uvek javljaju dva jezika: jezik koji razmatramo ili *objekt-jezik* i jezik u kome se takvo razmatranje izvodi ili *metajezik*. U opštem slučaju, to mogu biti bilo kakvi jezici, formalni, prirodni ili čak, jedan isti jezik može istovremenu biti i objekt-jezik i metajezik. Najčešće, objekt-jezik je formalni jezik, a metajezik je srpski jezik proširen terminologijom preuzetom iz stranih jezika i uobičajenim matematičkim simbolima. Ova razlika je uvek značajna, a u slučaju teorije skupova i aritmetike zapravo čini osnovu ovih teorija.

Objekt-jezici o kojima ćemo govoriti su formalni jezici u kojima se mogu formulisati matematičke teorije. Rečenicama takvih jezika izražavaju se svojstva matematičkih teorija poput aritmetike, analize, algebarskih teorija ili teorije skupova. Svojstva njihove sintakse i semantike izučavaju se i izražavaju u metajeziku koji je u potpunosti identičan jeziku matematike. To znači da se svojstva formalnih jezika dokazuju sredstvima kojima se dokazuju teoreme algebre, analize ili aritmetike. U tom smislu logika se ne razlikuje od drugih matematičkih teorija – problemi koje istražuje i metodi koje upotrebljava, po svojoj prirodi su matematički.

Tipična matematička struktura je neprazan skup na kome su definisane određene relacije i operacije. Takvi su brojevi, grupe, prsteni, polja, uređenja, mreže, vektorski i topološki prostori, a i sam jezik na kome se o tim strukturama govori. Pre nego što izložimo jedan jezik na kome je moguće izražavati svojstva matematičkih struktura razmotrićemo dva važna primera. To su strukture prirodnih i realnih brojeva. Veći deo matematičkog iskustva i znanja odnosi se na ove strukture, pa je stoga zanimljivo kako bi mogla izgledati formalizacija njihovih svojstava.

Prirodni brojevi

Strukturu prirodnih brojeva čine standardne aritmetičke operacije definisane na skupu prirodnih brojeva $\omega = \{0, 1, 2, \dots\}$. U pomalo opskurnom matematičkom jeziku *prirodni brojevi* se uobičajeno definišu kao struktura koja se grafički označava sa

$$\mathcal{N} = (\omega, +, \cdot, \leq, s, 0).$$

U oznaci strukture prirodnih brojeva javlja se sam skup prirodnih brojeva, jedna aritmetička relacija, tri operacije i jedan istaknuti element: grafički znak ω označava skup prirodnih brojeva, znak $+$ je grafička oznaka operacije sabiranja, $\cdot$ označava operaciju množenja, znakom $\leq$ označen je standardni poredak prirodnih brojeva, znak s označava funkciju naslednika i grafičkim znakom 0 označen je prirodan broj nula.

Svi matematički objekti su skupovi, pa dakle i jezik $\mathcal{L}$ na kome izražavamo svojstva strukture $\mathcal{N}$ mora biti skup. Elementi skupa $\mathcal{L}$ takođe su skupovi i nazivaćemo ih *simbolima*, slovima ili znacima. Kada je to neophodno simbole, kao elemente objekt-jezika, označavamo grafičkim znacima različitim od grafičkih oznaka objekata koji se javljaju u definiciji strukture $\mathcal{N}$. Vrste simbola koje treba da sadrži jezik $\mathcal{L}$ uslovljene su tipom strukture prirodnih brojeva i logičkim razlozima, tj. potrebama formalizacije logičkog fragmenta prirodnog jezika. To znači da jezik $\mathcal{L}$ sadrži grupu matematičkih i grupu logičkih simbola.

Pre svega, zapisivanje svojstva strukture $\mathcal{N}$ zahteva da jezik $\mathcal{L}$ sadrži simbole promenljivih. Svakom ko ima minimalno matematičko iskustvo, sama po sebi jasna je neophodnost ovakvih simbola. Pretpostavljamo da su promenljive jezika $\mathcal{L}$ individualne, što znači da *vrednosti promenljivih* mogu biti samo prirodni brojevi, tj. samo elementi domena strukture $\mathcal{N}$. Sami simboli promenljivih su elementi skupa $\mathcal{L}$, a označavamo ih grafičkim simbolima x, y, z ili na neki drugi način.

Drugo, jezik $\mathcal{L}$ morao bi da sadrži simbole aritmetičkih operacija, relacije poretka i konstante nula. U poretku u kome su navedene u definiciji strukture $\mathcal{N}$, njihove simbole, tj. elemente skupa $\mathcal{L}$, označavamo grafičkim simbolima $+$, $\cdot$, $\leq$, s i 0. Dakle, istim grafičkim simbolima označili smo dve različite stvari: elemente skupa $\mathcal{L}$ i operacije, relaciju i element skupa ω. To činimo da bismo izbegli grafičke komplikacije, a iz konteksta je uvek jasno na koje objekte referiraju konkretne grafičke oznake. U principu, kao skupovi, jezik $\mathcal{L}$ i struktura $\mathcal{N}$ ne moraju biti disjunktni. Jedan broj modelsko-teorijskih rezultata počiva na ideji da se strukture mogu konstruisati i od sintaksnog materijala.

Od operacijskih simbola, promenljivih i konstanti formiraju se matematički izrazi koje u logici uobičajeno nazivamo *termima*. Na primer, izrazi oblika $x + y, y \cdot (x + y)$ ili $s(s(y + x) + z)$ su termi jezika $\mathcal{L}$. Preciznije, kako su simboli $x, +$ i y skupovi, kao matematički objekt, izraz $x + y$ je zapravo uređena trojka $(+, x, y)$. U grafičkom zapisivanju terma upotrebljavamo levu i desnu zagradu, tj. jedan broj interpunkcijskih simbola. Oni obezbeđuju jednoznačno tumačenje ovih izraza ili jedinstveno čitanje. Pretpostavljamo da je intuitivno jasno kako terme interpretiramo u strukturi $\mathcal{N}$ prirodnih brojeva. Kada se zadaju vrednosti promenljivih u skupu prirodnih brojeva, izvršavanjem svih operacija koje se u njemu javljaju, svaki term dobija određenu vrednost u strukturi $\mathcal{N}$.

Osim terma, u izražavanju svojstava strukture $\mathcal{N}$ neophodni su nam i izrazi kojima se opisuju svojstva prirodnih brojeva. To podrazumeva da jezik $\mathcal{L}$ sadrži znak $\leq$ koji odgovara relaciji poretka $\leq$ u strukturi $\mathcal{N}$. Iako u oznaci strukture nije navedena, na svakom skupu definisana je relacija jednakosti. Stoga, pretpostavljamo da jezik $\mathcal{L}$ sadrži i binarni relacijski znak $=$ koji izražava jednakost elemenata strukture $\mathcal{N}$.

Koristeći terme i relacijske simbole, u jeziku $\mathcal{L}$ možemo izraziti jednostavna svojstva strukture $\mathcal{N}$. Kasnije ćemo precizno definisati postupak interpretacije svih formula jezika $\mathcal{L}$, a u ovom trenutku pretpostavljamo da je značenje formula poput $x + y = 0$ ili $x \cdot s(x) \leq z + y$ u strukturi $\mathcal{N}$ samo po sebi jasno. Takve formule, u kojima učestvuju samo relacijski simboli i termi jezika $\mathcal{L}$, nazivaćemo elementarnim formulama. Kada se u skupu ω pretpostave vrednosti promenljivih jezika $\mathcal{L}$, svaka elementarna formula izražava jedan konkretan odnos elemenata skupa ω, tj. istinita je ili lažna u strukturi $\mathcal{N}$. Za izražavanje složenijih svojstava strukture $\mathcal{N}$ koristimo simbole logičkih veznika, tj. simbole konjunkcije, disjunkcije, implikacije, ekvivalencije, negacije i kvantifikatora koje jezik $\mathcal{L}$ uvek sadrži.

Individualne promenljive, znak jednakosti i simboli logičkih veznika su univerzalni simboli. Sadrži ih jezik svake strukture, pa oni čine konstantni ili logički deo jezika $\mathcal{L}$. Sa druge strane, matematički deo jezika je promenljiv i sastoji se od simbola relacija, simbola operacija i simbola istaknutih elemenata pojedinih matematičkih struktura.

Polazeći od elementarnih formula, pomoću logičkih veznika, dobijamo formule jezika $\mathcal{L}$. Na primer, u jeziku $\mathcal{L}$, najznačajnija svojstva strukture $\mathcal{N}$ izražena su sledećim formulama:

$$
\begin{array}{lcl}
\varphi_1 & \equiv & \forall x\,(s(x) \neq 0), \\
\varphi_2 & \equiv & \forall x \forall y\,(s(x) = s(y) \rightarrow x = y), \\
\varphi_3 & \equiv & \forall x\,(x \neq 0 \rightarrow \exists y\,(x = s(y))), \\
\varphi_4 & \equiv & \forall x\,(x + 0 = x), \\
\varphi_5 & \equiv & \forall x \forall y\,(x + s(y) = s(x + y)), \\
\varphi_6 & \equiv & \forall x\,(x \cdot 0 = 0), \\
\varphi_7 & \equiv & \forall x \forall y\,(x \cdot s(y) = (x \cdot y) + x), \\
\varphi_8 & \equiv & \forall x \forall y\,(x \leq y \leftrightarrow \exists z\,(z + x = y)).
\end{array}
$$

Kakva je stvarno veza izmedju strukture $\mathcal{N}$ i navedenog niza objekata? Pre svega, napomenimo da se u svakom od grafičkih objekata sa leve strane prvog znaka jednakosti uvek javljaju metamatematičke oznake: grčko slovo φ indeksirano prirodnim brojevima od 1 do 8. Sa desne strane znaka $\equiv$ javlja se konačan niz elemenata jezika $\mathcal{L}$. Za svako $i = 1, ..., 8$, simbol φ_i je simbol metajezika kojim je označen odgovarajući niz elemenata objekt-jezika. Primetimo da se znak $\equiv$ u prethodnim grafičkim nizovima, javlja kao metamatematički znak, dok je jednakost $=$ znak objekt-jezika i javlja se u okviru samih nizova φ_i.

Oznake φ_i shvatamo kao metamatematičke promenljive čije vrednosti pripadaju skupu konačnih nizova simbola jezika $\mathcal{L}$. To su izrazi ili formule jezika $\mathcal{L}$ koje u strukturi $\mathcal{N}$ imaju odreden smisao. Ako te izraze pročitamo onako kako smo to navikli da činimo u matematici, na primer, smisao formule φ_1 jeste da nula nije vrednost funkcije s, a formula φ_2 izražava činjenicu da je s obostrano jednoznačna funkcija. Formule φ_4 i φ_5 predstavljaju rekurzivnu definiciju sabiranja, a formula φ_8 definiciju poretka prirodnih brojeva. Važno je primetiti da svaka od ovih formula izražava svojstva prirodnih brojeva, tj. elemenata domena strukture $\mathcal{N}$.

Pored osnovnih, u jeziku $\mathcal{L}$ može se izraziti većina svojstava prirodnih brojeva. Preciznije, specijalista u oblasti same aritmetike bez značajnijeg logičkog iskustva, teško može navesti svojstvo prirodnih brojeva koje nije izrazivo formulom jezika $\mathcal{L}$ i koje, ako je uopšte dokazivo, ne može biti dokazano njegovim sredstvima. Za svakodnevnu matematiku, jezik $\mathcal{L}$ ima više nego dovoljnu izražajnu moć.

Operacije $+$, $\cdot$ i relacija $\leq$ su apstraktne, tako da samu ideju brojanja u potpunosti ipak izražava *princip matematičke indukcije*:

– Za svaki skup prirodnih brojeva $X \subseteq \omega$, ako $0 \in X$ i za svako $x \in X$, $s(x) \in X$, onda je $X = \omega$.

Ovako formulisan, princip matematičke indukcije govori o skupovima prirodnih brojeva, tako da metamatematička promenljiva X, bar u odnosu na strukturu $\mathcal{N}$, nije individualna promenljiva. Ako tu stvar za trenutak zanemarimo, princip matematičke indukcije mogao bi se formalno zapisati sledećim nizom simbola:

$$\forall X\,((X(0) \wedge \forall x\,(X(x) \rightarrow X(s(x))) \rightarrow \forall y\, X(y)).$$

Pritom, promenljivu X shvatamo kao podskup skupa ω, niz slova $X(x)$ kao relaciju $x \in X$, a sva druga slova onako kako smo to i do sada činili. Tako interpretirana, ova formula zaista izražava princip matematičke indukcije. Ali, aprema našoj definiciji ona uopšte nije formula jezika $\mathcal{L}$, već jednog šireg lezika $\mathcal{L}'$, koji kao svoje logičke simbole sadrži i promenljive $X, Y, \ldots$ za unarne relacije. U odnosu na formule jezika $\mathcal{L}$, ovako izražen princip indukcije razlikuje se u tome što on ne izražava svojstvo prirodnih brojeva, već jedno svojstvo podskupova skupa prirodnih brojeva.

Ako strukturu $\mathcal{N}$ shvatimo kao strukturu jezika $\mathcal{L}'$ ona zadovoljava sve sve formule $\varphi_1, ..., \varphi_8$ i princip matematičke indukcije. Ako taj skup formula jezika $\updownarrow'$ shvatimo kao sistem aksioma prirodnih brojeva, onda taj sistem aksioma u izvesnom smislu govori sve o prirodnim brojevima.

Teorema 1. Sve strukture jezika $\mathcal{L}'$ koje zadovoljavaju aksiome prirodnih brojeva meḍusobno su izomorfne.

Dokaz: Neka je $\mathcal{A} = (A, +, \cdot, \leq, s, 0)$, struktura jezika $\mathcal{L}$ u kojoj su zadovoljene navedene aksiome i $f : \omega \rightarrow A$ funkcija definisana tako da:

$$\begin{aligned} &f(0) = 0, \\ &f(s(x)) = s(f(x)), \text{ za sve } x \in \omega. \end{aligned}$$

Koristeći princip indukcije, sasvim jednostavno se proverava da navedene relacije zaista definišu funkciju koja je jedinstveno određena.

Primenom principa indukcije u strukturi $\mathcal{A}$ dokazujemo da je preslikavanje f epimorfizam, tj. da je $A = \mathrm{codom}(f)$. Kako je $f(0) = 0$, to znači da $0 \in \mathrm{codom}(f)$. Za svako $x \in A$, ako $x \in \mathrm{codom}(f)$, postoji $y \in \omega$ takvo da

$x = f(y)$, pa je $s(x) = s(f(y)) = f(s(y))$, tj. $s(x) \in \mathrm{codom}(f)$. Na osnovu principa indukcije, $A = \mathrm{codom}(f)$.

Indukcijom po $y \in \omega$, u strukturi $\mathcal{N}$ dokazujemo da za svako $x \in \omega$,

$$x \neq y \ \Rightarrow\ f(x) \neq f(y).$$

Neka je $y = 0$. Ako je $x \neq 0$, postoji $z \in \omega$ takvo da $x = z + 1$, što znači da je $f(x) = s(f(z))$. Na osnovu aksiome φ_1, otuda sledi da mora biti $s(f(z)) \neq 0$, tj. važi $f(x) \neq f(0)$.

Neka je $x \neq y + 1$. Ako je $x = 0$, kao i u slučaju $y = 0$ dobijamo da je $f(y + 1) \neq 0$. Ako je $x \neq 0$, za neko $u \in \omega$, $x = u + 1$, pa dakle $u \neq y$. Prema induktivnoj pretpostavci, $f(u) \neq f(y)$, pa na osnovu aksiome φ_2, $s(f(u)) \neq s(f(y))$, tj. važi $f(x) \neq f(y + 1)$.

Po definiciji, preslikavanje f je homomorfizam u odnosu na operaciju sledbenika s i istaknutog elementa 0, a neposredno je lako proveriti da f čuva relaciju $\leq$ i operacije sabiranja $+$ i množenja $\cdot$, pa je preslikavanje f izomorfizam struktura $\mathcal{A}$ i $\mathcal{N}$. $\square$

Kada se ima u vidu jedinstvenost prirodnih brojeva, značajno bi bilo kada bi se princip indukcije mogao izraziti sredstvima jezika $\mathcal{L}$. Samo po sebi nije jasno zašto to nije moguće, ako ne jednom, onda beskonačnim skupom njegovih formula. Međutim, za bilo koji skup formula jezika $\mathcal{L}$ koje važe u strukturi $\mathcal{N}$, postoji struktura $\mathcal{N}^*$ koja zadovoljava isti skup formula i nije izomorfna sa $\mathcal{N}^*$.

Izgleda sasvim razumljivo i opravdano da formalnu analizu svojstava prirodnih brojeva vršimo u jeziku u kome se jedan takav princip može izraziti. Ako već u jeziku $\mathcal{L}$ uopšte ne postoji formulacija principa matematičke indukcije koja omogućava jedinstven opis strukture $\mathcal{N}$, onda bi bilo prirodno da kao jezik matematičkih struktura izaberemo jezik $\mathcal{L}'$.

Ali, iako sredstvima jezika $\mathcal{L}$ nije moguć jedinstven opis strukture $\mathcal{N}$, to opet ne znači da bi naš pravi izbor bila logika izražena u jeziku $\mathcal{L}'$. Naime, u definiciji strukture $\mathcal{N}$ pretpostavili smo da je skup prirodnih brojeva ω nekako sam po sebi dat i da su date neke jednostavne operacije i relacije tog skupa. U jeziku $\mathcal{L}'$ pretpostavljamo monogo više, tj. u formulaciji principa indukcije vrši se kvantifikacija preko skupa svih podskupova prirodnih brojeva. Kako skup $P(\omega)$ ni približno nije jednostavan kao sam skup ω, u karakterizaciji skupa prirodnih brojeva koristili smo svojstva jednog mnogo komplikovanijeg i nejasnog objekta. Sasvim jednostavno rečeno, preterano jakim sredstvima dobili smo relativno skroman rezultat.

Pored problema koji se u vezi s njom javljaju u teoriji saznanja, na čemu insistira veći deo filosofije matematike, definicija strukture $\mathcal{N}$ u jeziku $\mathcal{L}'$ ima i druge ozbiljne nedostatke, koji protivreče samoj ideji formalnog metoda, tako da se sa razlogom može postaviti pitanje njene opravdanosti.

Realni brojevi

Osim prirodnih, značajnu ulogu u matematici imaju i *realni brojevi*, tj. njihova struktura $\mathcal{R} = (R, +, \cdot, \leq, 0, 1)$. Domen strukture $\mathcal{R}$ je skup R realnih brojeva, $+$ i $\cdot$ su operacije sabiranja i množenja, $\leq$ standardni poredak realnih brojeva, a 0 i 1 konkretni elementi skupa R.

Poznato je da realni brojevi čine kompletno uređeno polje. Do na izomorfizam, to polje jedinstveno je određeno. Slično prirodnim brojevima, pokušaćemo da to izrazimo u jeziku $\mathcal{L}$ koji sada, osim univerzalnih logičkih simbola, promenljivih, jednakosti i logičkih veznika sadrži i specijalne simbole relacija, operacija i konstanti strukture $\mathcal{R}$.

Pre svega, u odnosu na operaciju $+$ i konstantu 0, struktura $(R, +, 0)$ je *komutativna grupa*, odnosno, u njoj su zadovoljene sledeće formule jezika $\mathcal{L}$:

$$
\begin{aligned}
\varphi_1 &\equiv \forall x \forall y \forall z\, (x + (y + z) = (x + y) + z),\\
\varphi_2 &\equiv \forall x\, (x + 0 = x),\\
\varphi_3 &\equiv \forall x \exists y\, (x + y = 0 \wedge y + x = 0),\\
\varphi_4 &\equiv \forall x \forall y\, (x + y = y + x).
\end{aligned}
$$

Svaka od navedenih formula izražava jedno svojstvo realnih brojeva. Kvantifikacije $\forall x$ i $\exists y$ odnose se na elemente skupa R. Treba primetiti da se ove formule mogu interpretirati u bilo kojoj strukturi oblika $(A, \circ, e)$ u kojoj je A neprazan skup, $\circ$ binarna operacija i e element skupa A. U tom slučaju znak $+$ interpretiramo kao operaciju $\circ$, a znak 0 kao element e skupa A. Razumljivo, svaka takva struktura je komutativna grupa. Osim navedenih svojstava i njihovih logičkih posledica, formulama jezika $\mathcal{L}$ mogu se izraziti i druga, specifična svojstva grupa. Na primer, svaka konačna grupa jedinstveno je određena formulom jezika $\mathcal{L}$, zatim, postoji skup formula koji karakteriše beskonačne grupe itd. Ipak, nisu sva svojstva grupa izraziva sredstvima jezika $\mathcal{L}$. I u odnosu na teoriju grupa, izražajna sredstva ovog jezika su takođe ograničena.

U odnosu na operacije $+$ i $\cdot$, kao i konstante 0 i 1, struktura realnih brojeva $(R, +, \cdot, 0, 1)$ je *komutativan prsten sa jedinicom*. To se u jeziku $\mathcal{L}$ može izraziti sledećim formulama:

$$\begin{aligned}
\varphi_5 &\equiv \forall x\,(x \cdot 1 = x \wedge 1 \cdot x = x),\\
\varphi_6 &\equiv \forall x \forall y \forall z\,(x \cdot (y \cdot z) = (x \cdot y) \cdot z),\\
\varphi_7 &\equiv \forall x \forall y\,(x \cdot y = y \cdot x),\\
\varphi_8 &\equiv \forall x \forall y \forall z\,(x \cdot (y + z) = x \cdot y + x \cdot z).
\end{aligned}$$

Prethodne formule takođe izražavaju svojstva elemenata skupa realnih brojeva. Kao sintaksni objekti, one se mogu interpretirati u svakoj strukturi oblika $(A, \circ, *, e_1, e_2)$ sa dve binarne operacije i dve konstante. Strukture u kojima važe ove formule su komutativi prsteni sa jedinicom. Svakako, struktura $\mathcal{R}$ nije jedini takav prsten.

Osim svojstava komutativnih prstena, struktura $(R, +, \cdot, 0, 1)$ zadovoljava i uslove koji karakterišu strukturu *polja*.

$$\begin{aligned}
\varphi_9 &= 0 \neq 1,\\
\varphi_{10} &= \forall x\,(x \neq 0 \rightarrow \exists y\,(x \cdot y = 1)).
\end{aligned}$$

Svaki komutativan prsten sa bar dva elementa, u kome svaki element različit od nule ima inverzni u odnosu na operaciju množenja, jeste polje. Kao strukture uopšte i polja smo definisali svojstvima njihovih elemenata, odnosno, formulama jezika $\mathcal{L}$.

Značajan deo teorije polja može se izraziti i analizirati sredstvima ovog jezika. Najvažnije ideje teorije modela nastale su upravo u ovoj oblasti. U kasnijim izlaganjima, polja će biti strukture na kojima se najbolje mogu razumeti i operacionalizovati pojmovi matematičke logike. Pored teorije grupa, za celovito razumevanje teorije modela jezika $\mathcal{L}$, podrazumeva se i dobro poznavanje teorije polja. Svakako, postoje svojstva ovih struktura koja se ne mogu formalizovati u jeziku $\mathcal{L}$.

Poredak realnih brojeva $\leq$ je linearan, odnosno, struktura $(R, \leq)$ je *linearno uređenje*. Ta činjenica može se izraziti formulama jezika $\mathcal{L}$:

$$\begin{aligned}
\varphi_{11} &= \forall x\,(x \leq x),\\
\varphi_{12} &= \forall x \forall y\,(x \leq y \wedge y \leq x \rightarrow x = y),\\
\varphi_{13} &= \forall x \forall y \forall z\,(x \leq y \wedge y \leq z \rightarrow x \leq z),\\
\varphi_{14} &= \forall x \forall y\,(x \leq y \vee y \leq x).
\end{aligned}$$

Prva tri svojstva relaciju $\leq$ određuju kao refleksivnu, simetričnu i tranzitivnu relaciju, odnosno, kao *parcijalno uređenje*, a poslednje svojstvo izražava njenu linearnost. Parcijalno uređenju može se definisati i kao striktno uređenje, tj. kao nerefleksivna i tranzitivna realcija.

Na osnovu relacije $\leq$, formulom $\forall x \forall y\,(x < y \leftrightarrow x \leq y \wedge x \neq y)$ jezika $\mathcal{L}$, u svakom parcijalnom uređenju definisan je *striktni poredak* $<$ koji karakterišu sledeća svojstva

$$\begin{aligned}
\varphi_{11}' &= \forall x\, \neg(x < x), \\
\varphi_{13}' &= \forall x \forall y \forall z\,(x < y \wedge y < z \rightarrow x < z).
\end{aligned}$$

Sa druge strane, kao simbol jezika $\mathcal{L}$, u kome znak $<$ zadovoljava formule φ_{11}' i φ_{2}', formulom $\forall x \forall y\,(x \leq y \leftrightarrow x < y \vee x = y)$, može se definisati poredak $\leq$. U sasvim strogom smislu - o tome će kasnije biti reči - parcijalno uređenje i striktno parcijalno uređenje su ekvivalentne strukture, pa ih u buduće nećemo razlikovati.

Odnos relacije poretka $\leq$ prema operacijama $+$ i $\cdot$ u strukturi realnih brojeva definisan je sledećim formulama jezika $\mathcal{L}$:

$$\begin{aligned}
\varphi_{15} &= \forall x \forall y \forall z\,(x \leq y \rightarrow (x + z \leq y + z)), \\
\varphi_{16} &= \forall x \forall y \forall z\,(x \leq y \wedge 0 \leq z \rightarrow (x \cdot z \leq y \cdot z)).
\end{aligned}$$

U strukturi $\mathcal{R} = (R, +, \cdot, \leq, 0, 1)$, formula φ_{15} postulira saglasnost relacije poretka sa operacijom sabiranja, a formula φ_{16} njenu uslovnu saglasnost sa operacijom množenja. Drugačije rečeno, struktura $\mathcal{R}$ je *uređeno polje*. Kao strukture, i uređena polja okarakterisali smo formulama jezika $\mathcal{L}$. Taj jezik ima dovoljnu izražajnu moć da se u njemu mogu definisati klase algebarskih struktura poput grupa, prstena, polja ili različitih uređenih struktura. Međutim, samo po sebi nije jasno koja i da li sva svojstva ovih struktura možemo izraziti rečenicama jezika $\mathcal{L}$.

Osim realnih i racionalni brojevi su uređeno polje. To znači da uslovi izraženi formulama $\varphi_1, ..., \varphi_{16}$ i njihove logičke posledice ni približno ne karakterišu realne brojeve u onom smislu u kome indukcija određuje strukturu prirodnih, a time i racionalnih brojeva.

Ključnu ulogu u karakterizaciji realnih brojeva ima takozvani *princip kompletnosti*: svaki neprazan odozgo ograničen skup elemenata uređenog polja ima supremum. U jeziku $\mathcal{L}'$ princip kompletnosti ima sledeću formulaciju:

$$\begin{aligned}
&\forall X\,(\exists x\, X(x) \wedge \exists x \forall y\,(X(y) \rightarrow y \leq x) \rightarrow \\
&\qquad \exists x\,(\forall z\,(X(z) \rightarrow z \leq x) \wedge \forall y\,(\forall z(X(z) \rightarrow z \leq y) \rightarrow x \leq y)).
\end{aligned}$$

Ako promenljivu X shvatimo kao podskup skupa R, niz slova $X(x)$ kao relaciju $x \in X$, a sva druga slova onako kako smo do sada činili, ova formula zaista izražava kompletnost realnih brojeva.

Opštije, svako uredjeno polje u kojem važi navedena formula je *kompletno uređeno polje*. Poput principa indukcije u slučaju prirodnih brojeva, kompletnost jedinstveno određuje realne brojeve.

Teorema 2. Svako kompletno uređeno polje izomorfno je polju realnih brojeva.

Dokaz ovog tvrđenja izložićemo kasnije. Za sada primetimo da se princip kompletnosti razlikuje od ostalih aksioma uređenih polja. On ne izražava svojstvo elemenata strukture $\mathcal{R}$, već jedno svojstvo njenih podskupova. Predstavljen je formulom jezika $\mathcal{L}'$ i ne može se izraziti čak ni beskonačnim skupom formula jezika $\mathcal{L}$. Kao u slučaju prirodnih brojeva, za svaki skup formula jezika $\mathcal{L}$, koje važe u strukturi $\mathcal{R}$, postoji struktura $\mathcal{R}^*$ koja zadovoljava isti skup formula i koja nije izomorfna polju $\mathcal{R}$. Ista stvar važi u proizvoljnom proširenju jezika $\mathcal{L}$ novim simbolima relacija, operacija i elemenata skupa realnih brojeva. Dakle, sredstvima jezika $\mathcal{L}$ jedinstvena karakterizacija polja realnih brojeva uopšte nije moguća.

Logički sistemi, poput jezika $\mathcal{L}$, u kojima formule izražavaju svojstva elemenata matematičkih struktura su sistemi prvog reda. Logika u kojoj, kao u jeziku $\mathcal{L}'$, formule izražavaju svojstva relacija matematičkih struktura je logika drugog reda.

Na osnovu primera prirodnih i realnih brojeva jasno je da logika prvog reda nije dovoljno snažna da izrazi neka važna svojstva matematičkih struktura. Kasnije ćemo videti da u jeziku $\mathcal{L}$ nije moguća potpuna karakterizavcija bilo koje beskonačne strukture. Stoga, izgleda da je logika drugog reda, ako ne pravi, sigurno bolji sistem za formalizaciju matematike od logike prvog reda. Međutim, osim ovih osobina, logika drugog reda ima i neka sasvim problematična svojstva. Kao što smo već jednom naglasili, osnovnu ideju matematičke logike čini matematizacija logičkih objekata, a to su pre svega teoreme i njihovi dokazi. U logici drugog reda ti objekti i skupovi takvih objekata nisu precizno definisani. Skup formula logike drugog reda koje važe u svim matematičkim strukturama nema rekurzivnu aksiomatizaciju, pa ova logika i nije formalni sistem u pravom smislu te reči. Uprošćeno rečeno, to jeste sistem koji ima veliku izražajnu moć, ali i sistem u kome ne znamo smisao svih njegovih formula.

Osim logike drugog reda, postoje i drugi sistemi u kojima je moguće dokazati jedinstvenost prirodnih i realnih brojeva. Umesto uvođenja relacijskih promenljivih, ekspresivna moć jezika $\mathcal{L}$ može se povećavati uopštavanjem logičkih veznika, na primer, tako što će se dopustiti beskonačne konjunkcije i disjunkcije ili uvesti novi kvantifikatori, ali se i u tim slučajevima dobijaju sistemi koji su problematični ili sa stanovišta same ideje formalizacije ili sa stanovišta njihovog značenja. Takođe, problem jedinstvene karakterizacije prirodnih i realnih brojeva je rešiv i u okviru logike prvog reda. To se postiže formulacijom teorije skupova u jeziku $\mathcal{L}$. U toj teoriji mogu se izraziti i dokazati teoreme jedinstvenosti, ali se i na takav dokaz može staviti niz sasvim principijelnih primedbi. Prvo, takav rezultat dobijen je nesrazmerno jakim sredstvima i drugo, sama teorija skupova nije potpuna.

Svakom od spomenutih rešenja problema jedinstvenosti prirodnih i realnih brojeva posvećena je određena pažnja. U poglavlju koje se bavi matematičkom logikom u užem smislu, pokazano je da u predikatskom računu prvog reda svaka aritmetika prirodnih i realnih brojeva ima nestandardne modele. Ovo poglavlje obuhvata stav potpunosti predikatskog računa i osnove njegove teorije modela. Teoriju skupova razvili smo do stepena koji uključuje dokaz neprotivrečnosti i nezavisnosti hipoteze kontinuuma. Poglavlje iz teorije izračunljivosti obuvata osnove ove teorije, raspravu svih važnijih logičkih sistema sa stanovišta njihove efektivnosti i teoreme nepotpunosti aritmetike. Pored navedena tri poglavlja, prvi deo našeg izlaganja posvećen je Bulovim algebrama.

Svaki od četiri dela ove knjige čini relativno zaokruženu celinu i predstavlja uvod u odgovarajuću oblast matematičke logike: Bulove algebre, teoriju modela, teoriju skupova i teoriju izračunljivosti. Na kraju svakog poglavlja date su istorijske i bibliografske napomene. Svaka bibliografska jedinica istovremeno znači i preporuku u eventualnom intenzivnijem bavljenju teorijom u čijem kontekstu je navedena.

Napomene

– Ideja strukture je prilično stara. U nekom smislu bila je poznata i Lajbnicu, ali se ipak veruje da je Šreder 1895. godine prvi put definisao pojam apstraktne strukture.

– Pojam formalnog sistema uveo je Frege 1879. godine, ali ne kao sredstvo izražavanja svojstava matematičkih struktura, već kao potpunu formalizaciju prirodnog jezika u kojem se problem različitih interpretacija njegovih simbola uopšte ne postavlja. Za razliku od većine matematičara, koji mogućnost različitih interpretacija formalnih simbola smatraju jednom od ključnih ideja matematičke logike, Frege je imao u vidu potpuni opis jedinstvenog matematičkog univerzuma.

Na specifičan način, ali dosledno, Frege je zastupao platonističko shvatanje matematike. Prema ovom stanovištu, matematički objekti postoje nezavisno od nas, kao što postoje nezavisno od nas objekti materijalnog sveta. Prirodni brojevi, neprebrojivi skupovi, Lebegova mera i skupovni univerzum nisu samo mentalne konstrukcije, već apstraktni objekti koji postoje nezavisno od iskustva i uslova pod kojim saznajemo njihova svojstva. Aksiome teorije skupova su evidentne istine na osnovu kojih dedukujemo sva druga svojstva matematičkih objekata, onako kao što se nekada zamišljalo da aksiome geometrije opisuju svojstva realnog prostora. Matematičari ne stvaraju matematički svet, već otkrivaju njegove istine. Osim Fregea, čije je stanovište je specifično utoliko što je on verovao da se matematika u sasvim strogom smislu može svesti na logiku, platonističko shvatanje matematike je dosledno zastupao Kurt Gedel.

– Kao matematičar sa posebnim autoritetom, Hilbert je početkom ovog veka imao ambiciju da matematiku zasnuje po jednom programu u kojem bi bile otklonjene sve dileme oko interpretacije i sadržaja njenih tvrđenja. Kako su se njegova shvatanja vremenom menjala, nikada nije do kraja razjašnjeno šta je pravi smisao njegovog *programa zasnivanja matematike*. Program zastupa jednu finitističku koncepciju po kojoj beskonačnost ima samo pomoćnu ulogu u matematici i može se eliminisati iz svake argumentacije o konačnim matematičkim objektima. Većina matematičara veruje da se u osnovi tog programa nalazi problem neprotivrečnosti aritmetike te da, s obzirom na rezultate Kurta Gedela iz tridesetih godina, Hilbert nije bio u pravu. Beskonačnost je ipak esencijalna pretpostavka matematike.

– Formalističko shvatanje matematike je sasvim suprotno platonističkom. Prema ovom stanovištu, matematička tvrđenja ne izražavaju svojstva nikakvog stvarnog sveta. Matematika je kolekcija aksioma, teorema i formalnih dedukcija, koja doduše nije slučajno nastala, ali može biti sasvim proizvoljno nematematički motivisana. Na primer, može biti inspirisana naučnim, praktičnim, estetskim ili čak ideološkim razlozima. Za matematičke iskaze nije ključno pitanje istinitosti, već njihove praktične celishodnosti.

– Osim platonizma i formalizma, u filosofiji matematike značajno je i konstruktivističko stanovište. Za razliku od čistog formalizma, koji negira bilo kakav stvarni sadržaj matematičkih tvrđenja, konstruktivisti smatraju da ova tvrđenja ipak imaju smisao u svetu koji su oni sami stvorili. Matematički objekti postoje, ali samo kao mentalne konstrukcije izvedene legitimnim sredstvima (u svesti idealnog matematičara). Insistiranjem na ovom principu, konstruktivizam se pretvorio u neku vrstu doktrinarne škole koja je preduzela radikalnu reviziju matematike.

U odnosu na formalizam i platonizam koji mogu biti filosofska osnova čitave savremene matematike, konstruktivizam odbacuje njen veliki deo, uključujući i logičke principe na kojima je matematika zasnovana. U okviru same logike, na osnovu intuicionističkih stanovišta kao posebne konstruktivističke škole, dobijeni su veoma zanimljivi rezultati [2], ali intuicionistička revizija matematike [1], s razlogom, nije imala značajniji uticaj.

– U okviru naših izlaganja nećemo zastupati nikakvo posebno filosofsko stanovište o prirodi matematičkih objekata, iako neki od rezultata o kojima će biti reči mogu imati i značajne posledice u ovom smislu. Sasvim uopšteno rečeno, matematiku shvatamo kao aprioran oblik saznanja, nezavisan od našeg iskustva. Svi njeni pojmovi, definicije pravila ili dokazi imaju nedvosmisleno značenje, a njeni rezultati ne mogu se preispitivati sa stanovišta eksperimentalnog iskustva. Eventualno, može se govoriti o adekvatnosti pojedinih teorija konkretnom empirijskom problemu, ili o uticaju takvih problema na razvoj određene matematičke discipline.

– Implicitno, deo Hilbertovog programa prisutan je u njegovom spisku značajnih problema iz 1900. godine, za koje je verovao da će bitno odrediti sadržaj matematičkih istraživanja tada nastupajućeg veka. Od ukupno 23 problema sa tog spiska, bar tri su značajna za matematičku logiku [3].

– Prvi Hilbertov problem je zapravo problem kontinuuma: "Kantorova istraživanja sugerišu ... da svaki sistem od beskonačno mnogo realnih brojeva, tj. svaki skup brojeva ili tačaka je ekvivalentan skupu prirodnih brojeva i prema tome i kontinuumu, tj. skupu svih tačaka na pravoj; što se tiče ekvivalencije postoje samo dva skupa brojeva, prebrojiv skup i kontinuum."

Savremena teorija skupova je nastala u pokušajima da se odgovori na ovo pitanje. Gedel je 1938. godine dokazao relativnu neprotivrečnost, a Koen 1963. godine nezavisnost hipoteze kontinuuma u odnosu na formalizaciju teorije skupova. Ipak, većina matematičara smatra da ovaj problem nije rešen. Iako je sam dokazao relativnu neprotivrečnost hipoteze kontinuuma, Gedel je izgleda verovao da u "stvarnom" svetu važi $2^\omega = \aleph_2$.

– Drugi problem Hilbert je ovako formulisao: "Dokazati da (aksiome aritmetike) nisu protivrečne, tj. da se polazeći od njih u konačnom broju logičkih koraka ne može doći do rezultata koji protivreče jedan drugom."

U vreme kada je postavio ovaj problem, Hilbert je imao u vidu aksiome aritmetike realnih brojeva. Dvadesetih godina problem je shvaćen kao problem aritmetike prirodnih brojeva. U tom obliku rešen je 1931. godine. Gedel je dokazao da, ako je uopšte neprotivrečna, sredstvima aritmetike nije moguće dokazati da je ona sama neprotivrečna. Iako je Hilbert to osporavao, Gedelov rezultat smatra se rešenjem ovog problema.

– Deseti Hilbertov problem: "Za datu diofantovsku jednačinu, sa bilo kojim brojem nepoznatih veličina i sa racionalnim celobrojnim koeficijentima, izmisliti postupak kojim se može odlučiti, koristeći konačan broj operacija, da li ta jednačina ima ili nema celobrojnih rešenja."

Slično prethodnim Hilbertovim problemima, u vreme kada je postavljen, ni ovaj problem uopšte nije bio jasan, ali se danas smatra rešenim. Na osnovu Čerčove teze, "postupak kojim se može odlučiti, koristeći konačan broj operacija ..." odgovara savremenom pojmu algoritma. Prema Matijasevičevoj teoremi - svi rekurzivno nabrojivi skupovi su diofantovski - postupak o kome govori Hilbret ne postoji.

– Kompletnu karakterizaciju prirodnih brojeva, u jednoj poluformalnoj, ali rigoroznoj varijanti, 1888. godine dokazao je Dedekind.

– Formulaciju aksioma prirodnih brojeva u jeziku nalik na $\mathcal{L}'$, koji sadrži dve vrste promenljivih, napravio je Peano 1889. godine. Danas je uobičajeno da se Peanovom aritmetikom naziva varijanta aritmetike izražena u predikatskom računu prvog reda.

– Zanimljivo je da su uopštenja logike prvog reda starija i od nje same. Sistem veoma blizak logici drugog reda koristio je Pers 1885. godine. Praktično, sve do 1930. godine preovladavaju sistemi drugog reda. Do tada, nije postojala opšta saglasnost oko notacije, a ni interpretacije formalnih simbola.

– Ova knjiga nastala je u okviru Seminara za matematičku logiku Matematičkog instituta Srpske akademije nauka i umetnosti i kurseva matematičke logike na Prirodnomatematičkom fakultetu u Podgorici.

Literatura

[1] Bishop, E. *Foundations of Constructive Analusis*, McGraw-Hill, New York, 1967.

[2] Kripke, S.A. *Semantical analysis of intuitionistic logic*, u: Crossley, J.N., Dummet, M.A.E. (eds.), *Formal Systems and Recursive Functions*, 92-130, North-Holland, Amsterdam, 1965.

[3] Mijajlović, Ž., Marković, Z., Došen, K. *Hilbertovi problemi i logika*, Zavod za izdavanje udžbenika, Beograd, 1986.

Bulove algebre

Uvod u logiku počinjemo izlaganjem teorije Bulovih algebri. Iako je to po svojoj prirodi čisto algebarska teorija ona se tradicionalno ipak smatra delom matematičke logike. Razloga zbog kojih smo se opredelili za takav pristup ima nekoliko. Prvo, smisao najznačajnijih rezultata logike teško je razumljiv bez određenog matematičkog iskustva. Delimično, ti rezultati predstavljaju sistematizaciju i razradu ideja koje se javljaju u različitim oblastima matematike i podrazumevaju poznavanje osnova intuitivne teorije skupova, algebre, osnova topologije i jednog dela matematičke analize. U izlaganju Bulovih algebri pojaviće se većina ključnih ideja spomenutih teorija.

Drugo, praktično svi opšti koncepti, o kojima ćemo govoriti u matematičkoj logici, mogu se interpretirati i njihov smisao razumeti u klasi ovih struktura. Budući da je dobar deo našeg izlaganja, posebno u okviru teorije modela, posvećen razmatranjima opštih svojstava matematičkih struktura, pored grupa, polja ili vektorskih prostora, sa kojima većina matematičara ima značajno iskustvo, Bulove algebre predstavljaju dobru ilustraciju opštih modelsko teorijskih rezultata.

I konačno, treći razlog zbog kojeg u logici pretpostavljamo poznavanje Bulovih algebri jeste sama struktura logičkih sistema. Iako priroda konjunkcije, disjunkcije, negacije i naročito implikacije nije u potpunosti algebarska, algebra je sredstvo bez kojeg izučavanje svojstava logičkih veznika praktično nije moguće. Svaki logički sistem do određenog stepena karakteriše neka algebarska struktura, a u slučaju klasične logike ta struktura jeste Bulova algebra. Na primer, ako logičke veznike shvatimo kao operacje na skupu svih formula jezika prvog reda, kao rezultujuća struktura dobija se Bulova algebra čija svojstva nose značajnu količinu informacija o samom jeziku.

Struktura Bulove algebre može se definisati dvojako: kao parcijalno uređenje sa određenim svojstvima, ili kao algebra u uobičajenom smislu. Ovaj dualizam omogućava da u okviru kombinatorne teorije istovremeno koristimo algebarska i topološka sredstva, a na nivou strukturne teorije predstavlja osnov dualnosti kategorija Bulovih algebri i totalno nepovezanih kompaktnih Hauzdorfovih prostora. Iz tih razloga, osim u logici i teoriji skupova, gde su nastale i zbog čega su za nas prevashodno značajne, Bulove algebre prirodno se javljaju i u drugim oblastima matematike. Na primer, u topologiji gde određuju spomenutu klasu prostora, u teoriji mere, kao algebre merljivih skupova ili u funkcionalnoj analizi, kao algebre projekcija Banahovog prostora.

Mreža je parcijalno uređenje $\mathcal{L} = (L, \leq)$ u kojem svaki par elemenata $x, y \in L$ ima supremum i infimum koje označavamo sa $x \vee y$ i $x \wedge y$.

Imajući u vidu njihovu interpretaciju u logici, supremum i infimum nazivamo disjunkcijom, odnosno, konjunkcijom.

Ako je $\mathcal{L}$ mreža, onda za sve $x, y \in L$, $x \leq y$ ako i samo ako $x \wedge y = x$ ako i samo ako $x \vee y = y$. Takođe, u svakoj mreži $\mathcal{L}$, za proizvoljne $x, y, z \in L$, zadovoljene su sledeće jednakosti:

$$\begin{array}{ll} x \wedge y = y \wedge x, & x \vee y = y \vee x, \\ x \wedge (y \wedge z) = (x \wedge y) \wedge z, & x \vee (y \vee z) = (x \vee y) \vee z, \\ x \wedge (x \vee y) = x, & x \vee (x \wedge y) = x. \end{array}$$

Otuda sledi da mrežu možemo razumeti na dva načina: kao parcijalno uređenje $\mathcal{L} = (L, \leq)$, u kojem svaki par elementa ima supremum i infimum, ili kao strukturu $\mathcal{L} = (L, \vee, \wedge)$ sa dve binarne operacije koja zadovoljava prethodne jednakosti.

Primer 1. Svako linearno uređenje $(X, \leq)$ je mreža. Pritom, za proizvoljne $x, y \in X$, $x \wedge y = \min(x, y)$ i $x \vee y = \max(x, y)$.

Primer 2. S obzirom na inkluziju kao poredak, skup svih podskupova $P(X)$ skupa X je mreža u kojoj za sve $x, y \in P(X)$,

$$x \wedge y = x \cap y, \quad x \vee y = x \cup y.$$

Primer 3. Familija otvorenih skupova topološkog prostora je mreža u odnosu na inkluziju. Konjunkcija i disjunkcija takođe odgovaraju skupovnim operacijama preseka i unije.

Primer 4. Neka je $\leq$ binarna relacija na skupu prirodnih brojeva ω, takva da za sve $x, y \in \omega$, $x \leq y$ ako i samo ako x deli y. Struktura $(\omega, \leq)$ je mreža u kojoj je $x \wedge y$ najveći delitelj, a $x \vee y$ najmanji sadržalac brojeva x i y.

Primer 5. (a) U vektorskom prostoru $\mathcal{V}$ nad poljem F, skup $S(\mathcal{V})$ svih potprostora prostora $\mathcal{V}$, s obzirom na inkluziju kao poredak, čini mrežu. U mreži $S(\mathcal{V})$, $\mathcal{M} \vee \mathcal{N} = \mathcal{M} + \mathcal{N}$ i $\mathcal{M} \wedge \mathcal{N} = \mathcal{M} \cap \mathcal{N}$.

(b) Skup svih podgrupa $S(\mathcal{G})$ grupe $\mathcal{G}$ čini mrežu u kojoj je disjunkcija dve podgrupe jednaka grupi koju generiše njihova unija, a konjunkcija jednaka njihovom preseku. Pojam mreže je nastao u ovom kontekstu.

(c) Za proizvojlnu strukturu $\mathcal{A}$, klasa svih njenih podstruktura $S(\mathcal{A})$ čini mrežu u odnosu na inkluziju kao poredak.

Mreža $\mathcal{L}$ je *distributivna* ako za sve $x, y, z \in L$ važe sledeće jednakosti:

$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z), \quad x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z).$$

Ako je X proizvoljan skup elemenata mreže $\mathcal{L}$, ukoliko uopšte postoji, sa $\bigvee X$ označavamo *supremum skupa* X, a sa $\bigwedge X$ njegov *infimum*.

Svaki konačan skup ima supremum i infimum, ali u opštem slučaju to se ne odnosi i na beskonačne skupove elemenata mreže.

Mreža je $\mathcal{L}$ je *kompletna* ako svaki skup elemenata ima supremum. U kompletnoj mreži, svaki skup ima infimum koji je definisan sa:

$$\bigwedge X = \bigvee \{x \in L : \forall y \in X\, (x \leq y)\}.$$

Primer 6. S obzirom na inkluziju, partitivni skup $P(X)$ skupa X je kompletna mreža u kojoj supremumu i infimumu odgovaraju skupovne operacije unije i preseka. Mreža otvorenih skupova topološkog prostora je takođe kompletna. Pritom, supremumu odgovara skupovna unija, a infimumu otvorenje skupovnog preseka.

Ako je $\mathcal{L}$ mreža, $x \in L$ je *najmanji element* ako za sve $y \in L$, $x \leq y$. Ako za sve $y \in L$, $y \leq x$, element $x \in L$ je *najveći element* mreže $\mathcal{L}$. Ukoliko postoje, najmanji i najveći elementi mreže su jedinstveno određeni i označavamo ih redom sa 0 i 1.

Mreža $\mathcal{L}$ sa najmanjim i najvećim elementom je *komplementirana* ako za svako $x \in L$ postoji $y \in L$ takvo da

$$x \vee y = 1, \quad x \wedge y = 0.$$

Ukoliko postoji, element $y \in L$ sa navedenom osobinom je *komplement* elementa $x \in L$. U opštem slučaju komplement ne mora biti jedinstven.

Teorema 1. U distributivnoj mreži sa najmanjim i najvećim elementom svaki element ima najviše jedan komplement.

Dokaz: Ako je $\mathcal{L}$ distributivna mreža i $y, z \in L$ komplementi elementa $x \in L$, onda $y = y \vee 0 = y \vee (x \wedge z) = (y \vee x) \wedge (y \vee z) = 1 \wedge (y \vee z) = y \vee z$. Na sličan način dobija se i da je $z = y \vee z$, tj. $y = z$. $\Box$

Dugo se verovalo da je svaka mreža sa jedinstvenom komplementacijom distributivna. Ipak, četrdesetih godina konstruisana je takva mreža koja nije distributivna. Danas je otvoren problem da li kompletna mreža sa jedinstvenom komplementacijom mora biti distributivna.

Na osnovu prethodne teoreme sledi da se u komplementiranoj distributivnoj mreži $\mathcal{L}$ može definisati funkcija * koja svakom $x \in L$ pridružuje komplement $x^* \in L$. Pritom, za svako $x \in L$, $x^{**} = x$.

Primer 7. Mreža $\mathrm{S}(\mathcal{V})$ potprostora vektorskog prostora $\mathcal{V}$ je komplementirana, ali nije distributivna.

Primer 8. Linearno uređenje $\mathcal{L}$ sa krajevima je distributivna mreža u kojoj svaki $x \in L$, $x \neq 0, 1$, nema komplement u $\mathcal{L}$.

Distributivna komplementirana mreža je *Bulova algebra*.

Potpunije rečeno, Bulova algebra je parcijalno uređenje $\mathcal{B} = (B, \leq)$ sa najmanjim i najvećim elementom, u kojem svaki par elemenata ima supremum i infimum koji su distributivni i u kojem svaki element ima komplement.

Iz prethodnih razmatranja neposredno sledi da u svakoj Bulovoj algebri $\mathcal{B} = (B, \leq)$, za sve $x, y, z \in B$, važe sledeće jednakosti:

$$
\begin{array}{ll}
x \wedge y = y \wedge x, & x \vee y = y \vee x, \\
x \wedge (y \wedge z) = (x \wedge y) \wedge z, & x \vee (y \vee z) = (x \vee y) \vee z, \\
x \wedge (x \vee y) = x, & x \vee (x \wedge y) = x, \\
x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z), & x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z), \\
x \wedge x^* = 0, & x \vee x^* = 1.
\end{array}
$$

Bulovu algebru $\mathcal{B} = (B, \leq)$ možemo shvatiti i kao algebarsku strukturu oblika $\mathcal{B}^a = (B, \vee, \wedge, ^*, 0, 1)$, sa dve binarne operacije $\vee$ i $\wedge$, jednom unarnom * i dve konstante 0 i 1, koje zadovoljavaju upravo navedene jednakosti. Dakle, operacije $\vee$ i $\wedge$ su komutativne, asocijativne, zadovoljavaju zakone apsorpcije, uzajamno su distributivne, a operacija * je komplementacija u algebri $\mathcal{B}^a$.

Obratno, ako se u strukturi $\mathcal{B} = (B, \vee, \wedge, ^*, 0, 1)$ definiše binarna relacija $\leq$ tako da za sve $x, y \in B$, $x \leq y$ ako i samo ako $x \wedge y = x$, onda je $\mathcal{B}^u = (B, \leq)$ komplementirana distributivna mreža, tj. Bulova algebra u smislu prvobitno formulisane definicije. Ako je struktura $\mathcal{B}$ uređenje, $(\mathcal{B}^a)^u = \mathcal{B}$ i slično, ako je $\mathcal{B}$ algebra, onda $(\mathcal{B}^u)^a = \mathcal{B}$ što znači da sasvim slobodno možemo koristiti obe definicije Bulovih algebri.

Primer 9. Neka je $P(X)$ skup svih podskupova skupa X. Struktura $(P(X), \cup, \cap, ^c, \emptyset, X)$ je Bulova algebra. Ako je X prazan skup, algebra $P(X)$ svodi se na jednoelementnu ili *trivijalnu* Bulovu algebru.

U daljim izlaganjima, ako to posebno ne naglasimo, uvek podrazumevamo netrivijalne Bulove algebre. Dakle, u svakoj Bulovoj algebri važi nejednakost $0 \neq 1$.

Svaka familija skupova zatvorena za preseke, unije i komplemente je Bulova algebra. Takvu algebru nazivamo *algebrom skupova*. Algebre skupova su podalgebre Bulovih algebri oblika $P(X)$.

Za svaku familiju $M \subseteq P(X)$, presek svih podalgebri skupova koje sadrže M je takođe algebra skupova. To je najmanja algebra skupova koja sadži familiju M.

Primer 10. Ako je X jednoelementni skup, $P(X)$ ima dva elementa $\emptyset$ i X koje, sledeći skupovno teorijsku notaciju, označavamo sa 0 i 1, a Bulovu algebru $P(X)$ sa $2 = \{0, 1\}$. Njene operacije su:

x	y	$x \vee y$	$x \wedge y$	x^*
0	0	0	0	1
0	1	1	0	1
1	0	1	0	0
1	1	1	1	0

Do na izomorfizam, algebra 2 je jedinstvena Bulova algebra sa dva elementa. Ova algebra ima ključnu ulogu u teoriji Bulovih algebri.

Primer 11. Neka je X beskonačan skup kardinalnosti κ i

$$B(X) = \{x \subseteq X : |x| < \omega \text{ ili } |x^c| < \omega\}.$$

Familija skupova $B(X)$ je algebra skupova. Nazivamo je *Frešeovom algebrom* nad skupom X i označavamo sa $\mathcal{B}(X)$.

Kako je kardinal κ beskonačan, kardinalnost algebre $\mathcal{B}(X)$ je takođe κ. Dakle, u svakom beskonačnom kardinalu κ, postoji bar jedna Bulova algebra kardinalnosti κ.

U slučaju konačnih kardinala ta stvar izgleda drugačije. Naime, kako ćemo kasnije videti, konačan broj k je kardinalnost Bulove algebre ako i samo ako za neki prirodan broj n, $k = 2^n$.

Ako je $\kappa = \omega$, za svaki kardinal λ, kardinalnost algebre $\mathcal{B}(X)$ je različita od 2^λ. Dakle, algebra $\mathcal{B}(X)$ nije oblika partitivnog skupa.

Primer 12. Neka je X topološki prostor i $C(X)$ familija svih zatvoreno otvorenih skupova prostora X. S obzirom na inkluziju kao poredak, $C(X)$ je Bulova algebra.

Algebra $C(X)$ je *karakteristična algebra* prostora X. Ako je prostor X povezan, njegova karakteristična algebra je algebra 2. Ako prostor ima $n \in \omega$ komponenti povezanosti, njegova karakteristična algebra je $P(n)$.

Primer 13. Neka je $\mathcal{P} = (P, \leq, 0)$ beskonačno linearno uređenje sa najmanjim elementom. Za proizvoljne $x, y \in P$,

$$[x, y) = \{z \in P : x \leq z < y\}, \quad [x, \infty) = \{z \in P : x \leq z\},$$

su poluotvoreni intervali u $\mathcal{P}$.

Familija $\mathrm{L}(\mathcal{P})$ svih konačnih unija poluotvorenih intervala je Bulova algebra. Algebra $\mathrm{L}(\mathcal{P})$ je *intervalna algebra* nad uređenjem $\mathcal{P}$.

Najveći element u algebri $\mathrm{L}(\mathcal{P})$ je interval $[0, \infty)$, a najmanji "interval" $[x, x) = [\infty, \infty)$ je prazan skup. Za svaki element $x \in \mathrm{L}(\mathcal{P})$, postoji najmanji prirodan broj $n \in \omega$ i niz $x_0 < y_0 < x_1 < \cdots y_{n-1} < x_n < y_n$, elemenata uređenja $\mathcal{P}$, $y_n \in P \cup \{\infty\}$, takav da

$$x = [x_0, y_0) \cup \cdots \cup [x_n, y_n)$$

i pritom, $x^* = [0, x_0) \cup [y_0, x_1) \cup \cdots \cup [y_{n-1}, x_n) \cup [y_n, \infty)$. To znači da familija $\mathrm{L}(\mathcal{P})$ zaista čini Bulovu algebru.

Primer 14. Neka je $\mathcal{V}$ vektorski prostor nad poljem $\mathcal{K}$ i $\mathrm{Hom}(\mathcal{V})$ skup svih linearnih operatora prostora $\mathcal{V}$. U odnosu na operacije sabiranja i kompozicije, $\mathrm{Hom}(\mathcal{V})$ čini prsten endomorfizama prostora $\mathcal{V}$.

Element f prstena $\mathrm{Hom}(\mathcal{V})$ je projekcija ako $f \circ f = f$. Neka je $\mathrm{A}(\mathcal{V})$ skup svih komutativnih projekcionih operatora prostora $\mathcal{V}$. Nula operator i identičko preslikavanje su projekcioni operatori. Za proizvoljne $f, g \in \mathrm{A}(\mathcal{V})$ neka je $f \vee g = f + g - f \circ g$, $f \wedge g = f \circ g$ i $f^* = 1 - f$. Sa tako definisanim operacijama, algebra $\mathrm{A}(\mathcal{V})$ je Bulova algebra.

Algebra $\mathrm{A}(\mathcal{V})$ je *algebra projekcija* prostora $\mathcal{V}$. Poredak u algebri projekcija je određen tako da, za sve $f, g \in \mathrm{A}(\mathcal{V})$, $f \leq g$ ako i samo ako $\mathrm{im}(f) \subseteq \mathrm{im}(g)$. Pritom, $\mathrm{im}(f)$ je slika operatora f, odnosno, operator f projektuje prostor $\mathcal{V}$ na potprostor $\mathrm{im}(f)$.

Pre nego što razmotrimo svojstva Bulovih algebri, formulisaćemo takozvani princip dualnosti, koji značajno pojednostavljuje njihovu aritmetiku. Formulacija ovog principa data je sasvim neformalno budući da njegova precizna verzija podrazumeva pozivanje na predikatski račun.

Neka je φ jednakost koja se odnosi samo na operacije $\vee, \wedge, {}^*$ i konstante 0 i 1. Označimo sa φ^* jednakost koja se iz φ dobija zamenom svih javljanja operacija $\vee$, $\wedge$ i konstanti 0 i 1 redom sa $\wedge$, $\vee$, 1 i 0. Jednakost φ^* je *dualna* jednakosti φ.

Teorema 2. Princip dualnosti: Jednakost φ važi u algebri $\mathcal{B}$ ako i samo ako jednakost φ^* važi u algebri $\mathcal{B}$.

Dokaz: Neka φ važi u svim Bulovim algebrama. Za proizvoljnu algebru $\mathcal{B} = (B, \leq)$ definišimo binarnu relaciju $\leq^*$ tako da za sve $x, y \in B$, $x \leq^* y$ ako i samo ako $y \leq x$. Struktura $\mathcal{B}^* = (B, \leq^*)$ je Bulova algebra čijoj operaciji $\vee$ odgovara operacija $\wedge$ u polaznoj algebri, operaciji $\wedge$ odgovara operacija $\vee$, konstanti 0 odgovara konstanta 1 i konstanti 1 odgovara konstanta 0 polazne algebre. Budući da φ važi u svim Bulovim algebrama, φ važi u $\mathcal{B}^*$, a to upravo znači da jednakost φ^* važi u $\mathcal{B}$. $\square$

Primer 15. Ako je $\mathcal{B}$ Bulova algebra, za sve $x, y \in B$, važe De Morganova pravila: $(x \vee y)^* = x^* \wedge y^*$ i $(x \wedge y)^* = x^* \vee y^*$.

Primer 16. (a) Ako je $\mathcal{B}$ Bulova algebra, onda za sve $x, y \in B$, $x \leq y$ ako i samo ako $y^* \leq x^*$ ako i samo ako $x \wedge y^* = 0$

(b) Za sve $x, y, z \in B$, $z \wedge x \leq y$ ako i samo ako $x \leq z^* \vee y$.

Ako $x \leq y$, onda $x \wedge y = x$, pa na osnovu De Morganovih zakona, $x^* \vee y^* = (x \wedge y)^* = x^*$, tj. $y^* \leq x^*$. Obratno, iz $y^* \leq x^*$ sledi da je $x = x^{**} \leq y^{**} = y$.

Ako $x \leq y$, onda $x = x \wedge y$, pa dakle $x \wedge y^* = x \wedge y \wedge y^* = 0$. Obratno, iz $x \wedge y^* = 0$, redom sledi da je $x = x \wedge (y \vee y^*) = (x \wedge y) \vee (x \wedge y^*) = (x \wedge y)$, tj. $x \leq y$.

U slučaju tvrđenja (b), ako pretpostavimo da važi $z \wedge x \leq y$, onda redom imamo $x = (z \vee z^*) \wedge x = (z \wedge x) \vee (z^* \wedge x) \leq y \vee z^*$.

Obratno, ako je $x \leq z^* \vee y$, onda $z \wedge x \leq z \wedge (z^* \vee y) \leq z \wedge y \leq y$.

U odnosu na beskonačne operacije supremuma $\bigvee$ i infimuma $\bigwedge$, ukoliko ih dopušta, Bulova algebra takođe zadovoljava određena svojstva. Međutim, ova aritmetika je mnogo komplikovanija i često počiva na složenim kombinatornim svojstvima Bulovih algebri. U ovim razmatranjima ćemo se osvrnuti na samo neka od tih svojstava.

Primer 17. Ako je $\mathcal{B}$ Bulova algebra, onda za svako $a \in B$ i svako $S \subseteq B$ važe sledeće jednakosti:

(a) $a \wedge \bigvee S = \bigvee\{a \wedge x : x \in S\}$ i $a \vee \bigwedge S = \bigwedge\{a \vee x : x \in S\}$,

(b) $(\bigvee S)^* = \bigwedge\{x^* : x \in S\}$ i $(\bigwedge S)^* = \bigvee\{x^* : x \in S\}$.

Sve navedene jednakosti treba razumeti na sledeći način: ukoliko je izraz na levoj strani definisan, definisan je i izraz na desnoj strani i međusobno su jednaki.

Neka je $s = \bigvee S$. Treba dokazati da je $a \wedge s$ najmanje gornje ograničenje za $\{a \wedge x : x \in S\}$. Za sve $x \in S$, $x \leq s$, tj. $x \wedge a \leq s \wedge a$, što znači da je $a \wedge s$ gornje ograničenje za $\{a \wedge x : x \in S\}$. Neka je $t \in B$ gornje ograničenje za $\{a \wedge x : x \in S\}$, onda za svako $x \in S$, $a \wedge x \leq t$, pa prema tvrđenju (b) iz prethodne teoreme, $x \leq a^* \vee t$, tj. $s \leq a^* \vee t$, što prema istom tvrđenju znači da je $a \wedge s \leq t$.

Da bi se dokazalo tvrđenje (b), treba dokazati da je s^* najveće donje ograničenje za $\{x^* : x \in S\}$. Za sve $x \in S$, $x \leq s$, pa dakle $s^* \leq x^*$, tj. s^* je donje ograničenje. Ako je $t \in B$ neko drugo donje ograničenje za $\{x^* : x \in S\}$, onda za svako $x \in S$, $t \leq x^*$, tj. $x \leq t^*$, pa dakle $s \leq t^*$, tj. $t \leq s^*$, a to znači $s^* = \bigwedge\{x^* : x \in S\}$.

Za svaki skup X, algebra $P(X)$ je kompletna. Frešeove algebre nisu kompletne. Ako je $\mathcal{B}(X)$ Frešeova algebra nad beskonačnim skupom X, za svako $Y \subseteq X$, ako $|Y|, |Y^c| \geq \omega$, skup $S = \{\{x\} : x \in Y\}$ nema supremum u $\mathcal{B}(X)$.

Primer 18. Ako je $\mathcal{A} \subseteq P(X)$ kompletna algebra skupova u kojoj za sve $M \subseteq A$, $\bigvee M = \bigcup M$ i $\bigwedge M = \bigcap M$, onda postoji skup Y takav da $\mathcal{B} \cong P(Y)$.

Definišimo relaciju ekvivalencije na skupu X tako da za proizvoljne $x, y \in X$, $x \sim y$ ako i samo ako za svako $a \subseteq X$, $x \in a \Leftrightarrow y \in a$. Ako je $Y = X_{/\sim}$, onda $P(Y) \cong \mathcal{A}$.

Dakle, algebra skupova $\mathcal{A}$ je kompletna ako i samo ako postoji X takav da $P(X) = \mathcal{A}$. Pritom, pojam izomorfizma upotrebljavamo u standardnom matematičkom smislu.

Bulova algebra u kojoj svaki prebrojiv skup ima supremum je *σ-kompletna algebra*. Opštije, za svaki kardinal κ, Bulova algebra $\mathcal{B}$ je *κ-kompletna* ako svaki skup elemenata algebre $\mathcal{B}$ kardinalnosti manje od κ ima supremum u algebri $\mathcal{B}$.

Primer 19. U topološkom prostoru X sa topologijom $O(X)$

$$\mathrm{Bor}(X) = \bigcap\{B \subseteq P(X) : \mathcal{B} \text{ je } \sigma\text{-algebra i } O(X) \subseteq B\}$$

je najmanja σ-algebra skupova nad skupom X koja sadrži sve otvorene skupove prostora X i naziva se *Borelovom algebrom* prostora X.

Primer 20. Algebra $\mathrm{L}(\mathcal{R})$ svih Lebeg-merljivih skupova realnih brojeva je σ-algebra. Kako je svaki otvoren skup realnih brojeva merljiv u Lebegovom smislu, $\mathrm{Bor}(R)$ je podalgebra algebre $\mathrm{L}(\mathcal{R})$.

Primer 21. (a) Frešeova algebra $\mathcal{B}(X)$ nije σ-kompletna. Svakako, da bi ovo tvrđenje imalo smisla pretpostavljamo da je $|X|$ beskonačan skup.

(b) Neka je κ beskonačan kardinal, $|X| \geq \kappa$ i

$$B_\kappa(X) = \{x \in X : |x| < \kappa \text{ ili } |x^c| < \kappa\}.$$

Familija $B_\kappa(X)$ je Bulova algebra i predstavlja prirodno uopštenje Frešeove algebre. Za svako $n \in \omega$, ako je $\kappa = \aleph_n$, algebra $\mathcal{B}_\kappa(X)$ je κ-kompletna, ali nije κ^+-kompletna.

(c) Ako je $\kappa = \aleph_\omega = \lim_{n\to\infty} \aleph_n$, algebra $\mathcal{B}_\kappa(X)$ nije σ-kompletna.

Primer 22. Ako je $\mathcal{P}$ beskonačno linearno uređenje, intervalna algebra $\mathrm{L}(\mathcal{P})$ nije σ kompletna.

Pored karakteristične algebre $C(X)$, zatvoreno otvorenih skupova prostora X, zatim Borelove algebre $\mathrm{Bor}(X)$ i nekih drugih primera sa kojima smo se do sada susreli, u svakom topološkom prostoru prirodno se javlja algebra njegovih regularno otvorenih skupova. Ova algebra determiniše univerzalnu konstrukciju kompletiranja Bulove algebre, pa u strukturnoj teoriji i primenama ima veliki značaj. Definiciju i konstrukciju algebre regularno otvorenih skupova izložićemo u sledećim primerima.

Ako je $u \subseteq X$ skup tačaka prostora X, onda je $\mathrm{r}(u) = \mathrm{int}(\mathrm{cl}(u))$ *regularizacija* skupa $u \subseteq X$. Ako je $\mathrm{r}(u) = u$, onda je $u \subseteq X$ *regularno otvoren* skup.

Primer 23. U svakom topološkom prostoru X, operator regularizacije zadovoljava sledeće uslove:

(a) Za svaki otvoren skup $u \subseteq X$, $u \subseteq \mathrm{r}(u)$.

(b) Za svako $x \subseteq X$, $\mathrm{r}(x)$ je regularno otvoren skup.

(c) Za svaki otvoren skup $u \subseteq X$, $\mathrm{r}(u)$ je najmanji regularno otvoren skup koji sadrži u.

(d) Za svako $x \subseteq X$ i svaki otvoren skup $u \subseteq X$, $u \cap \mathrm{r}(x) \subseteq \mathrm{r}(u \cap x)$.

U proizvoljnom topološkom prostoru X, familiju svih regularno otvorenih skupova označavaćemo sa $\mathrm{RO}(X)$. Koristeći prethodni primer, u familiji regularno otvorenih skupova može se definisati algebarska struktura.

Za proizvoljne regularno otvorene skupove $u, v \in \mathrm{RO}(X)$,

$$u \vee v = \mathrm{r}(u \cup v), \quad u \wedge v = u \cap v, \quad u^* = \mathrm{int}(u^c).$$

Najmanji element mreže $\mathrm{RO}(X)$ je $\emptyset$, a najveći prostor X. Supremum i infimum familije regularno otvorenih skupova $S \subseteq \mathrm{RO}(X)$ definišemo na sledeći način:

$$\bigvee S = \mathrm{r}(\bigcup S), \quad \bigwedge S = \mathrm{r}(\bigcap S).$$

Primer 24. U svakom topološkom prostoru X, algebra regularno otvorenih skupova $\mathrm{RO}(X)$ je kompletna Bulova algebra.

Podalgebre i homomorfizmi

U univerzalnoj algebri, klasa algebri istog tipa, koja zadovoljava određen skup jednakosti naziva se *varijetetom*. Budući da smo klasu Bulovih algebri $\mathcal{B}A$ upravo i definisali kao klasu algebri istog tipa, sa dve binarne, jednom unarnom operacijom i dve konstante, koja zadovoljava određen skup identiteta, $\mathcal{B}A$ je varijetet. Zanimljivo je da u klasi $\mathcal{B}A$, osim trivijalnog, nema drugih varijeteta. Preciznije, ako je $\mathcal{K} \subseteq \mathcal{B}A$ bilo koja klasa Bulovih algebri koja čini varijetet, onda se $\mathcal{K}$ sastoji od trivijalne algebre, pa dakle zadovoljava sve identite, ili je $\mathcal{K} = \mathcal{B}A$. Dakle, nema identiteta koji važi na nekoj netrivijalnoj Bulovoj algebri, a da ne važi na svim Bulovim algebrama.

Osnovni rezultat u teoriji varijeteta je Birkhofova teorema koja karakteriše varijetete kao klase algebri zatvorene za podalgebre, homomorfne slike i Dekartove proizvode. U slučaju Bulovih algebri, ova činjenica je posledica Stonove teoreme reprezentacije, pa se dokaz Birkhofove teoreme za klasu Bulovih algebri zapravo svodi na dokaz teoreme reprezentacije.

Ako je $\mathcal{B}$ Bulova algebra i $A \subseteq B$ zatvoren za operacije u $\mathcal{B}$, skup A je domen algebre $\mathcal{A}$. Algebra $\mathcal{A}$ je *podalgebra* Bulove algebre $\mathcal{B}$.

Zbog De Morganovih zakona, za sve $x, y \in B$, $x \wedge y = (x^* \vee y^*)^*$, pa je u definiciji podalgebre dovoljno pretpostaviti zatvorenost za operacije $\vee$ i *.

Presek svake familije podalgebri Bulove algebre $\mathcal{B}$ je podalgebra algebre $\mathcal{B}$. Za svaki skup $X \subseteq B$, presek familije svih podalgebri koje sadrže X je podalgebra u $\mathcal{B}$ koju označavamo sa $\langle X \rangle_B$ i nazivamo *algebrom generisanom skupom* X. Budući da podrazumevamo samo netrivijalne algebre, za svaku algebru B, $\langle \emptyset \rangle_B = \{0, 1\}$. Ako je $\langle X \rangle_B = B$, skup $X \subseteq B$ generiše algebru $\mathcal{B}$. Kada je iz konteksta jasno o kojoj algebri je reč, umesto $\langle X \rangle_B$ upotrebljavamo oznaku $\langle X \rangle$.

Primer 1. Frešeova algebra $\mathcal{B}(X)$, kao podalgebra algebre $P(X)$, generisana je skupom $\{\{x\} : x \in X\}$.

Intervalna algebra $\mathrm{L}(\mathcal{P})$ nad linearnim uređenjem $\mathcal{P}$ generisana je familijom $\{[0, x) : x \in P\}$ poluotvorenih intervala.

Primer 2. Ako je $\mathcal{B}$ Bulova algebra i $X \subseteq B$, onda

$$\langle X \rangle = \bigcup \{\langle P \rangle : P \subseteq X \text{ i } |P| < \omega\}.$$

Primer 3. Ako je $\mathcal{B}$ Bulova algebra i $X \subseteq B$ neprazan skup, onda

$$\langle X \rangle = \{\textstyle\bigvee_{j=1}^{n} \bigwedge_{i=1}^{m_j} x_{ij} : n, m_1, \ldots, m_n \in \omega, x_{ij} \in X \text{ ili } x_{ij}^* \in X\}.$$

Ako je $X \subseteq B$, element $x = \bigvee_{j=1}^{n} \bigwedge_{i=1}^{m_j} x_{ij}$ je predstavljen u disjunktivnoj *normalnoj formi* nad skupom X. Na osnovu prethodnog primera, dovoljno je pokazati da je za svaki konačan skup $X \subseteq B$ svaki element algebre $\langle X \rangle$ predstavljiv u normalnoj formi.

Neka je $n \in \omega$, $X = \{x_1, \dots, x_n\}$ i $E = 2^n$ skup svih funkcija skupa $\{1, \dots, n\}$ u skup $\{-1, +1\}$. Za svako $x \in B$, za svako $e \in E$ i za svako $i \in \{1, \dots, n\}$ neka je $x^{e(i)} = x$, ako je $e(i) = +1$, a $x^{e(i)} = x^*$ ako je $e(i) = -1$.

Za proizvoljno $e \in E$, neka je $p_e = x_1^{e(1)} \wedge \cdots \wedge x_n^{e(n)}$. Ako su $e, e^{'} \in E$ različite funkcije, onda $p_e \wedge p_{e'} = 0$. Takođe, $\bigvee_{e \in E} p_e = 1$.

Za svako $M \subseteq E$, element $s_M = \bigvee_{e \in M} p_e$ je u normalnoj formi nad X. Neka je $A = \{s_M : M \subseteq E\}$. Treba dokazati da je $\langle X \rangle \subseteq A$. Skup A sadrži 0 i 1 i zatvoren je za operacije $\vee$ i * jer: za sve $M, N \subseteq E$, $s_M \vee s_N = s_{M \cup N}$ i $s_M^* = s_{M^c}$. Dakle $\mathcal{A}$ je podalgebra algebre $\mathcal{B}$. Kako je za svako $i \in \{1, \dots, n\}$, $x_i = s_M$, gde je $M = \{e \in E : e(i) = +1\}$, to je $X \subseteq A$, tj. $\langle X \rangle$ je podalgebra algebre $\mathcal{A}$.

Primer 4. Neka je $X \subseteq B$ skup elemenata Bulove algebre $\mathcal{B}$.

(a) Ako je $|X| = n < \omega$, algebra $\langle X \rangle$ ima najviše 2^{2^n} elemenata.

(b) Ako je $|X| = \kappa \geq \omega$, algebra $\langle X \rangle$ ima kardinalnost κ.

Ako skup X ima $n \in \omega$ elemenata, algebra $\langle X \rangle$ sastoji se od elemenata oblika

$$x = \bigvee_{e \in M} \bigwedge_{x \in X} x^{e(x)},$$

za neko $M \subseteq \{+1, -1\}^X$, tj. $\langle X \rangle$ ima najviše 2^{2^n} elemenata. Dakle, svaka konačno generisana algebra je konačna.

Na uobičajeni način, homomorfizam Bulovih algebri definišemo kao preslikavanje koje čuva njihovu strukturu. Funkcija $f : A \to B$ je *homomorfizam* Bulovih algebri $\mathcal{A}$ i $\mathcal{B}$, ako za sve $x, y \in A$,

$$\begin{aligned}
&f(x \vee y) = f(x) \vee f(y), \\
&f(x \wedge y) = f(x) \wedge f(y), \\
&f(x^*) = f(x)^*, f(0) = 0 \text{ i } f(1) = 1.
\end{aligned}$$

Obostrano jednoznačni homomorfizam je *monomorfizam*, homomorfizam na je *epimorfizam*, a obostrano jednoznačni i na homomorfizam je *izomorfizam*. Relacija $\mathcal{A} \cong \mathcal{B}$ označava izomorfizam Bulovih algebri.

U definiciji homomorfizma svi navedeni uslovi nisu neophodni. Na primer, dovoljno je pretpostaviti saglasnost preslikavanja f sa operacijama $\vee$ i *, a sve druge saglasnosti su njihove posledice.

Homomorfizam je takođe saglasan sa poretkom, tj. za sve $x, y \in A$,

$$x \leq y \quad \Leftrightarrow \quad f(x) \leq f(y).$$

Međutim, obratno ne važi, tj. preslikavanje koje čuva poredak nije obavezno i homomorfizam.

Primer 5. Ako je $f : A \to B$ homomorfizam, skup $f[A]$ je podalgebra algebre $\mathcal{B}$, tj. klasa Bulovih algebri je zatvorena za homomorfne slike.

Primer 6. Homomorfizam $f : A \to B$ je monomorfizam ako i samo ako za svako $x \in A$, $f(x) = 0$ implicira $x = 0$.

Ako je $g : A \to B$ homomorfizam, $f = g$ ako i samo ako f i g imaju jednake vrednosti na nekom generatornom skupu algebre $\mathcal{A}$.

Na osnovu prethodnog primera, homomorfizam Bulovih algebri određen je vrednostima na generatornom skupu. Zanimljivo je pitanje pod kojim uslovima funkcija definisana na generatornom skupu Bulove algebre ima proširenje do homomorfizma. Odgovor na to pitanje nije sasvim trivijalan i izložen je u sledećoj teoremi.

Teorema 3. Neka je X skup koji generiše algebru $\mathcal{A}$ i $f : X \to B$ funkcija sa vrednostima u Bulovoj algebri $\mathcal{B}$.

Funkcija f može se proširiti do homomorfizma algebre $\mathcal{A}$ ako i samo ako za svako $n \in \omega$, za sve $x_1, \ldots, x_n \in X$ i sve $e_1, \ldots, e_n \in \{+1, -1\}$,

$$x_1^{e_1} \wedge \cdots \wedge x_n^{e_n} = 0 \quad \Rightarrow \quad f(x_1)^{e_1} \wedge \cdots \wedge f(x_n)^{e_n} = 0.$$

Dokaz: Kako smo ranije naglasili, algebra generisana skupom X može se predstaviti u obliku $\langle X \rangle = \bigcup\{\langle P \rangle : P \subseteq X \text{ i } |P| < \omega\}$.

Dokazaćemo da za svaki konačan skup $P \subseteq X$, restrikcija f_P funkcije f na skup P ima proširenje do homomorfizma $f_P : \langle P \rangle \to B$ algebre $\langle P \rangle$. U tom slučaju, proširenje g funkcije f do homomrfizma algebre $\langle X \rangle$ je

$$g = \bigcup\{f_P : P \subseteq X \text{ i } |P| < \omega\}.$$

Neposredno se proverava da je g homomorfizam algebre $\mathcal{A}$ koji proširuje funkciju f. Dakle, u dokazu teoreme možemo pretpostaviti da je generatorni skup X algebre $\mathcal{A}$ konačan.

Pretpostavimo da je $X = \{x_1, \ldots, x_n\}$, za neko $n \in \omega$. Kao i ranije, neka je $E = 2^n$ i za proizvoljno $e \in E$, neka je

$$p_e = x_1^{e(1)} \wedge \cdots \wedge x_n^{e(n)}.$$

Takođe, za svako $M \subseteq E$, neka je $s_M = \bigvee_{e \in M} p_e$ normalna forma (nad skupom X) elementa algebre $\mathcal{A}$.

Sa druge strane, u Bulovoj algebri $\mathcal{B}$, za svako $e \in E$, neka je

$$q_e = f(x_1)^{e(1)} \wedge \cdots \wedge f(x_n)^{e(n)}.$$

Za svako $M \subseteq E$, neka $t_M = \bigvee_{e \in M} q_e$.

Kako je $A = \langle X \rangle = \{s_M : M \subseteq E\}$, definišimo funkciju $g : A \to B$ tako da za svako $M \subseteq E$,

$$g(s_M) = t_M.$$

Tvrdimo da je g homomorfizam koji proširuje funkciju f.

Pre svega, treba dokazati da je preslikavanje g korektno definisano, tj. da za sve $M, N \subseteq E$,

$$s_M = s_N \ \Rightarrow \ t_M = t_N.$$

Za sve $M, N \subseteq E$, neka je $M \triangle N$ simetrična razlika skupova M i N. Ako su $M, N \subseteq E$ takvi da $s_M = s_N$, onda $s_M \wedge s_N^* = 0$ i $s_M^* \wedge s_N = 0$, tj. $s_{M \triangle N} = 0$. Otuda, za svako $e \in M \triangle N$, $p_e = 0$. Po pretpostavci teoreme, za svako $e \in M \triangle N$, mora biti $q_e = 0$, a to upravo znači da je $t_M = t_N$.

Na osnovu definicije funkcije g, za proizvoljne $M, N \subseteq E$,

$$g(s_M \vee s_N) = g(s_{M \cup N}) = t_{M \cup N} = t_M \vee t_N = g(s_M) \vee g(s_N) \text{ i}$$
$$g(s_M^*) = g(s_{M^c}) = t_{M^c} = t_M^* = g(s_M)^*,$$

što znači da je g homomorfizam.

Treba još dokazati da funkcija g zaista proširuje funkciju f. Za proizvoljan skup $M \subseteq E$, ako je $M = \{e \in E : e(i) = +1\}$, onda $s_M = x_i$, pa dakle $g(x_i) = t_M = f(x_i)$, što znači funkcija g proširuje f. $\square$

Ako je $\mathcal{A}$ podalgebra Bulove algebre $\mathcal{B}$, prirodno je pitanje pod kojim uslovima se homomorfizam podalgebre $\mathcal{A}$ može proširiti do homomorfizma algebre $\mathcal{B}$. Generalni odgovor na to pitanje nemamo, ali se u određenim slučajevima o tome ipak nešto može reći.

Neka je $\mathcal{A}$ podalgebra algebre $\mathcal{B}$. Za svako $x \in B$, algebru generisanu skupom $A \cup \{x\}$, u oznaci $A(x)$, nazivaćemo *prostom ekstenzijom* algebre $\mathcal{A}$. Koristeći disjunktivnu normalnu formu, prostu ekstenziju algebre $\mathcal{A}$ možemo predstaviti u obliku:

$$A(x) = \{(u \wedge x) \vee (v \wedge x^*) : u, v \in A\}.$$

Primer 7. Neka je $f : A \to B$ homomorfizam i $A(x)$ prosta ekstenzija algebre $\mathcal{A}$. Za svako $y \in B$, postoji homomorfizam $g : A(x) \to B$ koji proširuje f takav da $g(x) = y$ ako i samo ako za sve $u, v \in A$,

$$u \leq x \leq v \ \ \to \ \ f(u) \leq y \leq f(v).$$

Na osnovu teoreme o proširenju homomorfizma, egzistencija homomorfizma g ekvivalentna je sledećim uslovima: za sve $u, v \in A$,

$$u \wedge x = 0 \Rightarrow f(u) \wedge y = 0 \text{ i } v \wedge x^* = 0 \Rightarrow f(v) \wedge y^* = 0.$$

Iz $u \leq x$ sledi $u \wedge x^* = 0$, pa prema drugom uslovu, $f(u) \wedge y^* = 0$, tj. $f(u) \leq y$. Na osnovu prvog uslova, iz $x \leq v$ sledi $y \leq f(v)$.

Na primer, ako je $f : A \to B$ homomorfizam u kompletnu Bulovu algebru $\mathcal{B}$, opisano proširenje homomorfizma f na prostu ekstenziju algebre $\mathcal{A}$ postoji.

Naime, zbog kompletnosti algebre $\mathcal{B}$, postoje

$$s = \bigvee\{f(u) : u \leq x,\ u \in A\} \text{ i } t = \bigwedge\{f(v) : x \leq v,\ v \in A\},$$

pa se za $u, v \in A$, ako $u \leq x \leq v$, onda $f(u) \leq f(v)$, tj. $s \leq t$. To znači da svaki element $y \in B$, takav da $s \leq y \leq t$, zadovoljava uslov prethodnog primera, pa se proširenje g homomorfizma f na algebru $\mathcal{A}(x)$ može definisati sa $g(x) = y$.

Opštije, ako je $\mathcal{B}$ kompletna algebra, svaki homomorfizam algebre $\mathcal{A}$ u algebru $\mathcal{B}$ može se proširiti na proizvoljnu ekstenziju algebre $\mathcal{A}$. Ova činjenica zanimljiva je iz bar dva razloga. Prvo, ona počiva na jednom argumentu koji se na isti način javlja i u dokazu Banahove teoreme o proširenju funkcionala i drugo, ona u stvari karakteriše kompletne Bulove algebre budući da važi i obratno: ako se svaki homomorfizam algebre $\mathcal{A}$ u $\mathcal{B}$ može proširiti na proizvoljnu ekstenziju algebre $\mathcal{A}$, onda je $\mathcal{B}$ kompletna Bulova algebra.

Teorema 4. Neka je $\mathcal{A}$ podalgebra Bulove algebre $\mathcal{C}$. Svaki homomorfizam algebre $\mathcal{A}$ u kompletnu algebru $\mathcal{B}$ može se proširiti do homomorfizma algebre $\mathcal{C}$.

Dokaz: Neka je P skup svih homomorfizama koji proširuju homomorfizam $f : A \to B$. Skup P nije prazan i parcijalno je uređen inkluzijom. Ako je L lanac u P, onda je $\bigcup L$ je homomorfizam koji proširuje dati homomorfizam f. Dakle, svaki lanac u P ima gornje ograničenje, pa prema Cornovoj lemi, P sadrži maksimalni element g.

Tvrdimo da je $\operatorname{dom}(g) = C$. U suprotnom, ako je $\operatorname{dom}(g) = D$ i pritom $D \neq C$, onda postoji $x \in C$ takvo da $x \notin D$. Prema prethodnoj napomeni, postoji homomorfizam $h : D(x) \to B$. Dakle, h proširuje g, što protivreči pretpostavci o maksimalnosti homomorfizma g. $\square$

Primetimo da proširenje g homomorfizma f, u opštem slučaju, nije jedinstveno određeno.

Sa B^+ označavamo skup svih elemenata algebre $\mathcal{B}$ različitih od nule. Skup $X \subseteq B^+$ je *gust* u algebri $\mathcal{B}$ ako za svako $a \in B^+$, postoji $x \in X$ takvo da je $x \leq a$. Kardinal

$$\pi B = \min\{|X| : X \subseteq B^+ \text{ je gust u } B\},$$

je *gustina* algebre $\mathcal{B}$. Podalgebra $\mathcal{A}$ algebre $\mathcal{B}$ je *gusta* u $\mathcal{B}$ ako je skup A^+ gust u $\mathcal{B}$.

Na primer, skup otvorenih intervala sa racionalnim krajevima je gust u algebri $\mathrm{RO}(R)$ regularno otvorenih skupova realnih brojeva. To znači da je gustina $\pi(\mathrm{RO}(R)) = \omega$. Skup jednočlanih podskupova skupa X je gust u algebri $P(X)$, tj. $\pi(P(X)) = |X|$.

Primer 8. Ako je $\mathcal{B}$ Bulova algebra i $X \subseteq B^+$, sledeće su činjenice ekvivalentne:

(a) X je gust u $\mathcal{B}$,

(b) za svako $b \in B$, postoji familija $M \subseteq X$ međusobno disjunktnih elemenata, takva da je $b = \bigvee M$,

(c) za svako $b \in B$, postoji $M \subseteq X$ takav da je $b = \bigvee M$,

(d) za svako $b \in B$, $b = \bigvee\{x \in X : x \leq b\}$.

Jedina netrivijalna implikacija je (a) $\Rightarrow$ (b). Kao i u slučaju teoreme o proširenju homomorfizma i ovu činjenicu dokazujemo pozivajući se na Cornovu lemu. Neka je $b \in B$ i neka je

$$P = \{S \subseteq X : S \leq b \text{ i za sve } x, y \in S, x \neq y \quad \Rightarrow \quad x \wedge y = 0\}.$$

Pritom, $S \leq b$ označava da za sve $x \in S$, $x \leq b$. Skup P je parcijalno uređen inkluzijom. Ako je L lanac podskupova u P, onda je $\bigcup L$ takođe element skupa P, tj. svaki lanac u P ima gornje ograničenje. Prema Cornovoj lemi, P sadrži maksimalni element M. Tvrdimo da je $b = \bigvee M$.

Prema definiciji skupa P, element b je gornje ograničenje za M. Ako je $b \neq \bigvee M$, postoji gornje ograničenje $a \in B$ skupa M takvo da $a < b$. Kako je skup X gust u $\mathcal{B}$, postoji $x \in X$ takvo da $0 < x \leq b \wedge a^*$. Familija $M \cup \{x\}$ je familija disjunktnih elemenata jer, za svako $y \in M$, $y \leq a$, pa kako je $x \leq b \wedge a^*$, mora biti $x \leq a^*$, tj. $x \wedge y \leq a \wedge a^* = 0$. Dakle, M nije maksimalan element u uređenju P. $\Box$

Iz teoreme neposredno sledi da ako je $X \subseteq B$ gust u $\mathcal{B}$, onda $|B| \leq 2^{|X|}$, pa dakle $|B| \leq 2^{\pi B}$.

Ako je $\mathcal{A}$ podalgebra algebre $\mathcal{B}$, za razliku od osnovnih operacija $\vee$ i $\wedge$, infinitarne operacije $\bigvee^A$ i $\bigwedge^A$ u algebri $\mathcal{A}$, u opštem slučaju, ne koincidiraju sa odgovarajućim operacijama u algebri $\mathcal{B}$.

Na primer, u intervalnoj algebri $\mathrm{L}(\mathcal{R})$ nad realnim brojevima, familija $M = \{[x, \infty) : 0 < x,\ x \in R\}$ ima supremum $\bigvee^{\mathrm{L}(\mathcal{R})} M = [0, \infty)$, ali je on različit od odgovarajućeg supremuma $\bigvee^{P(R)} M = \bigcup M = (0, \infty)$ u algebri $P(R)$. Pritom, algebra $\mathrm{L}(\mathcal{R})$ je podalgebra algebre $P(R)$.

Kada se radi o gustim podalgebrama Bulove algebre takva neregularnost se ne može javiti.

Podalgebra $\mathcal{A}$ Bulove algebre $\mathcal{B}$ je *regularna* ako za svako $M \subseteq A$, ako postoji supremum $\bigvee^A M$, onda postoji supremum $\bigvee^B M$ i pritom $\bigvee^A M = \bigvee^B M$. I dualno, svaki skup koji ima infimum u $\mathcal{A}$, ima infimum u $\mathcal{B}$ koji je jednak infimumu u $\mathcal{A}$.

Teorema 5. Svaka gusta podalgebra je regularna.

Dokaz: Neka je $\mathcal{A}$ gusta u $\mathcal{B}$ i neka je $M \subseteq A$ i $m = \bigvee^A M$. Supremum m je gornje ograničenje skupa M u algebri $\mathcal{A}$, pa je m gornje ograničenje za M u $\mathcal{B}$. Neka je $n \in B$ neko drugo gornje ograničenje za M. Ako nije $m \leq n$, onda $m \wedge n^* \neq 0$. Kako je skup A^+ gust u $\mathcal{B}$, postoji $x \in A$, $0 < x$, takvo da je $x \leq m \wedge n^*$, tj. $n \leq x^*$. To znači da je $x^* \in A$ gornje ograničenje skupa M, pa mora biti $m \leq x^*$. Otuda sledi da je $x \leq m^*$. Kako je $x \in A^+$ izabran tako da $x \leq m$, to mora biti $x = 0$, suprotno pretpostavci $0 < x$. Dakle, $m = \bigvee^B M$, pa je $\mathcal{A}$ regularna podalgebra algebre $\mathcal{B}$. $\square$

Primer 9. Ako je $\mathcal{A}$ gusta podalgebra algebre $\mathcal{B}$ i $f : A \to C$ monomorfizam, svaki homomorfizam $g : B \to C$ koji proširuje f je monomorfizam.

Ako je algebra $\mathcal{A}$ gusta u kompletnoj algebri $\mathcal{B}$, algebra $\mathcal{B}$ je *kompletiranje* Bulove algebre $\mathcal{A}$.

Kako je svaka gusta podalgebra regularna, supremumi koji postoje u algebri $\mathcal{A}$ ostaju očuvani i imaju istu vrednost u kompletiranju $\mathcal{B}$.

Svaka Bulova algebra ima kompletiranje i ono je jedinstveno određeno. Ima nekoliko konstrukcija kompletiranja, ali u principu, sve one počivaju na Dedekindovoj konstrukciji kompletiranja racionalnih brojeva, odnosno, na ideji sečenja.

Na pomalo prikriven način, ideja sečenja prisutna je i u sledećoj konstrukciji: za proizvoljnu Bulovu algebru $\mathcal{B}$ neka je $P = B^+$ i $\mathcal{P} = (P, \leq)$. Za svako $p \in P$, neka je $u_p = \{q \in P : q \leq p\}$. Familija $\{u_p : p \in P\}$ je baza topologije na P. U toj topologiji, koju nazivamo *topologijom uređenja*, skup $u \subseteq P$ je otvoren ako i samo ako za sve $p, q \in P$, $p \in u$ i $q \leq p$ implicira $q \in u$. Neka je $\mathrm{RO}(P)$ algebra regularno otvorenih skupova prostora P sa topologijom uređenja. Kako smo ranije videli, $\mathrm{RO}(P)$ je kompletna Bulova algebra. Neka je $e : B \to \mathrm{RO}(P)$ preslikavanje definisano tako da: za svako

$p \in P$ $e(p) = \operatorname{int}(\operatorname{cl}(u_p))$ i $e(0) = 0$. Skup $e(p) = \operatorname{r}(u_p)$ je regularizacija skupa u_p. Preslikavanje e je kompletni monomorfizam, a algebra $e[B]$ je gusta u $\operatorname{RO}(B)$. Do na monomorfizam e, $\operatorname{RO}(B)$ je kompletiranje algebre $\mathcal{B}$.

Primer 10. Neka je $\mathcal{A}$ podalgebra kompletne Bulove algebre $\mathcal{B}$. Algebra $\mathcal{B}$ je kompletiranje algebre $\mathcal{A}$ ako i samo ako svaki monomorfizam algebre $\mathcal{A}$ u kompletnu algebru $\mathcal{C}$ ima proširenje do monomorfizma algebre $\mathcal{B}$ u $\mathcal{C}$.

Primer 11. Bulova algebra ima jedinstveno određeno kompletiranje.

Proizvodi i slobodne algebre

Kao univerzalna algebarska konstrukcija, proizvod ima određene specifičnosti u Bulovim algebrama. Glavni rezultat u tom smislu je činjenica da su sve faktorizacije dovoljno kompletnih algebri određene particijama jedinice.

Neka je $\mathcal{B}$ Bulova algebra. Za svako $a \in B$, neka je $B|a = \{x \in B : x \leq a\}$. Za svako $a \neq 1$, skup $B|a \subseteq B$ nije podalgebra u $\mathcal{B}$, ali ako se operacije algebre $\mathcal{B}$ relativizuju na a tako da za svako $x \in B|a$, $x^* = a \wedge x^*$ i $1 = a$, $B|a$ jeste Bulova algebra. Tako dobijena algebra je *relativna podalgebra* algebre $\mathcal{B}$ određena sa $a \in B$.

Na primer, za svaki skup X i svako $a \subseteq X$, $P(X)|a = P(a)$. Slično, ako je X topološki prostor, $C(X)$ algebra zatvoreno otvorenih skupova i $a \subseteq X$ zatvoreno otvoren skup, onda je $C(X)|a = C(a)$. Pritom, topologija na a indukovana je topologijom prostora X.

Za svako $a \in B$, algebri $B|a$ odgovara homomorfizam $p_a : B \to B|a$ definisan tako da za sve $x \in B$, $p_a(x) = a \wedge x$. Budući da za sve $x \in B|a$, $p_a(x) = x$, epimorfizam p_a nazivamo *projekcijom* algebre $\mathcal{B}$ na relativnu podalgebru $B|a$.

Osim podalgebri i količnika, važna algebarska konstrukcija su Dekartovi proizvodi Bulovih algebri. Pritom, u odnosu na istu konstrukciju u većini algebarskih struktura, proizvodi Bulovih algebri prilično su jednostavni. Svaka konačna faktorizacija algebre determinisana je konačnom particijom njene jedinice, a u slučaju beskonačnih faktorizacija, broj činilaca određen je stepenom kompletnosti Bulove algebre.

Proizvod Bulovih algebri $\mathcal{A}$ i $\mathcal{B}$ je algebra $\mathcal{A} \times \mathcal{B}$ sa domenom $A \times B$ u kojoj su operacije definisane po koordinatama, odnosno, za proizvoljne elemente $x, x_1, x_2 \in A$, $y, y_1, y_2 \in B$,

(a) $(x_1, y_1) \wedge (x_2, y_2) = (x_1 \wedge x_2, y_1 \wedge y_2)$,
(a) $(x_1, y_1) \vee (x_2, y_2) = (x_1 \vee x_2, y_1 \vee y_2)$,
(c) $(x, y)^* = (x^*, y^*)$, $0 = (0, 0)$ i $1 = (1, 1)$.

Primer 1. Za svako $a \in A$, $A \cong (A|a) \times (A|a^*)$.

Preslikavanje $g : A \to (A|a) \times (A|a^*)$ definisano tako da za svako $x \in A$, $g(x) = (x \wedge a, x \wedge a^*)$ je homomorfizam.

Sa druge strane, preslikavanje $h : (A|a) \times (A|a^*) \to A$, definisano tako da za sve $y, z \in A$, $h(y, z) = y \vee z$, je takođe homomorfizam. Pritom, g i h su jedno drugom inverzni.

Iako sasvim jednostavna, prethodna konstrukcija ima ključnu ulogu u izučavanju svojstava proizvoda Bulovih algebri. Na primer, prva od njenih posledica je sledeća teorema reprezentacije konačnih Bulovih algebri:

Primer 2. Za svaku konačnu Bulovu algebru $\mathcal{B}$, postoji prirodan broj $n \in \omega$ takav da $\mathcal{B} \cong 2^n$.

Tvrđenje se dokazuje indukcijom, a u induktivnom koraku koristi se faktorizacija oblika $\mathcal{B} \cong (\mathcal{B}|a) \times (\mathcal{B}|a^*)$.

Spomenuta faktorizacija važi u mnogo opštijem vidu. U toj faktorizaciji ključna stvar je činjenica da su elementi a i a^* disjunktni i da je njihova suma jednaka jedinici, tj. da oni čine particiju jedinice.

Neka je $\mathcal{B}$ Bulova algebra. Elementi $x, y \in B$ su *disjunktni* ako je $x \wedge y = 0$. Skup $X \subseteq B$ je *antilanac* u $\mathcal{B}$, ili *familija disjunktnih elemenata* algebre $\mathcal{B}$, ako $0 \notin X$ i ako su svaka dva elementa skupa X disjunktna. Antilanac je maksimalan u $\mathcal{B}$ ako nema pravo proširenje koje je takođe antilanac. Prema Zornovoj lemi, svaki antilanac može se proširiti do maksimalnog antilanca.

Primer 3. Antilanac $X \subseteq B$ je maksimalan ako i samo ako $\bigvee X = 1$.

U algebrama oblika $P(X)$, maksimalnim antilancima odgovaraju particije skupa X. Sa tom motivacijom, maksimalan antilanac Bulove algebre ponekad nazivamo i *particijom jedinice* ili prosto particijom.

Primer 4. Svaka beskonačna Bulova algebra sadrži beskonačan antilanac, beskonačan opadajući i beskonačan rastući lanac.

Primer 5. Neka je $\mathcal{B}$ κ-kompletna Bulova algebra. Za svaku familiju $(a_\alpha : \alpha < \kappa)$ elemenata algebre $\mathcal{B}$, postoji familija $(b_\alpha \leq a_\alpha : \alpha < \kappa)$ disjunktnih elemenata takva da je $\bigvee_{\alpha<\kappa} a_\alpha = \bigvee_{\alpha<\kappa} b_\alpha$.

Za svako $\alpha < \kappa$ neka je $b_\alpha = a_\alpha \wedge (\bigvee_{\beta<\alpha} a_\beta)^*$. Po ovoj definiciji, za svako α, $b_\alpha \leq a_\alpha$. Takođe, za sve $\beta < \alpha$, $b_\alpha \wedge b_\beta = 0$ jer, $b_\beta \leq a_\beta$ i $b_\alpha \leq a_\beta^*$.

Indukcijom po $\alpha < \kappa$ dokazuje se da je $\bigvee_{\beta<\alpha} a_\beta = \bigvee_{\beta<\alpha} b_\beta$. Dakle, familije $\{a_\alpha : \alpha < \kappa\}$ i $\{b_\alpha : \alpha < \kappa\}$ imaju iste skupove gornjih ograničenja u $\mathcal{B}$, tj. važi navedena jednakost.

Napomenimo da prethodna konstrukcija ne osigurava da je $(b_\alpha : \alpha < \kappa)$ familija disjunktnih pozitivnih elemenata algebre $\mathcal{B}$. Neki od njih mogu biti jednaki nuli. Na primer, ako $\mathcal{B}$ zadovoljava uslov prebrojivih lanaca i ako je κ neprebrojiv kardinal, samo prebrojivo mnogo b_α mogu biti pozitivni. Uz neke dodatne pretpostavke prethodna konstrukcija se, u ovom smislu, ipak može popraviti.

Neka je $\mathcal{B}$ Bulova algebra. Kardinal

$$c(\mathcal{B}) = \sup\{|X| : X \text{je antilanac u } \mathcal{B}\}$$

je *celularnost* Bulove algebre $\mathcal{B}$. Celularnost elementa $x \in B$ je kardinal $c_B(x) = c(B|x)$. Celularnost algebre $\mathcal{B}$ je dostignuta ako postoji familija disjunktnih elemenata $X \subseteq B$ takva da je $|X| = c(\mathcal{B})$.

Celularnost, kao kardinalna funkcija koja se javlja u topologiji, prirodno je povezana sa celularnošću u Bulovim algebrama. Podsetimo se, celularnost $c(X)$ je supremum kardinalnosti svih familija disjunktnih nepraznih otvorenih skupova prostora X.

Primer 6. Za svaki topološki prostor X, $c(X) = c(\mathrm{RO}(X))$. Na primer, ako je X beskonačan separabilan prostor, onda $c(X) = \omega$, pa je $c(\mathrm{RO}(X)) = \omega$. Pritom, kako postoji disjunktna prebrojiva familija regularno otvorenih skupova prostora X, celularnost algebre $\mathrm{RO}(X)$ je dostignuta.

Neka je $(a_\alpha : \alpha < \kappa)$ familija pozitivnih elemenata algebre $\mathcal{B}$. Familija $(b_\alpha : \alpha < \kappa)$ elemenata je *disjunktno profinjenje* familije $(a_\alpha : \alpha < \kappa)$ ako za svako $\alpha < \kappa$, $0 < b_\alpha \leq a_\alpha$ i za sve $\beta < \alpha$, $b_\beta \wedge b_\alpha = 0$.

Teorema 6. Neka je κ beskonačan kardinal i $\mathcal{B}$ Bulova algebra takva da za svako $a \in B^+$, $\kappa^+ \leq c_B(a)$. Svaka familija $(a_\alpha : \alpha < \kappa)$ pozitivnih elemenata algebre $\mathcal{B}$ ima disjunktno profinjenje.

Dokaz: Neka je $(a_\alpha : \alpha < \kappa)$ familija pozitivnih elemenata algebre $\mathcal{B}$. Za svaku familiju disjunktnih elemenata $X \subseteq B$ i svako $a \in B$ neka je $X(a) = \{x \in X : x \wedge a > 0\}$.

Dovoljno je konstruisati familiju disjunktnih elemenata X takvu da za svako $\alpha < \kappa$, $|X(a_\alpha)| \geq \kappa$. Ako takva familija postoji, za svako $\alpha < \kappa$, izaberimo $x_\alpha \in X$ tako da

$$x_\alpha \in X(a_\alpha) - \{x_\beta : \beta < \alpha\}$$

i definišimo $b_\alpha = x_\alpha \wedge a_\alpha$.

Da bismo odredili familiju X, rekurzijom po $\alpha < \kappa$, konstruišemo rastući niz $(X_\alpha : \alpha < \kappa)$ familija disjunktnih elemenata algebre $\mathcal{B}$.

Neka je $X_0 = \emptyset$. Za svaki granični ordinal $\lambda < \kappa$, neka je $X_\lambda = \bigcup_{\alpha<\lambda} X_\alpha$. Pretpostavimo da je familija X_α konstruisana.

Ako je $|X_\alpha(a_\alpha)| = \kappa^+$, onda je $X_{\alpha+1} = X_\alpha$.

Ako je $X_\alpha(a_\alpha) = \emptyset$, onda je $X_\alpha \subseteq B|a_\alpha^*$. Prema pretpostavci teoreme, $c_B(a_\alpha) \geq \kappa^+$, pa $B|a_\alpha$ sadrži familiju disjunktnih elemenata Y kardinalnosti κ^+. Pritom, $X_\alpha \cup Y$ je familija disjunktnih elemenata u $\mathcal{B}$. Definišimo

$$X_{\alpha+1} = (X_\alpha \cup Y) - \bigcup\{Y(a_\gamma) : \gamma < \kappa \text{ i } |Y(a_\gamma)| \leq \kappa\}.$$

Familiju X definišemo tako da $X = \bigcup_{\alpha<\kappa} X_\alpha$.

Primer 7. Ako je svaki antilanac algebre $\mathcal{B}$ najviše prebrojiv, svaki dobro uređen lanac u $\mathcal{B}$ je takođe najviše prebrojiv. Uz pretpostavku da je $\mathcal{B}$ σ-algebra, važi i obratno tvrđenje.

Primer 8. U Frešeovoj algebri nad beskonačnim skupom svaki lanac je prebrojiv, ali to obavezno ne važi i za svaki antilanac.

Primer 9. Postoji intervalna algebra koja sadrži neprebrojiv lanac i u kojoj je svaki antilanac prebrojiv.

Primer 10. Familija $X = \{(a, b) : a < b \text{ i } a, b \in Q\}$ u intervalnoj algebri realnih brojeva nema disjunktno profinjenje. To znači da je pretpostavka o celularnosti elemenata Bulove algebre u prethodnoj teoremi neophodna za egzistenciju disjunktnog profinjenja.

Primer 11. Svaka beskonačna σ-kompletna Bulova algebra ima kardinalnost bar 2^ω.

Svaka beskonačna σ-kompletna Bulova algebra $\mathcal{A}$ sadrži beskonačan antilanac $\{a_n : n \in \omega\}$. Preslikavanje $f : P(\omega) \to A$ definisano tako da za svako $M \subseteq \omega$, $f(M) = \bigvee_{n\in M} a_n$ je obostrano jednoznačno.

Primer 12. Algebra $P(\omega)$ može se utopiti u svaku beskonačnu σ-kompletnu Bulovu algebru. Takvo utapanje dobija se odgovarajućom modifikacijom preslikavanja f definisanog u prethodnom dokazu.

Dekartov proizvod familije $(\mathcal{A}_i : i \in I)$ algebri je algebra $\prod_{i\in I} \mathcal{A}_i$ čiji je domen Dekartov proizvod familije skupova $\prod_{i\in I} A_i$ na kojem su operacije definisane po koordinatama, tj. za sve $a, b \in \prod_{i\in I} A_i$ i svako $i \in I$,

$$(a \vee b)_i = a_i \vee b_i,\ (a \wedge b)_i = a_i \wedge b_i \text{ i } (a^*)_i = a_i^*.$$

Za svako $i \in I$, *i-ta projekcija* $p_i : \prod_{i\in I} A_i \to A_i$ je epimorfizam takav da za svako $a = (a_i : i \in I)$, $p_i(a) = a_i$.

Ako je $\mathcal{A}_i = \mathcal{A}$, za sve $i \in I$, odgovarajući proizvod označavamo sa $\mathcal{A}^I$ i nazivamo stepenom algebre $\mathcal{A}$.

Primer 13. Za svaki skup I, algebra 2^I je izomorfna algebri $P(I)$. Pritom, izomorfizam je određen preslikavanjem f definisanim tako da za svako $a \in 2^I$, $f(a) = \{i \in I : a_i = 1\}$.

Sledeći primeri pokazuju da postoji obostrano jednoznačna korespodencija između faktorizacija kompletne Bulove algebre i particija jedinice. Pritom, u ovom slučaju, u familiji $(a_i : i \in I)$ disjunktnih elemenata Bulove algebre $\mathcal{A}$ koja čini particiju jedinice, dopuštamo i da je neki od elemenata a_i jednak nuli.

Primer 14. Neka je $(a_i : i \in I)$ particija jedinice u Bulovoj algebri $\mathcal{A}$ i $f : A \to \prod_{i\in I}(A|a_i)$ preslikavanje definisano tako da za svako $x \in A$, $f(x) = (x \wedge a_i : i \in I)$. Tada je f monomorfizam.

Za svako $i \in I$, $p_i \circ f = p_{a_i}$, gde je p_{a_i} projekcija algebre $\mathcal{A}$ na relativnu podalgebru $A|a_i$, tj. f je homomorfizam.

Ako je $x \in A$, $x \neq 0$, onda za neko $i \in I$, $x \wedge a_i \neq 0$, tj. $f(x) \neq 0$, tj. f je monomorfizam.

Primer 15. Preslikavanje f, definisano u prethodnom primeru je epimorfizam ako i samo ako za svako $(c_i : i \in I) \in \prod_{i\in I}(A|a_i)$ postoji $\bigvee^{A}_{i\in I} c_i$. Drugačije rečeno, f je epimorfizam ako i samo ako algebra $\mathcal{A}$ je $|I|^+$-kompletna.

Ako je algebra $\mathcal{A}$ dovoljno kompletna i $(c_i : i \in I) \in \prod_{i\in I}(A|a_i)$, onda postoji $x = \bigvee^{A}_{i\in I} c_i$ i pritom je $f(x) = (c_i : i \in I)$, tj. f je epimorfizam.

Primer 16. Za svaki izomorfizam $f : A \to \prod_{i\in I} A_i$, postoji particija $(a_i : i \in I)$ jedinice algebre $\mathcal{A}$ takva da, za svako $i \in I$, $A_i \cong (A|a_i)$.

Za svako $i \in I$, neka je $e^i \in \prod_{i\in I} A_i$ takvo da $p_j(e^i) = 0$, ako $i \neq j$, a $p_i(e^i) = 1$.

Familija $(e^i : i \in I)$ je particija jedinice u algebri $\prod_{i\in I} A_i$. Ako je $a_i = f^{-1}(e^i)$, za sve $i \in I$, onda je $(a_i : i \in I)$ particija jedinice u $\mathcal{A}$. Za svako $i \in I$, restrikcija funkcije f na $A|a_i$ je izomorfizam na $(\prod_{i\in I} A_i)|e^i \cong A_i$. $\square$

Sledeća teorema za σ-kompletne Bulove algebre predstavlja jednu verziju klasične Šreder-Bernštajnove teoreme.

Teorema 7. Ako je svaka od dve σ-kompletne Bulove algebre $\mathcal{A}$ i $\mathcal{B}$ izomorfna faktoru druge, algebre $\mathcal{A}$ i $\mathcal{B}$ su izomorfne.

Dokaz: Neka su $\mathcal{A}$ i $\mathcal{B}$ σ-kompletne algebre. Prema pretpostavci i prethodnim primerima, postoje $p \in A$, $q \in B$ takvi da $f : A \cong B|q$ i $g : B \cong A|p$. Da bismo dokazali da je $\mathcal{A} \cong \mathcal{B}$, dovoljno je dokazati da važi sledeći uslov:

ako su $a, b \in A$, $b \leq a$, onda $\mathcal{A}|b \cong \mathcal{A}$ implicira $\mathcal{A}|a \cong \mathcal{A}$.

Ako to dokažemo, dovoljno je uzeti da je $a = p$ i $b = g(q)$. Pritom, $b \leq a$. Kako je proizvod $g \circ f$ izomorfizam, to je $\mathcal{A} \cong \mathcal{A}|b$, pa prema gornjoj pretpostavci $\mathcal{B} \cong \mathcal{A}|a \cong \mathcal{A}$.

Neka je $\mathcal{A}$ σ-kompletna algebra, $a, b \in A$ takvi da $b \leq a$ i neka je $f : A \to A|b$ izomorfizam.

Za svako $n \in \omega$, neka su $a_n, b_n \in A$ takvi da je $a_0 = 1$, $b_0 = a$ i $a_{n+1} = f(a_n)$, $b_{n+1} = f(b_n)$. Tvrdimo da je

$$a_0 \geq b_0 \geq a_1 \geq b_1 \geq a_2 \geq \cdots$$

Da bismo to dokazali, primetimo da je $a = b_0 \leq a_0 = 1$ i da je $a_1 = f(a_0) = b \leq a = b_0$. Iz $a_n \geq b_n \geq a_{n+1}$ sledi da je $a_{n+1} \geq b_{n+1} \geq a_{n+2}$, tj. navedeni poredak zaista važi.

Zbog σ-kompletnosti postoji $\wedge_{n\in\omega} a_n = \wedge_{n\in\omega} b_n = r$, pa kako je redom $f(r) = f(\bigwedge_{n\in\omega} a_n) = \bigwedge_{n\in\omega} f(a_n) = \bigwedge_{n\in\omega} a_{n+1} = r$, to mora biti

$$\begin{aligned} 1 &= \bigvee\nolimits_{n\in\omega}(a_n \wedge b_n^*) \vee \bigvee\nolimits_{n\in\omega}(b_n \wedge a_{n+1}^*) \vee r \\ a = b_0 &= \bigvee\nolimits_{n\in\omega}(a_{n+1} \wedge b_{n+1}^*) \vee \bigvee\nolimits_{n\in\omega}(b_n \wedge a_{n+1}^*) \vee r. \end{aligned}$$

Otuda, na osnovu teoreme o faktorizaciji, dobijamo da je

$$\begin{aligned} \mathcal{A} &\cong \prod\nolimits_{n\in\omega} \mathcal{A}|(a_n \wedge b_n^*) \times \prod\nolimits_{n\in\omega} \mathcal{A}|(b_n \wedge a_{n+1}^*) \times \mathcal{A}|r \\ \mathcal{A}|a &\cong \prod\nolimits_{n\in\omega} \mathcal{A}|(a_{n+1} \wedge b_{n+1}^*) \times \prod\nolimits_{n\in\omega} \mathcal{A}|(b_n \wedge a_{n+1}^*) \times \mathcal{A}|r. \end{aligned}$$

Kako za svako $n \in \omega$, $f(a_n \wedge b_n^*) = a_{n+1} \wedge b_{n+1}^* \in A|b$ to mora biti $\mathcal{A}|(a_n \wedge b_n^*) \cong (\mathcal{A}|b)|(a_{n+1} \wedge b_{n+1}^*) = \mathcal{A}|(a_{n+1} \wedge b_{n+1}^*)$, pa konačno dobijamo da je $\mathcal{A} \cong \mathcal{A}|a$. $\square$

Primer 17. Ako se prethodna teorema primeni na algebre tipa $P(X)$ i $P(Y)$, dobija se poznata Šreder-Bernštajnova teorema.

Na osnovu opštih svojstava varijeteta, u klasi Bulovih algebri, nad svakim skupom, postoji slobodno generisana Bulova algebra. Intuitivna ideja slobodne algebre sastoji se u nekoj vrsti najopštijeg generisanja Bulove algebre tako da njeni elementi zadovoljavaju samo one zakone koji slede iz aksioma Bulovih algebri.

Bulova algebra $\mathcal{B}$ je *slobodna algebra* nad skupom $X \subseteq B$ ako za svaku funkciju $f : X \to A$ postoji jedinstven homomorfizam $g : B \to A$ koji proširuje funkciju f.

U prethodnoj definiciji, ideja slobodnog generisanja precizirana je na jedan način u kojem nije sasvim jasno vidljiva, međutim, u njegovoj osnovi, ona je ipak prisutna. Sledeća teorema rasvetljava ovu činjenicu.

Slično kao i u dokazu teoreme o proširenju homomorfizma, sa E označavamo skup $\{0,1\}^n$, $n \in \omega$. Za svako $e \in E$, ako je x element Bulove algebre, $x^{e(i)} = x$, ako je $e(i) = 1$ i $x^{e(i)} = x^*$, ako je $e(i) = 0$.

Teorema 8. Bulova algebra $\mathcal{B}$ je slobodno generisana skupom X ako i samo ako $B = \langle X \rangle$ i za svako $e \in E$ i za različite $a_1, \ldots, a_n \in X$,

$$a_1^{e(1)} \wedge \cdots \wedge a_n^{e(n)} \neq 0.$$

Dokaz: Pretpostavimo da su $a_1, \ldots, a_n \in X$ različiti i $e \in E$. Nad jediničnim intervalom $I = [0,1]$ realnih brojeva, neka je F polje podskupova stepena I^n, $n \geq 1$, generisano skupovima oblika

$$A_i = \{(x_1, \ldots, x_n) : \tfrac{1}{2} \leq x_i \leq 1\}.$$

Neka je g preslikavanje takvo da $g(a_i) = A_i$. Algebra $\mathcal{B}$ je slobodna algebra nad X, pa postoji homomorfizam $h : B \to F$ koji proširuje g.

Kako je $(e(1), \ldots, e(n)) \in A_1^{e(1)} \cap \cdots \cap A_n^{e(n)}$, skup $A_1^{e(1)} \cap \cdots \cap A_n^{e(n)}$ nije prazan. Sa duge strane,

$$h(a_1^{e(1)} \wedge \cdots \wedge a_n^{e(n)}) = A_1^{e(1)} \cap \cdots \cap A_n^{e(n)} \neq \emptyset,$$

što znači da je $a_1^{e(1)} \wedge \cdots \wedge a_n^{e(n)} \neq 0$.

Obratno, ako je $\mathcal{B}$ algebra generisana skupom X u kojoj za proizvoljne različite $a_1, \ldots, a_n \in X$ i svako $e \in E$ $a_1^{e(1)} \wedge \cdots \wedge a_n^{e(n)} \neq 0$, onda se, na osnovu teoreme o proširenju homomorfizma, svako preslikavanje $f : X \to A$ može proširiti do homomorfizma $g : B \to A$. Budući da je $X \subseteq B$ generatorni skup, homomorfizam h je jedinstveno određen. $\square$

Slobodnu algebru nad skupom X označavamo sa $\mathcal{F}(X)$.

Skup $X \subseteq B$ je *nezavisan* u algebri $\mathcal{B}$ ako za svako $e \in E$ i različite $a_1, \ldots a_n \in X$, $a_1^{e(1)} \wedge \cdots \wedge a_n^{e(n)} \neq 0$.

Teorema 9. Ako su skupovi X i Y jednake kardinalnosti, slobodne algebre $\mathcal{F}(X)$ i $\mathcal{F}(Y)$ izomorfne.

Dokaz: Ako je $i : X \to Y$ bijekcija, preslikavanje $i : X \to F(Y)$ ima jedinstveno proširenje do homomorfizma $f : F(X) \to F(Y)$. Na isti način, preslikavanje $i^{-1} : Y \to F(X)$ ima jedinstveno proširenje do homomorfizma

$g : F(Y) \to F(X)$. Restrikcija homomorfizma $g \circ f$ na skup X jednaka je 1_X, tj. identičkom preslikavanju skupa X. Kako 1_X ima tačno jedno proširenje do homomorfizma algebre $\mathcal{F}(X)$, to je $g \circ f = 1_{F(X)}$, tj. algebre $\mathcal{F}(X)$ i $\mathcal{F}(Y)$ su izomorfne. $\Box$

Već je u ranijim primerima naglašena bliska veza između Bulovih algebri i topoloških prostora. Za razliku od univerzalno-algebarske konstrukcije, koja je tehnički prilično komplikovana, ova veza omogućava relativno jednostavnu konstrukciju slobodnih Bulovih algebri nad skupom slobodnih generatora proizvoljne kardinalnosti.

Teorema 10. Nad svakim skupom postoji slobodna Bulova algebra.

Dokaz: Pretpostavimo da je $\mathcal{F}$ algebra zatvoreno otvorenih skupova Kantorovog prostora 2^I.

Za svako $i \in I$, skup $u_i = \{x \in 2^I : x(i) = 1\}$ je zatvoreno otvoren skup prostora 2^I. Tvrdimo da je algebra $\mathcal{F}$ slobodno generisana skupom $X = \{u_i : i \in I\}$.

Neka su $i_1, \dots, i_n \in I$ različiti. Za svako $x \in 2^I$, $x \in u_{i_1}^{x(i_1)} \cap \dots \cap u_{i_n}^{x(i_n)}$. To znači da je $u_{i_1}^{x(i_1)} \cap \dots \cap u_{i_n}^{x(i_n)} \neq \emptyset$, tj. X je nezavisan skup.

Ako je $\mathcal{B}$ Bulova algebra generisana sa X, onda $\mathcal{B}$ sadrži predbazu prostora 2^I koju čine zatvoreno otvoreni skupovi $\{u_i : i \in I\} \cup \{u_i^c : i \in I\}$, pa mora biti $B \subseteq F$. Zbog kompaktnosti, svaki zatvoreno otvoren skup prostora 2^I je konačna unija baznih skupova, pa mora biti $F \subseteq B$. $\Box$

Primer 18. Ako je B_n slobodna Bulova algebra generisana sa $n \in \omega$ slobodnih generatora, onda je $B_n \cong 2^{2^n}$.

U Bulovoj algebri $\mathcal{B}$ element $x \in B$ je *atom* ako $0 < x$ i za svako $y \in B$, ako je $y \leq x$, onda $y = 0$ ili $y = x$.

Bulova algebra $\mathcal{B}$ je *atomična* ako za svako $y \in B$ postoji atom $x \in B$ takav da je $x \leq y$. Algebra $\mathcal{B}$ je bezatomična ako u $\mathcal{B}$ nema atoma.

Primer 19. Sve Bulove algebre oblika $P(X)$ su atomične.

Primer 20. Frešeova i sve konačne Bulove algebre su atomične.

Primer 21. Ako je $\mathcal{P}$ gusto linearno uređenje, algebra $\mathrm{RO}(P)$ je kompletna bezatomična Bulova algebra.

Primer 22. Algebra $\mathrm{L}(\mathcal{P})$ nad gustim uređenjem $\mathcal{P}$ je bezatomična.

Primer 23. Količnik algebre merljivih skupova realnih brojeva po idealu skupova mere nula je bezatomična Bulova algebra.

Primer 24. Ako je $\mathcal{P}$ linearno uređenje tipa $\omega + \eta$, gde je η tip uređenja racionalnih brojeva, intervalna algebra L($\mathcal{P}$) nije ni atomična ni bezatomična.

Primer 25. Proizvod atomične i bezatomične Bulove algebre nije ni atomična ni bezatomična algebra.

Primer 26. Ako je $\mathcal{B}$ Bulova algebra i $a \in B$, sledeći uslovi su ekvivalentni:

(a) a je atom u $\mathcal{B}$

(b) za svako $x \in B$, $a \leq x$ ili $a \leq x^*$, ali ne oba,

(c) $0 < a$ i za sve $x, y \in B$, $a \leq x \vee y$ ako i samo ako $a \leq x$ ili $a \leq y$.

Primer 27. Neka je $A \subseteq B$ skup svih atoma algebre $\mathcal{B}$ i $h : B \to P(A)$ preslikavanje takvo da za svako $x \in B$, $h(x) = \{a \in A : a \leq x\}$. Preslikavanje h je homomorfizam. Ako je $\mathcal{B}$ atomična algebra, h je monomorfizam, a ako je $\mathcal{B}$ kompletna algebra, h je epimorfizam.

Primer 28. Beskonačna slobodna Bulova algebra je bezatomična.

Funkcija $\mu : B \to [0, 1]$ je *pozitivna mera* na Bulovoj algebri $\mathcal{B}$ ako za sve $x, y \in B$,

$$\begin{aligned}
&\mu(x) = 0 \Leftrightarrow x = 0,\\
&\mu(1) = 1,\\
&x \wedge y = 0 \Rightarrow \mu(x \vee y) = \mu(x) + \mu(y).
\end{aligned}$$

Primer 29. Ako na Bulovoj algebri $\mathcal{B}$ postoji pozitivna mera, svaki antilanac u $\mathcal{B}$ je najviše prebrojiv.

Primer 30. Slobodna algebra dopušta pozitivnu meru.

Neka je $\mathcal{B}$ slobodna algebra nad skupom slobodnih generatora $X \subseteq B$. Neka je $Y \subseteq X$ i $x \in X - Y$. Označimo sa $\mathcal{A}$ podalgebru generisanu sa Y, a sa $\mathcal{C}$ podalgebru generisanu sa $A \cup \{x\}$. Svako $y \in C$ je oblika $y = (a \wedge x) \vee (b \wedge x^*)$, za neke $a, b \in A$.

Ako je μ pozitivna mera na $\mathcal{A}$ i $0 < r < 1$, neka je μ' realna funkcija na C takva da za svako $y \in C$, $\mu'(y) = r \cdot \mu(a) + (1 - r) \cdot \mu(b)$, gde je $y = (a \wedge x) \vee (b \wedge x^*)$, za neke $a, b \in A$.

Neposredno se proverava da je μ' pozitivna mera na $\mathcal{C}$ koja proširuje meru μ. Neka je P skup svih pozitivnih mera na podalgebrama Bulove algebre $\mathcal{B}$ koje su generisane podskupovima skupa X. S obzirom na inkluziju, P je parcijalno uređenje. Za svaki lanac $L \subseteq P$, $\bigcup L$ je gornje ograničenje za L. Prema Zornovoj lemi, lanac L sadrži maksimalan element μ. Tvrdimo da je μ pozitivna mera na $\mathcal{B}$.

Neka je A domen mere μ. Ako je $\mathcal{A}$ prava podalgebra algebre $\mathcal{B}$, prema prethodnoj konstrukciji, za neko $x \in B - A$ postoji proširenje mere μ na algebru generisanu skupom $A \cup \{x\}$, tj. μ nije maksimalan element u parcijalnom uređenju $\mathcal{P}$. $\Box$

Primer 31. Svaki lanac (antilanac) slobodne algebre je prebrojiv.

Osim uslova prebrojivosti antilanaca i bezatomičnosti u beskonačnom slučaju, slobodne Bulove algebre imaju i druga zanimljiva svojstva. Zaključujući izlaganje o slobodnim algebrama, lustrovaćemo prirodu njihove grupe automorfizama.

Bulova algebra $\mathcal{B}$ je *homogena* ako za svako $b \in B$, $b \neq 0$, relativna algebra $B|b$ je izomorfna sa $\mathcal{B}$.

Osim algebre 2, u kojoj se uslov homogenosti trivijalizuje, sve konačne Bulove algebre nisu homogene.

Teorema 11. Bulova algebra $\mathcal{B}$, $\mathcal{B} \neq 2^2$, je homogena ako i samo ako za sve $a, b \in B$, $0 < a, b < 1$, postoji automorfizam h algebre $\mathcal{B}$ takav da je $h(a) = b$.

Dokaz: Neka su $a, b \in B$, $0 < a, b < 1$. Zbog homogenosti algebre $\mathcal{B}$ postoje izomorfizmi $f : B|a \to B|b$ i $g : B|a^* \to B|b^*$. Preslikavanje $h : B \to B$ takvo da za svako $x \in B$, $h(x) = f(x \wedge a) \vee g(x \wedge a^*)$ je automorfizam koji a preslikava u b.

Obratno, pretpostavimo da je uslov teoreme zadovoljen. Dakle za sve $a, b \in B$, takve da $0 < a, b < 1$, imamo da je $B|a \cong B|b$. Treba dokazati da je $B|b \cong B$. Ne umanjujući opštost, možemo pretpostaviti da je $|B| \geq 8$. To znači da postoje disjunktni $x, y \in B^+$ takvi da je $a = x \vee y < 1$. Svi x, y, a i a^* su pozitivni i manji od 1, pa redom imamo

$$B|b \cong B|a \cong (B|x \times B|y) \cong (B|a \times B|a^*) \cong B. \ \Box$$

Primer 32. Svaka beskonačna slobodna algebra je homogena.

Teorema reprezentacije

Svaka funkcija $f : A \to B$ na skupu A određuje ekvivalenciju $\sim$ takvu da, za sve $x, y \in A$, $x \sim y$ ako i samo ako $f(x) = f(y)$. Ako je na skupovima A i B definisana algebarska struktura i f homomorfizam, relacija $\sim$ je saglasna u odnosu na takvu strukturu i naziva se jezgrom homomorfizma f. Dakle, svaki homomorfizam strukture $\mathcal{A}$ određuje kongruenciju u $\mathcal{A}$.

Obratno, ako je $\sim$ kongruencija strukture $\mathcal{A}$, na količničkom skupu $A_{/\sim}$ određena je struktura tipa algebre $\mathcal{A}$ i prirodni homomorfizam $h : A \to A_{/\sim}$ čije je jezgro upravo relacija $\sim$.

U slučaju Bulovih algebri, svaka kongruencija određena je klasom ekvivalencije najvećeg elementa, odnosno, filtrom Bulove algebre. Univerzalno-algebarska obostrano jednoznačna korespondencija između epimorfizama i kongruencija, u Bulovim algebrama svodi se na takvu korespodenciju između filtera i homomorfizama ovih struktura.

Neprazan skup $F \subseteq B$ je *filter* Bulove algebre $\mathcal{B}$ ako za sve $x, y \in B$,

(a) $x \in F$ i $x \leq y$ implicira $y \in F$,

(b) $x \in F$ i $y \in F$ implicira $x \wedge y \in F$.

Dualno, neprazan skup $I \subseteq B$ je *ideal* u Bulovoj algebri $\mathcal{B}$ ako za sve $x, y \in B$, $x \in I$ i $y \in B$, $y \leq x$ implicira $y \in I$ i $x, y \in I$ implicira $x \vee y \in I$.

U definiciji filtra, uslovi (a) i (b) se mogu zameniti sledećim uslovima: $1 \in F$ i za sve $x, y \in B$, $x \wedge y \in F$ ako i samo ako $x \in F$ i $y \in F$.

Dualizacijom ove definicije dobija se slična definicija ideala: $0 \in I$ i za sve $x, y \in B$, $x \vee y \in I$ ako i samo ako $x \in I$ i $y \in I$.

Ako je $a \in B$, skup $F = \{x \in B : a \leq x\}$ je filter algebre $\mathcal{B}$. Ako je $a = 1$, skup F svodi se na jednočlan skup $\{1\}$, a ako je $a = 0$, na domen B algebre $\mathcal{B}$.

Filter $F \subseteq B$ algebre $\mathcal{B}$ je *glavni* filter ako postoji element $a \in B$ za koji je $F = \{x \in B : a \leq x\}$.

Filter F je *trivijalan* filter ako $F = \{1\}$, a *pravi* filter ako $0 \notin F$, tj. ako je $F \neq B$. Ubuduće, pod terminom filter, podrazumevamo pravi filter. Dakle, svaki filter zadovoljava uslov $0 \notin F$.

Skup $E \subseteq B$ ima *svojstvo konačnih preseka* ako za svako $n \in \omega$ i proizvoljne $a_1, \ldots, a_n \in E$, $a_1 \wedge \cdots \wedge a_n \neq 0$.

Teorema 12. Skup $X \subseteq B$ može se proširiti do filtra ako i samo ako X ima svojstvo konačnih preseka.

Dokaz: Ako postoji filter koji sadrži X, po definiciji filtra, X ima svojstvo konačnih preseka. Obratno, neka X zadovoljava svojstvo konačnih preseka. Ako je $X = \emptyset$, neka je $F = \{1\}$. Ako je $X \neq \emptyset$, neka je

$$F = \{y \in B : \text{ za neke } x_1, \ldots, x_n \in X,\, x_1 \wedge \cdots \wedge x_n \leq y\}.$$

Uslov (a) definicije filtra je trivijalno zadovoljen. Ako su $x, y \in F$, onda za neke $x_1, \ldots, x_n, y_1, \ldots, y_m \in X$, $x_1 \wedge \cdots \wedge x_n \leq x$ i $y_1 \wedge \cdots \wedge y_m \leq y$, pa mora biti $x_1 \wedge \cdots \wedge x_n \wedge y_1 \wedge \cdots \wedge y_m \leq x \wedge y$, tj. $x \wedge y \in F$. Kako X ima svojstvo konačnih preseka to $0 \notin F$, tj. F je filter algebre $\mathcal{B}$. □

Filter F u dokazu prethodne teoreme je *filter generisan skupom* $X \subseteq B$. Naime, F je najmanji filter u $\mathcal{B}$ koji sadrži X, odnosno, F je presek svih filtera algebre $\mathcal{B}$ koji sadrže skup X.

Primer 1. (a) Neka je $h : B \to A$ homomorfizam Bulovih algebri. Skup $h^{-1}[1] = \{x \in B : h(x) = 1\}$ je filter algebre $\mathcal{B}$.

(b) Ako je F filter u $\mathcal{B}$, postoji homomorfizam algebre $\mathcal{B}$ čije je jezgro upravo filter F.

Tvrđenje (a) se neposredno proverava. Detaljno ćemo izložiti dokaz tvrđenja (b). Pretpostavimo da je F filter u algebri $\mathcal{B}$. Definišimo relaciju $\sim_F$ tako da za sve $x, y \in B$,

$$\begin{aligned} x \sim_F y \quad &\Leftrightarrow \quad \text{postoji } z \in F, x \wedge z = y \wedge z, \\ &\Leftrightarrow \quad (x \vee y^*) \wedge (x^* \vee y) \in F. \end{aligned}$$

Jednostavno se proverava da je relacija $\sim_F$ relacija ekvivalencije u B.

Relacija $\sim_F$ je *kongruencija* algebre $\mathcal{B}$, tj. za sve $x, y, x^{'}, y^{'} \in B$, ako $x \sim_F y$ i $x^{'} \sim_F y^{'}$, onda

$$x \vee x^{'} \sim_F y \vee y^{'},\, x \wedge x^{'} \sim_F y \wedge y^{'} \text{ i } x^* \sim_F y^*.$$

Saglasnost relacije $\sim_F$ sa operacijama $\vee$ i $\wedge$ se jednostavno proverava. Dokazaćemo njenu saglasnost sa komplementacijom. Neka je $x \sim_F y$. Po definiciji to znači da postoji $z \in F$ takvo da važi $x \wedge z = y \wedge z$.

Otuda je $z = z \wedge (x \vee x^*) = (z \wedge x) \vee (z \wedge x^*) = (z \wedge y) \vee (z \wedge x^*)$, pa dakle $y^* \wedge z = y^* \wedge ((z \wedge y) \vee (z \wedge x^*)) = (y^* \wedge x^*) \wedge z$. Na isti način dobija se i da je $x^* \wedge z = (y^* \wedge x^*) \wedge z$, što znači da postoji $z \in F$ takvo da je $x^* \wedge z = y^* \wedge z$, tj. da je $x^* \sim_F y^*$.

Za proizvoljno $x \in B$ neka je $|x| = \{y \in B : x \sim_F y\}$ klasa ekvivalencije elementa x i $B_{/F} = \{|x| : x \in B\}$ količnički skup s obzirom na relaciju $\sim_F$.

Saglasnost operacija Bulove algebre $\mathcal{B}$ sa relacijom $\sim_F$ omogućava da na količničkom skupu $B_{/F}$ definišemo strukturu Bulove algerbe.

Za sve $x, y \in B$, $|x| \vee |y| = |x \vee y|$, $|x| \wedge |y| = |x \wedge y|$ i $|x|^* = |x^*|$. Pritom, za svako $x \in B$, $|x| = 1$ ako i samo ako $x \in F$ i $|x| = 0$ ako i samo ako $x^* \in F$, tj. u algebri $B_{/F}$, $1 = F$ i $0 = F^* = \{x \in B : x^* \in F\}$.

S obzirom na tako definisane operacije, $\mathcal{B}_{/F}$ je količnik algebre $\mathcal{B}$ po filtru F. Preslikavanje $h : B \to B_{/F}$ takvo da za svako $x \in B$, $h(x) = |x|$ je kanonski homomorfizam algebre $\mathcal{B}$ na $\mathcal{B}_{/F}$, što znači da je filter F je jezgro homomorfizma h. □

Filter $F \subseteq B$ algebre $\mathcal{B}$ je *maksimalan* ako $F \subseteq G$ implicira $F = G$, za svaki pravi filter G algebre $\mathcal{B}$.

Ako za sve $x, y \in B$, $x \vee y \in F$ implicira $x \in F$ ili $y \in F$, filter F je *prost* filter algebre $\mathcal{B}$

Filter F je *ultrafilter* ako za svako $x \in B$, $x \in F$ ili $x^* \in F$.

U Bulovim algebrama pojmovi maksimalnog filtra, prostog filtra i ultrafiltra se ne razlikuju. Kao jezgra homomorfizama, takvi filtri određuju homomorfizme Bulove algebre na algebru 2.

Primer 2. Ako je F filter Bulove algebre $\mathcal{B}$, onda

$$\begin{aligned} \mathcal{B}_{/F} \cong 2 &\Leftrightarrow F \text{ je maksimalan filter algebre } \mathcal{B}, \\ &\Leftrightarrow F \text{ je prost filter u } \mathcal{B}, \\ &\Leftrightarrow F \text{ je ultrafilter algebre } \mathcal{B}. \end{aligned}$$

Pretpostavimo da je $\mathcal{B}_{/F} \cong 2$. Ako je $F \subseteq G$ i G pravi filter algebre $\mathcal{B}$, za svako $x \in G$, $x^* \notin F$. U suprotnom, $x, x^* \in G$, pa G ne bi bio pravi filter. To znači da $|x^*| \neq 1$, pa po pretpostavci, $|x^*| = 0$, odnosno, $|x| = 1$, a to znači da je $x \in F$. Dakle, $G \subseteq F$. tj. F je maksimalan filter u $\mathcal{B}$.

Neka je F maksimalan filter, $x \vee y \in F$ i $x \notin F$. Ako je G filter generisan sa $F \cup \{x\}$, po pretpostavci, G nije pravi filter, pa postoji $z \in X$ takvo da $z \wedge x = 0$. Kako $z \in F$ i $x \vee y \in F$, mora biti $z \wedge (x \vee y) = z \wedge y \in F$, pa dakle $y \in F$.

Ako je F prost filter, za svako $x \in B$, $x \vee x^* \in F$, pa dakle $x \in F$ ili $x^* \in F$, tj. F je ultrafilter.

Konačno, ako je F ultrafilter, neka je $|x| \in B_{/F}$ takvo da $|x| \neq 0$. Otuda sledi da $x \notin F$, pa kako je F ultrafilter, $x^* \in F$. To znači da je $|x^*| = |x|^* = 1$, odnosno, $|x| = 0$. Dakle, $\mathcal{B}_{/F} \cong 2$.

U principu, nije jasno da li svaka Bulova algebra sadrži ultrafilter, odnosno, da li svaka Bulova algebra ima homomorfizam na algebru 2. Sledeća teorema pokazuje da svaka Bulova algebra sadrži dovoljno bogatu klasu ultrafiltera. Za bilo koja dva različita elementa Bulove algebre postoji ultrafilter koji sadrži tačno jedan od tih elemenata.

Teorema 13. Teorema o ultrafiltru: Svaki filter Bulove algebre može se proširiti do ultrafiltra.

Dokaz: Neka je F filter algebre $\mathcal{B}$ i neka je P familija svih filtera u $\mathcal{B}$ koji sadrže filter F. Struktura $\mathcal{P} = (P, \subseteq)$ je parcijalno uređenje. Ako je L lanac u uređenju $\mathcal{P}$, tvrdimo da je $C = \bigcup L$ filter algebre $\mathcal{B}$ koji sadrži F.

Za proizvoljne $x, y \in B$, ako $x, y \in C$, postoje $G_1, G_2 \in L$ takvi da $x \in G_1$ i $y \in G_2$. Kako je L lanac to mora biti $G_1 \subseteq G_2$ ili $G_2 \subseteq G_1$.

Pretpostavimo da je $G_1 \subseteq G_2$. Tada $x, y \in G_2$, pa kako je G_2 filter u $\mathcal{B}$, mora biti $x \wedge y \in G_2$, tj. $x \wedge y \in C$.

Ako je $x \in C$ i $y \in B$ takvo da $x \leq y$, onda postoji $G \in L$ takvo da $x \in G$. Kako je G filter u $\mathcal{B}$, mora biti $y \in G$, tj. $y \in C$.

Za svako $G \in L$, $0 \notin G$, pa $0 \notin C$, tj. C je filter algebre $\mathcal{B}$. Po definiciji uređenja $\mathcal{P}$, $F \subseteq C$.

Kako svaki lanac u parcijalnom uređenju $\mathcal{P}$ ima gornje ograničenje, prema Zornovoj lemi, $\mathcal{P}$ sadrži maksimalan element G. Dakle, G je ultrafilter u $\mathcal{B}$ koji proširuje dati filter F. □

Teorema o ultrafiltru je posledica aksiome izbora, odnosno, Zornove leme kao jedne od njenih varijanti. Iako obratno ne važi, teorema o ultrafiltru je sasvim bliska principu izbora. U većini teorema koje se dokazuju na osnovu aksiome izbora, ova pretpostavka može se zameniti teoremom o ultrafiltru.

Kako se svaki skup elemenata Bulove algebre, koji zadovoljava svojstvo konačnih preseka, može proširiti do filtra, prema teoremi o ultrafiltru, svaki takav skup može se proširiti do ultrafiltra. U većini dokaza mi ćemo se pozivati na ovu činjenicu kao na teoremu o ultrafiltru.

Iz prethodne napomene neposredno sledi da je svaki pozitivan element Bulove algebre sadržan u nekom ultrafiltru. Više od toga, ako su $x, y \in B$ različiti elementi Bulove algebre $\mathcal{B}$, onda postoji ultrafilter koji ih razdvaja. Jer, ako $x \neq y$, onda $x \wedge y^* \neq 0$ ili $x^* \wedge y \neq 0$, pa bar jedan od skupova $\{x, y^*\}$ ili $\{x^*, y\}$ ima svojstvo konačnih preseka, tj. može se proširiti do ultrafiltra.

Primer 3. Ako je X proizvoljan skup, filter u Bulovoj algebri $P(X)$ nazivamo *filtrom nad skupom* X. Ako je F ultrafilter nad X, F je glavni ultrafilter ako i samo ako F sadrži konačan podskup od X ako i samo ako F je generisan jednočlanim skupom $\{x\}$, $x \in X$.

Primer 4. Ako je $|X| \geq \omega$, postoji neglavni ultrafilter nad X.

Primer 5. Ako je F ultrafilter nad X i $x_1, \ldots, x_n \subseteq X$ particija nekog elementa filtra F, tačno jedan od elemenata x_i pripada filtru F. Ova činjenica može se formulisati i važi u proizvoljnoj Bulovoj algebri.

Ultrafilter F nad X je *uniforman* ako za svako $Y \in F$, $|Y| = |X|$.

Primer 6. Ako je X beskonačan skup, postoji uniforman ultrafilter nad X. Nad prebrojivim skupom, svaki uniforman ultrafilter je neglavni i obratno, svaki neglavni ultrafilter je uniforman.

Ultrafilter F algebre $\mathcal{B}$ je *prebrojivo nekompletan* ako postoji prebrojiva familija $\{x_n : n \in \omega\} \subseteq F$ takva da $\bigcap_{n \in \omega} x_n \notin F$.

Primer 7. Ako je F prebrojivo nekompletan ultrafilter algebre $\mathcal{B}$, postoji lanac $x_0 \geq x_1 \geq \cdots$ takav da za svako $n \in \omega$, $x_n \in F$ i $\bigcap_{n\in\omega} x_n = \emptyset \notin F$.

Svaki neglavni ultrafilter nad ω je prebrojivo nekompletan.

Neka je x tačka topološkog prostora X i F_x familija okolina tačke x. Za svako $x \in X$, familija F_x je filter nad X. Filter F *konvergira* tački $x \in X$ ako $F_x \subseteq F$.

Primer 8. (a) Prostor X je Hauzdorfov ako i samo ako svaki ultrafilter nad X konvergira najviše jednoj tački prostora X.

(b) Prostor X je kompaktan ako i samo ako svaki ultrafilter nad X konvergira bar jednoj tački prostora X.

U nekim ključnim rezultatima matematičke logike, a takođe i u Bulovim algebrama i topološkim prostorima, osnovna varijanta teoreme o ultrafiltru nije neposredno primenljiva. Pojednostavljeno rečeno, u takvim rezultatima, potrebno je konstruisati ultrafiltre koji se regularno ponašaju u odnosu na supremume i infimume koji eventualno postoje u određenoj Bulovoj algebri.

Neka je $h : B \to A$ homomorfizam i $M \subseteq B$ takav da postoji supremum $\bigvee^B M$. Homomorfizam h je *kompletan za supremum* $\bigvee^B M$ ako u algebri $\mathcal{A}$ postoji $\bigvee^A h[M]$ i $h(\bigvee^B M) = \bigvee^A h[M]$.

Neka je F ultrafilter algebre $\mathcal{B}$ i $M \subseteq B$ takav da supremum $\bigvee M$ postoji u algebri $\mathcal{B}$. Ultrafilter F je *kompletan za supremum* $\bigvee M$ ako

$$\bigvee M \in F \quad \Leftrightarrow \quad \exists x \in M, x \in F.$$

Ultrafilter F je kompletan za supremum $\bigvee M$ ako i samo ako je kanonski homomorfizam $h_F : B \to 2$ kompletan za $\bigvee M$. Razumljivo, pojmovi kompletnog homomorfizma i kompletnog ultrafiltra za dati infimum, definišu se dualno.

Neka je S familija podskupova Bulove algebre $\mathcal{B}$ čiji svaki element ima supremum u $\mathcal{B}$. Ultrafilter F je *kompletan* za S ako za svako $M \in S$, ultrafilter F je kompletan za $\bigvee M$. Slično, homomorfizam $h : B \to A$ je kompletan za familiju S ako za svako $M \in S$, $h(\bigvee^B M) = \bigvee^A h[M]$.

Nije uopšte jasno da li za svaku familiju supremuma S algebre $\mathcal{B}$ postoji ultrafilter u $\mathcal{B}$ koji je kompletan za S.

Teorema 14. Postoji obostrano jednoznačna korespodencija između atoma kompletne algebre $\mathcal{B}$ i ultrafiltera kompletnih za familiju $P(B)$.

Dokaz: Za svaki atom $a \in B$ neka je F_a filter generisan sa a. Tvrdimo da je F_a ultrafilter kompletan za familiju $P(B)$.

Neka je G filter u $\mathcal{B}$ takav da $F_a \subseteq G$ i $x \in G - F_a$, $x \neq 0$. Tada $a \nleq x$, tj. $a \wedge x^* \neq 0$ i $a \wedge x^* < a$, što je u suprotnosti sa pretpostavkom da je $a \in B$ atom. Dakle, F_a je ultrafilter u $\mathcal{B}$.

Neka je $M \subseteq B$ takav da $\bigvee M \in F_a$, onda $a \leq \bigvee M$. Ako za sve $x \in M$, $x \notin F_a$, onda za sve $x \in M$, $a \nleq x$, pa dakle $a \wedge x^* \neq 0$. Kako je $a \in B$ atom algebre $\mathcal{B}$, za svako $x \in M$, $a \leq x^*$.

Otuda je $a \leq \bigwedge_{x \in M} x^* = (\bigvee_{x \in M} x)^*$, tj. $(\bigvee M)^* \in F_a$, što nije moguće, budući da je F_a ultrafilter.

Obratno, ako je ultrafilter F kompletan za $P(B)$, kako je $\mathcal{B}$ kompletna algebra, postoji $\bigwedge F$ u $\mathcal{B}$. Neka je $a = \bigwedge F$ i $F^* = \{x^* : x \in F\}$.

Zbog De Morganovih zakona, $a^* = \bigvee F^*$. Ultrafilter F je kompletan za $P(B)$ i $F \cap F^* = \emptyset$, pa mora biti $a^* \notin F$, tj. $a \in F$. Dakle, $a \in B$ generiše ultrafilter F. Jasno, a je atom algebre $\mathcal{B}$, jer u suprotnom, ultrafilter F bi imao netrivijalno proširenje.

Dakle, preslikavanje $a \mapsto F_a$ određuje obostrano jednoznačnu korespodenciju atoma kompletne algebre $\mathcal{B}$ i ultrafiltera kompletnih za familiju supremuma $P(B)$. $\Box$

Ako je $\mathcal{B}$ kompletna bezatomična Bulova algebra, na primer, algebra regularno otvorenih skupova intervala $[0,1]$, na osnovu prethodne teoreme, u algebri $\mathcal{B}$ ne postoji ultrafilter kompletan za familiju $P(B)$. Svaka kompletna bezatomična algebra $\mathcal{B}$ je beskonačna, pa je familija $P(B)$ neprebrojiva. Dakle, u opštem slučaju, nije jasno da li postoji ultrafilter kompletan za datu familija supremuma. Međutim, ukoliko je familija supremuma prebrojiva, konstrukcija takvog ultrafiltra je moguća.

Teorema 15. Neka je $M = \{M_n \subseteq B : n \in \omega\}$ familija podskupova algebre $\mathcal{B}$ takva da svaki M_n ima supremum. Za svako $x \in B$, $x \neq 0$, postoji M-kompletan ultrafilter F algebre $\mathcal{B}$ takav da $x \in F$.

Dokaz: Za svako $n \in \omega$ neka je $a_n = \bigvee M_n$. Indukcijom po $n \in \omega$, definisaćemo niz $(b_n \in M_n : n \in \omega)$ takav da skup $S = \{x, a_n^* \vee b_n : n \in \omega\}$ ima svojstvo konačnih preseka.

Ako takav niz postoji, ultrafilter F koji proširuje S je M-kompletan.

Za svako $n \in \omega$, ako $a_n \in F$, budući da po konstrukciji $a_n^* \vee b_n \in F$, mora biti $b_n = a_n \wedge b_n = a_n \wedge (a_n^* \vee b_n) \in F$. Kako je $b_n \in M_n$, filter F je kompletan za familiju M i naravno $x \in F$.

Ostaje da konstruišemo niz $(b_n \in M_n : n \in \omega)$. Neka je $n \in \omega$. Pretpostavimo da je za sve $m < n$ konstruisan član niza $b_m \in M_m$ takav da skup $\{a_0^* \vee b_0, \ldots, a_m^* \vee b_m\}$ ima infimum različit od nule. Neka je

$$y_n = \begin{cases} x & \text{ako } n = 0, \\ x \wedge (a_0^* \vee b_0) \wedge \cdots \wedge (a_{n-1}^* \vee b_{n-1}) & \text{ako } n > 0. \end{cases}$$

Po definiciji, $y_n \neq 0$ jer, ako je $n = 0$, onda $y_0 = x \neq 0$, a ako je $n > 0$, po induktivnoj pretpostavci $y_n \neq 0$. Pretpostavimo da za svako $b \in M_n$, $y_n \wedge (a_n^* \vee b) = 0$. To bi značilo da je

$$(y_n \wedge a_n^*) \vee (y_n \wedge b) = 0.$$

Dakle, $y_n \wedge a_n^* = 0$ i za sve $b \in M_n$, $y_n \wedge b = 0$. Zbog $y_n \wedge b = 0$, za sve $b \in M_n$, $y_n \leq b^*$, pa dakle

$$y_n \leq \bigwedge\{b^* : b \in M_n\} = (\bigvee M_n)^* = a_n^*.$$

Konačno, zbog $y_n \wedge a_n^* = 0$, to bi značilo da je $y_n = 0$, što protivreči definiciji elementa y, odnosno, induktivnoj pretpostavci. $\square$

Svojstva osnovnih operacija Bulove algebre su veoma bliska svojstvima iskaznih veznika; konjunkciji, disjunkciji i negaciji. Zahvaljujući toj činjenici, u poglavlju iz teorije modela pokazaćemo da se stav potpunosti iskaznog računa može jednostavno dokazati na osnovu teoreme o ultrafiltru. Sa druge strane, kvantifikatori se u Bulovoj algebri izražavaju supremumima i infimumima tako da je u dokazu stava potpunosti predikatskog računa neophodna prethodna teorema.

Pretpostavka prebrojivosti familije supremuma S dovoljna je za egzistenciju S-kompletnog ultrafiltra algebre $\mathcal{B}$, ali pitanje da li se pretpostavka o prebrojivosti može oslabiti, nema potpun odgovor.

Najznačajniji rezultat u teoriji Bulovih algebri je Stonova *teorema reprezentacije*. U strukturnoj teoriji, ona u potpunosti karakteriše Bulove algebre. Takođe, kako se u njenom dokazu uspostavlja sasvim bliska veza sa topologijom, Stonova teorema omogućava da se dobar deo kombinatorne teorije Bulovih algebri topološki interpretira.

Teorema 16. Svaka Bulova algebra izomorfna je algebri skupova.

Dokaz: Za proizvoljnu Bulovu algebru $\mathcal{B}$ neka je SB skup svih ultrafiltera u $\mathcal{B}$. Za svako $x \in B$, neka je

$$s(x) = \{F \in SB : x \in F\}.$$

Tako definisano preslikavanje $s : B \to P(SB)$ je monomorfizam Bulovih algebri. Preslikavanje s je homomorfizam jer, za sve $x, y \in B$ i svaki ultrafilter $F \in SB$,

$$\begin{aligned} F \in s(x \wedge y) &\Leftrightarrow x \wedge y \in F, \\ &\Leftrightarrow x \in F \text{ i } y \in F, \\ &\Leftrightarrow F \in s(x) \cap s(y), \end{aligned}$$

pa dakle $s(x \wedge y) = s(x) \cap s(y)$. U slučaju komplementa,

$$\begin{aligned} F \in s(x^*) &\Leftrightarrow x^* \in F, \\ &\Leftrightarrow x \notin F, \\ &\Leftrightarrow F \in s(x)^c, \end{aligned}$$

tj. $s(x^*) = s(x)^c$. Preslikavanje s je obostrano jednoznačno jer, za sve $x, y \in B$, ako $x \neq y$ postoji ultrafilter F koji, recimo, sadrži x i ne sadrži y, tj. $F \in s(x)$ i $F \notin s(y)$, što znači da je $s(x) \neq s(y)$.

Algebra $\mathcal{B}$ je izomorfna podalgebri $s[B]$ algebre $P(SB)$. Operacije u $s[B]$ su skupovne operacije, tj. $\mathcal{B}$ je izomorfna algebri skupova. $\square$

Na prvi pogled, Stonova teorema čini da Bulove algebre izgledaju sasvim jednostavno. Sve probleme ovih struktura možemo svesti na probleme algebri skupova. Međutim, to nikako ne znači da se takvim svođenjem ovi problemi trivijalizuju. Praktično svi dokazi koje smo do sada izložili ne bi bili lakši u algebrama skupova nego što je to bio slučaj u apstraktnim Bulovim algebrama. Ipak, u izvesnom smislu, Stonova teorema trivijalizuje aritmetiku Bulovih algebri.

Neka su $t_1(x_1, \ldots, x_n)$ i $t_2(x_1, \ldots, x_n)$ termi sastavljeni od operacija $\vee$, $\wedge$ i *, konstanti 0 i 1 i promenljivih $x_1, \ldots, x_n$. Izraz oblika

$$t_1(x_1, \ldots, x_n) = t_2(x_1, \ldots, x_n)$$

nazivamo *jednakost*. Jednakost $t_1 = t_2$ važi u algebri $\mathcal{B}$ ako za svaku valuaciju $a_1, \ldots, a_n \in B$, vrednosti $t_1[a_1, \ldots, a_n]$ i $t_2[a_1, \ldots, a_n]$ su jednake.

Primer 9. Jednakost $t_1 = t_2$ važi u svim Bulovim algebrama ako i samo ako važi na nekoj Bulovoj algebri ako i samo ako važi u Bulovoj algebri 2.

Dakle, važenje jednakosti $t_1 = t_2$ u svim Bulovim algebrama može se utvrditi proverom njenog važenja u algebri 2. Kako je za takvu proveru dovoljno konačno mnogo koraka, skup jednakosti Bulovih algebri je *odlučiv*.

Odlučiv je i skup nejednakosti $t_1 \leq t_2$ budući da je nejednakost $t_1 \leq t_2$ ekvivalentna jednakosti $t_1 \wedge t_2 = t_1$.

Međutim, ovakva procedura odlučivosti primenljiva je samo na jednakosti i nejednakosti koje sadrže konačne bulovske operacije. Jednakosti u kojima učestvuju infinitarne operacije $\bigvee$ i $\bigwedge$ mogu da važe na nekim, ali ne i na svim Bulovim algebrama. Naime, Stonov homomorfizam algebre

$\mathcal{B}$ u algebru $\mathrm{P}(SB)$, u opštem slučaju nije kompletan za supremume i infimume koji, eventualno, postoje u algebri $\mathcal{B}$. Na primer, uopšteni zakoni distributivnosti važe u algebrama oblika $\mathrm{P}(X)$, ali ne važe u bezatomičnim kompletnim Bulovim algebrama.

Primer 10. (a) Neka je $M \subseteq B$ takav da supremum $\bigvee M$ postoji u algebri $\mathcal{B}$. Stonov homomorfizam $s : B \to P(SB)$ je kompletan za $\bigvee M$ ako i samo ako $\bigvee M = \bigvee M_0$ za neko konačno $M_0 \subseteq M$.

(b) Ako su $M, N \subseteq B$ takvi da $\bigcap s[M] \subseteq \bigcup s[N]$, postoje konačni $M_0 \subseteq M$ i $N_0 \subseteq N$ takvi da $\bigcap s[M_0] \subseteq \bigcup s[N_0]$.

Primer 11. Ako je X kompaktan Hauzdorfov prostor, za svaki ultrafilter F algebre regularno otvorenih skupova $\mathrm{RO}(X)$, postoji jedinstvena tačka $x \in X$ takva da $x \in \bigcap\{\ \mathrm{cl}(u) : u \in F\}$

Primer 12. U algebri $\mathrm{RO}[0,1]$, regularno otvorenih skupova intervala $[0,1]$, neka je $S = \{(a,b) : a, b \in Q \cap [0,1]\} \subseteq \mathrm{RO}[0,1]$. Ne postoji ultrafilter algebre $\mathrm{RO}[0,1]$ koji je kompletan za supremume oblika $\bigvee M$, $M \subseteq S$.

Otuda sledi da kompletna algebra $\mathrm{RO}[0,1]$ nije izomorfna σ-kompletnoj algebri skupova. Dakle, kompletne Bulove algebre nisu predstavljive kao kompletne algebre skupova.

Svaka Bulova algebra $\mathcal{B}$, na skupu svojih ultrafiltera SB prirodno određuje topologiju sa bazom koju čini familija skupova oblika

$$s(x) = \{F \in SB : x \in F\},$$

za svako $x \in B$. Pokazaćemo da u tako definisanoj topologiji, karakteristična algebra CSB prostora SB je upravo Bulova algebra $\mathcal{B}$.

Takav oblik reprezentacije Bulove algebre uspostavlja obostrano jednoznačnu korespondenciju između Bulovih algebri i nula-dimenzionalnih, kompaktnih Hauzdorfovih prostora ili Bulovih prostora. Ta veza je višestruko zanimljiva i pokazuje da su Bulove algebre i Bulovi prostori u strukturalnom smislu dualni matematički objekti.

Topološki prostor X je *nula-dimenzionalan* ako je karakteristična algebra CX baza topologije na X. Kompaktan, Hauzdorfov i nula-dimenzionalan prostor je *Bulov prostor*.

Primer 13. Prostor iracionalnih brojeva sa topologijom indukovanom topologijom realne prave je nula-dimenzionalan. Njegovu bazu čine skupovi iracionalnih brojeva koji pripadaju otvorenim intervalima oblika (a,b), gde su a i b racionalni brojevi.

Primer 14. Bulov prostor nad skupom $2 = \{0, 1\}$ i diskretnom topologijom, označavamo sa 2. Svaki konačan diskretan prostor je Bulov prostor.

Primer 15. Proizvod svake familije Bulovih prostora je Bulov prostor.

Proizvod $X = \prod_{i \in I} X_i$ Bulovih prostora je Hauzdorfov prostor. Prema teoremi Tihonova, X je kompaktan. Za proizvoljno $i \in I$ i $b_i \in CX_i$ neka je $s(b_i) \subseteq X$ takav da

$$s(b_i) = \{x \in X : x(i) \in b_i\}$$

Kako je $s(b_i)^c = s(b_i^c)$, prema definiciji topologije proizvoda na X, skupovi $s(b_i)$ i $s(b_i^c)$ su otvoreni, pa dakle i zatvoreno otvoreni.

Prostor X je nula-dimenzionalan budući da skupovi oblika $s(b_i)$, $i \in I$, čine predbazu topologije proizvoda.

Primer 16. Za svaki skup I, Kantorov prostor 2^I je Bulov prostor.

Primer 17. Svaki zatvoren potprostor Y Bulovog prostora X je Bulov prostor.

Primer 18. Svaki zatvoren potprostor Kantorovog prostora 2^I je Bulov prostor. Kasnije ćemo videti da važi i obratno, tj. da je svaki Bulov prostor homeomorfan Kantorovom prostoru.

Primer 19. Neka je $f : X \to Y$ neprekidna funkcija Bulovih prostora. Slike zatvorenih skupova su zatvoreni skupovi. Ako je f obostrano jednoznačna funkcija, f je homeomorfizam prostora X na zatvoren potprostor $f[X]$ prostora Y.

Karakteristična algebra CX povezanog prostora X svodi se na Bulovu algebru 2. Međutim, u Bulovim prostorima algebra CX je mnogo veća. Ona zapravo čini bazu topologije prostora X, što znači da je povezanost Bulovih prostora sasvim slaba. U njima su komponente povezanosti jednočlani skupovi, tj. Bulovi prostori su *totalno nepovezani* prostori.

Iz tih razloga, Bulovi prostori praktično nemaju geometriju, tako da je njihov značaj prevashodno algebarski i skupovno-teorijski.

Teorema 17. Svaki Bulov prostor X zadovoljava sledeće uslove:

(a) Prostor X je totalno nepovezan.

(b) Ako je $B \subseteq CX$ baza prostora X zatvorena za konačne unije, onda je $\mathcal{B} \cong CX$.

(c) Ako je skup $Y \subseteq X$ zatvoren, onda je $CY = \{u \cap Y : u \in CX\}$.

(d) Ako su $Y_1, Y_2 \subseteq X$ disjunktni zatvoreni skupovi, postoji zatvoreno otvoren skup $u \in CX$ takav da $Y_1 \subseteq u$ i $Y_2 \subseteq u^c$.

Dokaz: (a) Ako je X Bulov prostor i $Y \subseteq X$ njegov potprostor sa bar dve različite tačke $x, y \in Y$, postoji zatvoreno otvoren skup $u \subseteq X$ takav da $x \in u$ i $y \notin u$. Dakle $Y \cap u$ je neprazan pravi podskup prostora Y koji je zatvoreno otvoren, tj. Y nije povezan.

Primetimo da važi i obratno, totalno nepovezan kompaktan Hauzdorfov prostor je nula-dimenzionalan.

(b) Neka je $u \in CX$. Kako je skup u otvoren i $\mathcal{B}$ baza prostora X, postoji familija $\{a_i \in B : i \in I\}$ čija je unija skup u. Kao zatvoren skup u kompaktnom prostoru X, skup u je kompaktan, pa za neko $n \in \omega$, postoje $i_1, \ldots, i_n \in I$ takvi da je $u = a_{i_1} \cup \cdots \cup a_{i_n}$. Po pretpostavci, baza $\mathcal{B}$ je zatvorena za konačne unije, pa $u \in B$.

(c) Familija $\{u \cap Y : u \in CX\}$ je zatvoreno otvorena baza Bulovog prostora Y. Zatvorena je za konačne unije, pa je dakle jednaka CY.

(d) Skup $Y = Y_1 \cup Y_2$ je zatvoren potprostor prostora X. Skupovi Y_1 i Y_2 su zatvoreno otvoreni u Y. Prema uslovu (c), postoji $u \in CX$ takav da je $Y_1 = u \cap Y$. $\Box$

Skupovi oblika $s(x) = \{F \in SB : x \in F\}$, $x \in B$ su zatvoreni za konačne preseke, pa familija $s[B] = \{s(x) : x \in B\}$ čini bazu jedinstvene topologije na SB. Prostor SB je *Stonov prostor* Bulove algebre $\mathcal{B}$.

Sledeći rezultat predstavlja topološku verziju Stonove teoreme: svaka Bulova algebra može se identifikovati sa karakterističnom algebrom njenog Stonovog prostora.

Teorema 18. Stonov prostor Bulove algebre $\mathcal{B}$ je Bulov prostor i algebra $\mathcal{B}$ je izomorfna sa CSB.

Dokaz: Prostor SB je Hauzdorfov: Pretpostavimo da su $F, G \in SB$ takvi da $F \neq G$. Tada za neko $x \in B$, $x \in F$ i $x \notin G$; tj. $x^* \in G$. To znači da je $F \in s(x)$ i $G \in s(x^*)$. Disjunktni otvoreni skupovi $s(x)$ i $s(x^*)$ razdvajaju tačke F i G prostora SB.

Prostor SB je kompaktan: Dovoljno je dokazati da svako pokrivanje prostora SB baznim skupovima sadrži konačno pokrivanje. Pretpostavimo da postoji pokrivanje $\{s(x_i) : i \in I\}$ prostora SB koje ne sadrži konačno potpokrivanje. Dakle za svaki konačan $I_0 \subseteq I$, $\bigcup_{i \in I_0} s(x_i) \neq SB$, pa kako je s homomorfizam redom imamo

$$s(\bigwedge_{i \in I_0} x_i^*) = \bigcap_{i \in I_0} s(x_i^*) = \bigcap_{i \in I_0} s(x_i)^c = (\bigcup_{i \in I_0} s(x_i))^c \neq \emptyset = s(0).$$

Funkcija s je obostrano jednoznačna, pa mora biti $\bigwedge_{i \in I_0} x_i^* \neq 0$, Otuda sledi da skup $\{x_i^* : i \in I\}$ ima svojstvo konačnih preseka, odnosno, da se može proširiti do ultrafiltra $F \in SB$. Kako za svako $i \in I$, $x_i^* \in F$, to znači da $F \notin \bigcup_{i\in I} s(x_i)$, suprotno pretpostavci $SB \subseteq \bigcup_{i\in I} s(x_i)$.

Prostor SB je nula-dimenzionalan. Za svako $x \in B$, $s(x)^c = s(x^*)$, pa je svaki bazni skup zatvoreno otvoren.

Prema teoremi reprezentacije $\mathcal{B} \cong s[B]$. Familija $s[B]$ je baza topologije u SB pa, prema prethodnoj teoremi, $s[B] = CSB$, tj. $\mathcal{B} \cong CSB$. □

Neka je X proizvoljan topološki prostor. Najmanji kardinal κ za koji postoji baza u X kardinalnosti κ je *težina* topološkog prostora X. Težinu prostora X označavamo sa $d(X)$.

Primer 20. Za svaku beskonačnu Bulovu algebru $\mathcal{B}$, $d(SB) = |B|$.

Jasno, $d(X) \leq |B|$. Neka je U baza prostora SB. Kako je algebra $\mathcal{B}$ beskonačna, prostor SB je beskonačan, pa baza U takođe mora biti beskonačna. Za svako $x \in B$ neka je $U_x \subseteq U$ takav da $s(x) = \bigcup U_x$. Za svako $x \in B$, skup $s(x)$ je kompaktan, pa skup U_x možemo birati tako da $|U_x| < \omega$. Dakle, $x \mapsto U_x$ je obostrano jednoznačno preslikavanje elemenata algebre $\mathcal{B}$ u skup konačnih podskupova baze U. Kako je U beskonačan skup, mora biti $|B| \leq |U|$.

Primer 21. Stonov prostor algebre $\mathcal{B}$ je metrizabilan ako i samo ako $\mathcal{B}$ je prebrojiva Bulova algebra.

Ovaj rezultat je neposredna posledica Urisonove teoreme po kojoj je kompaktan Hauzdorfov prostor metrizabilan ako i samo ako ima prevrojivu bazu.

Ako je X konačan Bulov prostor, onda $d(X) = |X|$. Kasnije ćemo dokazati da u beskonačnom slučaju važi nejednakost $d(X) \leq |X|$. Opštije, ova nejednakost važi u svakom kompaktnom Hauzdorfovom prostoru.

U Bulovim prostorima važi teorema reprezentacije dualna teoremi reprezentacije Bulovih algebri. Taj dualizam sistematski se ispoljava u svim svojstvima Bulovih algebri i Bulovih prostora.

Teorema 19. Svaki Bulov prostor homeomorfan je Stonovom prostoru svoje karakteristične algebre.

Dokaz: Neka je X Bulov prostor i SCX Stonov prostor njegove karakteristične algebre. Tvrdimo da je funkcija $t : X \to SCX$ definisana tako da za sve $x \in X$,

$$t(x) = \{u \in CX : x \in u\}$$

homeomorfizam Bulovih prostora X i SCX.

Za svako $x \in X$, $t(x)$ je ultrafilter u algebri CX.

Za svako $u \in CX$, $x \in u$ ili $x \in u^c$, tj. $u \in t(x)$ ili $u^c \in t(x)$. To pokazuje da za svako $x \in X$, $t(x) \in SCX$, odnosno, da funkcija t zaista preslikava X u SCX.

Preslikavanje t je obostrano jednoznačno: Ako su $x, y \in X$ različiti, kako je X Hauzdorfov prostor, postoje disjunktni bazni skupovi $u, v \in CX$ za koje je $x \in u$ i $y \in v$, pa dakle $t(x) \neq t(y)$.

Preslikavanje t je na: Pretpostavimo da je F ultrafilter u CX. To znači da je F familija zatvorenih podskupova kompaktnog prostora X sa svojstvom konačnih preseka, pa postoji tačka prostora $x \in X$ takva da za svako $u \in F$, $x \in u$, tj. $F \subseteq t(x)$. Kako je F ultrafilter to mora biti $F = t(x)$.

Za svako $u \in CX$ neka je $s(u)$ skup svih ultrafiltera algebre CX koji sadrže u, tj. $s(u)$ je bazni otvoren skup u prostoru SCX. Za svako $u \in CX$ i svako $x \in X$, $x \in t^{-1}[s(u)]$ ako i samo ako $t(x) \in s(u)$ ako i samo ako $u \in t(x)$ ako i samo ako $x \in u$, što znači da je $u = t^{-1}[s(u)]$. Dakle, inverzna slika baznog otvorenog skupa je bazni otvoren skup, što znači da je t neprekidna funkcija. Kako su X i SCX kompaktni Hauzdorfovi prostori, konačno dobijamo da je t homeomorfizam. $\Box$

Primer 22. Ultrafilter F algebre $\mathcal{B}$ je generisan atomom ako i samo ako F je izolovana tačka prostora SB.

Primer 23. Bulova algebra $\mathcal{B}$ je bezatomična ako i samo ako SB nema izolovanih tačaka. Algebra $\mathcal{B}$ je atomična ako i samo ako skup izolovanih tačaka je gust u SB.

Primer 24. Za svaki kardinal κ, postoji Bulov prostor X, $|X| = \kappa$.

Ako je κ konačan kardinal, diskretan prostor X na skupu od κ elemenata je Bulov prostor. U beskonačnom slučaju, ako je $X = SB$ Stonov prostor Frešeove algebre $\mathcal{B}$ nad skupom Y kardinalnosti κ, onda $|X| = \kappa$.

Za svako $x \in Y$, ako je $F_x = \{a \in B : x \in a\}$, skup F_x je ultrafilter algebre $\mathcal{B}$ generisan atomom $\{x\}$, $x \in Y$. U algebri $\mathcal{B}$ jedini neglavni filter je Frešeov filter $F = \{a \in B : |a^c| < \omega\}$, pa je $SB = \{F_x : x \in Y\} \cup \{P\}$. Tačke prostora SB oblika F_x su izolovane, F je beskonačno daleka tačka, odnosno, SB je jednotačkasta kompaktifikacija diskretnog prostora X.

Primer 25. (a) Beskonačan diskretan prostor X je gust u $SP(X)$.

(b) Za svaku (neprekidnu) funkciju $f : X \to Y$, gde je Y kompaktan Hauzdorfov prostor, postoji neprekidna funkcija $g : SP(X) \to Y$ koja proširuje f.

Dakle, prostor $SP(X)$ je najveći kompaktan prostor u kojem je prostor X svuda gust, odnosno, prostor $SP(X)$ je Ston-Čehova kompaktifikacija diskretnog prostora X, tj. $SP(X) = \beta X$.

Prostor je *ekstremno nepovezan* ako je zatvorenje svakog otvorenog skupa otvoren skup. Prostor je *bazno nepovezan* ako je zatvorenje svake prebrojive unije zatvoreno otvorenih skupova otvoren skup.

Primer 26. Ako je s Stonov homomorfizam algebre $\mathcal{B}$, skup $M \subseteq B$ ima supremum ako i samo ako zatvorenje skupa $\bigcup s[M]$ je otvoren skup u prostoru SB. Algebra $\mathcal{B}$ je kompletna ako i samo ako prostor SB je ekstremno nepovezan. Algebra $\mathcal{B}$ je σ-kompletna ako i samo ako SB je bazno nepovezan prostor.

Na osnovu teorme reprezentacije, za svaku algebru $\mathcal{B}$, prostor SB je Bulov prostor i obratno, za svaki Bulov prostor X, algebra CX je Bulova algebra. Ta korespodencija se prirodno proširuje na homomorfizme Bulovih algebri i neprekidne funkcije Bulovih Prostora.

Neka je $h : B_1 \to B_2$ homomorfizam Bulovih algebri. Za svaki ultrafilter $F \in SB_2$, $h^{-1}[F]$ je ultrafilter algebre $\mathcal{B}_1$, pa je time definisano preslikavanje Stonovih prostora $h^S : SB_2 \to SB_1$:

$$h^S(F) = h^{-1}[F].$$

Neka je $f : X_1 \to X_2$ neprekidna funkcija, tj. morfizam Bulovih prostora X_1 i X_2. Ako je V zatvoreno otvoren skup u X_2, $f^{-1}[V]$ je zatvoreno otvoren skup prostora X_1. Na taj način, definisano je preslikavanje $f^C : CX_2 \to CX_1$ odgovarajućih karakterističnih algebri. Pritom, za svako $V \in CX_2$,

$$f^C(V) = f^{-1}[V].$$

Za svaku Bulovu algebru $\mathcal{B}$ neka je $s : B \to CSB$ odgovarajući Stonov izomorfizam. Za svaki Bulov prostor X neka je $t : X \to SCX$ odgovarajući Stonov homeomorfizam.

Teorema 20. Neka je $h : B_1 \to B_2$ homomorfizam Bulovih algebri i neka je $f : X_1 \to X_2$ neprekidna funkcija Bulovih prostora.

(a) Preslikavanje h^S je neprekidna funkcija SB_2 u SB_1,

(b) Preslikavanje f^C je homomorfizam CX_2 u CX_1,

(c) Preslikavanje $h^{SC} : CSB_1 \to CSB_2$ je homomorfizam Bulovih algebri i sledeći dijagram komutira:

$$\begin{array}{ccc} B_1 & \xrightarrow{h} & B_2 \\ s_1 \downarrow & & \downarrow s_2 \\ CSB_1 & \xrightarrow{h^{SC}} & CSB_2. \end{array}$$

(d) Preslikavanje $f^{CS}\colon SCX_1 \to SCX_2$ je neprekidna funkcija Bulovih prostora i sledeći dijagram komutira:

$$\begin{array}{ccc} X_1 & \stackrel{f}{\longrightarrow} & X_2 \\ t_1 \downarrow & & \downarrow t_2 \\ SCX_1 & \stackrel{f^{CS}}{\longrightarrow} & SCX_2. \end{array}$$

Dokaz: (a) Dovoljno je pokazati da je inverzna slika svakog baznog otvorenog skupa u SB_1, pri preslikavanju h^S, bazni otvoren skup u SB_2. Svaki bazni otvoren skup u SB_1 je oblika $s_1(x)$ za neko $x \in B_1$, pa dakle

$$\begin{array}{rcl} (h^S)^{-1}[s_1(x)] & = & \{F \in SB_2 : h^S(F) \in s_1(x)\}, \\ & = & \{F \in SB_2 : h^{-1}[F] \in s_1(x)\}, \\ & = & \{F \in SB_2 : x \in h^{-1}[F]\}, \\ & = & \{F \in SB_2 : h(x) \in F\}, \\ & = & s_2(h(x)). \end{array}$$

(b) Kako se inverzne funkcije regularno ponašaju u odnosu na unije i preseke, sasvim jednostavno se pokazuje da je f^C homomorfizam algebre CX_2 u algebru CX_1.

(c) Na osnovu (a) i (b), preslikavanje h^{SC} je homomorfizam Bulovih algebri. Za svako $x \in B_1$, iz dokaza za (a) imamo da je:

$$(h^{SC} \circ s_1)(x) = h^{SC}(s_1(x)) = (h^S)^{-1}[s_1(x)] = s_2(h(x)).$$

Ako s obzirom na Stonov izomorfizam s identifikujemo algebre $\mathcal{B}$ i CSB, homomorfizam h može se identifikovati sa homomorfizmom h^{SC}.

(d) Na osnovu tvrđenja (b) i (a), preslikavanje f^{CS} je neprekidna funkcija Bulovih prostora, pa za svako $x \in X_1$ redom imamo:

$$\begin{array}{rcl} (f^{CS} \circ t_1)(x) & = & f^{CS}(t_1(x)), \\ & = & (f^C)^{-1}[t_1(x)], \\ & = & (f^C)^{-1}[\{u \in CX_1 : x \in u\}], \\ & = & \{v \in CX_2 : x \in f^C(v)\}, \\ & = & \{v \in CX_2 : x \in f^{-1}[v]\}, \\ & = & \{v \in CX_2 : f(x) \in v\}, \\ & = & t_2(f(x)). \end{array}$$

Dakle, navedeni dijagram komutira. Kao i u slučaju Bulovih algebri, ako se Bulov prostor X, do na homeomorfizam t, identifikuje sa prostorom SCX, u istom smislu se neprekidna funkcija f može identifikovati sa neprekidnom funkcijom f^{CS}. $\square$

Teorema 21. Ako su $h : A \to B$ i $h_1 : B \to C$ homomorfizmi Bulovih algebri, 1_A identičko preslikavanje algebre $\mathcal{A}$, $f : X \to Y$ i $f_1 : Y \to Z$ neprekidne funkcije Bulovih prostora i 1_X identičko preslikavanje prostora X, onda su zadovoljeni sledeći uslovi:

(a) $(1_A)^S = 1_{SA}$ i $(1_X)^C = 1_{CX}$,

(b) $(h \circ h_1)^S = h_1^S \circ h^S$ i $(f \circ f_1)^C = f_1^C \circ f^C$,

(c) h je monomorfizam ako i samo ako h^S je na,

(d) h je na ako i samo ako h^S je obostrano jednoznačna funkcija,

(e) funkcija f je obostrano jednoznačna ako i samo ako f^C je na,

(f) funkcija f je na ako i samo ako f^C je monomorfizam.

Dokaz: Uslovi (a) i (b) se proveravaju neposredno. Uslove (c), (d), (e) i (f) dokazujemo istovremeno. Prvo, ako je h epimorfizam, zbog $h^S = h^{-1}$, funkcija h^S je obostrano jednoznačna. Takođe, ako je f na, po definiciji $f^C = f^{-1}$, pa je f^C monomorfizam.

Neka je h monomorfizam. Ne umanjujući opštost, pretpostavimo da je $h = 1_A$ i da je $A \subseteq B$ podalgebra od $\mathcal{B}$. Za svako $F \in SB$, $h^S(F) = F \cap A$. Ako je U ultrafilter algebre $\mathcal{A}$, skup U ima svojstvo konačnih preseka u $\mathcal{B}$ i može se proširiti do ultrafiltra F algebre $\mathcal{B}$. Pritom $h^S(F) = F \cap A = U$, odnosno, h^S je na.

Neka je f obostrano jednoznačna funkcija. Možemo pretpostaviti da je $f = 1_X$, gde je X zatvoren potprostor prostora Y. Za svako $u \in CY$, $f^C(u) = u \cap X$. Kako smo ranije videli, svaki zatvoreno otvoren skup u X je oblika $u \cap X$, za neko $u \in CY$, pa je f^C epimorfizam.

Ako je h^S obostrano jednoznačna funkcija, prema upravo rečenom, h^{SC} mora biti epimorfizam. Kako je $h = s^{-1} \circ h^{SC} \circ s$, homomorfizam h je epimorfizam. Na isti način dokazuju se i preostale tri implikacije. $\square$

Sadržaj prethodne dve teoreme je po svojoj prirodi kategorijalno teoretski. Neka je $\mathcal{B}$ kategorija čiji su objekti Bulove algebre, a morfizmi homomorfizmi Bulovih algebri i neka je $\mathcal{T}$ kategorija čiji su objekti Bulovi prostori, a morfizmi neprekidne funkcije Bulovih prostora. Preslikavanja $S : \mathcal{B} \to \mathcal{T}$ i $C : \mathcal{T} \to \mathcal{B}$ su kontravarijantni funktori.

U sasvim strogom smislu funktori S i C su međusobno anti-inverzni, a kategorije $\mathcal{B}$ i $\mathcal{T}$ anti-ekvivalentne kategorije. Familija Stonovih homomorfizama $s_B : B \to CSB$, $B \in \mathcal{B}$, je *prirodna transformacija* $s : I \to CS$ identičkog funktora I kategorije $\mathcal{B}$ na funktor CS. Sa druge strane, familija Stonovih funkcija $t_X : X \to SCX$, $X \in \mathcal{T}$, je prirodna transformacija $t \colon I \to SC$ jediničnog funktora kategorije $\mathcal{T}$ na funktor SC.

Takva veza između funktora S i C, u teoriji kategorija se naziva *dualnom adjunkcijom*, a funktori S i C dualno adjungovanim funktorima. Ona je snažno uticala na razvoj teorije kategorija kao posebne matematičke discipline. Kada smo rekli da je Bertran Rasel ipak preterao označivši Bulove radove prvim koracima u uspostavljanju matematike kao nauke o apstraktnim strukturama, imali smo u vidu, pored ostalog, upravo prethodne rezultate. Sa mnogo više razloga bi se moglo reći da matematika postaje naukom o apstraktnim strukturama u radovima Maršala Stona.

Primer 27. Algebra $\mathcal{A}$ je izomorfna podalgebri algebre $\mathcal{B}$ ako i samo ako prostor SA je neprekidna slika prostora SB.

Primer 28. Algebra $\mathcal{A}$ je izomorfna količniku algebre $\mathcal{B}$ ako i samo ako prostor SA je homeomorfan zatvorenom potprostoru prostora SB.

Primer 29. Neka je F filter algebre $\mathcal{B}$. *Dual filtra* F u prostoru SB je zatvoren skup $\tilde{F} = \bigcap\{s(x) : x \in F\}$. Preslikavanje $F \mapsto \tilde{F}$ određuje obostrano jednoznačnu korespondenciju svih filtera algebre $\mathcal{B}$ i familije nepraznih zatvorenih skupova prostora SB. Kao potprostor prostora SB, $\tilde{F}$ je homeomorfan prostoru $S(B_{/F})$.

Primer 30. Svaki dobro uređen skup sa najvećim elementom je Bulov prostor u odnosu na topologiju indukovanu uređenjem.

Primer 31. Za svako $a \in B$, Stonov prostor relativne algebre $\mathcal{B}|a$ je homeomorfan zatvorenom podprostoru $s(a)$ prostora SB.

Primer 32. Skup $X \subseteq B$ generiše algebru $\mathcal{B}$ ako i samo ako skup $s[X] \subseteq CSX$ razdvaja tačke prostora SB, tj. za sve $x, y \in SB$, $x \neq y$, postoji $U \in s[X]$ takvo da $x \in U$ i $y \notin U$.

Primer 33. Ako je $X \subset SB$, homomorfizam $h : B \to P(X)$ definisan tako da za sve $a \in B$, $h(a) = \{F \in X : a \in F\}$ je obostrano jednoznačan ako i samo ako X je gust u Stonovom prostoru SB.

Kardinal $\min\{|X| : X$ je gust u $SB\}$ je najmanji kardinal κ za koji postoji skup X, $|X| = \kappa$, takav da se algebra $\mathcal{B}$ može utopiti u algebru $P(X)$.

Topološki prostor je *perfektan* ako je svaka njegova tačka istovremeno tačka nagomilavanja. Kako smo već napomenuli, Stonov prostor algebre $\mathcal{B}$ je perfektan ako i samo ako algebra $\mathcal{B}$ je bezatomična.

U svakom kardinalu κ postoji slobodna Bulova algebra, pa dakle u svakom kardinalu κ postoji bezatomična Bulova algebra. Ako je algebra $\mathcal{B}$ prebrojiva i bezatomična, Stonov prostor SB je perfektan i njegova baza zatvoreno otvorenih skupova je prebrojiva. Svaki takav prostor, odnosno, kompaktan Hauzdorfov perfektan prostor sa prebrojivom bazom zatvoreno otvorenih skupova je homeomorfan Kantorovom prostoru 2^ω. Dakle, do na izomorfizam, postoji samo jedna prebrojiva bezatomična Bulova algebra.

Teorema 22. Svaki perfektan Bulov prostor sa prebrojivom bazom homeomorfan je Kantorovom prostoru 2^ω.

Dokaz: Neka je X perfektan Bulov prostor sa prebrojivom bazom. Neka je $((u_n, v_n) : n \in \omega)$ prebrojavanje svih parova disjunktnih elemenata baze prostora X.

Prostor X je perfektan, pa je svaki neprazan otvoren skup u X beskonačan. Otuda, za svako $k \in \omega$ i svako $f \in 2^k$ postoji neprazan, zatvoreno otvoren skup $X_{f(0)\ldots f(k-1)} \subseteq X$ koji zadovoljava sledeće uslove:

(a) $X = X_0 \bigcup X_1$ i $X_{f(0)\ldots f(k-1)0} \bigcup X_{f(0)\ldots f(k-1)1} = X_{f(0)\ldots f(k-1)}$,

(b) $X_{f(0)\ldots f(k-1)0} \bigcap X_{f(0)\ldots f(k-1)1} = \emptyset$ i

(c) ako su $u = u_k \bigcap X_{f(0)\ldots f(k-1)}$ i $v = v_k \bigcap X_{f(0)\ldots f(k-1)}$ neprazni, onda je $u \subseteq X_{f(0)\ldots f(k-1)0}$ i $v \subseteq X_{f(0)\ldots f(k-1)1}$.

Za svako $f \in 2^\omega$, neka je

$$X_f = \bigcap_{k\in\omega} X_{f(0)\ldots f(k)}.$$

Skup X_f je presek familije zatvorenih skupova kompaktnog prostora sa svojstvom konačnih preseka, pa X_f nije prazan. Tvrdimo da X_f sadrži tačno jednu tačku.

Pretpostavimo da su $a, b \in X_f$ različiti. Prostor X je Hauzdorfov, pa postoje disjunktni elementi baze u_a i v_b takvi da je $a \in u_a$ i $b \in v_b$. Otuda sledi da postoji $n \in \omega$, takvo da $(u_a, v_b) = (u_n, v_n)$. Pritom,

$$a \in u = u_a \bigcap X_{f(0)\ldots f(n-1)} \;\text{ i }\; b \in v = v_b \bigcap X_{f(0)\ldots f(n-1)}.$$

Prema uslovu (c),

$$u \subseteq X_{f(0)\ldots f(n-1)0} \;\text{ i }\; v \subseteq X_{f(0)\ldots f(n-1)1}.$$

Prema uslovu (b), ako je $f(n) = 0$, onda $b \notin X_{f(0)\ldots f(n)}$, a u slučaju $f(n) = 1$, onda $a \notin X_{f(0)\ldots f(n)}$. Međutim, kako je $X_f \subseteq X_{f(0)\ldots f(n)}$, u oba slučaja imamo kontradikciju.

Dakle, za svako $f \in 2^\omega$, postoji jedinstven $x_f \in X_f$ i obratno, na osnovu uslova (a) sledi da za svako $x \in X$ postoji $f \in 2^\omega$ takvo da je $x = x_f$.

Definišimo funkciju $g : X \to 2^\omega$ tako da za svako $x \in X$,

$$g(x) = f \quad\Leftrightarrow\quad x = x_f.$$

Funkcija g je obostrano jednoznačna funkcija kompaktnih Hauzdorfovih prostora X na 2^ω, pa je za dokaz teoreme dovoljno dokazati njenu neprekidnost, odnosno, da je inverzna slika svakog predbaznog skupa u 2^ω otvoren skup u prostoru X.

Predbazu prostora 2^ω čine skupovi oblika

$$u_{ki} = \{f \in 2^\omega : f(k) = i\},$$

gde je $k \in \omega$ i $i \in \{0,1\}$. Za svako $k \in \omega$ i svako $i \in \{0,1\}$, neka je

$$U_{ki} = \bigcup\nolimits_{f \in 2^k} X_{f(0)\dots f(k-1)\, i}.$$

Za svako $k \in \omega$ i svako $i \in \{0,1\}$, U_{ki} je otvoren skup, pa

$$\begin{aligned} x_f \in U_{ki} \quad &\Leftrightarrow \quad f(k) = i, \\ &\Leftrightarrow \quad f \in u_{ki}, \end{aligned}$$

što konačno znači da $U_{ki} = g^{-1}(u_{ki})$. Dakle, g je neprekidna funkcija kompaktnih Hauzdorfovih prostora, tj. g je homeomorfizam. $\square$

Primer 34. Ako je $\mathcal{B}$ konačna Bulova algebra sa $n \in \omega$ atoma, broj ultrafiltera u $\mathcal{B}$ je takođe n, odnosno, $|SB| = n$. To znači da $|B| = 2^{|SB|}$, tj. da je $|B| > |SB|$.

Primer 35. Broj svih filtera u konačnoj algebri sa $n \in \omega$ atoma je 2^n.

Primer 36. Broj svih podalgebri algebre sa $n \in \omega$ atoma jednak je broju particija skupa od n elemenata.

U slučaju beskonačnih Bulovih algebri, ovi odnosi se bitno menjaju. Ako je $\mathcal{B}$ beskonačna Bulova algebra, $\mathrm{Fi}(B)$ skup svih njenih filtera i $\mathrm{Pa}(B)$ skup svih njenih podalgebri, onda

$$|B| \le |SB| \le |\,\mathrm{Fi}(B)| \le |\,\mathrm{Pa}(B)| \le 2^{|B|}.$$

U ovom nizu, ključne su nejednakosti $|B| \le |SB|$ i $|\,\mathrm{Fi}(B)| \le |\mathrm{Pa}(B)|$. Sve druge su same po sebi razumljive. Primetimo da i donja i gornja granica broja ultrafiltera algebre $\mathcal{B}$ može biti dostignuta. Na primer, ako je $\mathcal{B}$ Frešeova algebra, $|B| = |SB|$, a ako je $\mathcal{B}$ slobodna algebra, $|SB| = 2^{|B|}$.

Teorema 23. Ako je $\mathcal{A}$ prava podalgebra algebre $\mathcal{B}$, postoje različiti ultrafiltri $F, G \in SB$ takvi da $F \cap A = G \cap A$.

Dokaz: Za svaki ultrafilter F algebre $\mathcal{B}$, $F \cap A$ je ultrafilter algebre $\mathcal{A}$. Izaberimo $a \in B - A$. Neka je $U = \{x \in A : a \le x\}$ i $U' = \{x \in A : a^* \le x\}$. Skup $U \cup U'$ ima svojstvo konačnih preseka jer bi u suprotnom postojali

$x \in U$ i $y \in U'$ takvi da je $x \wedge y = 0$, tj. $x \leq y^* \leq a$. Otuda bi sledilo da je $x = a$, tj. da $a \in A$, što protivreči izboru elementa a. Neka je V ultrafilter algebre $\mathcal{A}$ koji proširuje $U \cup U'$.

Skup $V \cup \{a\}$ ima svojstvo konačnih preseka u algebri $\mathcal{B}$ jer u suprotnom bi postojalo $x \in V$ takav da $x \wedge a = 0$. To bi značilo da je $a \leq x^*$, tj. da $x^* \in U \subseteq V$, što protivreči pretpostavci da $x \in V$. Slično, skup $V \cup \{a^*\}$ ima svojstvo konačnih preseka. Dakle, postoje ultrafiltri $F, G \in SB$ takvi da $V \cup \{a\} \subseteq F$ i $V \cup \{a^*\} \subseteq G$. Pritom, $F \neq G$ i $F \cap A = V = G \cap A$. □

Teorema 24. Za svaku beskonačnu algebru $\mathcal{B}$, $|B| \leq |SB|$.

Dokaz: Pretpostavimo da su F i G različiti ultrafiltri i $a_{FG} \in F - G$. Neka je $\mathcal{A}$ podalgebra algebre $\mathcal{B}$ generisana sa $\{a_{FG} : F \neq G \text{ i } F, G \in SB\}$. To znači da je $|A| \leq |SB|$.

Prema prethodnoj teoremi $A = B$, jer za svaka dva različita ultrafiltra $F, G \in SB$, $a_{FG} \in A \cap (F - G)$, pa je $F \cap A \neq G \cap A$. □

Primer 37. Ako su $F_1, \ldots, F_n$, $n \in \omega$, različiti ultrafiltri algebre $\mathcal{B}$ i $F = F_1 \cap \cdots \cap F_n$, onda je $B_{/F} \cong 2^n$.

Primer 38. Za svaki filter F algebre $\mathcal{B}$, $F \cup F^*$ je podalgebra algebre $\mathcal{B}$. Ako su F i G različiti filtri i nisu maksimalni, $F \cup F^* \neq G \cup G^*$.

Primer 39. Ako je $\mathrm{Fi}(B) - SB$ skup filtera algebre $\mathcal{B}$ koji nisu maksimalni, onda je $|SB| \leq |\, \mathrm{Fi}(B) - SB|$.

Primer 40. Za svaku algebru $\mathcal{B}$, $|\, \mathrm{Fi}(B)| \leq |\, \mathrm{Pa}(B)|$.

Teorema 25. Ako je $\mathcal{B}$ slobodna Bulova algebra nad skupom slobodnih generatora kardinalnosti κ, onda je $|SB| = 2^\kappa$.

Dokaz: Svaki ultrafilter F algebre $\mathcal{B}$ određuje funkciju $f : \kappa \to 2$ takvu da za svako $i < \kappa$, $f(i) = 1$ ako i samo ako $x_i \in F$. I obratno, za svaku funkciju $f \in 2^\kappa$, skup $X_f = \{x_i^{f(i)} : i < \kappa\}$ ima svojstvo konačnih preseka, pa je sadržan u nekom ultrafiltru F. Ako su $f, g : \kappa \to 2$, različite funkcije, za neko $i < \kappa$, $f(i) \neq g(i)$, tj. za neko $i < \kappa$, $f(i) = 1$ i $g(i) = 0$. Ako su F_f i F_g ultrafiltri koji odgovaraju funkcijama f i g, onda $x_i \in F_f$ i $x_i \notin F_g$, tj. $F_f \neq F_g$. □

Dakle, broj ultrafiltera u slobodne algebre dostiže svoju gornju granicu. U narednim primerima ilustrovan je odnos kardinalnosti Bulove algebre i njenog Stonovog prostora.

Primer 41. (a) Za svako $n \in \omega$, postoji prebrojiva Bulova algebra sa tačno n atoma.

(b) Postoji prebrojiva Bulova algebra sa beskonačnim skupom atoma koja nije atomična. Postoje neizomorfne algebre sa takvim svojstvom.

Primer 42. Ako Bulova algebra $\mathcal{B}$ nije atomična, onda je $|SB| \geq 2^\omega$. Dakle, ako je prostor SB prebrojiv, algebra $\mathcal{B}$ je atomična.

Ako $\mathcal{B}$ nije atomična algebra, postoji $b \in B$, $b \neq 0$, takvo da za svako $x \leq b$, x nije atom u $\mathcal{B}$. Kako x nije atom, postoje disjunktni $y, z \in B$, različiti od nule, takvi da je $x = y \vee z$. Za svako $f \in 2^\omega$ može se konstruisati skup $X_f \subseteq \{x \in B : x \leq b\}$ sa svojstvom konačnih preseka takav da za sve $f, g \in 2^\omega$, ako je $f \neq g$, postoje $x, y \in B$ takvi da $x \in X_f$, $y \in X_g$ i $x \wedge y = 0$.

Primer 43. Ako je X Bulov prostor, algebra CX je gusta podalgebra algebre $\mathrm{RO}(X)$. Dakle, CX je regularna podalgebra algebre $\mathrm{RO}(X)$

Primer 44. Ako je X topološki prostor u kojem je svaka familija disjunktnih otvorenih skupova prebrojiva i S baza prostora X, onda je $|\mathrm{RO}(X)| \leq |S|^\omega$.

Za svako $U \in \mathrm{RO}(X)$ neka je S_U maksimalna familija disjunktnih elemenata u $P(U) \cap S$. Prema Zornovoj lemi, takva familija postoji i pritom je $U = \mathrm{int}(\mathrm{cl}(\bigcup S_U))$. Kako familija oblika S_U ima najviše $|S|^\omega$ to je $|\mathrm{RO}(X)| \leq |S|^\omega$.

Teorema o postojanju ultrafiltra kompletnog za prebrojivu familiju supremuma Bulove algebre ima i topološki dokaz. U tom dokazu koristi se Berova teorema prema kojoj je presek svake prebrojive familije gustih skupova kompaktnog Hauzdorfovog prostora gust skup.

Primer 45. Za svaku prebrojivu familiju supremuma S algebre $\mathcal{B}$ i svako $x \in B$, $x \neq 0$, postoji S-kompletan ultrafilter F u $\mathcal{B}$ takav da $x \in F$.

Ako je $S = \{S_n : n \in \omega\}$ familija skupova elemenata algebre $\mathcal{B}$, za svaki prirodan broj $n \in \omega$, skup $P_n = \{G \in SB$:G je kompletan za $\bigvee S_n\}$ je gust u prostoru SB. Prema Berovoj teoremi, skup $\bigcap_{n\in\omega} S_n$ je gust u SB. Kako je $x \neq 0$, skup $s(x)$ nije prazan, pa postoji $F \in \bigcap_{n\in\omega} S_n$ takav da $F \in s(x)$.

Napomene

– Kada smo rekli da Fregea smatramo osnivačem savremene logike, nismo želeli da potcenimo njenu dugu antičku i srednjevekovnu tradiciju. Pre Fregea, modernu logiku su nagovestili radovi Gotfrida Vilhelma Lajbnica, Bernharda Bolcana i posebno Džordža Bula. U svom "Istraživanju zakona mišljenja", objavljenom 1854. godine u Kembridžu, Bul je naveo spisak identiteta koji, kako je rekao, vladaju zakonima mišljenja. Iako ideja interpretacije formalnih objekata u konkretnim matematičkim strukturama u njegovom dobu nije bila u potpunosti razvijena, može se reći da je on imao u vidu dve interpretacije svojih identiteta.

Prva interpretacija odnosi se na ono što danas nazivamo dvoelementnom Bulovom algebrom, tj. na algebru $2 = \{0, 1\}$, u kojoj konstanta 0 označava "laž", konstanta 1 označava "istinu", i čije operacije odgovaraju logičkim operacijama disjunkcije, konjunkcije i negacije.

U drugoj interpretaciji, Bul je imao u vidu "algebru klasa" u kojoj njegovim operacijama odgovaraju operacije unije, preseka i komplementacije.

Značaj Bulovih rezultata svakako prevazilazi okvire same teorije Bulovih algebri. Na primer, sa nešto malo preterivanja, Bertrand Rasel je smatrao da je Bul otkrio čistu matematiku. Koliko god to bilo sporno, može se ipak reći da je Bul jedan od prvih matematičara koji matematiku nije shvatao samo kao neku vrstu kvantitativne analize, već prevashodno kao nauku o apstraktim strukturama.

– Kao matematičke strukture u strogom smislu, dakle kao klasa algebarskih struktura koja zadovoljava određene identitete, Bulove algebre izučavaju se tek početkom dvadesetog veka.

Pokazalo se da je Bul bio u pravu u odnosu na obe interpretacije koje je imao u vidu – u oba slučaja on je formulisao kompletnu aksiomatizaciju ovih struktura. Naime, 1921. godine, Emil Post je dokazao da se svaki identitet koji važi u dvoelementnoj Bulovoj algebri može izvesti iz Bulovih identiteta. Sa druge strane, 1936. godine, Maršal Ston je dokazao da svaka algebra koja zadovoljava Bulove identitete mora biti izomorfna algebri skupova.

– Ekvivalencija Bulovih algebri i komplementiranih distributivnih mreža formulisana je početkom ovog veka. Verovalo se da su Bulove algebre mreže sa jedinstvenom komplementacijom, ali se danas zna da to nije tačno. Otvoreno je pitanje da li to važi u slučaju kompletnih mreža sa jedinstvenom komplementacijom.

– Strukturalna i kombinatorna teorija Bulovih algebri razvijena je sredinom ovog veka. Konstrukcija kompletiranja nastala je u okviru opštijih ideja kompletiranja parcijalnih uređenja [4]. Veći deo teorije o proširenjima homomorfizama razvio je Roman Sikorski [5]. Faktorizaciju σ-kompletnih algebri dokazao je Alfred Tarski [1].

– Teoremu u ultrafiltru dokazao je Alfred Tarski 1930. godine. Kao skupovno teoretski princip, ona je nešto slabija od aksiome izbora. Ekvivalentna je stavu potpunosti predikatskog računa i kompaktnosti Kantorovog prostora 2^P, za svaki skup P. U monografiji [2] izložen je niz ekvivalentnih formulacija teoreme o ultrafiltru i detaljno raspravljen njen odnos sa aksiomom izbora. Koristeći topološke metode, teoremu o egzistenciji ultrafiltra koji je kompletan za prebrojive familije supremuma dokazali su Roman Sikorski i Helena Rašova 1951. godine. Dokaz koji smo ovde izložili je nešto kasnije formulisao Alfred Tarski [3].

– Teoremu reprezentacije dokazao je Maršal Ston 1936. godine [6]. Iste ideje uopštavane su u okviru teorije distributivnih mreža sa jedne, kao i u kontekstu problema reprezentacije komutativnih prstenova sa druge strane. Ovi rezultati predstavljali su inspiraciju glavnih ideja teorije kategorija u čijem okviru su po prvi put precizno definisani pojmovi kanonskog homomorfizma i prirodne ekvivalencije.

– Celovit pregled razvoja teorije Bulovih algebri do 1989. godine izložen je u *Priručniku Bulovih algebri* [3]. Monografija *Bulove Algebre* [4], objavljena na srpskom jeziku, obuhvata i jedan broj najnovijih rezultata u ovoj oblasti.

Literatura

[1] Halmos, P.R. *Lectures on Boolean Algebras*, Van Nostrand, New York, 1963.

[2] Mijajlović, Ž. *An Introduction to Model Theory*, Univ. of Novi Sad, Novi Sad, 1987.

[3] Monk, J.D., Bonnet, R. *Handbook of Boolean Algebras*, North-Holland, Amsterdam, 1989.

[4] Perović, Ž. *Bulove Algebre*, Beograd, 1996.

[5] Sikorski, R. *Boolean Algebras*, Springer, Berlin, 1964.

[6] Stone, M.H. *The representation theorem for Boolean Algebras*, Trans. Am. Math. Soc. 40, 37-111, 1936.

Teorija modela

Kao specifična grana matematike, logika se bavi izučavanjem jezika u kojem se izražavaju matematička tvrđenja. Preciznije, ona se bavi odnosom između matematičkih teorija izraženih u formalnom jeziku i matematičkih struktura u kojima se takve teorije realizuju. Ovo poglavlje obuhvata onaj deo logike koji se u užem smislu bavi takvim pitanjima i uobičajeno se naziva *teorijom modela*. Ta teorija biće razvijena do jednog nivoa na kojem se u ovom kontekstu može sagledati većina standardnih matematičkih teorija. Sa druge strane, kao u svim ostalim oblastima nauke, u logici se razvio i jedan krug problema koji su zanimljivi za nju samu, nezavisno od uloge koju ona ima u matematici ili filosofiji, pa izlaganje teorije modela predstavlja uvod u logiku kao potpuno samostalnu nauku.

Iskazni račun

U zasnivanjima matematike zanimljivi su logički sistemi u kojima se mogu izražavati svojstva matematičkih struktura. Centralno mesto u tom smislu ima predikatski račun prvog reda čiju smo skicu napravili u dosadašnjem izlaganju. Iako iskazni račun nije takav sistem, njegove izražajne mogućnosti su u sasvim ograničene, on ipak zaslužuje određenu pažnju. Na prirodan način, on je deo predikatskog računa, pa se na njemu, kao najjednostavnijem logičkom sistemu, mogu definisati i razumeti glavne ideje koje su relevantne u izučavanjima svih drugih logičkih sistema. Iz tih razloga, u ovom poglavlju, bavićemo se i osobinama iskaznog računa.

Iskazni račun formalizuje deo logike u kojem legitimnost argumentacije zavisi samo od toga kako su rečenice konstruisane, a ne i od njihovog značenja ili unutrašnje strukture. U ovom kontekstu irelevantno je zašto je neki iskaz istinit ili lažan, kako je interpretiran i šta je njegov smisao. Bitna je samo njegova struktura u odnosu na logičke veznike. Sasvim uopšteno, kada se radi o bilo kom logičkom sistemu, priroda strukture njegovih veznika izučava se tako što se izabere skup rečenica ili *aksioma* i skup *pravila izvođenja*. Polazeći od aksioma, pravila izvođenja generišu skup rečenica koje, iz različitih razloga, smatramo legitimnim u datom sistemu.

U slučaju izkaznog i predikatskog računa, izbor aksioma i pravila izvođenja pretežno je motivisan matematičkim razlozima.

Sa formalnog stanovišta, jezik je određen skupom simbola i skupom pravila po kojima se formiraju gramatički korektne rečenice. Skup simbola S iskaznog računa, sadrži sledeće simbole:

(a) beskonačan skup *iskaznih slova* $P = \{p_n : n \in \omega\}$,
(b) *logičke veznike* negaciju $\neg$ i implikaciju $\rightarrow$,
(c) *interpunkcijske simbole* desnu ")" i levu "(" zagradu.

Osim u problemima odlučivosti, kada podrazumevamo da je skup iskaznih slova zadat na neki efektivan način, pretpostavka o njegovoj prebrojivosti nije suštinska. Praktično sve što budemo rekli o prebrojivom iskaznom računu važi i u neprebrojivim računima.

Na skupu simbola $\mathcal{S}$, kao nad nekom vrstom azbuke, definisaćemo gramatička pravila pomoću kojih se formulišu rečenice jezika $\mathcal{S}$. U slučaju iskaznog računa, umesto rečenice, za gramatički korektno formiran niz simbola upotrebljavaćemo termin *formula*.

Skup formula F iskaznog računa je najmanji skup konačnih nizova simbola koji zadovoljava sledeće uslove:

(a) $P \subseteq F$,
(b) za sve $\varphi, \psi \in F$, $\neg\varphi \in F$ i $(\varphi \rightarrow \psi) \in F$.

Skup simbola S na kojem je definisan skup formula F je *jezik iskaznog računa*.

Na primer, niz simbola $(p_0 \rightarrow (p_1 \rightarrow p_0))$ jeste formula iskaznog računa. Međutim, konačni nizovi simbola $p_0(\rightarrow p_1\neg$ i $p_0p_1p_2$ nisu formule.

Sa algebarskog stanovišta, skup formula F je slobodna algebra nad skupom slobodnih generatora P u kojoj operacije $\neg$ i $\rightarrow$ ne zadovoljavaju nikakav zakon.

Rekurzivna definicija skupa formula ima suštinsku ulogu u svim argumentacijama matematičke logike. Ona omogućava da se sva svojstva skupa formula definišu ili provere indukcijom po složenosti njegovih elemenata.

Broj logičkih veznika koji se javljaju u formuli φ iskaznog računa je *složenost formule* φ. Pritom, iskazna slova su formule složenosti nula. Prema ovoj definiciji, dokaz da svi elementi skupa F imaju svojstvo $\mathcal{P}$ podrazumeva:

(a) da sva iskazna slova imaju svojstvo $\mathcal{P}$,

(b) iz pretpostavke da formule φ i ψ imaju svojstvo $\mathcal{P}$ sledi da formule $(\varphi \rightarrow \psi)$ i $\neg\varphi$ imaju svojstvo $\mathcal{P}$.

Složenost formule je prirodan broj, pa ovaj tip argumentacije predstavlja indukciju u uobičajenom smislu, odnosno, indukciju u strukturi prirodnih brojeva. To zapravo znači da naša metateorija sadrži aritmetiku.

Kako se logika prevashodno bavi svojstvima implikacije, kao osnovne logičke veznike izabrali smo negaciju i implikaciju. Ostali standardni veznici su samo konvencija koju uvodimo radi preglednijeg zapisivanja formula. Za sve $\varphi, \psi \in F$,

$(\varphi \wedge \psi) = \neg(\varphi \to \neg\psi)$ je *konjunkcija* formula φ i ψ,
$(\varphi \vee \psi) = (\neg\varphi \to \psi)$ je *disjunkcija* formula φ i ψ,
$(\varphi \leftrightarrow \psi) = (\varphi \to \psi) \wedge (\psi \to \varphi)$ je *ekvivalencija* formula φ i ψ.

Ponekad, radi lakšeg čitanja formula, izostavljamo neke od interpunkcijskih simbola. Svakako, uvek odgovarajuće parove, tako da je u svakoj formuli broj levih zagrada jednak broju desnih zagrada i tako da se svaka takva formula može pročitati na jedinstven način.

Kako smo ranije napomenuli, iskazni račun formalizuje deo logike u kojem valjanost argumentacija zavisi samo od veznika pomoću kojih su konstruisane rečenice prirodnog jezika. U ovom slučaju interesuje nas struktura prirodnog jezika samo u odnosu na iskazne veznike. Rečenice su istinite ili lažne i to zavisi samo od toga kakvi su u tom smislu njihovi sastavni delovi. Pritom, potpuno je irelevantno na koji način je interpretiran iskaz označen slovom p_n, $n \in \omega$. Bitno je da svaki takav iskaz može biti samo istinit ili lažan. Ove vrednosti interpretiramo kao jedinicu i nulu Bulove algebre 2, a logičke veznike kao njene operacije. Pritom, negacija se interpretira komplementacijom, a implikacija sledećom operacijom algebre 2: za sve $x, y \in 2$, $x \to y = x^* \vee y$. Kao binarna operacija, implikacija se na ovaj način može definisati u svakoj Bulovoj algebri.

Valuacija iskaznih slova je funkcija $f : P \to 2$. Za svako $n \in \omega$, vrednost $f(p_n)$ je *interpretacija* iskaznog slova p_n za valuaciju $f \in 2^P$.

Neka je $f \in 2^P$ valuacija. *Interpretaciju* $f(\varphi)$ formule $\varphi \in F$, za valuaciju f, definišemo indukcijom po složenosti formule φ: za sve $\varphi, \psi \in F$, ako su interpretacije $f(\varphi)$ i $f(\psi)$ definisane, onda

(a) $f(\neg\varphi) = f(\varphi)^*$,
(b) $f(\varphi \to \psi) = f(\varphi) \to f(\psi)$.

Faktički, funkciju $f : P \to 2$ definisanu na iskaznim slovima $P \subseteq F$, proširili smo do funkcije $f : F \to 2$ koja je definisana na svim formulama iskaznog računa. Zbog jedinstvenosti takvog proširenja, na isti način označili smo valuaciju f skupa P i njeno proširenje f na skup F.

Interpretacija uvedenih logičkih veznika definisana je na sledeći način: za svaku valuaciju iskaznih slova $f \in 2^P$,

$$f(\varphi \wedge \psi) = f(\varphi) \wedge f(\psi),$$
$$f(\varphi \vee \psi) = f(\varphi) \vee f(\psi).$$

Za svaku formulu $\varphi \in F$ i svaku valuaciju $f \in 2^P$, ako je $f(\varphi) = 1$, onda f *zadovoljava formulu* φ. Ovu relaciju označavamo sa $f \models \varphi$ i ako važi $f \models \varphi$, ponekad kažemo da je valuacija f *model formule* φ.

Neka je Σ skup formula. Valuacija $f \in 2^P$ *zadovoljava* Σ ako za svaku formulu $\varphi \in \Sigma$, $f \models \varphi$. Ovu relaciju označavamo sa $f \models \Sigma$. Ako važi $f \models \Sigma$, valuacija f je *model* skupa formula Σ.

Skup formula Σ je *zadovoljiv* ako ima model, odnosno, ako postoji valuacija f takva da za svako $\varphi \in \Sigma$, važi $f \models \varphi$.

Primetimo da je relacija $\models$ konkretna matematička relacija između skupa valuacija i skupa formula iskaznog računa, odnosno, $\models \subseteq 2^\omega \times F$. Njena definicija može se formulisati i induktivno:

(a) za svako $n \in \omega$, $f \models p_n$ ako i samo ako $f(p_n) = 1$,
(b) $f \models \neg\varphi$ ako i samo ako ne važi $f \models \varphi$,
(c) $f \models \varphi \rightarrow \psi$ ako i samo ako $f \models \varphi$ implicira $f \models \psi$.

Formula $\varphi \in F$ je *tautologija*, u oznaci $\models \varphi$, ako za svaku valuaciju $f \in 2^P$, važi $f \models \varphi$. Osim termina tautologija, upotrebljavaju se i termini *valjana formula* i *logička istina*.

Primer 1. Ako su $\varphi, \psi \in F$ iskazne formule, za svaku valuaciju $f \in 2^P$,

$f(\varphi \rightarrow \psi) = 0$ ako i samo ako $f(\varphi) = 1$ i $f(\psi) = 0$,
$f(\varphi \wedge \psi) = 1$ ako i samo ako $f(\varphi) = 1$ i $f(\psi) = 1$,
$f(\varphi \vee \psi) = 0$ ako i samo ako $f(\varphi) = 0$ i $f(\psi) = 0$,
$f(\varphi \leftrightarrow \psi) = 1$ ako i samo ako $f(\varphi) = f(\psi)$.

Primer 2. Ako su $\varphi, \psi, \varphi_1, \ldots, \varphi_n \in F$ iskazne formule takve da svaka valuacija koja zadovoljava $\varphi, \varphi_1, \ldots, \varphi_n$ takođe zadovoljava i ψ, sledeća formula je tautologija:

$$(\varphi_1 \wedge \cdots \wedge \varphi_n) \rightarrow (\varphi \rightarrow \psi).$$

Skup valuacija 2^P je beskonačan, pa na prvi pogled, izgleda da je za proveru valjanosti formule potrebno beskonačno mnogo izračunavanja njenih vrednosti. Međutim, kako svaka formula sadrži samo konačno mnogo iskaznih slova, za takvu proveru dovoljan je konačan broj valuacija.

Teorema 1. Predikat "φ je tautologija" je odlučiv.

Dokaz: Neka je φ formula i $p_0, \ldots, p_n$, $n \in \omega$, sva iskazna slova koja učestvuju u formuli φ. Ako su valuacije $f, g \in 2^P$, takve da za sve $i \leq n$

važi $f(p_i) = g(p_i)$, onda je $f(\varphi) = g(\varphi)$. Faktički, koristeći tablice bulovskih operacija, dovoljno je izvršiti 2^n provera. $\square$

Ideja istinosnih tablica je veoma stara. Antički logičar, Filon iz Megare, izmislio je istinosnu tablicu implikacije koju smo definisali u prvom primeru.

Semantička odlučivost, u logičkom smislu trivijalizuje iskazni račun. Osim sa nekom specifičnom motivacijom u analizi njegovih fragmenata, aksiomatizacija iskaznog računa nije potrebna. Umesto da dokazujemo logičku istinitost neke formule, tako što ćemo pokazati da ona sledi iz nekog skupa aksioma, jednostavno možemo proveriti njenu valjanost pomoću procedure koju smo definisali u prethodnoj teoremi.

Aksiomatizacija je značajna u logičkim sistemima koji nisu semantički odlučivi. U takvim sistemima ona je neophodno sredstvo pomoću kojeg generišemo skup valjanih formula. Na primer, predikatski račun prvog reda, za koji je vezan veći deo naših izlaganja, nije semantički odlučiv, pa u tom kontekstu ideja formalizacije ima suštinski značaj. Stoga, razlozi zbog kojih se izvodi formalizacija odlučivih sistema, poput iskaznog računa, prevashodno su motivisani analizom njihovih fragmenata. U ovom izlaganju mi to činimo iz didaktičkih razloga. Ideja formalizacije ima veliki zanačaj u logici i matematici, pa je korisno da se ona izloži na jednostavnom primeru iskaznog računa.

Neka je Σ skup formula jezika $\mathcal{S}$. U najopštijem slučaju, formalizacija skupa Σ podrazumeva izbor sledećih skupova:

(a) izbor odlučivog skupa formula $\Gamma \subseteq \Sigma$ i
(b) skupa pravila izvođenja koja, polazeći od Γ, generišu skup Σ.

Problem formalizacije ima više rešenja. Na primer, u iskaznom računu, ako je Σ skup svih tautologija, skup aksima može se izabrati tako da sadrži samo jednu shema aksiomu $\varphi \to \varphi$, ali je u tom slučaju skup pravila izvođenja nešto složeniji. Druga krajnost je formalizacija sa jednim pravilom izvoenja i nešto složenijim skupom aksioma. Opredelili smo se za drugu mogućnost. Ona više odgovara formalizaciji koja je motivisana problemima zasnivanja matematike.

Problem formalizacije može se postaviti i drugačije. Pretpostavi se određen broj aksioma i pravila izvođenja, a potom, postavi pitanje karakterizacije skupa formula koji aksiome i pravila izvođenja proizvode. Ako granica između filosofske i matematičke logike uopšte postoji, mogla bi se definisati upravo navedenom razlikom. Matematičari prevashodno rešavaju problem formalizacije svojstava matematičkih objekata, a filosofi, problem smisla određenih logičkih principa. U prvom slučaju, za datu semantiku traži se potpuna sintaksa, u drugom slučaju, obratno, za datu sintaksu traži se semantika u odnosu na koju je takva sintaksa potpuna.

Skup aksioma sastoji se od tri skupa formula koji su određeni sa tri *sheme aksioma*. Za sve $\varphi, \psi, \theta \in F$ sledeće formule su aksiome:

$$\begin{array}{l} \varphi \to (\psi \to \varphi), \\ (\varphi \to (\psi \to \theta)) \to ((\varphi \to \psi) \to (\varphi \to \theta)), \\ (\neg\varphi \to \neg\psi) \to (\psi \to \varphi). \end{array}$$

Prva shema određuje sledeći skup formula iskaznog računa:

$$A_1 = \{(\varphi \to (\psi \to \varphi)) : \varphi, \psi \in F\}.$$

Na isti način, preostale dve sheme aksioma određuju skupove formula iskaznog računa A_2 i A_3. Za datu formulu $\varphi \in F$, u konačno mnogo koraka može se proveriti da li formula φ pripada nekom od navedenih skupova. To znači da je predikat "φ je aksioma" odlučiv.

Intuitivno, aksioma $\varphi \to (\psi \to \varphi)$ kaže da ako važi formula φ, onda φ sledi iz bilo čega. Logički princip na kojem počivaju aksiome A_1 naziva se *slabljenje* (tvrđenje $\psi \to \varphi$ je slabije od tvrđenja φ) ili kako bi klasični logičari rekli *verum ex quodlibet*. Jedna filosofska škola to osporava. Ako iz ψ sledi φ, formule ψ i φ moraju imati nešto zajedničko. U *relevantnoj logici* nisu legitimna zaključivanja koja se oslanjaju na taj princip. Moglo bi se reći da su mnogi, ako ne i svi, oblici neformalnih matematičkih argumentacija relevantni, tako da ova primedba klasičnoj logici ima određenu težinu.

U aksiomi $(\varphi \to (\psi \to \theta)) \to ((\varphi \to \psi) \to (\varphi \to \theta))$ formulisana je neka vrsta distributivnosti implikacije u odnosu na samu sebe. Ovaj princip je opšte prihvaćen i smatra se suštinskim za implikaciju.

Aksioma $(\neg\varphi \to \neg\psi) \to (\psi \to \varphi)$ je jaka kontrapozicija. Ona aksiomatizuje princip na koji se u zaključivanju često pozivamo: ako iz $\neg\varphi$ dokažemo $\neg\psi$, onda iz ψ sledi φ.

Konstruktivističke logičke škole, poput *intuicionista*, takvu vrstu zaključivanja ne prihvataju. One smatraju legitimnom samo slabu kontrapoziciju $(\varphi \to \psi) \to (\neg\psi \to \neg\varphi)$. Međutim, sistem aksioma sa slabom kontrapozicijom, umesto jake, nije potpun u odnosu na našu semantiku.

Jedino *pravilo izvođenja* je *modus ponens*: za proizvoljne $\varphi, \psi \in F$, formula ψ je neposredna posledica formula φ i $\varphi \to \psi$.

Konačan niz formula $\varphi_1, \dots, \varphi_n$ je *dokaz* formule φ ako $\varphi = \varphi_n$ i za sve $k \leq n$, φ_k je aksioma ili za neke $i, j < k$, φ_k je neposredna posledica formula

φ_i i φ_j. Ako ima dokaz, formula φ je *teorema*. Za teoreme upotrebljavamo oznaku $\vdash \varphi$.

Primer 3. Za svaku formulu $\varphi \in F$, $\vdash \varphi \to \varphi$.

Dokaz teoreme $\vdash \varphi \to \varphi$ je sledeći niz formula:

$$\begin{aligned}
\varphi_1 &= (\varphi \to ((\varphi \to \varphi) \to \varphi)) \to ((\varphi \to (\varphi \to \varphi)) \to (\varphi \to \varphi)),\\
\varphi_2 &= \varphi \to ((\varphi \to \varphi) \to \varphi),\\
\varphi_3 &= (\varphi \to (\varphi \to \varphi)) \to (\varphi \to \varphi),\\
\varphi_4 &= \varphi \to (\varphi \to \varphi),\\
\varphi_5 &= \varphi \to \varphi.
\end{aligned}$$

Formula φ_1 je aksioma iz A_2, formula φ_2 je aksioma iz A_1, formula φ_3 je neposredna posledica formula φ_2 i φ_1, formula φ_4 je aksioma iz A_1, a formula φ_5 je neposredna posledica formula φ_4 i φ_3.

Teorema $\vdash \varphi \to \varphi$ izražava princip *identiteta*. Prema ovom principu, $\vdash \neg\varphi \to \neg\varphi$, za svaku formulu φ. Stoga, na osnovu definicije disjunkcije, u iskaznom računu važi zakon isključenja trećeg: $\vdash \varphi \vee \neg\varphi$.

Kada se u jednom matematičkom dokazu prvi put pozvao na princip isključenja trećeg, Hilbert je izazvao veliku zabunu. Naime, on je dokazao da pretpostavka o nepostojanju određene funkcije vodi do kontradikcije i zaključio da takva funkcija postoji. Većina matematičara devetnaestog veka je to smatrala nekom vrstom prevare budući da Hilbert nije eksplicitno konstruisao objekat čiju egzistenciju dokazuje. Konstruktivisti nipošto ne prihvataju ovaj princip.

U našim razmatranjima, princip isključenja trećeg ili *tertium non datur* javlja se kao posledica činjenice da smo disjunkciju i konjunkciju uveli kao definisane logičke veznike.

Dokaz sasvim jednostavne teoreme $\vdash \varphi \to \varphi$ upućuje na to da bi dokazi složenijih teorema mogli izmaći svakoj razumnoj kontroli. Da bismo u tom smislu stvari pojednostavili, ali i zbog njenog posebnog značaja u logici, prethodno ćemo dokazati teoremu dedukcije. Ona predstavlja primer izvedenog pravila zaključivanja koje je u izvesnom smislu obratno modus ponensu.

Neka je $\Sigma \subseteq F$ skup formula. Konačan niz formula $\varphi_1, \dots, \varphi_n$ je *dokaz formule* φ *iz pretpostavki* Σ ako $\varphi = \varphi_n$ i za sve $k \leq n$, φ_k je aksioma ili jedna od formula skupa Σ ili za neke $i, j < k$, φ_k je neposredna posledica formula φ_i i φ_j.

Formula φ je dokaziva iz skupa pretpostavki Σ ako postoji dokaz za φ iz pretpostavki Σ, u oznaci $\Sigma \vdash \varphi$. Dokaz je konačan niz formula, pa $\Sigma \vdash \varphi$ ako i samo ako postoji konačan $\Sigma_0 \subseteq \Sigma$, $\Sigma_0 \vdash \varphi$.

Teoremu dedukcije dokazujemo indukcijom po dužini dokaza iz skupa pretpostavki Σ. Dužina dokaza je prirodan broj, pa je takva indukcija isto što i indukcija po prirodnim brojevima.

Teorem 2 Teorema dedukcije: $\Sigma \cup \{\varphi\} \vdash \psi \quad \Leftrightarrow \quad \Sigma \vdash \varphi \to \psi$.

Dokaz: Ako $\Sigma \vdash \varphi \to \psi$, primenom modus ponensa neposredno dobijamo da važi $\Sigma \cup \{\varphi\} \vdash \psi$.

Obratnu implikaciju dokazujemo indukcijom po dužini dokaza formule ψ iz pretpostavki $\Sigma \cup \{\varphi\}$. Neka je $n \geq 1$ i $\psi_1, \ldots, \psi_n$ proizvoljan dokaz za ψ iz pretpostavki $\Sigma \cup \{\varphi\}$. Tvrdimo da za svako $i \leq n$, $\Sigma \vdash \varphi \to \psi_i$.

Neka je $n = 1$. Ako je ψ_1 aksioma ili $\psi_1 \in \Sigma$, onda $\Sigma \vdash \psi_1$. Kako u skupu A_1 imamo aksiomu $\psi_1 \to (\varphi \to \psi_1)$, po modus ponensu, $\Sigma \vdash \varphi \to \psi_1$. Ako je $\psi_1 = \varphi$, onda zbog $\vdash \varphi \to \varphi$, važi $\Sigma \vdash \varphi \to \psi_1$.

Neka je ψ_i neposredna posledica firmula ψ_j i $\psi_k = \psi_j \to \psi_i$. Po induktivnoj pretpostavci, $\Sigma \vdash \varphi \to \psi_j$ i $\Sigma \vdash \varphi \to \psi_k$. Kako u skupu A_2 imamo aksiomu $(\varphi \to (\psi_j \to \psi_i)) \to ((\varphi \to \psi_j) \to (\varphi \to \psi_i))$, primenom modus ponensa u dva koraka dobijamo $\Sigma \vdash \varphi \to \psi_i$. $\Box$

U dosadašnjim razmatranjima, termin teorema upotrebljavali smo u dva značenja. U formalnom smislu, teorema je formula iskaznog računa koja ima dokaz, tj. za koju postoji konačan niz formula koje zadovoljavaju uslove definicije dokaza. Biti teorema iskaznog računa je jedno konkretno svojstvo njegovih formula.

U neformalnom smislu, kao u slučaju teoreme dedukcije, teorema govori o određenim svojstvima teorema iskaznog računa. Kao sintaksne objekte, teoreme ćemo nazivati objekt teoremama, a matematička tvrđenja o sintaksnim objektima nazivaćemo metateoremama. Teorema $\vdash \varphi \to \varphi$ je objekt teorema, a teorema dedukcije je metateorema.

Teorema dedukcije omogućuje nam da pojednostavimo dokaze. Treba napomenuti da je teorema dedukcije konzervativno pravilo zaključivanja, odnosno, pozivanje na to pravilo ne proširuje skup teorema: svaka njegova primena može se eliminisati.

Primer 4. Za proizvoljne formule $\varphi, \psi, \theta \in F$, imamo da važi

$$\vdash (\psi \to \theta) \to ((\varphi \to \psi) \to (\varphi \to \theta)).$$

Ova teorema izražava *tranzitivnost implikacije*. Na osnovu definicije dokaza iz hipoteza i primenom teoreme dedukcije redom se dobija:

$$\begin{array}{rcl}
\{\psi \to \theta, \varphi \to \psi, \varphi\} & \vdash & \varphi, \\
\{\psi \to \theta, \varphi \to \psi, \varphi\} & \vdash & \varphi \to \psi, \\
\{\psi \to \theta, \varphi \to \psi, \varphi\} & \vdash & \psi, \\
\{\psi \to \theta, \varphi \to \psi, \varphi\} & \vdash & \psi \to \theta, \\
\{\psi \to \theta, \varphi \to \psi, \varphi\} & \vdash & \theta, \\
\{\psi \to \theta, \varphi \to \psi\} & \vdash & \varphi \to \theta, \\
\{\psi \to \theta\} & \vdash & (\varphi \to \psi) \to (\varphi \to \theta), \\
 & \vdash & (\psi \to \theta) \to ((\varphi \to \psi) \to (\varphi \to \theta)).
\end{array}$$

Dokaz je dat tako da sugeriše kako bi se on mogao transformisati u direktan dokaz tranzitivnosti implikacije. To pokazuje da je pozivanje na teoremu dedukcije potpuno legitimno.

Primer 5. Za proizvoljne $\varphi, \psi \in F$, važi $\vdash \neg\varphi \to (\varphi \to \psi)$.

$$\begin{array}{rcl}
\{\neg\varphi, \varphi\} & \vdash & \neg\varphi \to (\neg\psi \to \neg\varphi), \\
\{\neg\varphi, \varphi\} & \vdash & (\neg\psi \to \neg\varphi) \to (\varphi \to \psi), \\
\{\neg\varphi, \varphi\} & \vdash & (\varphi \to \psi), \\
\{\neg\varphi, \varphi\} & \vdash & \psi, \\
\{\neg\varphi\} & \vdash & (\varphi \to \psi), \\
 & \vdash & \neg\varphi \to (\varphi \to \psi).
\end{array}$$

Klasični logičari su ovaj princip nazivali *ex falso quodlibet*.

Primer 6. Za svaku formulu $\varphi \in F$, važi $\vdash \neg\neg\varphi \to \varphi$.

$$\begin{array}{rcl}
\{\neg\neg\varphi\} & \vdash & \neg\neg\varphi \to (\neg\neg\neg\neg\varphi \to \neg\neg\varphi), \\
\{\neg\neg\varphi\} & \vdash & (\neg\neg\neg\neg\varphi \to \neg\neg\varphi) \to (\neg\varphi \to \neg\neg\neg\varphi), \\
\{\neg\neg\varphi\} & \vdash & (\neg\varphi \to \neg\neg\neg\varphi) \to (\neg\neg\varphi \to \varphi), \\
\{\neg\neg\varphi\} & \vdash & \neg\neg\varphi \to \varphi, \\
\{\neg\neg\varphi\} & \vdash & \varphi, \\
 & \vdash & \neg\neg\varphi \to \varphi.
\end{array}$$

Na sličan način, koristeći kontrapoziciju, dokazuje se i obratna implikacija, tj. za svaku formulu $\varphi \in F$, važi $\vdash \varphi \to \neg\neg\varphi$.

Primer 7. Za sve $\varphi, \psi \in F$, $\vdash (\varphi \to \psi) \to ((\varphi \to \neg\psi) \to \neg\varphi)$.

Treba pokazati da se iz skupa pretpostavki $\{\varphi \to \psi, \varphi \to \neg\psi\}$ može dokazati $\neg\varphi$. Postupićemo na način koji često primenjujemo u dokazima matematičkih tvrđenja. Pretpostavićemo *suprotno*, tj. da nije $\neg\varphi$. Iz skupa pretpostavki $\{\varphi \to \psi, \varphi \to \neg\psi, \neg\neg\varphi\}$ dokazaćemo kontradikciju $\neg(\varphi \to \varphi)$. Uz pomoć kontrapozicije oslobodićemo se pretpostavke $\neg\neg\varphi$ i dokazati $\neg\varphi$. Ovaj tip dedukcije naziva se *svođenje na apsurd*.

$$\begin{array}{rcl}
\{\varphi \to \psi, \varphi \to \neg\psi, \neg\neg\varphi\} & \vdash & \varphi, \\
\{\varphi \to \psi, \varphi \to \neg\psi, \neg\neg\varphi\} & \vdash & \psi, \\
\{\varphi \to \psi, \varphi \to \neg\psi, \neg\neg\varphi\} & \vdash & \neg\psi, \\
\{\varphi \to \psi, \varphi \to \neg\psi, \neg\neg\varphi\} & \vdash & \neg\psi \to (\psi \to \neg(\varphi \to \varphi)), \\
\{\varphi \to \psi, \varphi \to \neg\psi, \neg\neg\varphi\} & \vdash & \neg(\varphi \to \varphi), \\
\{\varphi \to \psi, \varphi \to \neg\psi\} & \vdash & \neg\neg\varphi \to \neg(\varphi \to \varphi), \\
\{\varphi \to \psi, \varphi \to \neg\psi\} & \vdash & (\neg\neg\varphi \to \neg(\varphi \to \varphi)) \to ((\varphi \to \varphi) \to \neg\varphi), \\
\{\varphi \to \psi, \varphi \to \neg\psi\} & \vdash & (\varphi \to \varphi) \to \neg\varphi, \\
\{\varphi \to \psi, \varphi \to \neg\psi\} & \vdash & \varphi \to \varphi, \\
\{\varphi \to \psi, \varphi \to \neg\psi\} & \vdash & \neg\varphi, \\
 & \vdash & (\varphi \to \psi) \to ((\varphi \to \neg\psi) \to \neg\varphi).
\end{array}$$

Primer 8. Slično prethodnim primerima, može se dokazati slaba kontrapozicija $(\varphi \to \psi) \to (\neg\psi \to \neg\varphi)$.

Primer 9. Za proizvoljne $\varphi, \psi \in F$, važi $\vdash ((\varphi \to \psi) \to \varphi) \to \varphi$.

Navedeni teorema naziva se Persovim pravilom i ne može se dokazati samo pomoću aksioma A_1 i A_2. Uz ove aksiome, Persovo pravilo aksiomatizuje implikativni fragment iskaznog računa, tj. svaka teorema iskaznog računa u kojoj se od logičkih veznika javlja samo implikacija dokaziva je polazeći od aksioma A_1, A_2 i Persovog pravila.

Primer 10. Za proizvoljne formule $\varphi, \psi \in F$,

(a) $\vdash (\varphi \to (\psi \to \theta)) \to (\psi \to (\varphi \to \theta))$,
(b) $\vdash (\varphi \to (\varphi \to \psi)) \to (\varphi \to \psi)$.

Teorema (a) izražava princip *permutacije premisa*, a teorema (b) princip njihove *kontrakcije*.

Principi identiteta, tranzitivnosti implikacije, permutacije i kontrakcije premisa, uz aksiomu A_1 dovoljni su da se dokaže aksioma A_2. Tako se dobija ekvivalentna aksiomatizacija iskaznog računa.

Primer 11. Ako implikaciju shvatimo kao neku vrstu poretka među formulama, konjunkcija u takvom poretku ima svojstvo infimuma:

(a) $\vdash (\varphi \wedge \psi) \to \varphi$, $\vdash (\varphi \wedge \psi) \to \psi$,
(b) $\vdash (\theta \to \varphi) \to ((\theta \to \psi) \to (\theta \to (\varphi \wedge \psi)))$.

Primer 12. Slično tvrđenje važi i za disjunkciju. U odnosu na implikaciju kao poredak, ona se ponaša kao supremum:

(a) $\vdash \varphi \to (\varphi \vee \psi)$, $\vdash \psi \to (\varphi \vee \psi)$,
(b) $\vdash (\varphi \to \theta) \to ((\psi \to \theta) \to ((\varphi \vee \psi) \to \theta))$.

Primer 13. Konjunkcija i disjunkcija su uzajamno distributivne, odnosno, formule koje izražavaju njihovu distributivnost su teoreme iskaznog računa. Isto važi i za formule koje izražavaju De Morganove zakone.

Sintaksu iskaznog računa definisali smo izborom jednog skupa tautologija kao aksioma i modus ponensa kao pravila izvođenja. Sasvim prirodno očekujemo da nas dokazi ne izvode iz skupa tautologija, tj. da je skup teorema T_e sadržan u skupu tautologija T_a. Ta činjenica se u logici označava kao saglasnost sintakse sa semantikom koju želimo da formalizujemo.

Teorema 3. Teorema saglasnosti: Ako $\vdash \varphi$ onda $\models \varphi$, za svako $\varphi \in F$.

Dokaz: Teoremu saglasnosti dokazujemo indukcijom po složenosti dokaza formule $\varphi \in F$. Baza indukcije su aksiome, tj. treba dokazati da za svaku aksiomu φ i svaku valuaciju $f \in 2^P$, $f(\varphi) = 1$.

U slučaju aksioma iz A_1, pretpostavimo suprotno, tj. da postoji valuacija $f \in 2^P$ takva da $f(\varphi \to (\psi \to \varphi)) = 0$. To znači da mora biti $f(\varphi) = 1$ i $f(\psi \to \varphi) = 0$, odnosno, $f(\varphi) = 1$ i $f(\psi) = 1$ i $f(\varphi) = 0$, što nije moguće. Na sličan način proveravaju se i sve ostale aksiome.

Induktivni korak je primena pravila izvođenja, odnosno modus ponensa. Ako je $f(\psi) = 1$ i $f(\psi \to \varphi) = 1$, onda $f(\varphi) = 1$, tj. modus ponens čuva tautologije. $\Box$.

Primetimo da je i definicija dokaza iz hipoteza saglasna sa semantikom iskaznog računa. Ako $\Sigma \vdash \varphi$, svaka valuacija koja zadovoljava svaku formulu od skupa Σ takođe zadovoljava i formulu φ.

Formula φ je semantička, odnodno, *logička posledica* skupa formula Σ, u oznaci $\Sigma \models \varphi$, ako svaka valuacija koja zadovoljava Σ, zadovoljava i φ.

Osim saglasnosti pojma teoreme sa pojmom tautologije iskaznog računa, i pojam sintaksne posledice saglasan je sa pojmom logičke posledice, odnosno, saglasnost sintakse iskaznog računa sa njegovom semantikom sada možemo izraziti na sledeći način.

Primer 14. Proširena teorema saglasnosti: Za svaki skup $\Sigma \subseteq F$ i svaku formulu $\varphi \in F$ iskaznog računa,

$$\Sigma \vdash \varphi \quad \Rightarrow \quad \Sigma \models \varphi.$$

Proširenu teoremu saglasnosti dokazujemo indukcijom po dužini dokaza formule φ iz pretpostavki Σ. U principu, taj dokaz ne razlikuje se od dokaza njene posebne varijante.

Skup formula F izkaznog računa ima svojstva bliska Bulovoj algebri. Implikacija je refleksivna i tranzitivna, a konjunkcija i disjunkcija imaju sva svojstva bulovskih operacija. Međutim, sam po sebi, skup formula F shvaćen kao slobodna algebra nad operacijama $\neg$ i $\rightarrow$ ipak nije Bulova algebra. Na primer, formule $\varphi \vee \psi$ i $\psi \vee \varphi$ su različite. Implikacija nije simetrična, pa se ne može shvatiti kao poredak. Tek izjednačavanjem ekvivalentnih formula, na količničkoj stukturi dobija se Bulova algebra. Zapravo, radi se o slobodnoj Bulovoj algebri nad prebrojivim skupom slobodnih generatora.

Za proizvoljne formule iskaznog računa $\varphi, \psi \in F$, neka je

$$\varphi \sim \psi \quad \Leftrightarrow \vdash \varphi \rightarrow \psi \ \text{ i } \ \vdash \psi \rightarrow \varphi.$$

Zbog refleksivnosti i tranzitivnosti implikacije, relacija $\sim$ je relacija ekvivalencije skupa F. Za svako $\varphi \in F$, neka je $|\varphi|$ klasa ekvivalencije formule φ i $B_F = \{|\varphi| : \varphi \in F\}$ odgovarajući količnik skupa formula F po relaciji $\sim$.

Na prirodan način, sada se na količniku B_F može definisati struktura poretka. Za sve $\varphi, \psi \in F$, neka je

$$|\varphi| \leq |\psi| \quad \Leftrightarrow \ \vdash \varphi \rightarrow \psi.$$

Definicija relacije $\leq$ je korektna. Ako $\varphi \sim \varphi'$ i $\psi \sim \psi'$, onda $\vdash \varphi \rightarrow \psi$ ako i samo ako $\vdash \varphi' \rightarrow \psi'$.

Teorema 4. Struktura $\mathcal{B}_F = (B_F, \leq)$ je Bulova algebra.

Dokaz: Zbog $\vdash \varphi \rightarrow \varphi$, relacija $\leq$ je refleksivna. Po definiciji, ona je simetrična, a zbog tranzitivnosti struktura $\mathcal{B}_F$ je parcijalno uređenje.

Za proizvoljne $\varphi, \psi \in F$,

$$\vdash (\varphi \wedge \psi) \rightarrow \varphi \quad \text{i} \quad \vdash (\varphi \wedge \psi) \rightarrow \psi,$$

što znači da je $|\varphi \wedge \psi| \leq |\varphi|$ i $|\varphi \wedge \psi| \leq |\psi|$. Ako je $|\theta|$ donje ograničenje za $\{|\varphi|, |\psi|\}$, onda $\vdash \theta \rightarrow \varphi$ i $\vdash \theta \rightarrow \psi$, pa kako se konjunkcija u odnosu na implikaciju ponaša kao infimum, $\vdash \theta \rightarrow \varphi \wedge \psi$, što znači da je klasa ekvivalencije $|\varphi \wedge \psi|$ je infimum skupa $\{|\varphi|, |\psi|\}$.

Slično, $|\varphi \vee \psi|$ je supremum skupa $\{|\varphi|, |\psi|\}$, a kako je distributivnost teorema iskaznog računa, struktura $\mathcal{B}_F$ je distributivna mreža.

Najveći element u distributivnoj mreži $\mathcal{B}_F$ određen je klasom ekvivalencije teorema, a najmanji klasom kontradikcija. Komplementaciju u $\mathcal{B}_F$ određuje negacija. Naime, za svaku formulu $\varphi \in F$,

$$|\varphi| = 1 \ \Leftrightarrow \vdash \varphi \ \text{ i } \ |\varphi| = 0 \ \Leftrightarrow \vdash \neg\varphi.$$

Ako je $|\varphi| = 1$, za svaku formulu ψ, $|\psi| \leq |\varphi|$, tj. $\vdash \psi \to \varphi$. Ako $\vdash \psi$, po modus ponensu $\vdash \varphi$. Obratno, ako $\vdash \varphi$, prema aksiomi iz skupa A_1, za proizvoljnu formulu $\psi \in F$, $\vdash \varphi \to (\psi \to \varphi)$, pa po modus ponensu dobijamo da je $\vdash \psi \to \varphi$, tj. $|\psi| \leq |\varphi|$. Dakle, $|\varphi| = 1$.

Ako je $|\varphi| = 0$, za svaku formulu $\psi \in F$, imamo $\vdash \varphi \to \psi$, pa zbog slabe kontrapozicije, $\vdash \neg\psi \to \neg\varphi$. Ako formulu ψ biramo tako da $\vdash \neg\psi$, onda $\vdash \neg\varphi$. Obratno, ako $\vdash \neg\varphi$, zbog $\vdash \neg\varphi \to (\varphi \to \psi)$, prema modus ponensu, $\vdash \varphi \to \psi$, za svaku formulu ψ, tj. $|\varphi| = 0$.

Zbog $\vdash \varphi \vee \neg\varphi$ mora biti $|\varphi| \vee |\neg\varphi| = 1$, a prema De Morganovom zakonu, iz $\vdash \neg(\varphi \wedge \neg\varphi)$ dobija se da je $|\varphi| \wedge |\neg\varphi| = 0$. Dakle, za svaku formulu $\varphi \in F$, $|\varphi|^* = |\neg\varphi|$. To konačno znači da je struktura $\mathcal{B}_F$ komplementirana distributivna mreža. $\square$

Bulova algebra $\mathcal{B}_F$ se uobičajeno naziva *Lindenbaumovom algebrom* iskaznog računa. Lindenbaumova algebra je zapravo slobodna Bulova algebra nad skupom slobodnih generatora $P_{/\sim} = \{|p_n| : n \in \omega\}$.

Svaki ultrafilter G algebre $\mathcal{B}_F$ određuje valuaciju $f_G \in 2^P$ takvu da za svako $n \in \omega$, $f_G(p_n) = 1$ ako i samo ako $|p_n| \in G$.

I obratno, za svaku valuaciju $f \in 2^P$, skup $G_f = \{|\varphi| : f(\varphi) = 1\}$ je ultrafilter Lindenbaumove algebre $\mathcal{B}_F$.

Primetimo da jedinicu Lindenbaumove algebre čini skup T_e svih teorema iskaznog računa.

Teorema 5 Stav potpunosti iskaznog računa: Za svaku formulu $\varphi \in F$,

$$\vdash \varphi \quad \Leftrightarrow \quad \models \varphi.$$

Dokaz: Imajući u vidu saglasnost iskaznog računa, dovoljno je dokazati da svaku formulu $\varphi \in F$, $\models \varphi$ implicira $\vdash \varphi$.

Pretpostavimo da nije $\vdash \varphi$. To znači da u Lindenbaumovoj algebri mora biti $|\varphi| \neq 1$, odnosno, $|\neg\varphi| \neq 0$.

Neka je G ultrafilter koji sadrži $|\neg\varphi|$ i neka $f_G \in 2^P$ valuacija određena ultrafiltrom G. Kako $|\neg\varphi| \in G$ to mora biti $f_G(\neg\varphi) = 1$, tj. važi $f_G(\varphi) = 0$, pa nije $\models \varphi$. $\square$.

Stav potpunosti iskaznog računa dokazan je 1921. godine. U tom dokazu, Emil Post nije koristio teoremu o ultrafiltru. On je dokazao nešto jači rezultat, odnosno, definisao je efektivan postupak kojim se rekonstruiše dokaz svake tautologije.

Zbog semantičke odlučivosti, na osnovu stava potpunosti, izkazni račun je i sintaksno odlučiv, tj predikat "$\vdash \varphi$" je odlučiv.

U narednim razmatranjima pokazaćemo da stav potpunosti važi i u proširenom obliku. Sintaksna posledica i semantička posledica u iskaznom računu su iste relacije. Naime, za svako $\Sigma \subseteq F$ i svaku formulu φ,

$$\Sigma \vdash \varphi \quad \Leftrightarrow \quad \Sigma \models \varphi.$$

Skup formula Σ je *protivrečan* ako $\Sigma \vdash \varphi$, za svaku formulu φ. U suprotnom, Σ je *neprotivrečan* skup formula. Skup formula Σ je *maksimalno neprotivrečan* ako je svako njegovo pravo proširenje protivrečan skup formula.

Sa $\mathrm{Cn}(\Sigma)$ označavamo deduktivno zatvorenje skupa formula Σ, tj. skup svih formula dokazivih iz pretpostavki Σ. Primetimo da operator Cn ima sledeća svojstva:

Primer 15. Ako je $\Sigma \subseteq F$, sa Σ_{fin} označavamo skup svih konačnih podskupova skupa Σ. Za proizvoljne $\Sigma, \Gamma \subseteq F$,

(a) $\Sigma \subseteq \mathrm{Cn}(\Sigma)$,
(b) $\mathrm{Cn}(\mathrm{Cn}(\Sigma)) \subseteq \mathrm{Cn}(\Sigma)$,
(c) ako $\Sigma \subseteq \Gamma$, onda $\mathrm{Cn}(\Sigma) \subseteq \mathrm{Cn}(\Gamma)$ i
(d) $\mathrm{Cn}(\Sigma) \subseteq \bigcup_{\Gamma \in \Sigma_{\mathrm{fin}}} \mathrm{Cn}(\Gamma)$.

Primer 16. (a) Ako je Σ neprotivrečan skup, $\mathrm{Cn}(\Sigma)$ je takođe neprotivrečan skup formula.

(b) Neka je Σ maksimalno neprotivrečan skup formula. Za proizvoljnu formulu φ, $\Sigma \vdash \varphi$ ako i samo ako $\varphi \in \Sigma$.

(c) Skup $\Sigma \cup \{\varphi\}$ je neprotivrečan ako i samo ako ne važi $\Sigma \vdash \neg\varphi$.

(d) Skup Σ je protivrečan ako i samo ako za svako φ, $\Sigma \vdash \varphi \wedge \neg\varphi$.

Teorema 6. Lindenbaumova lema: Svaki neprotivrečan skup rečenica može se proširiti do maksimalno neprotivrečnog skupa.

Dokaz: Ako je Σ neprotivrečan, skup $B(\Sigma) = \{|\varphi| : \varphi \in \Sigma\}$ ima svojstvo konačnih preseka. U suprotnom, ako postoji konačan skup $\Sigma_0 \subseteq \Sigma$ takav da $\bigcap B(\Sigma_0) = 0$, onda $\Sigma_0 \vdash \varphi \wedge \neg\varphi$, tj. Σ je protivrečan skup.

Neka je G ultrafilter u $\mathcal{B}_F$ koji proširuje $B(\Sigma)$ i $\Gamma = \{\varphi : |\varphi| \in G\}$. Skup Γ je maksimalno neprotivrečan i proširuje Σ. $\square$

Primer 17. Neka je Σ maksimalno neprotivrečan skup formula.

(a) Za svaku formulu φ, tačno jedna od formula φ i $\neg\varphi$ pripada Σ.
(b) Za sve $\varphi, \psi \in F$, $\varphi \wedge \psi \in \Sigma$ ako i samo ako $\varphi \in \Sigma$ i $\psi \in \Sigma$,
(c) Za sve $\varphi, \psi \in F$, $\varphi \vee \psi \in \Sigma$ ako i samo ako $\varphi \in \Sigma$ ili $\psi \in \Sigma$.

Egzistencija maksimalno neprotivrečnog proširenja omogućava konstrukciju modela svakog neprotivrečnog skupa formula, odnosno, dokaz proširenog stava potpunosti.

Teorema 7. Teorema o postojanju modela: Skup formula Σ je neprotivrečan ako i samo ako Σ ima model.

Dokaz: Pretpostavimo da je $f \in 2^P$ model skupa formula Σ. Indukcijom po dužini dokaza iz pretostavki Σ dokazuje se da svaka formula dokaziva u Σ važi u modelu f. Dokaz je potpuno isti kao i u slučaju teoreme saglasnosti iskaznog računa.

Obratno, ako je Σ neprotivrečan treba konstruisati model koji zadovoljava Σ. Na osnovu Lindenbaumove leme, neka je Γ maksimalno neprotivrečan skup formula koji proširuje Σ i neka je $f \in 2^P$ valuacija takva da za svako $n \in \omega$, $f(p_n) = 1$ ako i samo ako $p_n \in \Gamma$. Indukcijom po složenosti formule $\varphi \in F$ dokazujemo da važi sledeća relacija:

$$(*) \quad \varphi \in \Gamma \;\Leftrightarrow\; f \models \varphi.$$

Ako je φ iskazno slovo, prema definiciji valuacije f, $f \models \varphi$ ako i samo ako $\varphi \in \Gamma$. Na osnovu uslova (a) iz prethodnog primera, ako φ zadovoljava $(*)$, onda $\neg\varphi$ zadovoljava $(*)$, a na osnovu uslova (b), ako φ i ψ zadovoljavaju $(*)$, onda formula $\varphi \to \psi$ zadovoljava $(*)$.

Zbog relacije $(*)$, $f \models \Gamma$, pa kako je $\Sigma \subseteq \Gamma$, $f \models \Sigma$. $\Box$

Iz teoreme o postojanju modela neposredno sledi ekvivalencija sintaksne i logičke posledice iskaznog računa, odnosno, prošireni stav potpunosti.

Teorema 8. Prošireni stav potpunosti: Za svaki skup formula Σ i svaku formulu $\varphi \in F$ iskaznog računa,

$$\Sigma \vdash \varphi \;\Leftrightarrow\; \Sigma \models \varphi.$$

Dokaz Implikacija sa leva na desno je proširena teorema saglasnosti. Obratno, ako $\Sigma \nvdash \varphi$, skup formula $\Sigma \cup \{\neg\varphi\}$ je neprotivrečan, pa dakle prema proširenom stavu potpunosti, ima model. Otuda sledi da $\Sigma \not\models \varphi$. $\Box$

Na osnovu teoreme o postojanju modela, neposredno se dobija i stav kompaktnosti iskaznog računa. Nizom primera ilustrovaćemo značaj ovog rezultata. Njegova čisto semantička priroda, zbog stava potpunosti ima značajne posledice u sintaksi iskaznog računa.

Teorema 9. Stav kompaktnosti: Svaki konačan skup $\Sigma_0 \subseteq \Sigma$ ima model ako i samo ako skup rečenica Σ ima model.

Dokaz: Pretpostavimo da Σ nema model. Prema proširenom stavu potpunosti, Σ je protivrečan, tj. imamo dokaz za $\varphi \wedge \neg\varphi$ iz pretpostavki Σ i samo konačan skup Σ_0 formula iz Σ učestvuje u tom dokazu. Kako $\Sigma_0 \vdash \varphi \wedge \neg\varphi$, skup Σ_0 je protivrečan. Prema teoremi o postojanju modela, konačan $\Sigma_0 \subseteq \Sigma$ nema model. $\Box$

Primer 18. Stav kompaktnosti zapravo izražava kompaktnost Kantorovog prostora 2^P, što opravdava njegov naziv.

Za svaku formulu φ, $\widetilde{\varphi} = \{f \in 2^P : f \models \varphi\}$ je otvoren skup prostora 2^P. Kako za svaku valuaciju $f \in 2^P$, $f \models \varphi$ ako i samo ako ne važi $f \models \neg\varphi$, za svaku formulu $\varphi \in F$, komplement skupa $\widetilde{\varphi}$ je takođe otvoren, što znači da je $\widetilde{\varphi}$ zatvoren skup prostora 2^P.

Ako je Σ neprotivrečan skup, prema pretpostavci stava kompaktosti, familija zatvorenih skupova $\widetilde{\Sigma} = \{\widetilde{\varphi} : \varphi \in \Sigma\}$ ima svojstvo konačnih preseka. Zbog kompaktnosti prostora 2^P, presek $\bigcap\{\widetilde{\varphi} : \varphi \in \Sigma\}$ nije prazan, pa postoji f koja je model skupa rečenica Σ.

Skup formula Σ nazivamo *teorijom* iskaznog računa. Teorija Σ je *zatvorena* ako važi $\mathrm{Cn}(\Sigma) = \Sigma$. Skup formula Γ je *skup aksioma* teorije Σ ako $\mathrm{Cn}(\Gamma) = \mathrm{Cn}(\Sigma)$.

Primer 19. Skup formula Γ je skup aksioma teorije Σ ako i samo ako svaki model skupa Γ je model skupa Σ i obratno.

Primer 20. Teorija Σ je *konačno aksiomatska* ako postoji konačan skup aksioma za Σ.

Ako su Σ_1 i Σ_2 teorije iskaznog računa takve da za svaki model $f \in 2^P$, f je model za Σ_1 ako i samo ako f nije model za Σ_2, onda su teorije Σ_1 i Σ_2 konačno aksiomatske teorije.

Primer 21. Skup formula Σ je *nezavisan* ako za svaku formulu $\varphi \in \Sigma$, formula φ nije posledica skupa formula $\Sigma - \{\varphi\}$. Svaka teorija ima nezavisan skup aksioma.

Obe aksomatizacije iskaznog računa koje su spomenute u dosadašnjim izlaganjima su nezavisne.

Skup svih modela teorije Σ označavaćemo sa $\mathrm{Mod}(\Sigma)$.

Primer 22. Za svaki konačan skup modela $G \subseteq 2^P$ postoji teorija Σ takva da je $G = \mathrm{Mod}(\Sigma)$.

Primer 23. Postoji teorija Σ za koju važi $|\mathrm{Mod}(\Sigma)| = \omega$.

Primer 24. Postoji prebrojiv skup modela $G \subseteq 2^P$ takav da za svaku teoriju Σ, $G \neq \mathrm{Mod}(\Sigma)$.

Primer 25. Za svaku formulu φ, skup modela $\mathrm{Mod}(\varphi)$ je prazan ili kardinalnosti 2^ω.

Primer 26. Za svaku teoriju Σ, skup modela $\mathrm{Mod}(\Sigma)^c$ je prazan ili kardinalnosti 2^ω

Teorija Σ je *kompletna* ako za svaku formulu φ važi tačno jedan od uslova: $\Sigma \models \varphi$ ili $\Sigma \models \neg\varphi$.

Primer 27. Ako je Σ teorija, sledeći uslovi su ekvivalentni:

(a) teorija Σ je kompletna,

(b) skup rečenica $\mathrm{Cn}(\Sigma)$ je maksimalno neprotivrečan,

(c) teorija Σ ima tačno jedan model,

(d) postoji model $f \in 2^P$ takav da za svako $\varphi \in F$, $\Sigma \models \varphi$ ako i samo ako $f \models \varphi$.

Primer 28. Za svaku teoriju Σ neka je $B(\Sigma) = \{|\varphi| : \Sigma \vdash \varphi\}$. Struktura $\mathcal{B}(\Sigma) = (B(\Sigma), \leq)$ je Bulova algebra ili Lindenbaumova algebra teorije Σ.

Svaka Bulova algebra može se predstaviti kao algebra skupova. Tvrdeći da je formulisao spisak identiteta "koji izražavaju sve zakone mišljenja," Bul je možda imao u vidu sledeću reprezentaciju ovih algebri:

Primer 29. Za svaku Bulovu algebru $\mathcal{A}$, u iskaznom računu postoji teorija Σ takva da $\mathcal{A} \simeq \mathcal{B}(\Sigma)$.

Predikatski račun

Izražajne mogućnosti iskaznog računa su veoma ograničene. One se uglavnom iscrpljuju na svojstvima logičkih veznika tako da jezik u kojem bi se sistematski mogla izražavati svojstva matematičkih struktura mora biti mnogo bogatiji. Pre nego što izložimo jedan takav jezik, precizira ćemo kontekst u kojem će on biti interpretiran, odnosno, definisaćemo pojam *matematičke strukture*.

U dosadašnjim razmatranjima spomenuli smo grupe, prstene, polja, uređenja, uređena polja, vektorske prostore, mreže, Bulove algebre, prirodne brojeve itd. U svakom od tih slučajeva radilo se o nepraznom skupu na kojem je definisan određen broj relacija, operacija i konstanti.

U opštem slučaju *struktura* $\mathcal{A}$ je matematički objekt koji sadrži sledeće komponente:

(a) neprazan skup A, ili *domen strukture* $\mathcal{A}$, čija kardinalnost $|A|$ je *kardinalnost strukture* $\mathcal{A}$,

(b) za svaki prirodan broj $n \in \omega$, moguće prazan skup relacija dužine n definisanih na skupu A, odnosno, podskupova skupa A^n,

(c) za svako $n \in \omega$, moguće prazan skup operacija dužine n skupa A, odnosno, preslikavanja oblika $f : A^n \to A$.

(d) moguće prazan skup konstanti, odnosno, elemenata skupa A.

Opskurnim matematičkim jezikom rečeno, struktura $\mathcal{A}$ je niz skupova (A, R, F, C) u kojem je A neprazan skup, R skup relacija, F skup operacija i C skup konstanti skupa A.

Ovakva definicija matematičke strukture sugeriše da jezik na kojem bi se mogla izražavati njena svojstva treba da sadrži odgovarajuće oznake za svaku od njenih relacija, operacija i konstanti. Stoga, *jezik $\mathcal{L}$ predikatskog računa prvog reda* sadrži sledeće skupove simbola:

(a) skup *predikatskih konstanti* $\{P_i : i \in I\}$; za svako $i \in I$, zadat je prirodan broj $n_i \geq 1$ koji određuje dužinu konstante P_i,

(b) skup *operacijskih konstanti* $\{F_j : j \in J\}$; za svako $j \in J$, zadat je prirodan broj $n_j \geq 1$ koji određuje dužinu konstante F_j i

(c) skup *individualnih konstanti* $\{c_k : k \in K\}$, $\{c_k : k \in K\}$,

(d) skup *individualnih promenljivih* $V = \{v_n : n \in \omega\}$,

(e) iskazne logičke veznike, *egzistencijalni kvantifikator* $\exists$ i znak jednakosti $=$ i

(f) *interpunkcijske znake*: zapetu, desnu) i levu (zagradu.

Individualne promenljive, logički veznici, egzistencijalni kvantifikator, znak jednakosti i interpunkcijski znaci su sastavni deo svakog jezika predikatskog računa prvog reda. Iz tih razloga, ovu grupu simbola nazivamo *logičkim simbolima*.

Svi drugi simboli čine nelogički deo jezika. On je promenljiv uključujući i mogućnost da svaki od skupova relacijskih, opreracijskih i individualnih konstanti bude prazan. Kada zadajemo jezik, dovoljno je navesti samo skup njegovih *nelogičkih simbola* – relacijske, operacijske i individualne konstante koje on eventualno sadrži.

Svaka operacija $f : A^n \to A$, dužine $n \geq 1$ određuje relaciju R_f dužine $(n+1)$ takvu da za sve $x_1, \ldots, x_n, y \in A$, $R_f(\vec{x}, y)$ ako i samo ako $f(\vec{x}) = y$.

Dakle, svaka n-arna operacija f može se shvatiti kao relacija R_f takva da za svako $\vec{x} \in A^n$, postoji $y \in A$ za koje važi $R_f(\vec{x}, y)$ i koja ima funkcijsko svojstvo, tj. za svako $\vec{x} \in A^n$ i sve $y, z \in A$, ako $R_f(\vec{x}, y)$ i $R_f(\vec{x}, z)$ tada

$y = z$. Važi i obratno; svaka relacija dužine $n+1$ sa navedenim svojstvima, određuje operaciju dužine n.

Svaka konstanta može se shvatiti kao operacija dužine nula, odnosno, kao relacija dužine jedan, pa su sve strukture zapravo relacijske strukture. Iz tih razloga jezik matematičkih struktura se naziva predikatskim računom.

U definiciji jezika pretpostavili smo da on sadrži jednakost kao logički simbol. Pritom, znak jednakosti uvek interpretiramo kao stvarnu jednakost, odnosno, kao relaciju $\{(x, x) : x \in A\}$, na svakom nepraznom skupu A.

Svaki neprazan skup može shvatiti kao struktura (sa jednakošću kao relacijom), pa nelogički deo jezika može biti i prazan.

Primer 1. Bulove algebre mogu se definisati kao čisto algebarske strukture ili kao parcijalna uređenja.

U prvom slučaju, jezik Bulovih algebri $\mathcal{L}_1 = \{\vee, \wedge, ^*, 0, 1\}$ sadrži dve binarne operacijske konstante $\vee$ i $\wedge$, jednu unarnu * i dve individualne konstante 0 i 1. Ako Bulove algebre shvatimo kao parcijalna uređenja, jezik Bulovih algebri $\mathcal{L}_2 = \{\leq, 0, 1\}$ sadrži jednu binarnu relacijsku konstantu $\leq$ i dve individualne konstante 0 i 1.

Sa stanovišta Bulovih algebri, izbor bilo kojeg od navedenih jezika nije esencijalan. Postoji uniforman prelaz sa klase Bulovih algebri kao operacijskih struktura u klasu Bulovih algebri kao parcijalnih uređenja. Ali, klase modela jezika $\mathcal{L}_1$ i $\mathcal{L}_2$ se značajno razlikuju.

Primer 2. (a) Grupa $\mathcal{G} = (G, \cdot, 1)$ je struktura sa jednom binarnom operacijom i jednom konstantom. Stoga, jezik teorije grupa $\mathcal{L} = \{\cdot, 1\}$ sadrži jednu binarnu operacijsku konstantu $\cdot$ i jednu individualnu konstantu 1. Takođe, grupa se može definisati i kao struktura oblika $\mathcal{G} = (G, \cdot, ^{-1}, 1)$. U tom slučaju, jezik teorije grupa je $\mathcal{L} = \{\cdot, ^{-1}, 1\}$.

(b) Kada se ima u vidu struktura $\mathcal{N}$ prirodnih brojeva, jezik aritmetike je $\mathcal{L} = \{+, \cdot, \leq, s, 0\}$.

(c) Jezik uređenih polja je $\mathcal{L}' = \{+, \cdot, \leq, 0, 1\}$. U odnosu na jezik teorije grupa, on je proširen jednim brojem novih nelogičkih simbola.

Ako je $\mathcal{L} \subseteq \mathcal{L}'$, jezik $\mathcal{L}'$ je *proširenje jezika* $\mathcal{L}$. Proširenje $\mathcal{L}'$ koje, kao nove simbole, sadrži samo simbole individualnih konstanti nazivamo *prostim proširenjem* jezika $\mathcal{L}$.

Kardinalnost jezika $\mathcal{L}$, u oznaci $\|\mathcal{L}\|$, je kardinalnost skupa svih njegovih simbola. Kako je logički deo jezika prebrojiv to je $\|\mathcal{L}\| = \sup\{\omega, |\mathcal{L}|\}$.

Za razliku od iskaznog računa, predikatski račun sadrži dve vrste sintaksnih objekata: terme i formule. Termi su svi konačni izrazi koji se mogu dobiti od promenljivih, konstanti i operacijskih simbola i koji, kao reči, imaju smisla. Formule su izrazi sastavljeni od predikata (nad termima), logičkih veznika i kvantifikatora.

Skup *terma* jezika $\mathcal{L}$ je skup konačnih nizova simbola koji zadovoljava sledeće uslove:

(a) individualne promenljive i konstante su termi jezika $\mathcal{L}$,

(b) za svaku operacijsku konstantu F dužine $n \geq 1$, ako su $t_1, \ldots, t_n$ termi, onda je $F(t_1, \ldots, t_n)$ term jezika $\mathcal{L}$,

(c) svaki term jezika $\mathcal{L}$ može se dobiti samo konačnom primenom prethodnih pravila.

Drugačije rečeno, skup terma jezika $\mathcal{L}$ je najmanji skup konačnih nizova njegovih simbola koji sadrži individualne promenljive, individualne konstante i zatvoren je za pravilo (b).

Skup formula jezika $\mathcal{L}$ je takođe skup konačnih nizova njegovih simbola i definiše indukcijom po složenosti njegovih elemenata. U ovom slučaju, bazu indukcije čini skup *elementarnih formula*:

(a) ako su t_1 i t_2 termi jezika $\mathcal{L}$, onda je $t_1 = t_2$ elementarna formula,

(b) ako je P predikatska konstanta dužine $n \geq 1$ i $t_1, \ldots, t_n$ termi jezika $\mathcal{L}$, onda je $P(t_1, \ldots, t_n)$ elementarna formula,

(c) elementarne formule jezika $\mathcal{L}$ mogu se dobiti samo primenom prethodnih pravila.

Skup *formula* jezika $\mathcal{L}$ je najmanji skup njegovih konačnih nizova koji sadrži elementarne formule i zatvoren je za sledeće pravilo:

(d) ako su φ i ψ formule, $x \in V$ promenljiva, reči $\neg\varphi$, $\varphi \to \psi$ i $\exists x \varphi$ su formule jezika $\mathcal{L}$.

Standardne logičke veznike, disjunkciju, konjunkciju i implikaciju u predikatskom računu definišemo isto kao u iskaznom slučaju, a univerzalni kvantifikator na sledeći način: za svaku formulu φ i svaku promenljivu $x \in V$, $\forall x\, \varphi = \neg\exists x\, \neg\varphi$.

Svakako, u prethodnoj definiciji znak jednakosti je upotrebljen u neformalnom smislu. Kao elemet jezika $\mathcal{L}$, jednakost $=$ je binarna relacijska konstanta. Iako u oznakama tu razliku nismo napravili, upotreba jednakosti će u datom kontekstu uvek biti jasno određena.

Kako su formule induktivno definisane, za svaku formulu određen je skup njenih potformula. Niz susednih simbola u formuli φ koji je sam po sebi formula je *potformula* formule φ. Za svaku formulu, rekurzivno po složenosti, definisan je skup svih njenih potformula.

Za proizvoljne promenljive $x, y \in V$, javljanje promenljive u formulu φ je pod *dejstvm kvantifikatora* $\exists y$, ako se x javlja u formuli $\exists y\, \psi$, za neku potformulu ψ formule φ.

Javljanje promenljive $x \in V$ u formuli φ je *vezano* ako se, u tom javljanju, promenljiva x nalazi pod dejstvom kvantifikatora $\exists x$. Javljanje promenljive x koje nije vezano je *slobodno*. U istoj formuli promenljiva x može imati više vezanih i više slobodnih javljanja.

Promenljiva y je *slobodna za promenljivu* x u formuli φ ako se promenljiva x ne nalazi pod dejstvom kvantifikatora $\exists y$ u formuli φ.

Term t je *slobodan za promenljivu* x u formuli φ ako su sve njegove promenljive slobodne za x u formuli φ.

Primer 3. U formuli $\varphi(v_1) = \neg\exists v_0\, (v_0 < v_1)$ jezika parcijalnih uređenja, svaka promenljiva različita od v_0 je slobodna za v_1 u formuli φ.

Ako se interpretira u parcijalnom uređenju, smisao formule $\varphi(v_1)$ je: "v_1 je minimalan element u parcijanom uređenju P." Zamenom promenljive v_1 bilo kojom od promenljivih v_k, koja je raziličita od v_0, dobija se formula $\varphi(v_k)$ koja ima isti smisao kao i formula $\varphi(v_1)$. Međutim, formula $\varphi(v_0) = \neg\exists v_0\, P(v_0, v_1)$ ima sasvim drugo značenje, pa zamena promenljive v_1 promenljivom v_0 u formuli φ nije legitimna.

Primer 4. Neka je $\varphi(x, y) = \exists z\, (y = z \cdot x)$ formula jezika aritmetike. Svaka promenljiva u različita od od promenljivih y i z je slobodna za x u formuli φ.

Semantika

U primerima smo istakli da je svaki jezik predikatskog računa vezan za klasu struktura istog tipa. Tip strukture, odnosno njegove relacije, operacije i konstante determinišu skup nelogičkih simbola jezika $\mathcal{L}$ koji je odgovarajući za datu klasu struktura. Međutim, bez obzira kako je nastao, jezik je sintaktički objekt i može se interpretirati na svakom nepraznom skupu. Kada se njegovi nelogički simboli interpretiraju relacijama, operacijama i konstantama skupa $A \neq \emptyset$, valuacija promenljivih jezika $\mathcal{L}$ elementima skupa A određuje istinosnu vrednost svih njegovih formula.

Neka je $\mathcal{L}$ jezik i A neprazan skup. Ako je P predikatska konstanta dužine $n \geq 1$, *interpretacija* konstante P je relacija R skupa A dužine n. Ako je F operacijska konstanta dužine $n \geq 1$, interpretacija konstante F

je operacija f skupa A dužine n. Interpretacija individualne konstante c je element a skupa A.

Struktura $\mathcal{A}$ čije su sve relacije interpretacije relacijskih konstanti, sve operacije interpretacije operacijskih konstanti i sve konstante interpretacije individualnih konstanti jezika $\mathcal{L}$ je *interpretacija jezika* $\mathcal{L}$ na nepraznom skupu A. Najčešće, umesto o interpretaciji, govorićemo o *modelu jezika* $\mathcal{L}$.

Jasno je da, na istom skupu, jezik može imati više interpretacija. Da bismo odredili smisao njegovih sintaksnih objekata, neophodno je najpre precizirati pravila po kojima se interpretiraju termi i određuje njihova vrednost u modelu jezika $\mathcal{L}$.

Vrednost terma u datom modelu $\mathcal{A}$ zavisi samo od vrednosti promenljivih koje se u njemu javljaju. Jednostavnosti radi, u određivanju vrednosti terma, pretpostavljamo da su zadate vrednosti svih promenljivih, odnosno valuacija promenljivih jezika $\mathcal{L}$ u modelu $\mathcal{A}$.

Ako je $\mathcal{A}$ model jezika $\mathcal{L}$, niz $x \in A^\omega$ je *valuacija promenljivih* jezika $\mathcal{L}$ u modelu $\mathcal{A}$.

Ako je $x = (x_0, x_1, \ldots, x_n, \ldots)$ valuacija i $a \in A$, sa $x(n/a)$ označavamo valuaciju $(x_0, x_1, \ldots, x_{n-1}, a, x_{n+1}, \ldots)$.

Ako je $\mathcal{A}$ model i t term jezika $\mathcal{L}$, *vrednost terma* t u modelu $\mathcal{A}$ za valuaciju $x \in A^\omega$, koju označavamo sa $[t]_x^A$, definišemo indukcijom po složenosti terma t:

(a) za svako $n \in \omega$, $[v_n]_x^A = x_n$,

(b) ako je c individualna konstanta i $a \in A$ njena interpretacija u modelu $\mathcal{A}$, onda je $[c]_x^A = a$,

(c) ako je F operacijska konstanta dužine $n \geq 1$, operacija f njena interpretacija u modelu $\mathcal{A}$ i $t_1, \ldots, t_n$ termi jezika $\mathcal{L}$, onda je

$$[F(t_1, \ldots, t_n)]_x^A = f([t_1]_x^A, \ldots, [t_n]_x^A).$$

Primer 1. Indukcijom po složenosti terma, pokazuje se da za svaku valuaciju $x \in A^\omega$ promenljivih jezika $\mathcal{L}$, svaki term t u modelu $\mathcal{A}$ ima jedinstveno određenu vrednost $[t]_x^A \in A$.

Interpretacija nelogičkih simbola jezika $\mathcal{L}$ u modelu $\mathcal{A}$ i denotacija njegovih terma, omogućava interpretaciju formula jezika $\mathcal{L}$ i određuje njihovu istinitost u modelu $\mathcal{A}$.

Neka je $\mathcal{A}$ model u jeziku $\mathcal{L}$, $x \in A^\omega$ valuacija promenljivih jezika $\mathcal{L}$ i φ formula. Relaciju "*valuacija x zadovoljava formulu φ u modelu $\mathcal{A}$*," koju označavamo sa $\mathcal{A} \models_x \varphi$, definišemo indukcijom po složenosti formule φ:

(a) Ako je φ elementarna formula oblika $t_1 = t_2$, gde su t_1 i t_2 termi jezika $\mathcal{L}$, onda

$$\mathcal{A} \models_x t_1 = t_2 \text{ ako i samo ako } \quad [t_1]^A_x = [t_2]^A_x,$$

(b) ako je φ elementarna formula oblika $P(t_1, \ldots, t_n)$, gde je P relacijska konstanta dužine $n \geq 1$ i $t_1, \ldots, t_n$ termi jezika $\mathcal{L}$, onda

$$\mathcal{A} \models_x P(t_1, \ldots, t_n) \text{ ako i samo ako } ([t_1]^A_x, \ldots, [t_n]^A_x) \in P^A,$$

(c) ako su φ i ψ formule jezika $\mathcal{L}$, onda

$$\mathcal{A} \models_x \neg\varphi \;\text{ ako i samo ako }\; \text{ne važi } \mathcal{A} \models_x \varphi,$$

$$\mathcal{A} \models_x \varphi \to \psi \quad \text{ako i samo ako } \; \mathcal{A} \models_x \varphi \text{ implicira } \mathcal{A} \models_x \psi \text{ i}$$

$$\mathcal{A} \models_x \exists v_n\, \varphi \text{ ako i samo ako postoji } a \in A,\ \mathcal{A} \models_{x(n/a)} \varphi.$$

Ako $\mathcal{A} \models_x \varphi$, kažemo da formula φ *važi u modelu* $\mathcal{A}$ za valuaciju promenljivih $x \in A^\omega$. Uz denotaciju terma, definicija važenja formule može se shvatiti kao neka vrsta rečnika koji, u zadatom kontekstu, prevodi formule jezika $\mathcal{L}$ na neformalni jezik matematike.

Primer 2. Indukcijom po složenosti formule, može se dokazati da istinitost formule, za datu valuaciju, zavisi samo od njenih slobodnih promenljivih.

Preciznije, ako je φ formula, $\mathcal{A}$ model jezika $\mathcal{L}$ i $x, y \in A^\omega$ valuacije takve da za svaku promenljivu v_n koja ima slobodno javljanje u formuli φ, $[v_n]^A_x = [v_n]^A_y$, onda $\mathcal{A} \models_x \varphi$ ako i samo ako $\mathcal{A} \models_y \varphi$.

Kako istinitost formule zavisi samo od njenih slobodnih promenljivih, umesto oznake $\mathcal{A} \models_x \varphi$, kada su sve slobodne promenljive formule φ neke od promenljivih $v_0, \ldots, v_n$, za istinitost formule φ u strukturi $\mathcal{A}$ za valuaciju x upotrebljavaćemo i oznaku $\mathcal{A} \models \varphi[x_0, \ldots, x_n]$.

Neka je Σ skup formula jezika $\mathcal{L}$. Formula φ je *logička posledica* skupa formula Σ, u oznaci $\Sigma \models \varphi$, ako za svaki model $\mathcal{A}$ jezika $\mathcal{L}$ i svaku valuaciju $x \in A^\omega$, važi $\mathcal{A} \models_x \Sigma$ implicira $\mathcal{A} \models_x \varphi$.

Pritom, sa $\mathcal{A} \models_x \Sigma$ označili smo činjenicu da u modelu $\mathcal{A}$, za valuaciju x, važe sve formule skupa Σ.

Formulu bez slobodnih promenljivih nazivamo *rečenicom*. Ako je φ rečenica i $\mathcal{A}$ model jezika $\mathcal{L}$, za svaku valuaciju promenljivih $x \in A^\omega$ važi $\mathcal{A} \models_x \varphi$ ili $\mathcal{A} \models_x \neg\varphi$.

Relaciju "rečenica φ važi u modelu $\mathcal{A}$", odnosno relaciju "$\mathcal{A}$ je model rečenice φ," označavamo sa $\mathcal{A} \models \varphi$.

Model $\mathcal{A}$ jezika $\mathcal{L}$ je model skupa rečenica Σ, u oznaci $\mathcal{A} \models \Sigma$ ako za svaku rečenicu $\varphi \in \Sigma$, važi $\mathcal{A} \models \varphi$.

Rečenica φ je *valjana* ili logička istina predikatskog računa, u oznaci $\models \varphi$, ako φ važi u svakom modelu jezika $\mathcal{L}$. Dakle, rečenica je valjana ako je istinita u svakoj interpretaciji. Istinitost takve rečenice ne zavisi od toga kako smo interpretirali njene nelogičke simbole već isključivo od njene logičke strukture. Ova definicija istinite rečenice u potpunosti odgovara neformalnom pojmu istine koji matematičari inače upotrebljavaju.

Skup valjanih formula predikatskog računa sadrži tautologije. Međutim, za razliku od tautologije, rečenica može imati beskonačno mnogo neizomorfnih modela tako da postupak za proveru njene istinitosti u svim modelima nemamo. Problem odlučivosti predikatskog računa je mnogo suptilniji od iskaznog slučaja. U okviru teorije izračunljivosti, izložićemo rešenje ovog problema i pokazati da uopšte ne postoji algoritam koji za svaku rečenicu φ može proveriti da li φ jeste ili nije logička istina.

U nekim slučajevima, za rečenice određenog tipa, procedura za proveravanje istinitosti ipak postoji. Jedna grupa takvih postupaka zasniva se na sledećim primerima.

Primer 3. Ako je jezik $\mathcal{L}$ konačan, za svako $n \in \omega$ postoji samo konačno mnogo neizomorfnih modela jezika $\mathcal{L}$ kardinalnosti n.

U konačnom modelu $\mathcal{A}$, sa domenom $A = \{a_1, \ldots, a_k\}$, relacija $\mathcal{A} \models \exists v_n \, \varphi$ svodi se na disjunkciju: $\mathcal{A} \models \varphi[a_1]$ ili ... ili $\mathcal{A} \models \varphi[a_n]$. Dakle, u konačnim modelima predikat $\mathcal{A} \models_x \varphi$ može se proveriti u konačno mnogo koraka.

Primer 4. Pretpostavimo da jezik $\mathcal{L}$, kardinalnosti $k \in \omega$, sadrži samo unarne predikatske konstante. Za svaku formulu φ jezika $\mathcal{L}$, $\models \varphi$ ako i samo ako φ važi u svim modelima kardinalnosti $\leq 2^k$.

Za svaku formulu φ, ako je $\mathcal{A} = (A, R_1, \ldots, R_k)$ model jezika $\mathcal{L}$ i $\vec{a} \in A^n$ takvo da $\mathcal{A} \models \neg\varphi[\vec{a}]$, onda postoji model $\mathcal{A}^*$ kardinalnosti $\leq 2^k$ u kojem ne važi formula φ.

Na skupu A definišimo relaciju ekvivalencije $\sim$ tako da za sve $a, b \in A$,

$$a \sim b \quad \Leftrightarrow \quad \text{za svako } i = 1, \ldots, k,\ R_i(a) \text{ ako i samo ako } R_i(b).$$

Postoji najviše 2^k klasa ekvivalencije relacije $\sim$. Takođe, relacija $\sim$ je kongruencija u odnosu na sve relacije $R_1, \ldots, R_n$, pa je na količniku A^* relacije $\sim$ definisan model $\mathcal{A}^*$ jezika $\mathcal{L}$.

Za svaku formulu $\psi(x_1, \ldots, x_m)$ jezika $\mathcal{L}$, indukcijom po njenoj složenosti, neposredno se proverava da za svako $\vec{c} \in A^m$,

$$\mathcal{A} \models \psi[\vec{c}] \quad \Leftrightarrow \quad \mathcal{A}^* \models \psi[\vec{c^*}].$$

Otuda sledi da $\mathcal{A}^* \models \neg\varphi[\vec{a^*}]$ što znači da, ako formula φ ne važi u nekom modelu jezika $\mathcal{L}$, onda postoji model kardinalnosti $\leq 2^k$ u kojem ne važi φ.

Neka su $\mathcal{A}$ i $\mathcal{B}$ modeli jezika $\mathcal{L}$. Model $\mathcal{B}$ je *podmodel* modela $\mathcal{A}$, u oznaci $\mathcal{B} \subseteq \mathcal{A}$, ako su zadovoljeni sledeći uslovi:

(a) domen modela $\mathcal{B}$ je podskup domena modela $\mathcal{A}$,

(b) za svaku relacijsku konstantu P dužine $n \geq 1$, $P^B = P^A \cap B^n$,

(c) za svaku operacijsku konstantu F dužine $n \geq 1$ i svako $\vec{b} \in B^n$, $F^B(\vec{b}) = F^A(\vec{b})$,

(d) skup B sadrži interpretacije svih individualnih konstanti jezika $\mathcal{L}$.

Jednostavnije rečeno, model $\mathcal{B}$ je podmodel modela $\mathcal{A}$ ako $B \subseteq A$, a interpretacije svih konstanti jezika $\mathcal{L}$ u modelu $\mathcal{B}$ se dobijaju kao restrikcije njihovih interpretacija u modelu $\mathcal{A}$ na skup B.

Primer 5. Ako su $\mathcal{A}$ i $\mathcal{B}$ modeli jezika $\mathcal{L}$, $\mathcal{B} \subseteq \mathcal{A}$ ako i samo ako za $B \subseteq A$ i za svaku valuaciju $x \in B^\omega$ i svaku elementarnu formulu φ

$$\mathcal{B} \models_x \varphi \quad \Leftrightarrow \quad \mathcal{A} \models_x \varphi.$$

Primer 6. Ako je $\mathcal{B}$ model jezika $\mathcal{L}$ i $X \subseteq B$ neprazan skup, sledeći uslovi su ekvivalentni:

(a) skup X je domen modela $\mathcal{A} \subseteq \mathcal{B}$,

(b) za svaku konstantu c jezika $\mathcal{L}$, $c^B \in X$ i za svako $n \geq 1$, ako je F operacijska konstanta dužine n i $x_1, \ldots, x_n \in X$, onda $F^A(x_1, \ldots, x_n) \in X$.

Neka je $\mathcal{A}$ model jezika $\mathcal{L}$ i $X \subseteq A$ skup koji, ukoliko jezik $\mathcal{L}$ sadrži bar jednu konstantu, može biti i prazan. Prema prethodnom primeru, skup

$$\langle X \rangle_A = \bigcap \{B : \mathcal{B} \subseteq \mathcal{A} \text{ i } X \subseteq B\}$$

je domen podmodela modela $\mathcal{A}$ koji označavamo sa $\langle X \rangle_\mathcal{A}$. Model $\langle X \rangle_\mathcal{A}$ jedinstveno je određen i naziva se *modelom generisanim skupom* $X \subseteq A$.

Skup $X \subseteq A$ je *skup generatora* modela $\mathcal{A}$ ako $\langle X \rangle_\mathcal{A} = \mathcal{A}$. Ako je skup X konačan, model $\mathcal{A}$ je *konačno generisan*.

Primer 7. Ako je $X \subseteq A$, onda $\langle X \rangle_\mathcal{A} = \{[t]_x^A : t \text{ term u } \mathcal{L} \text{ i } x \in X^\omega\}$, za svaki model $\mathcal{A}$ jezika $\mathcal{L}$. Pritom, $|X| \leq |\langle X \rangle_A| \leq \sup\{|X|, \|\mathcal{L}\|\}$.

Konstrukcija modela $\langle X \rangle_\mathcal{A}$ definisana je u okviru datog modela $\mathcal{A}$ jezika $\mathcal{L}$. Međutim, po ugledu na konstrukciju slobodne algebre, ona se može izvesti i nezavisno od modela jezika $\mathcal{L}$. Ta ideja je izložena u sledećem primeru.

Primer 8. Neka je $X \subseteq V$ skup promenljivih jezika $\mathcal{L}$ koji sadrži bar jednu operacijsku ili individualnu konstantu. Modela $\mathcal{A}$ je *slobodna algebra jezika* $\mathcal{L}$ ako zadovoljava sledeće uslove:

(a) domen A sadrži sve terme jezika čije promenljive pripadaju skupu X,

(b) $c^A = c$, za svaku individualnu konstantu c,

(c) $F^A(t_1, \ldots, t_n) = F(t_1, \ldots, t_n)$, za svaku operacijsku konstantu F dužine $n \geq 1$ i proizvoljne $t_1, \ldots, t_n \in A$,

(d) $P^A = \emptyset$, za svaku relacijsku konstantu P jezika $\mathcal{L}$.

Ako je $\mathcal{A}$ slobodna algebra nad skupom X i $\mathcal{B}$ proizvoljan model jezika $\mathcal{L}$, onda za svaku funkciju $f : X \to B$, postoji jedinstveni homomorfizam $g : A \to B$ koji proširuje funkciju f.

Primer 9. (a) Pretpostavimo da jezik $\mathcal{L}$ sadrži samo predikatska slova i da je $\mathcal{A}$ model jezika $\mathcal{L}$. Za svaki neprazan skup $X \subseteq A$, model $\mathcal{A}$ sadrži podmodel sa domenom X.

(b) Ako $\mathcal{L}$ ne sadrži operacijske konstante, prethodno tvrđenje važi za svaki neprazan skup $X \subseteq A$ koji sadrži sve konstante jezika $\mathcal{L}$.

U oba slučaja, podmodel generisan skupom X dobija se restrikcijom relacija modela $\mathcal{A}$ na X.

Primer 10. Ako je $\mathcal{A} \subseteq \mathcal{B}$ i φ formula bez kvantifikatora, onda za svaku valuaciju $x \in A^\omega$, važi sledeća relacija: $\mathcal{A} \models_x \varphi \quad \Leftrightarrow \quad \mathcal{B} \models_x \varphi$.

Tvrđenje se dokazuje indukcijom po složenosti formule φ. Slučaj elementarnih formula pokriven je definicijom podmodela.

Ako su $x_1, \ldots, x_n \in V$ promenljive jezika $\mathcal{L}$, sa $\forall \vec{x}\, \varphi$ označavamo formulu $\forall x_1 \ldots \forall x_n\, \varphi$. Sličnu oznaku koristimo i u slučaju formule sa nizom egzistencijalnih kvantifikatora.

Primer 11. Rečenica φ jezika $\mathcal{L}$ je *univerzalna* ako postoji formula ψ bez kvantifikatora takva da $\varphi = \forall \vec{x}\, \psi$.

(a) Ako je φ univerzalna rečenica i $\mathcal{A} \subseteq \mathcal{B}$, onda $\mathcal{B} \models \varphi$ implicira $\mathcal{A} \models \varphi$.

(b) Ako je φ univerzalna rečenica i $\mathcal{A}$ model jezika $\mathcal{L}$, onda $\mathcal{A} \models \varphi$ ako i samo ako za svaki konačno generisan podmodel $\mathcal{B} \subseteq \mathcal{A}$, važi $\mathcal{B} \models \varphi$.

Primer 12. Rečenica φ jezika $\mathcal{L}$ je *egzistencijalna* ako postoji formula ψ bez kvantifikatora za koju je $\varphi = \exists \vec{x}\, \psi$.

Za svaku egzistencijalnu rečenicu φ jezika $\mathcal{L}$, ako je $\mathcal{A} \subseteq \mathcal{B}$, onda $\mathcal{A} \models \varphi$ implicira $\mathcal{B} \models \varphi$.

Primer 13. Neka su $n, m \in \omega$, $\vec{x} \in V^n$, $\vec{y} \in V^m$ i φ rečenica jezika $\mathcal{L}$ takva da $\varphi = \exists \vec{x} \forall \vec{y}\, \psi$, za neku formulu ψ koja ne sadrži kvantifikatore, funkcijske simbole i konstante.

(a) Ako rečenica φ ima model, onda φ ima model kardinalnosti $\leq n$.

(b) Rečenica φ je valjana ako i samo ako φ je valjana u svim modelima kardinalnosti $\leq n$.

Tvrđenje važi i pod pretpostavkom da se u formuli φ javlja m različitih konstanti. U tom slučaju, ako φ ima model, onda φ ima model kardinalnosti $\leq m + n$. Međutim, ovo tvrđenje ne važi ako se odbaci i uslov da formula φ ne sadrži operacijske konstante.

Osim standardne matematičke ideje podstrukture ili proširenja strukture, u logici je važna sledeća konstrukcija:

Neka je $\mathcal{A}$ model jezika $\mathcal{L}$. Ako je $\mathcal{L}'$ proširenje jezika $\mathcal{L}$, model $\mathcal{A}$ može se proširiti do modela $\mathcal{A}'$ jezika $\mathcal{L}'$ tako što se novi simboli proširenog jezika interpretiraju kao relacije, funkcije ili konstante skupa A. U tom slučaju model $\mathcal{A}'$ je *ekspanzija modela* $\mathcal{A}$ na jezik $\mathcal{L}'$. Ili obratno, model $\mathcal{A}$ je *redukcija modela* $\mathcal{A}'$ na jezik $\mathcal{L}$.

Na primer, uređeno polje realnih brojeva je ekspanzija grupe realnih brojeva na jezik uređenih polja. Važno je napomenuti da se u ekspanzijama i redukcijama ne menja domen modela.

Ako je proširenje $\mathcal{L}'$ jezika $\mathcal{L}$ dobijeno dodavanjem samo novih konstanti, jezik $\mathcal{L}'$ je *prosto proširenje* jezika $\mathcal{L}$. U tom slučaju, model $\mathcal{A}'$ je jezika $\mathcal{L}'$ je *prosta ekspanzija* modela $\mathcal{A}$ jezika $\mathcal{L}$.

Sintaksa

Zbog semantičke neodlučivosti predikatskog računa, poseban značaj ima činjenica da on ipak ima sintaksu koja potpuno opisuje sve njegove istine. Takva sintaksa omogućava da, polazeći od rekurzivnog skupa aksioma, generišemo sve istine predikatskog računa. Zapravo, to znači da je predikat "$\models \varphi$" parcijalno odlučiv, tj. da postoji program koji proizvodi sve istine predikatskog računa. Ta osobina logiku prvog reda čini bitno različitom od logike drugog reda, odnosno, čini je logikom u pravom smislu te reči.

Aksiome predikatskog računa su sheme, odnosno, skupovi formula jezika $\mathcal{L}$. Podelili smo ih u tri grupe. Prvu grupu čine aksiome iskaznog tipa, drugu aksiome kvantifikatora i treću, aksiome jednakosti.

Formula jezika $\mathcal{L}$ koja se iz formule φ iskaznog računa dobija zamenom svih iskaznih slova formulama jezika $\mathcal{L}$ je *supstituciona instanca* formule φ.

Iskazne aksiome: Supstitucione instance iskaznih aksioma A_1, A_2 i A_3 su aksiome predikatskog računa prvog reda.

Za svaku formulu φ jezika $\mathcal{L}$, u konačno monogo koraka može se utvrditi da li φ pripada skupu A_1, tj. skup aksioma A_1 je rekurzivan. Isto važi i za skupove A_2 i A_3, tj. predikat "formula φ je aksioma iskaznog tipa" je odlučiv.

Primer 1. Svaka supstituciona instanca tautologije je valjana formula.

Prema stavu potpunosti iskaznog računa, budući da sintaksa predikatskog računa sadrži modus ponens kao jedno od pravila, sve substitucione instance tautologija su teoreme predikatskog računa.

Aksiome kvantifikatora: Drugu grupu aksioma, koja karakteriše svojstva kvantifikatora, čine dva skupa formula predikatskog računa.

Ako su φ i ψ formule jezika $\mathcal{L}$ i $x \in V$ promenljiva koja nije slobodna u formuli φ, onda je formula

$$\forall x\,(\varphi \to \psi) \to (\varphi \to \forall x\,\psi)$$

aksioma predikatskog računa prvog reda. Skup svih formula tog oblika označavamo sa A_4.

Za datu formulu φ jezika $\mathcal{L}$, u konačno mnogo koraka može se utvrditi da li formula φ pripada skupu A_4, tj. skup aksioma A_4 je rekurzivan.

Ako je $\varphi(x)$ formula jezika $\mathcal{L}$, term t slobodan za promenljivu $x \in V$ u formuli $\varphi(x)$ i $\varphi(t)$ formula dobijena iz $\varphi(x)$ zamenom svih slobodnih javljanja promenljive x termom t, onda je formula

$$\forall x\,\varphi(x) \to \varphi(t).$$

aksioma predikatskog računa prvog reda. Skup svih formula tog oblika označavamo sa A_5. Jasno, skup aksioma A_5 je rekurzivan.

Primer 2. Ograničenje koje se u odnosu na promenljivu $x \in V$ javlja u aksiomi A_4 je neophodno.

Na primer, neka su skupovi $X, Y \subseteq A$ takvi da $X \subseteq Y$, $X \neq \emptyset$ i $Y \neq A$. Skupove X i Y možemo shvatiti kao unarne relacije $X(x)$ i $Y(x)$ skupa A. Neka je $\mathcal{A} = (A, X, Y)$ model jezika $\mathcal{L}$ koji sadrži unarne relacijske konstante P_1 i P_2. Bez ograničenja na promenljivu $x \in V$, formula

$$\forall x\,(P_1(x) \to P_2(x)) \to (P_1(x) \to \forall x\,P_2(x))$$

bi bila instanca aksiome A_4. Međutim, postoji valuacija promenljivih $a \in A^\omega$ za koju navedena formula ne važi u modelu $\mathcal{A}$. Dovoljno je izabrati valuaciju u kojoj vrednost promenljive x pripada skupu X.

Primer 3. Ograničnje na term t u odnosu na promenljivu x formule φ, koje se javlja u aksiomi A_5, takođe je neophodno.

Na primer, ako predikat P u formuli $\forall x \exists y\, P(x, y) \to \exists y\, P(y, y)$ interpretiramo kao striktno uređenje $<$ prirodnih brojeva, pretpostavka $\forall x \exists y\, P(x, y)$

je tačna, međutim, ne postoji prirodan broj $n \in \omega$ za koji je $n < n$. Dakle, bez navedenog ograničenja, instance sheme aksioma A_5 nisu valjane formule.

Aksiome jednakosti: Poslednju grupu aksioma čine aksiome jednakosti. Kako smo već napomenuli, jednakost uvek interpretiramo na isti način, kao jednakost elemenata domena modela.

Za svaku promenljivu $x \in V$, formula

$$\forall x\,(x = x).$$

je aksioma predikatskog računa. Skup svih formula tog oblika označavamo sa A_6. U ovom slučaju, skup aksioma A_6 indeksiran je skupom individualnih promenljivih. Jasno, skup A_6 je rekurzivan.

Za svaku formulu φ jezika $\mathcal{L}$ u kojoj je promenljiva y slobodna za promenljivu x, ako se formula φ' dobija iz φ zamenom nekih slobodnih javljanja promenljive x u formuli φ, ne obavezno svih, sa promenljivom y, onda je sledeća formula aksioma predikatskog računa:

$$\forall x \forall y\,(x = y \to (\varphi \to \varphi')).$$

Skup svih formula tog oblika označavamo sa A_7. On je takođe rekurzivan i čini završnu grupu aksioma predikatskog računa prvog reda.

Pravila izvođena: Pravila izvođenja pomoću kojih u predikatskom računu generišemo valjane formule su sledeća:

Modus ponens: za proizvoljne formule φ i ψ jezika $\mathcal{L}$, formula φ je neposredna posledica formula ψ i $\psi \to \varphi$,

Generalizacija: za svaku formulu φ i svaku promenljivu $x \in V$, formula $\forall x\,\varphi$ je neposredna posledica formule φ.

Pojam sintaksne posledice u predikatskom računu definiše se u principu isto kao u iskaznom računu. Jedina razlika je u primeni pravila generalizacije u dokazima iz hipoteza. Mi smo ovo pravilo ograničili na promenljive koje se u pretpostavkama ne javljaju kao slobodne promenljive. U primeru koji sledi odmah posle definicije pojma sintaksne posledice, ilustrovana je neophodnost restrikcije na pravilo generalizacije. Napominjemo da se ovaj problem može rešiti i tako što će se teorema dedukcije primenjivati samo na rečenice predikatskog računa.

Neka je Σ skup formula i φ formula jezika $\mathcal{L}$ i $n \geq 1$ prirodan broj. Konačan niz formula $\varphi_1, \ldots, \varphi_n$ je *dokaz formule φ iz pretpostavki* Σ ako $\varphi_n = \varphi$ i za svako $k \leq n$,

(a) φ_k je aksioma predikatskog računa ili
(b) $\varphi_k \in \Sigma$ ili
(c) za neke $i, j < k$, $\varphi_i = \varphi_j \to \varphi_k$ ili
(d) za neko $i < k$, $\varphi_k = \forall x\, \varphi_i$, gde je $x \in V$ promenljiva koja nije slobodna u formulama skupa Σ.

Restrikcija na pravilo generalizacije u dokazima iz hipoteza je zaista neophodna kao što pokazuje sledeći primer.

Primer 4. Ako skup pretpostavki Σ sadrži formulu oblika $x = 0$, neograničenom primenom generalizacije iz pretpostavke $x = 0$ dobija se dokaz formule $\forall x\, (x = 0)$.

U standardnom modelu prirodnih brojeva $\mathcal{N} = (\omega, +, \cdot, \leq, s, 0)$, svaka valuacija promenljivih $a \in \omega^\omega$ za koju je vrednost promenljive x jednaka nuli zadovoljava $x = 0$. Međutim, u modelu $\mathcal{N}$ ne važi formula $\forall x\, (x = 0)$.

Oznake i terminologiju koje smo fiksirali u iskaznom računu upotrebljavaćemo i u predikatskom računu. Tako, $\Sigma \vdash \varphi$ označava dokazivost formule φ iz pretpostavki Σ, a $\vdash \varphi$ označava dokazivost formule φ iz praznog skupa pretpostavki, odnosno, činjenicu da je φ teorema predikatskog računa.

Dokaz iz hipoteza je konačan niz formula. Stoga, ako $\Sigma \vdash \varphi$, onda postoji konačan skup formula $\Sigma_0 \subseteq \Sigma$ takav da $\Sigma_0 \vdash \varphi$.

Primer 3. Jednakost je simetrična i tranzitivna relacija, tj. za proizvoljne promenljive $x, y, z \in V$,

$$\vdash \forall x \forall y\, (x = y \to y = x),$$
$$\vdash \forall x \forall y \forall z\, (x = y \to (y = z \to x = z)).$$

Primer 4. Ako je $\varphi(x_1, \ldots, x_n)$ formula i $t_1, \ldots, t_n$ termi jezika $\mathcal{L}$ takvi da je svaki term t_i slobodan za promenljivu x_i u formuli φ, onda

$$\vdash (x_1 = t_1 \wedge \cdots \wedge x_n = t_n) \to (\varphi(x_1, \ldots, x_n) \to \varphi(t_1, \ldots, t_n)).$$

Primer 5. Neka su P, F i c konstante jezika $\mathcal{L}$ i $x, y, x_1, \ldots, x_n$ proizvoljne promenljive. Formula oblika $x = y$, $x = c$, $F(x_1, \ldots, x_n) = y$ ili $P(x_1, \ldots, x_n)$ je *prosta* formula.

Za svaku formulu φ, postoji formula φ^*, čije su sve elementarne potformule proste, takva da važi $\vdash \varphi \leftrightarrow \varphi^*$.

Na osnovu ovog primera, u dokazima indukcijom po složenosti formule može se pretpostaviti da su sve njene elementarne potformule proste.

Primer 6. Za svaku formulu $\varphi(x_1, \ldots, x_n)$ jezika $\mathcal{L}$, važi

$$\vdash \varphi(x_1, \ldots, x_n) \quad \Leftrightarrow \vdash \forall x_1 \cdots \forall x_n\, \varphi(x_1, \ldots, x_n).$$

Postoji formula φ za koju ne važi $\vdash \varphi \leftrightarrow \forall x_1 \cdots \forall x_n \, \varphi$.

Formula φ jezika $\mathcal{L}$ ima *normalni preneksni oblik* ako postoji formula ψ bez kvantifikatora takva da $\varphi = Q_1 x_1 \cdots Q_n x_n \, \psi$. Pritom, Q_i označava jedan od kvantifikatora $\forall$ ili $\exists$.

Primer 7. S obzirom na negaciju, kvantifikatori zadovoljavaju sledeća pravila: za svaku formulu φ jezika $\mathcal{L}$, važi

$$\vdash \neg \forall x \, \varphi \leftrightarrow \exists x \, \neg \varphi \quad \text{i} \quad \vdash \neg \exists x \, \varphi \leftrightarrow \forall x \, \neg \varphi.$$

Pravila koja kvantifikatori zadovoljavaju u odnosu na binarne logičke veznike ilustrovaćemo odgovarajućim pravilima u odnosu na implikaciju.

Primer 8. Ako promenljiva x nije slobodna u formuli ψ, za proizvoljnu formulu φ jezika $\mathcal{L}$,

$$\begin{aligned} &\vdash (\forall x \, \varphi(x) \to \psi) \leftrightarrow \exists x \, (\varphi(x) \to \psi), \quad \vdash (\exists x \, \varphi(x) \to \psi) \leftrightarrow \forall x \, (\varphi(x) \to \psi), \\ &\vdash (\psi \to \forall x \, \varphi(x)) \leftrightarrow \forall x \, (\psi \to \varphi(x)), \quad \vdash (\psi \to \exists x \, \varphi(x)) \leftrightarrow \exists x \, (\psi \to \varphi(x)). \end{aligned}$$

Pod istim uslovima, slična pravila važe i za ostale logičke veznike. Zapravo, prethodni primeri sugerišu da se svaka formula može transformisati u ekvivalentnu preneksnu normalnu formu.

Teorema 10. Teorema o preneksnoj normalnoj formi: Svaka formula φ ima normalni preneksni oblik φ^* za koji važi relacija: $\vdash \varphi \leftrightarrow \varphi^*$.

Dokaz: Indukcijom po složenosti formule φ. Ako je φ elementarna formula ili formula oblika $\exists \, \psi$, gde je ψ formula u normalnom preneksnom obliku, tvrđenje je trivijalno.

U slučaju formule oblika $\exists x \, \psi$, neposredno koristimo svojstva koja kvantifikatori imaju u odnosu na negaciju.

Ako formula φ ima oblik $\varphi_1 \to \varphi_2$, da bi se omogućila primena pravila kvantifikacije u odnosu na implikaciju, sva vezana javljanja promenljivih treba zameniti promenljivim koje se uopšte ne javljaju u formuli φ. Ta operacija je moguća budući da $\vdash \exists x \, \varphi(x) \leftrightarrow \exists y \, \varphi(y)$, za svaku formulu φ. $\square$

Sintaksu predikatskog računa definisali smo tako da ona generiše samo valjane formule, odnosno, tako da bude saglasna sa njegovom semantikom. Kao u iskaznom slučaju, to predstavlja lakši deo stava potpunosti.

Teorema 11. Teorema saglasnosti predikatskog računa: Za svaki skup rečenica Σ i svaku rečenicu φ jezika $\mathcal{L}$,

$$\Sigma \vdash \varphi \quad \Rightarrow \quad \Sigma \models \varphi.$$

Dokaz: Dokaz ove teoreme izložićemo sa nešto više detalja. Neka $\Sigma \vdash \varphi$. Tada postoji konačan $\Sigma_0 \subseteq \Sigma$ takav da $\Sigma_0 \vdash \varphi$.

Indukcijom po dužini dokaza $\varphi_1, \ldots, \varphi_n$ za φ iz pretpostavki Σ_0, dokazaćemo da za svako $i \leq n$, $\Sigma_0 \models \varphi_i$.

Ako je φ_i supstituciona instanca tautologije, onda $\Sigma_0 \models \varphi_i$. To sledi iz teoreme saglasnosti iskaznog računa.

Neka je $\varphi_i = \forall v_n\, (\psi \to \chi) \to (\psi \to \forall v_n\, \chi)$, gde je v_n promenljiva koja nije slobodna u formuli ψ. Pretpostavimo da je $\mathcal{A}$ model jezika $\mathcal{L}$ takav da za valuaciju $x \in A^\omega$, $\mathcal{A} \models_x \forall v_n\, (\psi \to \chi)$. Prema definiciji relacije zadovoljenja, za svako $a \in A$, $\mathcal{A} \models_{x(n/a)} v_n(\psi \to \chi)$. Otuda, $\mathcal{A} \models_a \psi$ implicira da za svako $a \in A$, $\mathcal{A} \models_{x(n/a)} \chi$, što konačno znači da $\mathcal{A} \models_x \psi \to \forall v_n\, \chi$.

Pretpostavimo da je $\varphi_i = \forall v_n\, \varphi(v_n) \to \varphi(t)$, gde je t term slobodan za promenljivu v_n u formuli φ. Neka je $\mathcal{A}$ model jezika $\mathcal{L}$ i $x \in A^\omega$ valuacija promenljivih u modelu $\mathcal{A}$. Pretpostavimo da važi $\mathcal{A} \models_x \forall v_n\, \varphi(v_n)$. Tada za svako $a \in A$, $\mathcal{A} \models_{x(n/a)} \varphi(v_n)$. Specijalno, ako je $a = [t]_x^{\mathcal{A}}$, prema posledicama aksiome jednakosti, $\mathcal{A} \models_x \varphi(t)$.

Ako je φ_i aksioma jednakosti ili ako je $\varphi_i \in \Sigma_0$, onda $\Sigma_0 \models \varphi_i$.

Pretpostavimo da za neke $j, k < i$, $\varphi_i = \varphi_j \to \varphi_k$. Po induktivnoj pretpostavci $\Sigma_0 \models \varphi_k$ i $\Sigma_0 \models \varphi_j$, tj. ako $\mathcal{A} \models_x \Sigma_0$, onda $\mathcal{A} \models_x \varphi_j$ i $\mathcal{A} \models_x \varphi_k$. Prema definiciji relacije zadovoljenja $\mathcal{A} \models_x \varphi_i$, tj. $\Sigma_0 \models \varphi_i$.

Konačno, pretpostavimo da je $\varphi_i = \forall v_n\, \varphi_j$ za neko $j < i$. Prema definiciji posledice iz hipoteza, promenljiva v_n nije slobodna u Σ_0. Prema definiciji relacije zadovoljenja, za svaki model $\mathcal{A}$ jezika $\mathcal{L}$ i svaku valuaciju $x \in A^\omega$, $\mathcal{A} \models_x \Sigma_0$ implicira da za svako $a \in A$, $\mathcal{A} \models_{x(n/a)} \Sigma_0$. Prema induktivnoj pretpostavci, ako $\mathcal{A} \models_x \Sigma_0$, onda $\mathcal{A} \models_{x(n/a)} \varphi_j$. Kako se promenljiva v_n ne javlja kao slobodna u Σ_0, $\mathcal{A} \models_x \Sigma_0$ implicira $\mathcal{A} \models_x \forall v_n\, \varphi_j$, odnosno, $\Sigma_0 \models \varphi_i$. $\Box$

U sledećim primerima naveden je jedan broj neposrednih posledica teoreme saglasnosti. Njihovi dokazi se, u principu, ne razlikuju od odgovarajućih tvrđenja u iskaznom računu.

Primer 9. Skup rečenica Σ jezika $\mathcal{L}$ je neprotivrečan ako i samo ako svaki konačan podskup od Σ je neprotivrečan.

Primer 10. Neka je φ rečenica i Σ skup rečenica jezika $\mathcal{L}$. Skup rečenica $\Sigma \cup \{\varphi\}$ je neprotivrečan ako i samo ako ne važi $\Sigma \vdash \neg\varphi$.

Primer 11. Ako je Σ maksimalno neprotivrečan skup rečenica i φ, ψ rečenice jezika $\mathcal{L}$, onda:

$\Sigma \vdash \varphi$ ako i samo ako $\varphi \in \Sigma$,
$\varphi \notin \Sigma$ ako i samo ako $\neg\varphi \in \Sigma$,

$\varphi \wedge \psi \in \Sigma$ ako i samo ako $\varphi, \psi \in \Sigma$.

Primer 12. Teorema dedukcije: ako je Σ skup formula i φ, ψ formule jezika $\mathcal{L}$, onda $\Sigma \cup \{\varphi\} \vdash \psi$ ako i samo ako $\Sigma \vdash \varphi \to \psi$.

Primer 13. Ako je term t slobodan za promenljivu x u formuli $\varphi(x)$, onda $\vdash \varphi(t) \to \exists x\, \varphi(x)$.

Primer 14. Neka je Σ skup formula, φ i ψ formule i c konstanta jezika $\mathcal{L}$ koja se ne javlja u Σ, ψ i φ, onda $\Sigma \cup \{\varphi(c)\} \vdash \psi$ implicira $\Sigma \cup \{\exists x\, \varphi(x)\} \vdash \psi$.

Primer 15. Pretpostavimo da se konstanta c ne javlja u Σ. Za svaku formulu φ jezika $\mathcal{L}$, ako $\Sigma \vdash \varphi(c)$, onda $\Sigma \vdash \forall x\, \varphi(x)$.

Primer 16. Za svaku formulu φ, $\vdash \exists x \forall y\, \varphi(x, y) \to \forall y \exists x\, \varphi(x, y)$. U opštem slučaju ne važi $\vdash \forall y \exists x\, \varphi(x, y) \to \exists x \forall y\, \varphi(x, y)$.

Primer 17. Pretpostavimo da formula φ jezika $\mathcal{L}$ ne sadrži operacijske konstante i logičke veznike različite od $\vee$, $\wedge$, $\neg$, $\forall$ i $\exists$. Ako je φ^* formula koja se dobija iz formule φ zamenom svih javljanja $\vee$ sa $\wedge$, $\wedge$ sa $\vee$, $\forall$ sa $\exists$ i $\exists$ sa $\forall$, kao i zamenom svih elementarnih potformula formule φ njihovim negacijama, onda $\vdash \varphi$ ako i samo ako $\vdash \neg\varphi^*$.

Primer 18. Pretpostavimo da formula φ zadovoljava uslove prethodnog primera i da je $\mathcal{A} = (A, R_1, \ldots, R_k, c_1, \ldots, c_m)$ model jezika $\mathcal{L}(\varphi)$. Neka je $\mathcal{A}^* = (A, R_1^*, \ldots, R_k^*, c_1, \ldots, c_m)$ model u kojem je $R_i^* = A^{\gamma(i)} - R_i$, gde je $\gamma(i)$ dužina relacije R_i.

Za svaku valuaciju $x \in A^\omega$, $\mathcal{A} \models_x \varphi$ ako i samo ako $\mathcal{A}^* \models_x \neg\varphi^*$.

Stav potpunosti

Dokaz stava potpunosti za prebrojive jezike predikatskog računa u principu počiva na istoj ideji kao i dokaz potpunosti iskaznog računa. Jedina bitna razlika je u konstrukciji ultrafiltra Lindenbaumove algebre. U ovom slučaju, nije dovoljan samo ultrafilter koji sadrži određen element ove algebre, već to mora biti ultrafilter koji se regularno ponaša u odnosu na kvantifikatore. Ključnu ulogu u konstrukciji takvog ultrafiltra ima teorema Alfreda Tarskog koja tvrdi da za svaku prebrojivu familiju supremuma u Bulovoj algebri postoji ultrafilter kompletan za datu familiju.

U prvom koraku dokazaćemo stav potpunosti za prebrojive jezike, a potom ćemo dati drugi dokaz proširenog stava potpunosti za jezike proizvoljne kardinalnosti. U osnovi prvog dokaza nalazi se ideja bulovsko vrednosnih modela, a u osnovi drugog, ideja imenovanja matematičkih objekata. Drugi dokaz je interesantan jer, iako sasvim jednostavna, ideja imanovanja elemenata domena modela individualnim konstantama predstavlja osnov opšte teorije modela. Takođe, ona je osnov metode forsinga, najmoćnijeg sredstva teorije skupova. Dakle, izlaganje dva dokaza stava potpunosti ima smisla utoliko što svaki od njih ima specifičan značaj u logici.

Na skupu formula F jezika $\mathcal{L}$ definišemo relaciju ekvivalencije $\sim$ tako da $\varphi \sim \psi$ ako i samo ako $\vdash \varphi \to \psi$ i $\vdash \psi \to \varphi$, za proizvoljne formule φ i ψ. Klasu ekvivalencije formule φ označavamo sa $|\varphi|$, a skup svih klasa ekvivalencije sa B_F.

Poredak u B_F definišemo tako da za sve $\varphi, \psi \in F$, $|\varphi| \leq |\psi|$ ako i samo ako $\vdash \varphi \to \psi$. Taj poredak je korektno definisan i struktura $\mathcal{B} = (B_F, \leq)$ je Bulova algebra. Nazivamo je Lindenbaumovom algebrom predikatskog računa. Detalji ove konstrukcije su potpuno isti kao u iskaznom računu, pa ih stoga ovde nećemo ponavljati.

Posebnost Lindenbaumove algebre predikatskog računa, u odnosu na iskazni slučaj, jeste u tome što se u jeziku $\mathcal{L}$ javljaju kvantifikatori. Zapravo, kvantifikatori u algebri $\mathcal{B}$ određuju dve infinitarne parcijalno definisane operacije, što ovu algebru čini komletnom u odnosu na specifične familije elemenata. Iz tih razloga je neophodno precizirati uslove pod kojima se mogu izračunavati vrednosti tih operacija.

Primer 1. Za svako $n \in \omega$ neka je $\varphi(v_0, \ldots, v_{n-1})$ formula jezika $\mathcal{L}$ čije su sve slobodne promenljive neke od promenljivih $v_0, \ldots, v_{n-1}$. Označimo sa B_n skup klasa ekvivalencije formula oblika $\varphi(v_0, \ldots, v_{n-1})$. Za svako $n \in \omega$, na skupu $B_n \subseteq B_F$ određena je podalgebra $\mathcal{B}_n$ Lindenbaumove algebre $\mathcal{B}$. Algebra $\mathcal{B}_0$ je algebra rečenica jezika $\mathcal{L}$.

Primer 2. Neka je Σ skup rečenica jezika $\mathcal{L}$. Saglasno konvenciji koju smo usvojili u iskaznom računu, svaki skup rečenica nazivaćemo teorijom. Neka je $F_\Sigma = \{|\varphi| : \Sigma \models \varphi\}$.

(a) Teorija Σ je neprotivrečna ako i samo ako F_Σ je filter u $\mathcal{B}_0$.

(b) Teorija Σ je neprotivrečna i konačno aksiomatska ako i samo ako F_Σ je glavni filter u $\mathcal{B}_0$.

(c) Teorija Σ je kompletna ako i samo ako F_Σ je ultrafilter u $\mathcal{B}_0$.

(d) Teorija Σ je kompletna i konačno aksiomatska ako i samo ako F_Σ je glavni ultrafilter u $\mathcal{B}_0$.

Primer 3. Važi i obratno, proizvoljan skup $F \subseteq B_0$ određuje teoriju $\Sigma_F = \{\varphi : |\varphi| \in F\}$ jezika $\mathcal{L}$. Pritom, Σ_F i F zadovoljavaju sva svojstva iz prethodnog primera. Dakle, postoji obostrano jednoznačna korespodencija između teorija u jeziku $\mathcal{L}$ i filtera Lindenbaumove algebre $\mathcal{B}_0$.

Isti rezultat bi se dobio da smo u definiciji skupa F_Σ, umesto semantičke, pretpostavili sintaksnu posledicu. To važi bez pozivanja na stav potpunosti.

Kako smo već napomenuli, Lindenbaumova algebra predikatskog računa se značajno ne razlikuje od Lindenbaumove algebre iskaznog računa. Jedina razlika je u tome što se u predikatskom slučaju javljaju formule sa kvantifikatorima, pa se njihova vrednost računa na specifičan način. Zapravo, u Lindenbaumovoj algebri kvantifikatori su predstavljeni parcijalno definisanim infinitarnim operacijama.

Za svaku formulu $\varphi \in F$ neka je $\varphi(v_k/v_n)$ formula koja se iz formule φ dobija u sledeća dva koraka:

(a) zamenom svih vezanih javljanja promenljive v_n promenljivom v_{k+1}, gde je k najveći indeks svih promenljivih koje se javljaju u formuli φ, a zatim

(b) zamenom svih slobodnih javljanja promenljive v_k promenljivom v_n.

Teorema 12. Za svaku formulu φ jezika $\mathcal{L}$

$$|\forall v_k\, \varphi| = \inf\{|\varphi(v_k/v_p)| : p \in \omega\}.$$

Dokaz: Prema aksiomi A_4, $\vdash \forall v_k\, \varphi \to \varphi(v_k/v_p)$. Stoga, za svako $p \in \omega$, $|\forall v_k\, \varphi| \leq |\varphi(v_k/v_p)|$, pa dakle $|\forall v_k\, \varphi| \leq \inf\{|\varphi(v_k/v_p)| : p \in \omega\}$.

Pretpostavimo da je ψ donje ograničenje za $\{|\varphi(v_k/v_p)| : p \in \omega\}$. Ako izaberemo $q \in \omega$ tako da promenljiva v_q nema javljanja u φ i ψ, onda važi $\vdash \psi \to \varphi(v_k/v_q)$. Na osnovu generalizacije i A_5, $\vdash \psi \to \forall v_q\, \varphi(v_k/v_q)$.

Kako, prema aksiomi A_4, $\vdash \forall v_q\, \varphi(v_k/v_q) \to \varphi$ to na osnovu generalizacije i aksiome A_5 dobijamo $\vdash \forall v_q\, \varphi(v_k/v_q) \to \forall v_k\, \varphi$. Konačno, primenom tranzitivnosti implikacije dobija se $\vdash \psi \to \forall v_k\, \varphi$. To znači da je klasa ekvivalencije $|\forall v_k\, \varphi|$ najveće donje ograničenje familije $\{|\varphi(v_k/v_p)| : p \in \omega\}$. $\square$

Primer 4. Iz istih razloga, u slučaju egzistencijalnog kvantifikatora, za svaku formulu φ jezika $\mathcal{L}$, $|\exists v_k\, \varphi| = \sup\{|\varphi(v_k/v_p)| : p \in \omega\}$.

Osim što karakteriše specifičnost strukture Lindenbaumove algebre jezika $\mathcal{L}$, prethodna teorema ima ključnu ulogu u dokazu stava potpunosti predikatskog računa prvog reda. U samoj formulaciji teoreme, nismo pretpostavili nikakvo ograničenje na kardinalnost jezika $\mathcal{L}$. Budući da se dokaz sastoji u konstrukciji modela samo jedne rečenice jezika $\mathcal{L}$, koja sadrži samo konačan broj simbola, pretpostavka o prebrojivosti jezika $\mathcal{L}$ nije potrebna.

Teorema 13. Stav potpunosti: Za svaku rečenicu φ jezika $\mathcal{L}$,

$$\models \varphi \quad \Leftrightarrow \vdash \varphi.$$

Dokaz: Kako je teorema saglasnosti je već dokazana, dovoljno je dokazati da za svaku rečenicuφ, $\models \varphi$ implicira $\vdash \varphi$. Dokazujemo kontrapoziciju tvrđenja. Pretpostavićemo da φ nije teorema i konstruisati model jezika $\mathcal{L}$ u kojem ne važi φ. To će značiti da φ nije valjana formula.

Neka je $\mathcal{L}_\varphi$ jezik rečenice φ. On se sastoji od svih nelogičkih simbola jezika $\mathcal{L}$ koji se javljaju u formuli φ. Kako svaka formula sadrži samo konačno mnogo simbola, $\mathcal{L}_\sigma = \{P_1, \ldots, P_i, F_1, \ldots, F_j, c_1, \ldots, c_k\}$.

Ako nije $\vdash \varphi$, u Lindenbaumovoj algebri jezika $\mathcal{L}_\varphi$ važi $|\varphi| \neq 1$, što znači da mora biti $|\neg\varphi| \neq 0$. Prema prethodnoj teoremi, za proizvoljnu formulu ψ jezika $\mathcal{L}_\varphi$,

$$\text{(a)} \quad |\forall v_k\, \psi| = \inf\{|\psi(v_k/v_p)| : p \in \omega\}.$$

Jezik $\mathcal{L}_\varphi$ je prebrojiv, pa je familija infimuma tipa (a) prebrojiva. Prema teoremi Tarskog, postoji ultrafilter F Lindenbaumove algebre koji čuva familiju (a) i sadrži $|\neg\varphi|$. To znači da za svaku formulu ψ jezika $\mathcal{L}_\varphi$ i svako $k \in \omega$,

$$|\forall v_k\, \psi| \in F \quad \Leftrightarrow \quad \text{za svako } p \in \omega, |\psi(v_k/v_p)| \in F.$$

Prema definiciji kvantifikatora, filter koji čuva infimume tipa (a) takođe čuva i supremume tipa

$$\text{(b)} \quad |\exists v_k\, \psi| = \sup\{|\psi(v_k/v_p)| : p \in \omega\},$$

tj. za svaku formulu ψ jezika $\mathcal{L}_\varphi$,

$$|\exists v_k\, \psi| \in F \quad \Leftrightarrow \quad \text{postoji } p \in \omega, |\psi(v_k/v_p)| \in F.$$

Treba konstruisati model $\mathcal{A}$ jezika $\mathcal{L}_\varphi$ u kojem ne važi rečenica φ. Kako osim sintaksnih objekata na raspolaganju nemamo nikakve druge objekte, prirodno je da takav model konstruišemo od sintaksnog materijala. Na skupu promenljivih V definisaćemo domen takvog modela i u njemu interpretaciju svih nelogičkih simbola jezika $\mathcal{L}_\varphi$.

Intuitivno, svaka formula φ jezika $\mathcal{L}$ određuje element $|\varphi|$ Lindenbaumove algebre $\mathcal{B}_F$. Da bi se od takvog "$\mathcal{B}_F$-vrednosnog" modela dobio standardni "2-vrednosni" model zadate rečenice, neophodna je kompletnost ultrafiltra F u odnosu na familiju supremuma koju u algebri $\mathcal{B}_F$ definišu egzistencijalne kvantifikacije formula jezika $\mathcal{L}$.

Na skupu promenljivih $V = \{v_0, v_1, \ldots\}$ jezika $\mathcal{L}$, definišemo binarnu relaciju $\sim$ tako da za proizvoljne $m, n \in \omega$,

$$v_m \sim v_n \quad \Leftrightarrow \quad |v_m = v_n| \in F.$$

U jednom od ranijih primera pokazali smo da je jednakost relacija ekvivalencije u sintaksičkom smislu, tj. da su refleksivnost, simetričnost i tranzitivnost jednakosti teoreme predikatskog računa. Iz tih razloga, relacija $\sim$ je relacija ekvivalencije.

Za svako $v \in V$ neka je $\widetilde{v} = \{u \in V : v \sim u\}$. Količnik po relaciji $\sim$ je skup $\widetilde{V} = \{\widetilde{v} : v \in V\}$ koji je prebrojiv i nije prazan. Na skupu $\widetilde{V}$ interpretiraćemo sve simbole jezika $\mathcal{L}_\varphi$.

Za svaku konstantu $c \in \mathcal{L}_\varphi$, $\vdash \exists v_0\,(c = v_0)$. Kako ultrafilter F čuva supremume, postoji $k \in \omega$ takvo da je $|c = v_k| \in F$. Interpretacija konstante c je klasa ekvivalencije $\widetilde{v}_k \in \widetilde{V}$.

Neka je G operacijska konstanta jezika $\mathcal{L}_\varphi$ dužine $n \in \omega$. Za proizvoljne $v, v_{i_1}, \ldots, v_{i_n} \in V$ neka je

$$g(\widetilde{v}_{i_1}, \ldots, \widetilde{v}_{i_n}) = \widetilde{v} \quad \Leftrightarrow \quad |G(v_{i_1}, \ldots, v_{i_n}) = v| \in F.$$

Ako je $t = G(v_{i_1}, \ldots, v_{i_n})$ i v_k promenljiva koja nema javljanja u t, onda je $\vdash \exists v_k\,(t = v_k)$, tj. $|\exists v_k\,(t = v_k)| \in F$. Kako ultrafilter F čuva supremume, postoji $m \in \omega$ takvo da $|(t = v_m)| \in F$, tj. $g(\widetilde{v}_{i_1}, \ldots, \widetilde{v}_{i_n}) = \widetilde{v}_m$. Dakle, g je zaista n-arna operacija skupa $\widetilde{V}$. Na osnovu sintaksnih svojstava jednakosti, operacija g je dobro definisana.

Neka je P predikat jezika $\mathcal{L}_\varphi$ dužine $n \in \omega$, neka je R relacija skupa $\widetilde{V}$ definisana tako da za sve $v_{i_1}, \ldots, v_{i_n} \in V$,

$$(\widetilde{v}_{i_1}, \ldots, \widetilde{v}_{i_n}) \in R \quad \Leftrightarrow \quad |P(v_{i_1}, \ldots, v_{i_n})| \in F.$$

Prema osobinama jednakosti, za sve $k \in \{1, \ldots, n\}$, ako $v_{i_k} \sim u_{i_k}$, onda

$$|P(v_{i_1}, \ldots, v_{i_n})| \in F \quad \Leftrightarrow \quad |P(u_{i_1}, \ldots, u_{i_n})| \in F.$$

To znači da je definicija relacije R korektna.

Neka je $\mathcal{A} = (\widetilde{V}, R_1, \ldots, R_i, f_1, \ldots, f_j, c_1, \ldots, c_k)$ model jezika $\mathcal{L}_\varphi$. Za svaku valuaciju $x \in V^\omega$ oblika $x = (x_1, x_2, \ldots)$ neka je $\widetilde{x} \in \widetilde{V}$ valuacija $\widetilde{x} = (\widetilde{x}_1, \widetilde{x}_2, \ldots)$.

Tvrdimo da za svaku formulu $\psi(v_0, \ldots, v_n)$ jezika $\mathcal{L}_\varphi$ i svako $x \in V^\omega$,

$$(*) \quad \mathcal{A} \models_{\widetilde{x}} \psi \quad \Leftrightarrow \quad |\psi(v_0/x_0, \ldots, v_n/x_n)| \in F.$$

Relaciju $(*)$ dokazujemo indukcijom po složenosti formule ψ. Na osnovu aksioma jednakosi, možemo pretpostaviti da su elementarne formule proste što znači da relacija $(*)$ za elementarne formule važi po definiciji.

Ako nije elementarna, formula ψ može imati oblik $\neg\theta$ ili $\theta \to \theta_1$ ili $\exists v_n\, \theta$, za neke formule θ i χ. U prva dva slučaja relacija $(*)$ sledi neposredno iz definicije relacije zadovoljenja i svojstava ultrafiltra.

Pretpostavimo da je ψ oblika $\exists v_n\, \theta$, gde je θ formula čije su slobodne promenljive neke od promenljivih $v_0, \ldots, v_n$. Po definiciji relacije zadovoljenja, $\mathcal{A} \models_{\widetilde{x}} \psi$ ako i samo ako postoji $\widetilde{v} \in \widetilde{V}$, $\mathcal{A} \models_{\widetilde{x}(n/\widetilde{v})} \theta$ ako i samo ako za neko $p \in \omega$, $\mathcal{A} \models_{\widetilde{x}(n/\widetilde{v}_p)} \theta$.

Formula θ je manje složenosti od ψ, pa prema induktivnoj pretpostavci, poslednja relacija važi ako i samo ako postoji $p \in \omega$,

$$|\theta(v_0/x_0, \ldots, v_{n-1}/x_{n-1}, v_n/v_p)| \in F,$$

a kako F čuva supremume, $|\exists v_n \theta\, (v_0/x_0, \ldots, v_{n-1}/x_{n-1}, v_n)| \in F$. Dakle, za svaku formulu ψ važi relacija $(*)$.

Specijalno, kako ultrafilter F sadrži $|\neg\varphi|$, u modelu $\mathcal{A}$ jezika $\mathcal{L}_\varphi$ važi formula $\neg\varphi$. Kako je $\mathcal{L}_\varphi \subseteq \mathcal{L}$, ako se na skupu $\widetilde{V}$ svi simboli iz $\mathcal{L} - \mathcal{L}_\varphi$ interpretiraju sasvim proizvoljno, dobija se model $\mathcal{A}'$ u jeziku $\mathcal{L}$ u kojem važi $\neg\varphi$. To znači da φ nije valjana formula. $\square$

Ako skup rečenica dokazivih u predikatskom računu označimo sa T_d, a skup rečenica valjanih u svim modelima sa T_i, stav potpunosti može se izraziti u obliku $T_d = T_i$.

Ako sa T_ω označimo skup rečenica jezika $\mathcal{L}$ koje su istinite u svim prebrojivim modelima, naš dokaz stava potpunosti zapravo pokazuje da je $T_d = T_\omega = T_i$. Dakle, skup logički valjanih rečenica se svodi na skup logički valjanih rečenica u prebrojivim strukturama.

Primer 5. Neka je Σ skup rečenica u prebrojivom jeziku $\mathcal{L}$. Označimo sa $\mathcal{B}(\Sigma)$ Lindenbaumovu algebru oblika $\mathcal{B}(\Sigma) = \{|\varphi| : \Sigma \vdash \varphi\}$. Ako je Σ neprotivrečan skup rečenica, onda se nad skupom promenljivih predikatskog računa može konstruisati model teorije Σ.

Ovaj primer pokazuje da se konstrukcija modela izložena u dokazu stava potpunosti može se izvesti i u slučaju proširenog stava potpunosti za prebrojive jezike.

Kako smo već napomenuli, ključni korak u izloženom dokazu stava potpunosti je konstrukcija ultrafiltra koji obezbeđuje realizaciju kvantifikovanih formula kao supremuma, odnosno, infimuma u Lindenbaumovoj algebri. Egzistencija takvog filtra pretpostavlja prebrojivost jezika tako da nije odmah jasno kako bi se taj dokaz mogao izvesti u slučaju proširenog stava potpunosti.

Umesto rešenja spomenutog problema, prošireni stav potpunosti za jezike proizvoljne kardinalnosti, a time i stav kompaktnosti predikatskog računa, dokazaćemo Henkinovom metodom konstanti.

Za datu neprotivrečnu teoriju jezika $\mathcal{L}$, dokaz stava potpunosti podrazumeva konstrukciju njenog modela. Ako jezik $\mathcal{L}$ nije prebrojiv, u opštem slučaju za takvu konstrukciju nije dovoljan skup njegovih promenljivih. U takvim okolnostima prirodno je da se jezik proširi dovoljno velikim skupom individualnih konstanti, čiju egzistenciju nalaže data teorija, pa da se na tom skupu izvrši konstrukcija modela.

Neka je Σ skup rečenica i C skup konstanti jezika $\mathcal{L}$. Skup C je *skup svedoka* teorije Σ ako za svaku formulu $\varphi(x)$ jezika $\mathcal{L}$ takvu da $\Sigma \vdash \exists x\, \varphi(x)$, postoji konstanta $c \in C$ takva da $\Sigma \vdash \varphi(x/c)$.

Dokaz proširenog stava potpunosti zasniva se na činjenici da se svaka neprotivrečna teorija može proširiti do neprotivrečne teorije sa unapred zadatim skupom svedoka. Konstrukcija modela izvodi se na skupu svedoka na sličan način na koji smo konstruisali model prebrojivog jezika nad skupom njegovih promenljivih.

U sledećoj teoremi pretpostavljamo da je Σ teorija u jeziku $\mathcal{L}$ i da je C skup novih individualnih konstanti, koje se ne javlju u jeziku $\mathcal{L}$, kardinalnosti $|C| = \|\mathcal{L}\|$. Sa $\mathcal{L}_C$ označavamo prosto proširenje jezika $\mathcal{L}$ skupom C individualnih konstanti.

Teorema 14. Neka je Σ neprotivrečna teorija jezika $\mathcal{L}$ i C skup novih individualnih konstanti kardinalnosti $|C| = \|\mathcal{L}\|$. Teorija Σ ima neprotivrečno proširenje Σ' u jeziku $\mathcal{L}_C$ takvo da je C skup svedoka teorije Σ'.

Dokaz: Pretpostavimo da je $C = \{c_\beta : \beta < \alpha\}$ skup individualnih konstanti koje ne pripadaju jeziku $\mathcal{L}$ kardinalnosti $\|\mathcal{L}\| = \alpha$.

Prema aksiomi izbora, neka je $(\varphi_\beta : \beta < \alpha)$ dobro uređenje svih formula jezika $\mathcal{L}_C$ sa najviše jednom slobodnom promenljivom i $(c_\beta : \beta < \alpha)$ dobro uređenje skupa C. Polazeći od teorije Σ, konstruišemo rastući niz $(\Sigma_\beta : \beta < \alpha)$ neprotivrečnih teorija jezika $\mathcal{L}_C$.

Neka je $\Sigma_0 = \Sigma$. Za svako $\beta < \alpha$, $\Sigma_{\beta+1} = \Sigma_\beta \cup \{\exists x\, \varphi_\beta \to \varphi_\beta(x/c)\}$, gde je c prva konstanta u nizu $(c_\beta : \beta < \alpha)$ koja se ne javlja u Σ_β. Za svaki granični ordinal β neka je $\Sigma_\beta = \bigcup_{\gamma<\beta} \Sigma_\gamma$.

Tvrdimo da je $\Sigma_{\beta+1}$ neprotivrečna teorija. U suprotnom, imali bi smo da $\Sigma_\beta \vdash \neg(\exists x\, \varphi_\beta \to \varphi_\beta(x/c))$, odnosno, $\Sigma_\beta \vdash \exists x\, \varphi_\beta \wedge \neg\varphi_\beta(x/c)$. Po pretpostavci, konstanta c se ne javlja u Σ_β, pa $\Sigma_\beta \vdash \forall x\, (\exists x\, \varphi_\beta \wedge \neg\varphi_\beta(x))$, a to zapravo znači da $\Sigma_\beta \vdash \exists x\, \varphi_\beta \wedge \neg\exists x\, \varphi_\beta(x)$, što je suprotno pretpostavci o neprotivrečnosti teorije Σ_β.

Kada je $\beta < \alpha$ granični ordinal, teorija $\Sigma_\beta = \bigcup_{\gamma<\beta} \Sigma_\gamma$ je neprotivrečna.

Neka je $\Sigma' = \bigcup_{\beta<\alpha} \Sigma_\beta$. Po konstrukciji, teorija Σ' u jeziku $\mathcal{L}_C$ je neprotivrečno proširenje teorije Σ sa skupom svedoka C. $\Box$

U dokazu teoreme o postojanju modela, konstrukcija modela neprotivrečne teorije izvodi se nad skupom njenih svedočkih konstanti. Kako ona u svemu ostalom odgovara konstrukciji modela u dokazu stava potpunosti za prebrojive jezike, ovaj dokaz je izložen sa nešto manje detalja.

Teorema 15. Teorema o postojanju modela: Skup rečenica Σ ima model ako i samo ako Σ je neprotivrečan.

Dokaz: Pretpostavimo da je Σ_C maksimalno neprotivrečno proširenje teorije Σ koje ima skup svedoka C u jeziku $\mathcal{L}_C$. Prema prethodnoj teoremi, takvo proširenje se uvek može napraviti.

Na skupu individualnih konstanti C, definišimo binarnu relaciju $\sim$ tako da za sve $c, d \in C$,

$$c \sim d \iff (c = d) \in \Sigma_C.$$

Relacija $\sim$ je relacija ekvivalencije i neka je $A = \{\widetilde{c} : c \in C\}$ skup njenih klasa ekvivalencije.

Za svaki relacijsku konstantu P jezika $\mathcal{L}$, dužine $n \geq 1$, neka je R relacija skupa A takva da za sve $c_1, \ldots, c_n \in C$,

$$(\widetilde{c}_1, \ldots, \widetilde{c}_n) \in R \iff P(c_1, \ldots, c_n) \in \Sigma_C.$$

Na osnovu sintaksnih svojstava jednakosti, definicija relacije R je korektna.

Za svaku operacijsku konstantu F dužine $n \geq 1$ i sve $c_1, \ldots, c_n \in C$, formula $\exists x\,(F(c_1, \ldots, c_n) = x)$ pripada teoriji Σ_C. Za sve $c, c_1, \ldots, c_n \in C$, neka je

$$f(\widetilde{c}_1, \ldots, \widetilde{c}_n) = \widetilde{c} \iff (F(c_1, \ldots, c_n) = c) \in \Sigma_C.$$

Zbog sintaksnih svojstava jednakosti, definicija operacije f je korektna.

Ako je c individualna konstanta jezika $\mathcal{L}$, kako rečenica $\exists x\,(x = c)$ pripada teoriji Σ_C, neka je $c^A = \widetilde{c}$. Kao i u slučaju operacijske konstante, zbog sintaksnih svojstava jednakosti, interpretacija individualne konstante c je korektna.

Na taj način, na skupu A interpretirani su svi nelogički simboli jezika $\mathcal{L}_C$, odnosno, definisan je model $\mathcal{A}'$ u jeziku $\mathcal{L}_C$. Pokazaćemo da je tako dobijeni model prosta ekspanzija modela teorije Σ.

Tvrdimo da za svaku rečenicu φ jezika $\mathcal{L}_C$ važi sledeća relacija:

$$\mathcal{A}' \models \varphi \quad \Leftrightarrow \quad \varphi \in \Sigma_C.$$

Zanimljivo je da se ovo tvrđenje, zbog maksimalne neprotivrečnosti skupa Σ_A, može dokazati indukcijom po složenosti rečenice φ. U ovoj indukciji, jedini slučaj koji zahteva objašnjenje jeste induktivni korak $\varphi = \exists x\, \psi$.

Pretpostavimo da u modelu $\mathcal{A}'$ važi formula $\exists x\, \psi$. Po definiciji relacije zadovoljenja, postoji $c \in C$ takvo da $\mathcal{A}' \models \psi\, [\widetilde{c}]$. To znači da $\mathcal{A}' \models \psi(x/c)$, pa prema induktivnoj pretpostavci, $\psi(x/c) \in \Sigma_C$. Zbog $\vdash \psi(x/c) \rightarrow \exists x\, \psi$, dobijamo da $\varphi \in \Sigma_C$.

Obratno, ako $\varphi \in \Sigma_C$, kako Σ_C ima svedoke u C, postoji $c \in C$ takvo da $\Sigma_C \vdash \exists x\, \psi \rightarrow \psi(x/c)$. Kako je Σ_C maksimalno neprotivrečna teorija, imamo $\psi(x/c) \in \Sigma_C$, pa prema induktivnoj pretpostavci, $\mathcal{A}' \models \psi(x/c)$. To znači da postoji $c \in C$ takvo da $\mathcal{A}' \models \psi[\widetilde{c}]$, tj. $\mathcal{A}' \models \varphi$.

Dakle, $\mathcal{A}'$ je model teorije Σ_C u jeziku $\mathcal{L}_C$. Redukcijom jezika $\mathcal{L}_C$ na jezik $\mathcal{L}$ dobijamo model $\mathcal{A}$ jezika $\mathcal{L}$ u kojem važi Σ. $\Box$.

Teorema o postojanju modela ima izvanredno značajne i zanimljive posledice. Njegovu snagu neposredno izražava sama konstrukcija modela nad svedočkim konstantama date teorije. Ona je prisutna u osnovi većine modelsko-teorijskih rezultata.

Primer 6. Prošireni stav potpunosti: Za svaki skup rečenica Σ i svaku rečenicu φ jezika $\mathcal{L}$,

$$\Sigma \models \varphi \quad \Leftrightarrow \quad \Sigma\varphi.$$

Sledeća posledica teoreme o postojanju modela je jedna verzija donje Skolemove teoreme o kojoj ćemo kasnije govoriti.

Primer 7. Svaka neprotivrečna teorija jezika $\mathcal{L}$ ima model čija je kardinalnost manja ili jednaka kardinalnosti jezika $\mathcal{L}$.

Sledeća posledica teoreme o postojanju modela je stav kompaktnosti predikatskog računa za teorije proizvoljne kardinalnosti.

Primer 8. Stav kompaktnosti: Skup rečenica Σ ima model ako i samo ako svaki konačan podskup skupa Σ ima model.

Ako svaki konačan podskup skupa Σ ima model, onda je svaki njegov konačan podskup neprotivrečan. Dakle, Σ je neprotivrečan, pa prema stavu potpunosti, Σ ima model. $\Box$

U daljim izlaganjima, kada se pozivamo na stav potpunosti, podrazumevamo jednu od njegovih ekvivalentnih varijanti, teoremu o postojanju modela ili prošireni stav potpunosti.

Elementarna ekvivalencija

Osnovna ideja u algebarskim konstrukcijama, kao što su podalgebre, homomorfizmi i razne vrste proizvoda, jeste očuvanje algebarske strukture nad kojom se takva konstrukcija izvodi. Isto važi i za sve druge matematičke strukture, relacijske ili relacijsko operacijske. U teoriji modela takve konstrukcije podrazumevaju očuvanje svih svojstava izraženih u jeziku strukture, odnosno svih formula jezika $\mathcal{L}$.

Na primer, ako su $\mathcal{A}$ i $\mathcal{B}$ modeli jezika $\mathcal{L}$, onda: $\mathcal{A}$ je podmodel modela $\mathcal{B}$ ako i samo ako za svaku elementarnu formulu φ jezika $\mathcal{L}$ i svaku valuaciju $x \in A^\omega$ važi $\mathcal{A} \models_x \varphi$ ako i samo ako $\mathcal{B} \models_x \varphi$.

Umesto samo o elementarnim, u teoriji modela vodimo računa o svim formulama predikatskog računa. Ako se to ima u vidu, algebru možemo shvatiti kao deo teorije modela, odnosno, kao elementarnu teoriju modela. Isti odnos postoji između aritmetike i modelsko-teorijske aritmetike ili između analize i modelsko-teorijske analize.

Sasvim uopšteno rečeno, teorija modela se bavi odnosom matematičkih struktura i jezika u kojima izražavamo njihova svojstva. Ključni pojam u toj teoriji jeste elementarna ekvivalencija. Sa stanovišta teorije modela dve strukture su iste ako imaju ista svojstva izražena u predikatskom računu prvog reda, tj. ako zadovoljavaju iste rečenice.

Modeli $\mathcal{A}$ i $\mathcal{B}$ jezika $\mathcal{L}$ su *elementarno ekvivalentni*, u oznaci $\mathcal{A} \equiv \mathcal{B}$, ako za svaku rečenicu φ jezika $\mathcal{L}$, $\mathcal{A} \models \varphi$ implicira $\mathcal{B} \models \varphi$.

Elementarna ekvivalencija je relacija ekvivalencije. Ako su $\mathcal{A}$ i $\mathcal{B}$ elementarno ekvivalentni modeli jezika $\mathcal{L}$, za svaku rečenicu φ jezika $\mathcal{L}$, $\mathcal{A} \models \varphi$ ako i samo ako $\mathcal{B} \models \varphi$.

Ako je $\mathcal{A}$ model jezika $\mathcal{L}$, sa $\mathrm{Th}(\mathcal{A})$ označavamo skup svih rečenica jezika $\mathcal{L}$ koje važe u modelu $\mathcal{A}$. Teorija $\mathrm{Th}(\mathcal{A})$ je kompletna teorija. Pritom, $\mathrm{Th}(\mathcal{A}) = \mathrm{Th}(\mathcal{B})$ ako i samo ako $\mathcal{A} \equiv \mathcal{B}$.

Neka su $\mathcal{A}$ i $\mathcal{B}$ modeli jezika $\mathcal{L}$. Preslikavanje $h : A \to B$ je *homomorfizam modela* $\mathcal{A}$ u model $\mathcal{B}$, u oznaci $h : \mathcal{A} \to \mathcal{B}$, ako:

(a) za sve $a_1, \ldots, a_n \in A$,
$$(a_1, \ldots, a_n) \in R \ \Rightarrow\ (h(a_1), \ldots, h(a_n)) \in S,$$
(b) za sve $a, a_1, \ldots, a_n \in A$,
$$f(a_1, \ldots, a_n) = a \ \Rightarrow\ g(h(a_1), \ldots, h(a_n)) = h(a),$$
(c) za svaku konstantu c jezika $\mathcal{L}$, $h(c^A) = c^B$.

Pritom, podrazumevamo da su R i S interpretacije predikata jezika $\mathcal{L}$ u modelu $\mathcal{A}$, odnosno u modelu $\mathcal{B}$, a f i g odgovarajuće interpretacije operacijskih simbola jezika $\mathcal{L}$.

Kao i u slučaju podmodela, preslikavanje $h : A \to B$ je homomorfizam modela $\mathcal{A}$ u model $\mathcal{B}$ ako i samo ako za svaku elementarnu formulu φ i svaku valuaciju $x \in A^\omega$.

$$\mathcal{A} \models_x \varphi \quad \Rightarrow \quad \mathcal{B} \models_{h(x)} \varphi.$$

Pritom, za svako $x \in A^\omega$, $h(x) = (h(x_0), \ldots, h(x_n), \ldots) \in B^\omega$.

Homomorfizam $h : \mathcal{A} \to \mathcal{B}$ je *izomorfizam* ako je preslikavanje h^{-1} homomorfizam. Modeli $\mathcal{A}$ i $\mathcal{B}$ su izomorfni, u oznaci $\mathcal{A} \cong \mathcal{B}$, ako postoji izomorfizam modela $\mathcal{A}$ u model $\mathcal{B}$.

Homomorfizam h je *utapanje* ako $\mathcal{A} \cong h[\mathcal{A}]$, odnosno. ako za svaku elementarnu formulu φ jezika $\mathcal{L}$ za svaku valuaciju $x \in A^\omega$,

$$\mathcal{A} \models_x \varphi \quad \Leftrightarrow \quad \mathcal{B} \models_{h(x)} \varphi.$$

Primer 1. Neka je $X \subseteq A$ skup koji generiše model $\mathcal{A}$. Ako je f obostrano jednoznačna funkcija skupa X u model $\mathcal{B}$, onda postoji najviše jedno izomorfno utapanje modela $\mathcal{A}$ u model $\mathcal{B}$ koje proširuje funkciju f.

Kako smo ranije naglasili, ako je $\mathcal{A} \subseteq \mathcal{B}$ i φ formula bez kvantifikatora, za svaku valuaciju $x \in A^\omega$,

$$\mathcal{A} \models_x \varphi \quad \Leftrightarrow \quad \mathcal{B} \models_x \varphi.$$

Ako navedena ekvivalencija važi za sve formule jezika $\mathcal{L}$, $\mathcal{A}$ je *elementarni podmodel* modela $\mathcal{B}$, odnosno $\mathcal{B}$ je *elementarna ekstenzija* modela $\mathcal{A}$. Ovu relaciju označavamo sa $\mathcal{A} \preceq \mathcal{B}$.

Utapanje h modela $\mathcal{A}$ u model $\mathcal{B}$ je *elementarno utapanje* ako za svaku formulu φ i svaku valuaciju $x \in A^\omega$,

$$\mathcal{A} \models_x \varphi \quad \Leftrightarrow \quad \mathcal{B} \models_{h(x)} \varphi.$$

Primer 2. Ako je $\mathcal{A} \subseteq \mathcal{B}$, onda $\mathcal{A} \preceq \mathcal{B}$ ako i samo ako inkluzija $i : A \to B$ je elementarno utapanje modela $\mathcal{A}$ u model $\mathcal{B}$.

Kako smo već naglasili, osnovni pojam u teoriji modela jeste elementarna ekvivalencija. Međutim, relacija $\equiv$ je definisana u odnosu na rečenice jezika $\mathcal{L}$ koje, osim u izuzetnim slučajevima, ne dopuštaju indukciju po složenosti. Sa druge strane, budući da je definisana u odnosu na sve formule jezika $\mathcal{L}$, relacija $\preceq$ je mnogo operativnija od elementarne ekvivalencije.

Svakako, iako sasvim bliske, elementarna ekvivalencija $\equiv$ i elementarni podmodel $\preceq$ su ipak različite relacije. Ako $\mathcal{A} \preceq \mathcal{B}$, onda $\mathcal{A} \equiv \mathcal{B}$, ali obratno ne važi. U narednim primerima ilustrovaémo odnos ovih relacija.

Primer 3. Izomorfni modeli su elementarno ekvivalentni. Izomorfizam f modela $\mathcal{A}$ i $\mathcal{B}$ je elementarno utapanje, tj. za svaku formulu φ jezika $\mathcal{L}$ i svaku valuaciju $x \in A^\omega$,

$$\mathcal{A} \models_x \varphi \quad \Leftrightarrow \quad \mathcal{B} \models_{f(x)} \varphi.$$

Ova činjenica se dokazuje indukcijom po složenosti formule φ. Slučaj elementarnih formula pokriven je definicijom elementarnog utapanja.

Primer 4. (a) Postoje elementarno ekvivalentni modeli iste kardinalnosti koji nisu izomorfni.

(b) Postoje izomorfni modeli $\mathcal{A}$ i $\mathcal{B}$ takvi da $\mathcal{B} \subseteq \mathcal{A}$ i nije $\mathcal{B} \preceq \mathcal{A}$.

Ako je $\mathcal{A} = (\omega, <)$ i $\mathcal{B} = (\omega^+, <)$, gde je ω^+ skup pozitivnih prirodnih brojeva, onda $\mathcal{B} \subseteq \mathcal{A}$ i $\mathcal{B} \cong \mathcal{A}$.

Neka je $\varphi(v_0) = \exists v_1\, (v_1 < v_0)$. Jedinica u skupu ω ima prethodnika, pa $\mathcal{A} \models \varphi\,[1]$. Sa druge strane, u ω^+ jedinica nema prethodnika, pa $\mathcal{B} \models \neg\varphi\,[1]$. Dakle, nije $\mathcal{B} \preceq \mathcal{A}$.

Teorema 16. Teorema o elementarnom podmodelu: Neka je $\mathcal{A} \subseteq \mathcal{B}$. Model $\mathcal{A}$ je elementarni podmodel modela $strukB$ ako i samo ako za svaku formulu φ i svaku valuaciju promenljivih $x \in A^\omega$,

$$\mathcal{B} \models_x \exists v_n\, \varphi \quad \Rightarrow \quad \text{za neko } a \in A,\ \mathcal{B} \models_{x(n/a)} \varphi.$$

Dokaz: Pretpostavimo da je $\mathcal{A} \preceq \mathcal{B}$. To znači da za svaku valuaciju $x \in A^\omega$, ako $\mathcal{B} \models_x \exists v_n\, \varphi$, onda $\mathcal{A} \models_x \exists v_n\, \varphi$, pa prema definiciji relacije zadovoljenja, postoji $a \in A$ takvo da $\mathcal{A} \models_{x(n/a)} \varphi$. Zbog $\mathcal{A} \preceq \mathcal{B}$, postoji $a \in A$ takvo da $\mathcal{B} \models_{x(n/a)} \varphi$.

Obratno, pretpostavimo da za svaku formulu φ i svaku valuaciju $x \in A^\omega$, $\mathcal{B} \models_x \exists v_n\, \varphi$ implicira da postoji $a \in A$, $\mathcal{B} \models_{x(n/a)} \exists\, \varphi$. Treba dokazati da je $\mathcal{A} \preceq \mathcal{B}$, odnosno, po definiciji relacije $\preceq$, treba dokazati da za svaku formulu φ i svako $x \in A^\omega$,

$$(*) \qquad \mathcal{B} \models_x \varphi \quad \Leftrightarrow \quad \mathcal{A} \models_x \varphi.$$

Relaciju $(*)$ dokazujemo indukcijom po složenosti formule φ. Ako je φ elementarna formula, relacija $(*)$ važi zbog pretpostavke $\mathcal{A} \subseteq \mathcal{B}$.

U induktivnom koraku, jedini netrivijalan slučaj jeste slučaj formule oblika $\varphi = \exists v_n\, \psi$.

Ako $\mathcal{A} \models_x \exists v_n \psi$, postoji $a \in A$ takvo da $\mathcal{A} \models_{x(n/a)} \psi$. Prema induktivnoj pretpostavci, relacija $(*)$ važi u slučaju formule ψ, pa dakle $\mathcal{B} \models_{x(n/a)} \psi$, odnosno, $\mathcal{B} \models_x \exists v_n \psi$.

Ako $\mathcal{B} \models_x \exists v_n \psi$, onda prema pretpostavci teoreme, postoji $a \in A$ takvo da $\mathcal{B} \models_{x(n/a)} \psi$. Kako po induktivnoj pretpostavci važi $\mathcal{A} \models_{x(n/a)} \psi$, konačno dobijamo $\mathcal{A} \models_x \exists v_n \psi$. $\square$

Dakle, podmodel $\mathcal{A}$ modela $\mathcal{B}$ je elementarni podmodel ako i samo ako za svaku formulu $\varphi(v_0, \ldots, v_n)$ jezika $\mathcal{L}$ i sve $a_0, \ldots, a_{n-1} \in A$, ako postoji $b \in B$ takvo da $\mathcal{B} \models \varphi\,[a_0, \ldots, a_{n-1}, b]$, onda postoji $a \in A$ takvo da $\mathcal{B} \models \varphi\,[a_0, \ldots, a_{n-1}, a]$.

Primer 5. Neka je $\mathcal{A} = (Q, \leq)$ uređenje racionalnih i $\mathcal{B} = (R, \leq)$ uređenje realnih brojeva. Dokazaćemo da je $\mathcal{A} \preceq \mathcal{B}$, a to znači i da je $\mathcal{A} \equiv \mathcal{B}$.

Pretpostavimo da je φ formula jezika $\mathcal{L} = \{<\}$ sa slobodnim promenljivim $v_0, \ldots, v_n$ takva da za neke $a_0, \ldots, a_{n-1} \in Q$ i $b \in R$,

$$\mathcal{B} \models \varphi\,[a_0, \ldots, a_{n-1}, b].$$

Ne umanjujući opštost, možemo pretpostaviti da je $a_0 < \cdots < a_{n-1}$ i $a_k < b < a_{k+1}$, za neko $k + 1 \leq n - 1$. Neka je $c \in Q$ takvo da $a_k < c < a_{k+1}$ i h izomorfizam uređenja $\mathcal{B}$ za koji je $h(a_i) = a_i$, $0 \leq i \leq n - 1$ i $h(b) = c$. Kako je svaki izomorfizam je elementarno utapanje imamo

$$\mathcal{B} \models \varphi\,[h(a_0), \ldots, h(a_{n-1}), h(b)] \quad \Leftrightarrow \quad \mathcal{B} \models \varphi\,[a_0, \ldots, a_{n-1}, c].$$

Prema prethodnoj teoremi $\mathcal{A} \preceq \mathcal{B}$, odnosno, kao uređenja, realni i racionalni brojevi su elementarno ekvivalentni.

Primer 6. Kao uređena grupa $(Q, +, \leq, 0)$, racionalni brojevi su elementarni podmodel uređene grupe $(R, +, \leq 0)$ realnih brojeva.

Primer 7. Neka je (S) sistem linearnih jednačina i nejednačina nad racionalnim brojevima. Sistem (S) ima rešenje u racionalnim brojevima ako i samo ako (S) ima rešenje u realnim brojevima.

Primer 8. Kao polje, racionalni brojevi $\mathcal{Q}$ nisu elementarno ekvivalentni polju $\mathcal{R}$ realnih brojeva.

Proširivanje jezika imenima jednog niza elemenata domena modela omogućava da njihove odnose u datom modelu zapišemo rečenicama i eventualno sačuvamo u modelsko-teorijskim konstrukcijama. Iako sasvim jednostavna, procedura imenovanja u principu pretpostavlja jedan oblik principa izbora. Ako svakom elementu modela treba pridružiti ime, jasno je da to u opštem slučaju podrazumeva princip dobrog uređenja ili aksiomu izbora. Svakako, radimo u metateoriji koja sadrži takve principe.

Neka je $\mathcal{A}$ model jezika $\mathcal{L}$ i $a = (a_\beta : \beta < \alpha)$ niz elemenata skupa $\mathcal{A}$ dužine α, tj. $a \in A^\alpha$. Pritom, α je ordinal, odnosno, tip linearnog dobrog uređenja. Sa $\mathcal{L}_\alpha$ označavamo prosto proširenje jezika $\mathcal{L}$ nizom različitih konstanti $(c_\beta : \beta < \alpha)$. Za svako $\beta < \alpha$, konstantu c_β interpretiramo elementom a_β.

Ako je $\mathcal{B}$ model jezika $\mathcal{L}$ sa $(\mathcal{B}, a)$ označavamo model jezika $\mathcal{L}_\alpha$ koji se iz $\mathcal{B}$ dobija interpretacijom konstanti $(c_\beta : \beta < \alpha)$ elementima modela $\mathcal{B}$.

Model $(\mathcal{B}, a)$ je prosta ekspanzija modela $\mathcal{B}$. Kako smo ranije napomenuli, ekspanzija ne menja domen modela.

Teorema 17. Ako je $\mathcal{A}$ podmodel modela $\mathcal{B}$ i β proizvoljan ordinal, sledeći uslovi su ekvivalentni:

(a) $\mathcal{A} \preceq \mathcal{B}$,

(b) za svako $a \in A^\beta$, $(\mathcal{A}, a) \preceq (\mathcal{B}, a)$,

(c) za svako $a \in A^\beta$, $(\mathcal{A}, a) \equiv (\mathcal{B}, a)$,

(d) za svako $a \in A^\beta$, $\beta < \omega$, $(\mathcal{A}, a) \equiv (\mathcal{B}, a)$,

Dokaz: U prvom slučaju, $\mathcal{A}$ je elementarni podmodel modela $\mathcal{B}$ u smislu jezika $\mathcal{L}$, a u preostala tri slučaja elementarni podmodel i elementarna ekvivalencija se odnose na jezik $\mathcal{L}_\beta$.

Pretpostavimo da je $\mathcal{A} \preceq \mathcal{B}$. Neka je β ordinal, $a \in A^\beta$ i φ formula jezika $\mathcal{L}_\beta$. Pretpostavimo da za neku valuaciju $b \in A^\omega$, $(\mathcal{A}, a) \models_b \varphi$.

Ne umanjujući opštost, pretpostavimo da φ sadrži samo jednu konstantu c_γ, $\gamma < \beta$, jezika $\mathcal{L}_\beta$. Neka je v_k promenljiva koja se ne javlja u formuli φ i neka je φ^* formula koja se dobija iz formule φ zamenom svih javljanja konstante c_γ promenljivom v_k. Tako dobijena formula φ^* jeste formula u $\mathcal{L}$.

Kako je sa a_γ interpretirana konstanta c_γ, $(\mathcal{A}, a) \models_{b(k/a_\gamma)} \varphi^*$. Formula φ^* je formula jezika $\mathcal{L}$, pa $\mathcal{A} \models_{b(k/a_\gamma)} \varphi^*$. Iz pretpostavke da je $\mathcal{A} \preceq \mathcal{B}$ sledi da $\mathcal{B} \models_{b(k/a_\gamma)} \varphi^*$, pa dakle $(\mathcal{B}, a) \models_b \varphi$.

Očigledno, (b) implicira (c) i (c) implicira (d).

Pretpostavimo da važi uslov (d). Neka je φ formula jezika $\mathcal{L}$ i $b \in A^\omega$ valuacija takva da $\mathcal{A} \models_b \varphi$. Zamenimo sve različite slobodne promenljive $v_{i_1}, \ldots, v_{i_n}$ formule φ redom konstantama $c_1, \ldots, c_n$. Tako dobijena formula φ^* je rečenica jezika $\mathcal{L}_{n+1}$. Neka je $b^* = (b_{i_1}, \ldots, b_{i_n})$ niz elemenata domena $\mathcal{A}$ dobijen iz valuacije b. Ako konstante $c_1, \ldots, c_n$ interpretiramo redom elementima $b_{i_1}, \ldots, b_{i_n}$, onda $(\mathcal{A}, b^*) \models \varphi^*$. Prema uslovu (d), $(\mathcal{B}, b^*) \models \varphi^*$, pa dakle $\mathcal{B} \models_b \varphi$. $\square$

Neka je A proizvoljan skup i α ordinal. Niz $a \in A^\alpha$ je *numeracija* skupa A ako se svaki njegov element bar jednom javlja u nizu $a \in A^\alpha$.

Ako je A domen modela $\mathcal{A}$ jezika $\mathcal{L}$, numeracijom elemenata skupa A svaki njegov element $x \in A$ je u proširenom jeziku $\mathcal{L}_\alpha$ dobio svoje ime c_x. Ako je $a \in A^\alpha$ numeracija bez ponavljanja, svaki element je dobio tačno jedno ime.

Teorema 18. Neka su $\mathcal{A}$ i $\mathcal{B}$ modeli jezika $\mathcal{L}$ i $a \in A^\alpha$ numeracija skupa $\mathcal{A}$. Model $\mathcal{A}$ može se elementarno utopiti u $\mathcal{B}$ ako i samo ako postoji niz $b \in B$ takav da, u proširenom jeziku $\mathcal{L}_\alpha$, $(\mathcal{A}, a) \equiv (\mathcal{B}, b)$.

Dokaz: Neka je $h : \mathcal{A} \to \mathcal{B}$ elementarno utapanje. Niz $b \in B^\alpha$ definišemo tako da za svako $\gamma < \alpha$, $b_\gamma = h(a_\gamma)$. Kako je h elementarno utapanje to mora biti $(\mathcal{A}, a) \equiv (\mathcal{B}, b)$.

Obratno, neka je niz $b \in B^\alpha$ takav da $(\mathcal{A}, a) \equiv (\mathcal{B}, b)$. Za svako $\gamma < \alpha$, neka je $h(a_\gamma) = b_\gamma$. Preslikavanje h je elementarno utapanje modela $\mathcal{A}$ u model $\mathcal{B}$. $\square$

Primer 9. Ako su $\mathcal{A}$ i $\mathcal{B}$ modeli jezika $\mathcal{L}$ iste kardinalnosti i $a \in A^\alpha$ numeracija skupa A, onda

(a) ako $\mathcal{A} \cong \mathcal{B}$, onda postoji $b \in B^\alpha$ takvo da $(\mathcal{A}, a) \equiv (\mathcal{B}, b)$
(b) ako je $b \in B^\alpha$ numeracija i $(\mathcal{A}, a) \equiv (\mathcal{B}, b)$, onda je $\mathcal{A} \cong \mathcal{B}$,
(c) ako $\mathcal{A} \subseteq \mathcal{B}$, onda $\mathcal{A} \preceq \mathcal{B}$ ako i samo ako $(\mathcal{A}, a) \equiv (\mathcal{B}, a)$.

Primer 10. Ako su $\mathcal{A}$ i $\mathcal{B}$ elementarno ekvivalentni modeli konačne kardinalnosti, onda $\mathcal{A} \cong \mathcal{B}$.

Neka je $\mathcal{A}$ model jezika $\mathcal{L}$ i $a \in A^\alpha$ numeracija skupa A. Teorija $\mathrm{Th}(\mathcal{A}, a)$ je *dijagram* modela $\mathcal{A}$. Zapravo, dijagram modela $\mathcal{A}$ je skup svih rečenica jezika $\mathcal{L}_\alpha$ koje važe u modelu $(\mathcal{A}, a)$.

Skup Δ_A svih elementarnih rečenica i negacija elementarnih rečenica jezika $\mathcal{L}_\alpha$ koje važe u modelu $(\mathcal{A}, a)$ je *elementarni dijagram* modela $\mathcal{A}$.

Skup svih elementarnih rečenica jezika $\mathcal{L}_\alpha$ koje važe u modelu $(\mathcal{A}, a)$ je *pozitivni elementarni dijagram* modela $\mathcal{A}$, u oznaci Δ_A^+.

Teorema 19. Teorema o elementarnom utapanju: Model $\mathcal{A}$ može se elementarno utopiti u model $\mathcal{B}$ ako i samo ako postoji ekspanzija modela $\mathcal{B}$ koja je model elementarnog dijagrama modela $\mathcal{A}$.

Dokaz: Neka je $h : \mathcal{A} \to \mathcal{B}$ elementarno utapanje. Za svaku numeraciju $a \in A^\alpha$ važi $(\mathcal{A}, a) \equiv (\mathcal{B}, h(a))$, pa je $(\mathcal{B}, h(a))$ model za Δ_A.

Obratno, neka je $a \in A^\alpha$ numeracija skupa A i $(\mathcal{B}, b)$ model jezika $\mathcal{L}_\alpha$ koji zadovoljava elementarni dijagram modela $\mathcal{A}$. Za svako $\beta < \alpha$, neka je $h(a_\beta) = b_\beta$. Homomorfizam h je elementarno utapanje modela $\mathcal{A}$ u $\mathcal{B}$. $\square$

Primer 11. Pretpostavimo da jezik $\mathcal{L}$ ne sadrži operacijske simbole i konstante. Neka je Σ teorija i $\mathcal{A}$ model jezika $\mathcal{L}$. Model $\mathcal{A}$ može se elementarno utopiti u model teorije Σ ako i samo ako svaki konačan podmodel modela $\mathcal{A}$ može se elementarno utopiti u model teorije Σ.

Da to dokažemo, pretpostavimo da se svaki konačan podmodel modela $\mathcal{A}$ može elementarno utopiti u neki model teorije Σ. Tvrdimo da je teorija $\Sigma' = \Sigma \cup \Delta_A$ neprotivrečna.

Neka je $a \in A^\alpha$ numeracija skupa A. Svaki konačan $\Sigma_0 \subseteq \Sigma'$ sadrži konačan broj konstanti jezika $\mathcal{L}_\alpha$. Neka su to konstante $c_{\beta_1}, \ldots, c_{\beta_n}$. Kako jezik $\mathcal{L}$ ne sadrži operacijske simbole i konstante, konačan skup $A' = \{a_{\beta_1}, \ldots, a_{\beta_n}\}$ generiše konačan podmodel $\mathcal{A}'$ modela $\mathcal{A}$. Neka je $\mathcal{B}'$ model skupa rečenica Σ u koji se $\mathcal{A}'$ može utopiti.

Prema prethodnoj teoremi, model $\mathcal{B}'$ ima ekspanziju $(\mathcal{B}', b)$ koja je model elementarnog dijagrama $\Delta_{A'}$ modela $\mathcal{A}'$. Dakle, $\Sigma_0 \subseteq \Sigma \cup \Delta_{A'}$ ima model. Prema stavu kompaktnosti, Σ' ima model $\mathcal{B}$. Ponovo, prema prethodnoj teoremi, redukcijom modela $\mathcal{B}$ na jezik $\mathcal{L}$ dobija se model teorije Σ u koji se model $\mathcal{A}$ može elementarno utopiti.

Utapanje $h : \mathcal{A} \to \mathcal{B}$ je *homomorfno* ako za svaku formulu φ i svaku valuaciju $x \in A^\omega$, $\mathcal{A} \models_x \varphi$ implicira $\mathcal{B} \models_{h(x)} \varphi$.

Primer 12. Model $\mathcal{A}$ može se homomorfno utopiti u model $\mathcal{B}$ ako i samo ako postoji ekspanzija modela $\mathcal{B}$ koja je model elementarnog pozitivnog dijagrama modela $\mathcal{A}$.

Teorema 20. Svako parcijalno uređenje može se proširiti do linearnog uređenja.

Dokaz: Svako parcijalno uređenje $(A, \leq)$ skupa $A = \{a_0, \ldots, a_n\}$ može se proširiti do linearnog uređenja $(A, \leq^*)$. Ovo tvrđenje se jednostavno dokazuje indukcijom po $n \in \omega$.

Pretpostavimo da je $\mathcal{A} = (A, \leq)$ parcijalno uređenje. Neka je $a \in A^\alpha$ numeracija skupa A, Δ_A^+ pozitivni elementarni dijagram modela $\mathcal{A}$ i $\varphi = \forall x \forall y\,(x \leq y \vee y \leq x)$ rečenica koja izražava činjenicu da je uređenje $\leq$ linearno. Neka je

$$\Sigma = \Delta_A^+ \cup \{c_a \neq c_b : a, b \in A, a \neq b\} \cup \{\varphi\}.$$

Ako je Σ_0 konačan podskup od Σ i $a_{\beta_0}, \ldots, a_{\beta_n} \in A$ svi elementi čija se imena javljaju u Σ_0, restrikcija uređenja $\leq$ na skup $\{a_0, \ldots, a_n\}$ ima proširenje $\leq^*$ do linearnog uređenja, tj. Σ_0 ima model. Prema stavu kompaktnosti, skup rečenica Σ jezika $\mathcal{L}_\alpha$ ima model $(\mathcal{B}, b)$.

Model $(\mathcal{B}, b)$ je linearno uređenje u kojem je zadovoljen pozitivni dijagram Δ_A^+ modela $\mathcal{A}$. Za svako $\beta < \alpha$ neka je $h(a_\beta) = b_\beta$. Ekspanzija modela

$\mathcal{B}$ je model pozitivnog dijagrama Δ_A^+, pa prema prethodnom primeru, preslikavanje h je homomorfno utapanje modela $\mathcal{A}$ u model $\mathcal{B}$. Preslikavanje h^{-1} u modelu $\mathcal{A}$ indukuje linearno uređenje koje proširuje relaciju $\leq$. $\square$

Primer 13. Primenom stava kompaktnosti može se dokazati da se svaki skup može linearno urediti.

Parcijalno uređenje $\mathcal{P}$ je usmereno ako za sve $p, q \in P$, postoji $r \in P$ takvo da $p \leq r$ i $q \leq r$.

Ako je $\mathcal{P}$ usmereno uređenje, familija modela $(\mathcal{A}_p : p \in P)$ jezika $\mathcal{L}$ je usmerena ako za sve $p \leq q$, $\mathcal{A}_p \subseteq \mathcal{A}_q$.

Unija usmerene familije $(\mathcal{A}_p : p \in P)$ je model $\mathcal{A}$ jezika $\mathcal{L}$ takav da:

(a) $A = \bigcup_{p \in P} A_p$,

(b) ako je R relacijska konstanta jezika $\mathcal{L}$ i R_p, $p \in P$, njena interpretacija u modelu $\mathcal{A}_p$, relacija $R^A = \bigcup_{p \in P} R_p$ je interpretacija relacijske konstante R u modelu $\mathcal{A}$,

(c) za sve $a_1, \ldots, a_n \in A$, ako je F operacijska konstanta jezika $\mathcal{L}$, onda $F^A(a_1, \ldots, a_n) = F_p(a_1, \ldots a_n)$, gde je F_p interpretacija operacijske konstante F u modelu $\mathcal{A}_p$, $a_1, \ldots, a_n \in A_p$.

(d) individualnu konstantu c jezika $\mathcal{L}$ u modelu $\mathcal{A}$ interpretiramo elementom $c_p \in A_p$, za proizvoljno $p \in P$.

Sasvim jednostavno se proverava da su interpretacije relacijskih, operacijskih i individualnih konstanti jezika $\mathcal{L}$ korektno definisane.

Primer 14. Ako je $(\mathcal{A}_p : p \in P)$ usmerena familija modela jezika $\mathcal{L}$, takva da $\mathcal{A}_p \preceq \mathcal{A}_q$, za sve $p, q \in P$, $p \leq q$, onda je $\mathcal{A}_p \preceq \mathcal{A}$, za svako $p \in P$.

Skolemove teoreme

U našim uvodnim napomenama naglasili smo da predikatski račun ima određena ograničenja. Njegovim sredstvima nije moguć jedinstven opis bilo koje beskonačne strukture. Ta činjenica sledi iz stava kompaktnosti, ali je u potpunosti izražava Skolemova teorema.

Teorema 21. Skolemova teorema: Neka je Σ skup rečenica jezika $\mathcal{L}$ koji ima beskonačan model.

(a) Ako je Σ konačan skup, Σ ima model svake beskonačne kardinalnosti.

(b) Ako je Σ beskonačan skup kardinalnosti κ, Σ ima model svake kardinalnosti $\geq \kappa$.

Dokaz Skolemove teoreme izložićemo u okviru dva nešto informativnija reziltata. Zapravo, ova teorema predstavlja rešenje sledećeg problema: ako je $\mathcal{A}$ model kardinalnosti κ,

(a) u kojim kardinalnostima model $\mathcal{A}$ ima elementarni podmodel i
(b) u kojim kardinalnostima model $\mathcal{A}$ ima elementarnu ekstenziju?

Kada je κ konačan kardinal, ovaj problem je rešen u jednom od prethodnih primera. U beskonačnom slučaju, odgovor na prvo pitanje daje donja, a odgovor na drugo pitanje gornja Skolemova teorema.

Teorema 22. Neka je $\mathcal{A}$ model kardinalnosti α u jeziku $\mathcal{L}$. Ako je $\|\mathcal{L}\| \leq \beta \leq \alpha$, za svaki skup $X \subseteq A$ kardinalnosti β, postoji elementarni podmodel $\mathcal{B}$ modela $\mathcal{A}$ takav da $|B| = \beta$ i $X \subseteq B$.

Dokaz: Pretpostavimo da je $\mathcal{A}$ model kardinalnosti α i $X \subseteq A$ skup kardinalnosti $\beta \geq \|\mathcal{L}\|$. Neka je $(A, <)$ dobro uređenje skupa A. U odnosu na relaciju $<$, svaki podskup skupa $\mathcal{A}$ ima minimalni element.

Indukcijom definišemo niz $(B_n : n \in \omega)$ podskupova skupa A čija će unija biti domen traženog modela.

Neka je $B_0 = X$ i za svako $n > 0$, B_{n+1} skup elemenata $a \in A$ takav da, za neku formulu $\varphi(v_0, \ldots, v_n)$ jezika $\mathcal{L}$ i neke $a_0, \ldots, a_{n-1} \in B_n$, a je najmanji elemenat skupa A u smislu uređenja $<$ koji zadovoljava uslov

$$\mathcal{A} \models \varphi\,[a_0, \ldots, a_{n-1}, a].$$

Za svako $b \in B_n$, $b = \min\{a \in A : \mathcal{A} \models (v_0 = v_n)[b, a]\}$, pa je $b \in B_{n+1}$, tj. $B_n \subseteq B_{n+1}$. Pritom, b je najmanji element u smislu relacije $<$.

Kako je $\|\mathcal{L}\| \leq \beta$, za svako $n \in \omega$, skup B_n je kardinalnosti β. Neka je $B = \bigcup_{n \in \omega} B_n$. Jasno, B je kardinalnosti β i neka je $\mathcal{B}$ podmodel modela $\mathcal{A}$ generisan skupom B. Kako je B prebrojiva unija skupova kardinalnosti $\leq \beta$, model $\mathcal{B}$ ima kardinalnost β.

Neka je $\varphi(v_0, \ldots, v_n)$ formula jezika $\mathcal{L}$ i $a_0, \ldots, a_{n-1} \in B$ takvi da

$$\mathcal{A} \models \exists v_n\, \varphi[a_0, \ldots, a_{n-1}].$$

Po definiciji skupa B, postoji $m \in \omega$ takvo da $a_0, \ldots, a_{n-1} \in B_m$. Po pretpostavci skup $\{a \in A : \mathcal{A} \models \varphi\,[a_0, \ldots, a_{n-1}, a]\}$ nije prazan, pa sadrži najmanji element $b \in B_{m+1}$.

Stoga, postoji $b \in B$ takvo da $\mathcal{A} \models \varphi\,[a_0, \ldots, a_{n-1}, b]$. Kako je $\mathcal{B} \subseteq \mathcal{A}$, prema teoremi o elementarnim podmodelima, $\mathcal{B} \preceq \mathcal{A}$. $\square$.

Sledeća posledica prethodne teoreme uobičajeno se naziva donja Skolemova teorema. Jednu varijantu ove teoreme dokazli smo kao posledicu stava potpunosti.

Teorema 23. Donja Skolemova teorema: Ako je Σ skup rečenica kardinalnosti α, koji ima beskonačan model kardinalnosti $\beta \geq \alpha$, onda Σ ima model svake beskonačne kardinalnosti λ, $\alpha \leq \lambda \leq \beta$.

Dokaz: Neka je $\delta = \max\{\omega, \alpha\}$ i $\mathcal{L}'$ skup nelogičkih simbola jezika $\mathcal{L}$ koji se javljaju u rečenicama skupa Σ. Skup Σ možemo shvatiti kao teoriju u jeziku $\mathcal{L}'$ kardinalnosti δ.

Po pretpostavci, postoji model $\mathcal{A}$ jezika $\mathcal{L}$ kardinalnosti $\beta \geq \alpha$ takav da $\mathcal{A} \models \Sigma$. Ispuštajući sve nelogičke simbole jezika $\mathcal{L}$ koji nisu u $\mathcal{L}'$ dobijamo model $\mathcal{A}'$ jezika $\mathcal{L}'$ kardinalnosti β u kojem važi Σ.

Prema prethodnoj teoremi, ako je $\delta \leq \lambda\beta$, model $\mathcal{A}'$ sadrži elementarni podmodel $\mathcal{B}'$ kardinalnosti λ. Zbog $\mathcal{B}' \preceq \mathcal{A}'$, model $\mathcal{B}'$ je model jezika $\mathcal{L}'$ kardinalnosti λ u kojem važi Σ. Ako u modelu $\mathcal{B}'$, na proizvoljan način, interpretiramo nelogičke simbole koji se ne javljaju u Σ, dobijamo model $\mathcal{B}$ jezika $\mathcal{L}$ kardinalnosti λ u kojem važi Σ. $\square$

Donja Skolemova teorema ima veoma zanimljive i ponekad zbunjujuće posledice. U njenom dokazu pretpostavljen je princip dobrog uređenja, odnosno, aksioma izbora. Kasnije ćemo videti da iz donje Skolemove teoreme sledi aksioma izbora.

Sledeća teorema predstavlja odgovor na naše drugo pitanje o kardinalnosti modela teorije u jeziku $\mathcal{L}$. U njenom dokazu koriste se stav kompaktnosti i donja Skolemova teorema.

Teorema 24. Svaki beskonačan model $\mathcal{A}$ kardinalnosti α ima elementarnu ekstenziju proizvoljne kardinalnosti $\beta \geq \alpha$.

Dokaz: Neka je $\mathcal{A}$ model jezika $\mathcal{L}$ kardinalnosti α i neka $a \in A^\alpha$ numeracija skupa A i Γ_A dijagram modela $\mathcal{A}$. Podsetimo se da je Γ_A teorija u jeziku $\mathcal{L}_\alpha$.

Neka je $C = \{c_\gamma : \gamma < \beta\}$ skup konstanti različitih od svih konstanti jezika $\mathcal{L}_\alpha$ i neka je $\mathcal{L}_{\alpha+\beta} = \mathcal{L}_\alpha \cup C$.

Označimo sa Σ skup formula $\{\neg(c_\gamma = c_\delta) : \gamma < \delta < \beta\}$. Tvrdimo da svaki konačan podskup skupa $\Sigma \cup \Gamma_A$ ima model.

Dovoljno je dokazati da za svaki konačan $\Sigma_0 \subseteq \Sigma$, skup $\Sigma_0 \cup \Gamma_A$ ima model. Neka su $c_{\gamma_1}, \ldots, c_{\gamma_n}$ sve konstante skupa C koje se javljaju u Σ_0 i $a'_1, \ldots, a'_n$ različiti elementi skupa A.

Definišimo numeraciju $a^* \in A^{\alpha+\beta}$ skupa A tako da za sve $\gamma < \alpha + \beta$,

$$a^*_\gamma = \begin{cases} a_\gamma & \text{ako } \gamma < \alpha, \\ a'_i & \text{ako } \gamma = \alpha + \gamma_i,\ 1 \leq i \leq n, \\ a_0 & \text{inače.} \end{cases}$$

Kako su $a_i^{'}$ različiti, $(\mathcal{A}, a^*)$ je model za $\Sigma_0 \cup \Gamma_A$. Prema stavu kompaktnosti $\Sigma \cup \Gamma_A$ ima model. Kako konstante c_γ imaju različite vrednosti u svakom modelu za $\Sigma \cup \Gamma_A$, taj model mora biti kardinalnosti $\geq \beta$.

Prema donjoj Skolemovoj teoremi $\Sigma \cup \Gamma_A$ ima model $(\mathcal{B}, b')$ kardinalnosti β. Kako je Γ_A dijagram modela $\mathcal{A}$, mora biti $(\mathcal{A}, a) \equiv (\mathcal{B}, b)$, gde je niz b sastavljen od prvih α članova niza b'. Kako je $a \in A^\omega$ numeracija skupa $\mathcal{A}$, model $\mathcal{A}$ može se elementarno utopiti u model $\mathcal{B}$. Dakle, do na izomorfizam, $\mathcal{B}$ je elementarna ekstenzija modela $\mathcal{A}$ kardinalnosti β. $\Box$

Teorema 25. Gornja Skolemova teorema: Ako skup rečenica Σ ima model kardinalnosti $\alpha \geq \omega$, onda Σ ima model svake kardinalnosti $\beta \geq \alpha$.

Gornja Skolemova teorema neposredno sledi iz prethodnog rezultata. U sledećim primerima izložene su posledice stava kompaktnosti i Skolemove teoreme u aritmetici prirodnih i realnih brojeva. Kako smo nagovestili u uvodnim napomenama, predikatski račun nije dovoljno snažan da izrazi teoreme jedinstvenosti prirodnih i realnih brojeva.

Prirodne brojeve definisali smo kao strukturu $\mathcal{N} = (+, \cdot, \leq, s, 0)$. Pretpostavićemo da su prirodni brojevi na određeni način zadati. Naš cilj je da sredstvima predikatskog računa prvog reda, ukoliko je to uopšte moguće, u potpunosti opišemo strukturu $\mathcal{N}$.

Navedena pretpostavka u filosofskom smislu podrazumeva jedan oblik platonizma. Ona izražava uverenje da matematički iskazi imaju smisao koji je nezavisan od naših izražajnih, stvaralačkih ili saznajnih mogućnosti. Prema platonističkom shvatanju, u izvesnom idealnom smislu, matematički objekti zaista postoje. Ta egzistencija se nužno manifestuje u svim odnosima realnog sveta i u svim sferama mišljenja. Čovek ne stvara, već otkriva matematička tvrđenja. Ne upuštajući se u podrobniju raspravu platonističkog stanovišta, o tome je bilo reči u napomenama uvodnog poglavlja, reći ćemo samo to da pretpostavkom o postojanju prirodnih brojeva u ovoj stvari nismo preterali. Većina matematičara i filosofa ipak pretpostavlja bar potencijalnu egzistenciju prirodnih brojeva nad kojima su izvedene sve ostale matematičke konstrukcije.

Jezik strukture $\mathcal{N}$ u predikatskom računu prvog reda označavamo sa $\mathcal{L}_{PA}$ i nazivaćemo ga jezikom prirodnih brojeva ili jezikom aritmetike. Jasno, jezik aritmetike $\mathcal{L}_{PA} = \{+, \cdot, \leq, s, 0\}$ je prebrojiv. Struktura $\mathcal{N}$ prirodnih brojeva je standardni model, a svaki drugi model jezika $\mathcal{L}_{PA}$ koji nije izomorfan sa $\mathcal{N}$ je nestandardni model jezika aritmetike.

Primer 1. U jeziku $\mathcal{L}_{PA}$ mogu se definisati sve uobičajene aritmetičke relacije i operacije: polinomi, deljivost, prosti brojevi itd.

Teorija $\mathrm{Th}(\mathcal{N})$ koja se sastoji od svih rečenica jezika $\mathcal{L}_{PA}$ istinitih u modelu $\mathcal{N}$ je kompletna aritmetika. Zbog prebrojivosti jezika $\mathcal{L}_{PA}$, kompletna aritmetika je prebrojiva teorija.

Primer 2. Kompletna aritmetika ima model proizvoljne beskonačne kardinalnosti.

Teorija $\mathrm{Th}(\mathcal{N})$ je prebrojiva i ima beskonačan model $\mathcal{N}$. Prema Skolemovoj teoremi, teorija $\mathrm{Th}(\mathcal{N})$ ima model svake beskonačne kardinalnosti.

Budući da kompletna aritmetika ima nestandardne modele, ona prirodne brojeve ne određuje na jedinstven način. Kao kompletna teorija, ona se u jeziku $\mathcal{L}_{PA}$ ne može neprotivrečno proširivati, pa u jeziku aritmetike nije moguća jedinstvena karakterizacija prirodnih brojeva. Na osnovu Skolemove teoreme, isti rezultat bi se dobio u svakom proširenju jezika $\mathcal{L}_{PA}$, odnosno, u predikatskom računu prvog reda takva karakterizacija nije uopšte moguća. Na osnovu Dedekindove teoreme o jedinstvenosti prirodnih brojeva, to znači da se princip matematičke indukcije, formulisan u logici drugog reda ili kao metamatematički princip, ne može izraziti sredstvima predikatskog računa prvog reda.

Primer 3. Postoji prebrojiv nestandardni model kompletne aritmetike.

Ovo tvrđenje pokazuje da postoje elementarno ekvivalentni modeli jezika $\mathcal{L}$ iste kardinalnosti koji nisu izomorfni. U njegovom dokazu javlja se kombinacija argumenata kompaktnosti i donje Skolemove teoreme koju smo već koristili u dokazu gornje Skolemove teoreme.

Neka je $\mathcal{L}_{\omega,PA}$ jezik koji se dobija proširivanjem jezika aritmetike $\mathcal{L}_{PA}$ skupom individualnih konstanti $C = \{c_n : n \in \omega\}$. Svakom prirodnom broju $n \in \omega$ dato je ime c_n, odnosno, u strukturi prirodnih brojeva konstantu c_n interpretiramo kao prirodan broj n.

Neka je c individulna konstanta koja ne pripada jeziku $\mathcal{L}_{\omega,PA}$. Neka je Σ teorija u jeziku $\mathcal{L}_{\omega,PA} \cup \{c\}$ takva da

$$\Sigma = \mathrm{Th}(\mathcal{N}) \cup \{c_n \neq c : n \in \omega\}$$

Svaki konačan skup $\Sigma_0 \subseteq \Sigma$ sadrži samo konačan broj konstanti jezika $\mathcal{L}_{\omega,PA} \cup \{c\}$, pa postoji najveći prirodan broj $k \in \omega$ za koji se konstanta oblika c_n javlja u skupu rečenica Σ_0. Ako se konstanta c interpretira prirodnim brojem većim od k, u modelu $\mathcal{N}$ važi Σ_0. Prema stavu kompaktnosti, teorija Σ ima model. Kako je Σ teorija u prebrojivom jeziku $\mathcal{L}_{\omega,PA} \cup \{c\}$, prema donjoj Skolemovoj teoremi, teorija Σ ima prebrojiv model $\mathcal{M}'$. Njegova redukcija na jezik aritmetike $\mathcal{L}_{PA}$ je prebrojiv model $\mathcal{M}$ teorije $\mathrm{Th}(\mathcal{N})$.

Element $c^M \in M$, kojim je u modelu $\mathcal{M}$ interpretirana konstanta c, razlikuje se od interpretacije c_n^M svakog standardnog prirodnog broja $n \in \omega$. Takav broj c^M je beskonačan prirodan broj.

Peanova aritmetika je teorija u jeziku $\mathcal{L}_{PA}$. Ona se sastoji od rečenica $\varphi_1, \ldots, \varphi_8$, koje su navedene u uvodnom poglavlju i sheme indukcije, odnosno skupa rečenica oblika

$$\varphi(0) \wedge \forall x\, (\varphi(x) \to \varphi(s(x))) \to \forall x\, \varphi(x),$$

za svaku formulu $\varphi(x)$ jezika $\mathcal{L}_{PA}$ koja sadrži bar jednu slobodnu promenljivu $x \in V$. Peanovu aritmetiku označavamo sa PA.

Jasno je da kompletana aritmetika $\mathrm{Th}(\mathcal{N})$ sadrži teoriju PA. Međutim, obratno ne važi, odnosno, Peanova aritmetika nije kompletna teorija. Tu činjenicu dokazaćemo u okviru teorije izračunljivosti. Slično kompletnoj aritmetici, Peanova aritmetika ima nestandardne modele, ali postoje modeli teorije PA koji nisu modeli kompletne aritmetike.

Neka je $0 = 0$ i za svako $n \in \omega$, $n + 1 = s(n)$. Termi jezika $\mathcal{L}_{PA}$ oblika n su numerali.

Primer 4. Za svaki term $t(x_1, \ldots, x_k)$ jezika $\mathcal{L}_{PA}$ i sve $n, n_1, \ldots, n_k \in \omega$,

$$PA \vdash n = t(n_1, \ldots, n_k) \quad \Leftrightarrow \quad n = t^N[n_1, \ldots, n_k].$$

Primer 5. Ako je $\mathcal{M}$ model Peanove aritmetike, onda postoji jedinstveno utapanje modela $\mathcal{N}$ u inicijalni segment modela $\mathcal{M}$.

Isto tvrđenje važi i za kompletnu aritmetiku, odnosno, za bilo koje proširenje Peanove aritmetike. U modelu $\mathcal{M}$ jezika $\mathcal{L}_{PA}$, elemente inicijalnog segmenta koji je izomorfan sa $\mathcal{N}$, nazivamo standardnim prirodnim brojevima modela $\mathcal{M}$.

Primer 6. U teoriji $\mathrm{Th}(\mathcal{N})$, pa dakle ni u teoriji PA nije moguće formulisati princip dobrog uređenja.

Primer 7. (a) U svakom nestandardnom modelu Peanove aritmetike postoji beskonačan prost broj.

(b) Postoji model $\mathcal{M}$ Peanove aritmetike koji sadrži prirodan broj $m \in M$ deljiv svim standardnim prostim brojevima modela $\mathcal{M}$.

Primer 8. Svaki model $\mathcal{M}$ Peanove aritmetike ima sledeći tip uređenja $(M, \leq) = \omega + (\omega^* + \omega) \cdot \theta$. Pritom, $(\omega^* + \omega)$ je tip uređenja celih brojeva, a θ tip linearnog gustog uređenja bez krajeva.

Primer 8. Postoji 2^ω nestandardnih neizomorfnih prebrojivih modela Peanove aritmetike.

Pretpostavumo da je c konstanta koja ne pripada jeziku $\mathcal{L}_{PA}$ i $S \subseteq P$ proizvoljan skup prostih brojeva. Za svaki prost broj $p \in P$ neka je $\varphi_p = \exists x\, (c = x \cdot p)$, gde je p numeral broja p i neka je

$$\Sigma(S) = PA \cup \{\varphi_p : p \in S\} \cup \{\neg\varphi_p : p \in P \backslash S\}.$$

Prema stavu kompaktnosti i zbog prebrojivosti jezika $\mathcal{L}_{PA}$, teorija $\Sigma(S)$ ima prebrojiv model $\mathcal{M}(S)$. Ako su $S_1, S_2 \subseteq P$ neprazni različiti skupovi prostih brojeva, modeli $\mathcal{M}(S_1)$ i $\mathcal{M}(S_2)$ nisu izomorfni.

Na osnovu poslednja dva primera i kada se ima u vidu činjenica da je tip prebrojivog gustog uređenja bez krajeva jedinstveno određen, može se zaključiti da sa stanovišta uređenja postoji samo jedan prebrojiv model Peanove aritmetike koji nije izomorfan strukturi $\mathcal{N}$. Svi drugi neizomorfni prebrojivi modeli realizuju svojstva operacija prirodnih brojeva.

Uređeno polje $\mathcal{F}$ je struktura jezika $\mathcal{L} = \{+, \cdot, \leq, 0, 1\}$ koja zadovoljava aksiome $\varphi_1, \ldots, \varphi_{16}$ navedene u uvodnom poglavlju. Takođe, u istom kontekstu definisali smo pojam kompletnog uređenog polja, kao polja u kojem svaki neoprazan ograničen skup ima supremum i formulisali teoremu o jedinstvenosti kompletnog uređenog polja realnih brojeva. Naglašavamo da princip kompletnosti nismo definisali u predikatskom računu prvog reda. Slično principu indukcije, on je bio izražen u logici drugog reda, odnosno, kao metamatematički princip.

Dokaz jedinstvenosti polja realnih brojeva biće izložen u poglavlju o teoriji skupova. U ovom kontekstu, slično prirodnim brojevima, pretpostavljamo da je uređeno polje realnih brojeva $\mathcal{R} = (+, \cdot, \leq, 0, 1)$ nekako zadato, odnosno, konstruisano nad prirodnim brojevima. Naš cilj je da odredimo meru u kojoj se ova struktura može okarakterisati sredstvima predikatskog računa.

Primer 10. Svako uređeno polje sadrži izomorfnu kopiju strukture prirodnih brojeva.

U svakom uređenom polju $\mathcal{A} = (A, +, \cdot, \leq, 0, 1)$, za svako $x \in A$, važi nejednakost $x < x + 1$.

Otuda redom sledi da je $0 < 1 < 1 + 1 < \cdots$. Za svako $n \in \omega$, ako izraz oblika $\underbrace{1 + \cdots + 1}_{n}$ identifikujemo brojem n, onda $\omega \subseteq A$. Takvom idenitifikacijom dobija se utapanje prirodnih brojeva u polje $\mathcal{A}$.

Primer 11. Svako uređeno polje sadrži kopiju jedinstveno određenih racionalnih brojeva.

Neka je $\mathcal{Q}$ polje racionalnih brojeva. Svaki racionalan broj $q \in Q$ može se predstviti u obliku $q = \frac{m}{n}$ ili $q = -\frac{m}{n}$, za neke $m, n \in \omega$ i $n \neq 0$.

Svaki izomorfizam prirodnih brojeva $\mathcal{N} \subseteq \mathcal{Q}$ ima jedinstveno proširenje na polje racionalnih brojeva. Ako se pretpostavi princip indukcije, polje $\mathcal{Q}$ jedinstveno je određeno. Utapanje prirodnih brojeva $\mathcal{N}$ u proizvoljno uređeno polje $\mathcal{A}$, na jedinstven način proširuje se do utapanja polja racionalnih brojeva $\mathcal{Q}$ u polje $\mathcal{A}$.

Uređeno polje $\mathcal{F}$ je arhimedovsko polje ako za svako $x \in F$, postoji prirodan broj $n \in \omega$ takav da je $x < n$.

Primer 12. (a) Skup racionalnih brojeva je gust u svakom arhimedovskom polju.

(b) Svako kompletno uređeno polje je arhimedovsko.

Neka je $\mathcal{F}$ arhimedovsko polje. Ne umanjujući opštost, pretpostavićemo da su $x, y \in F$ takvi da $0 < x < y$. Kako je $\mathcal{F}$ arhimedovsko polje, postoji prirodan broj $n \in \omega$ koji zadovljava nejednakost $\frac{1}{y-x} < n$. Otuda se dobija da je $ny - nx > 1$, pa ako je $m \in \omega$ najmanji prirodan broj takav da $nx < m$, onda je $nx < m < ny$, odnosno, $x < \frac{m}{n} < y$.

Ako kompletno uređeno polje $\mathcal{F}$ nije arhimedovsko, postoji $x \in F$ takvo da za svako $n \in \omega$, $n < x$. Kako je $x \in F$ gornje ograničenje skupa ω u kompletnom uređenom polju, skup ω ima supremum $a \in F$. Kako je a najmanje gornje ograničenje, $a - 1$ nije gornje ograničenje skupa ω, pa postoji $n \in \omega$ takav da $a - 1 < n$, odnosno, $a < n + 1$, što nije moguće.

Primer 13. Postoji uređeno polje koje nije arhimedovsko.

Neka je $\mathcal{L}$ jezik teorije uređenih polja, $a \in Q^\omega$ numeracija racionalnih brojeva i $\mathrm{Th}(\mathcal{Q}, a)$ dijagram strukture $\mathcal{Q}$. Podsetimo se da je dijagram teorija u proširenju $\mathcal{L}_\omega$ jezika $\mathcal{L}$ koje sadrži imena svih racionalnih brojeva.

Neka je c individualna konstanta koja ne pripada jeziku $\mathcal{L}_\omega$ i Σ skup rečenica jezika $\mathcal{L}_\omega \cup \{c\}$ takav da

$$\Sigma = \mathrm{Th}(\mathcal{Q}, a) \bigcup \{c_n < c : n \in \omega\}.$$

U svakom konačnom skupu rečenica $\Sigma_0 \subseteq \Sigma$, javlja se konačan broj individualnih konstanti jezika $\mathcal{L}_\omega \cup \{c\}$, pa postoji racionalan broj $q \in Q$ veći od svakog racionalnog broja čije se ime javlja u skupu rečenica Σ_0. Ako se konstanta c interpretira sa q, onda je $\mathcal{Q}$ model za Σ_0.

Prema stavu kompaktnosti, skup rečenica Σ ima model, a njegova redukcija na jezik $\mathcal{L}$ je nearhimedovsko polje $\mathcal{F}$ koje elementarno proširuje polje racionalnih brojeva.

Egzistencija nearhimedovskih polja približava nas ideji nestandardne analize. U takvim poljima postoje beskonačno male veličine.

Nearhimedovsko polje $\mathcal{F}$ sadrži kopiju standardnih prirodnih brojeva, tj. $\omega \subseteq F$. Ako je $c_F \in F$ interpretacija konstante c, za svako $n \in \omega$, $n < c_F$, odnosno, element c_F je beskonačno veliki element polja $\mathcal{F}$. Kako je $c_F > 0$, za svako $n \in \omega$, $0 < \frac{1}{c_F} < \frac{1}{n}$, odnosno, $\frac{1}{c_F} \in F$ je pozitivan beskonačno mali element polja $\mathcal{F}$.

Primer 14. (a) Postoji prebrojivo uređeno polje $\mathcal{A}$ elementarno ekvivalentno uređenom polju $\mathcal{R} = (R, +, \cdot, \leq, 0, 1)$ realnih brojeva. Dakle, sa stanovišta logike prvog reda, postoje prebrojivi realni brojevi.

(b) Postoje prebrojivi modeli teorije $\mathrm{Th}(\mathcal{R})$ koji nisu izomorfni.

Sama po sebi, egzistencija nearhimedovskih proširenja uređenih polja nije dovoljna u zasnivanju nestandardne analize. Izučavanje pojmova konvergencije, neprekidnosti ili diferencijabilnosti u nestandardnim proširenjima realnih brojeva, podrazumeva da svojstva standardnih objekata dokazana sredstvima proširenja važe u samom polju realnih brojeva. Neophodan je princip prenosa, odnosno, elementarna ekvivalencija polja $\mathcal{R}$ i njegovog nestandadnog proširenja $\mathcal{R}^*$. Lajbnic je implicitno pretpostavljao i koristio ovaj princip, ali se on u svom punom smislu izražava u okviru teoreme o ultraproizvodu, koja će biti izložena u sledećem poglavlju.

Teorema o ultraproizvodu

U teoriji modela značajne su konstrukcije koje čuvaju elementarnu strukturu modela. Osim elementarnih podmodela i elementarnih utapanja, jedna konstrukcija takve vrste je ultraproizvod familije modela jezika $\mathcal{L}$. Po svojoj prirodi, ova konstrukcija je algebarska i možemo je shavtiti kao specifičan slučaj proizvoda matematičkih struktura. Ta specifičnost ogleda se upravo u činjenici da ultraproizvod čuva sva svojstva prvog reda koja važe u "filter mnogo" njegovih faktora.

Pretopstavimo da je $(\mathcal{A}_i : i \in I)$ familija struktura jezika $\mathcal{L}$, indeksirana nepraznim skupom I. Njen ultraproizvod je potproizvod Dekartovog prizvoda koji se dobija izjednačavanjem elemenata po ultrafiltru indeksnog skupa. Pritom, Dekartov proizvod familije skupova $(A_i : i \in I)$ je skup funkcija

$$\prod_{i \in I} A_i = \{f : I \to \bigcup_{i \in I} A_i : \text{ za svako } i \in I, f(i) \in A_i\}.$$

Kada je iz konteksta jasno o kom indeksnom skupu je reč, Dekartov proizvod $A = \prod_{i \in I} A_i$ označavamo sa $A = \prod A_i$.

Pretpostavimo da je F familija podskupova skupa I. Definišimo binarnu relaciju $\sim$ na Dekartovom proizvodu A tako da za sve $f, g \in A$,

$$f \sim g \quad \Leftrightarrow \quad \{i \in I : f(i) = g(i)\} \in F.$$

Primer 1. Ako je F filter nad I, relacija $\sim$ je relacija ekvivalencije na A. Ako svaki skup A_i sadrži bar tri elementa, važi i obratno.

Za svako $f \in A$, neka je $f_F = \{g \in A : f \sim g\}$ klasa ekvivalencije s obzirom na relaciju $\sim$. Količnik po relaciji $\sim$ označavamo sa $\prod_{i\in I} A_i/F$.

Simbole jezika $\mathcal{L}$ interpretiramo u količniku $\prod_{i\in I} A_i/F$ na sledeći način:

Ako je P relacijska konstanta jezika $\mathcal{L}$, njena interpretacija je relacija R_F skupa $\prod_{i\in I} A_i/F$ takva da za sve $f, g \in A$,

$$(f_F, g_F) \in R_F \quad \Leftrightarrow \quad \{i \in I : (f(i), g(i)) \in R_i\} \in F.$$

Interpretacija operacijske konstante G je operacija G_F takva da za sve $f, g, h \in A$,

$$G_F(f_F, g_F) = h_F \quad \Leftrightarrow \quad \{i \in I : G_i(f(i), g(i)) = h(i)\} \in F.$$

Interpretaciju c_F konstante c definišemo tako da svako $f \in A$,

$$f_F = c_F \quad \Leftrightarrow \quad \{i \in I : f(i) = c_i\} \in F.$$

Jednostavnosti radi i ne umanjujući opštost, definisali smo interpretacije binarnih relacijskih i operacijskih konstanti jezika $\mathcal{L}$. Jasno je da ista definicija važi i za konstante proizvoljne dužine $n \geq 1$.

Primer 2. Ako je F filter nad skupom I, definicije relacija R_F, operacija G_F i konstanta c_F proizvoda $\prod_{i\in I} A_i/F$ su korektne.

Treba dokazati da je relacija $\sim$ kongruencija u odnosu na relaciju R_F i operaciju G_F i konstanti c_F. Na primer, u slučaju relacije R_F iz pretpostavki $f \sim g$, $f' \sim g'$ i $(f_F, g_F) \in R_F$, po definiciji relacije $\sim$ i iz svojstava filtra F, treba dokazati da $(f^{'}_F, g^{'}_F) \in R_F$.

Struktura $\prod \mathcal{A}_i/F = (\prod A_i/F, R_F, G_F, c_F)$ je redukovani proizvod familije modela $(\mathcal{A}_i, i \in I)$ po filtru F. Nas će prevashodno zanimati redukovani proizvodi po ultrafiltru. U tom slučaju, redukovani proizvod $\prod A_i/F$ je ultraproizvod. Kada je $\mathcal{A}_i = \mathcal{A}$, za sve $i \in I$, odgovarajući redukovani proizvod se svodi na ultrastepen, u oznaci $\mathcal{A}^I_{/F}$, modela $\mathcal{A}$ po filtru F.

Modelsko-teorijski značaj ove konstrucije je u tome što ona čuva sva svojstva izražena u jeziku $\mathcal{L}$ koja u familiji $(\mathcal{A}_i : i \in I)$ važe na filter mnogo mesta. Da bi se ta činjenica izrazila potrebno je prethodno usaglasiti oznake valuacija u proizvodu i valuacija u njegovim činiocima.

Svaki niz $f = (f^1, f^2, \dots)$ elemenata proizvoda $A = \prod A_i$ određuje valuaciju promenljivih $f_F = (f^1_F, f^2_F, \dots)$ jezika $\mathcal{L}$ u modelu $\prod \mathcal{A}_i/F$ i obratno, svaka valuacija promenljivih u modelu $\prod \mathcal{A}_i/F$ određena je nizom elemenata

Dekartovog proizvoda A. Za svako $i \in I$, sa $f(i)$ označavamo valuaciju promenljivih $(f^1(i), f^2(i), \dots)$ u modelu $\mathcal{A}_i$ određenu nizom $f \in A^\omega$.

Teorema 26. Teorema o ultraproizvodu Neka je F ultrafilter nad skupom I. Za svaku formulu φ jezika $\mathcal{L}$ i svaku valuaciju $f_F \in (\prod A_i/F)^\omega$,

$$\prod \mathcal{A}_i/F \models_{f_F} \varphi \quad \Leftrightarrow \quad \{i \in I : \mathcal{A}_i \models_{f(i)} \varphi\} \in F.$$

Dokaz: Teoremu dokazujemo indukcijom po složenosti formule φ. U slučaju elementarnih formula, na osnovu sintaksnih svojstava jednakosti, dovoljno je dokazati da teorema važi za proste elementarne formule, odnosno, za formule oblika $v_m = v_n$, $G(v_m, v_n) = v_p$ i $P(v_m, v_n)$ jezika $\mathcal{L}$.

Ako je φ elementarna formula oblika $v_m = v_n$, za svaku valuaciju $f \in A^\omega$, na osnovu definicije relacije $\sim$ i po definiciji relacije zadovoljenja redom se dobija:

$$\begin{array}{rcl}\prod \mathcal{A}_i/F \models_{f_F} v_m = v_n & \Leftrightarrow & f_F^m = f_F^n, \\ & \Leftrightarrow & f^m \sim f^n, \\ & \Leftrightarrow & \{i \in I : f^m(i) = f^n(i)\} \in F, \\ & \Leftrightarrow & \{i \in I : \mathcal{A}_i \models_{f(i)} v_m = v_n\} \in F.\end{array}$$

Ako je φ elementarna formula oblika $G(v_m, v_n) = v_p$, na osnovu definicije operacije G_F, za svako $f \in A^\omega$,

$$\begin{array}{rcl}\mathcal{A} \models_{f_F} G(v_m, v_n) = v_p & \Leftrightarrow & G_F(f_F^m, f_F^n) = f_F^p, \\ & \Leftrightarrow & \{i \in I : G(f^m(i), f^n(i)) = f^p(i)\} \in F, \\ & \Leftrightarrow & \{i \in I : \mathcal{A}_i \models_{f(i)} G(v_m, v_n) = v_p\} \in F,\end{array}$$

gde smo sa $\mathcal{A}$ označili model $\prod \mathcal{A}_i/F$.

Slično, ako je φ elementarna formula $P(v_m, v_n)$, na osnovu definicije relacije R_F, za svaku valuaciju $f \in A^\omega$,

$$\begin{array}{rcl}\prod \mathcal{A}_i/F \models_{f_F} P(v_m, v_n) & \Leftrightarrow & (f_F^m, f_F^n) \in R_F, \\ & \Leftrightarrow & \{i \in I : (f^m(i), f^n(i)) \in R\} \in F, \\ & \Leftrightarrow & \{i \in I : \mathcal{A}_i \models_{f(i)} P(v_m, v_n)\} \in F.\end{array}$$

Pretpostavimo da je $\varphi = \psi \wedge \theta$. Za proizvoljnu valuaciju $f \in A^\omega$ neka je $D_\psi = \{i \in I : \mathcal{A}_i \models_{f(i)} \psi\}$ i $D_\theta = \{i \in I : \mathcal{A}_i \models_{f(i)} \theta\}$, što znači da je $D_\psi \cap D_\theta = \{i \in I : \mathcal{A}_i \models_{f(i)} \psi \wedge \theta\}$.

Otuda, na osnovu definicionih svojstava filtra i po induktivnoj pretpostavci redom dobijamo da važi:

$$\begin{array}{rcl}\prod \mathcal{A}_i/F \models_{f_F} \psi \wedge \theta & \Leftrightarrow & \prod \mathcal{A}_i/F \models_{f_F} \psi \text{ i } \prod \mathcal{A}_i/F \models_{f_F} \theta, \\ & \Leftrightarrow & D_\psi \in F \text{ i } D_\theta \in F, \\ & \Leftrightarrow & D_\psi \cap D_\theta \in F.\end{array}$$

Ako je formula ψ oblika $\neg\psi$, za svaku valuaciju $f \in A^\omega$, na osnovu činjenice da je F ultrafilter i po induktivnoj pretpostavci redom imamo:

$$\begin{aligned}\prod \mathcal{A}_i/F \models_{f_F} \neg\psi \quad &\Leftrightarrow \quad \text{ne važi } \prod \mathcal{A}_i/F \models_{f_F} \psi,\\ &\Leftrightarrow \quad D_\psi \notin F,\\ &\Leftrightarrow \quad D_\psi^c \in F,\\ &\Leftrightarrow \quad \{i \in I : \mathcal{A}_i \models_{f(i)} \neg\psi\} \in F.\end{aligned}$$

Pretpostavimo da je φ oblika $\exists v_n\, \psi$. Za svaku valuaciju $f \in A^\omega$, neka je $D_{\exists v_n \psi} = \{i \in I : A_i \models_{f(i)} \exists v_n\, \psi\}$. Treba dokazati da važi

$$\prod \mathcal{A}_i/F \models_{f_F} \exists v_n\, \psi \quad \Leftrightarrow \quad D_{\exists v_n \psi} \in F.$$

Pretpostavimo da je $\prod \mathcal{A}_i/F \models_{f_F} \exists v_n\, \psi$. Tada postoji $b \in \prod A_i$ takvo da $\prod \mathcal{A}_i/F \models_{f(n/b)_F} \psi$. Neka je $D_\psi = \{i \in I : A_i \models_{f(n/b)(i)} \psi\}$. Po induktivnoj pretpostavci $D_\psi \in F$. Za sve $i \in I$, $f(n/b)(i) = f(i)(n/b_i)$, pa mora biti $D_\psi \subseteq D_{\exists v_n \psi}$, tj. $D_{\exists v_n \psi} \in F$.

Pretpostavimo da $D_{\exists v_n \psi} \in F$. Za svako $i \in D_{\exists v_n \psi}$, $\mathcal{A}_i \models_{f(i)} \exists v_n\, \psi$, pa postoji $b_i \in A_i$ takvo da $\mathcal{A}_i \models_{f(i)(n/b_i)} \psi$. Prema aksiomi izbora, postoji $c \in \prod \mathcal{A}_i$ takvo da za sve $i \in D_{\exists v_n\, \psi}$, $c_i = b_i$.

Otuda sledi da je $D_{\exists v_n \psi} \subseteq \{i \in I : \mathcal{A}_i \models_{f(n/c)(i)} \psi\}$. Kako $D_{\exists v_n \psi} \in F$, mora biti $\{i \in I : \mathcal{A}_i \models_{f(n/c)(i)} \psi\} \in F$. Prema induktivnoj pretpostavci $\prod \mathcal{A}_i/F \models_{f(n/c)_F} \psi$, odnosno, $\prod \mathcal{A}_i/F \models_{f_F} \exists v_n\, \psi$. $\square$

Iz teoreme o ultraproizvodu neposredno sledi da ako je φ rečenica jezika $\mathcal{L}$, onda: $\prod \mathcal{A}_i/F \models \varphi$ ako i samo ako $\{i \in I : \mathcal{A}_i \models \varphi\} \in F$.

Pretpostavimo da je $\mathcal{A}$ model jezika $\mathcal{L}$ i F ultrafilter nad skupom I. Za svako $a \in A$, neka je $a^* \in A^I$ takvo da za svako $i \in I$, $a^*(i) = a$. Definišimo preslikavanje $h : A \to A^I_{/F}$ tako da za svako $a \in A$, $h(a) = a^*_F$. Preslikavanje h je obostrano jednoznačno i naziva se kanonsko utapanje modela $\mathcal{A}$ u ultrastepen $\mathcal{A}^I_{/F}$.

Teorema 27. Kanonsko utapanje je elementarno utapanje.

Dokaz: Iz ove teoreme neposredno sledi da je svaki model $\mathcal{A}$ elementarno ekvivalentan svakom svom ultrastepenu $\mathcal{A}^I_{/F}$. Samo u specifičnim okolnostima, ultrastepen $\mathcal{A}^I_{/F}$ je izomorfan modelu $\mathcal{A}$, pa se konstrukcijom ultrastepena modela dobija njegova prava elementarna ekstenzija.

Ako je $\varphi(v_0, \ldots, v_n)$ formula jezika $\mathcal{L}$ i $a^0, \ldots, a^n \in A$, na osnovu teoreme o ultraproizvodu i po definiciji kanonskog utapanja, redom imamo:

$$\begin{aligned}\mathcal{A}^I_{/F} \models \varphi[a^*_{0F}, \ldots, a^*_{nF}] \quad &\Leftrightarrow \quad \{i \in I : \mathcal{A} \models \varphi[a^*_0(i), \ldots, a^*_n(i)]\} \in F,\\ &\Leftrightarrow \quad \{i \in I : \mathcal{A} \models \varphi[a_0, \ldots, a_n]\} \in F,\\ &\Leftrightarrow \quad \mathcal{A} \models \varphi[a_0, \ldots, a_n]. \quad \square\end{aligned}$$

Primer 3. Neka je F ultrafilter nad skupom I i $G \in F$. Familija skupova $G_F = \{x \cap F : x \in G\}$ je ultrafilter nad skupom G.

Primer 4. Ako je $(\mathcal{A}_i : i \in I)$ familija modela jezika $\mathcal{L}$, F ultrafilter nad I i $G \in F$, onda je $\prod_{i \in I} \mathcal{A}_i/F \simeq \prod_{i \in G} \mathcal{A}_i/G_F$.

Primer 5. Ako je F glavni ultrafilter nad I, onda postoji $k \in I$ takvo da $\prod_{i \in I} \mathcal{A}_i/F \simeq \mathcal{A}_k$.

Primer 6. Ako je F neglavni ultrafilter nad skupom I, onda postoji $J \subseteq I$ i uniforman ultrafilter G nad J takav da za svaku familiju modela $(\mathcal{A}_i : i \in I)$ jezika $\mathcal{L}$, $\prod_{i \in I} \mathcal{A}_i/F \simeq \prod_{i \in J} \mathcal{A}_i/G$.

U ovom primeru, treba izabrati element ultrafiltra F najmanje kardinalnosti i primeniti rezultat prethodnog primera.

Primer 7. Ako je $\mathcal{A}$ model jezika $\mathcal{L}$ kardinalnosti $|A| \leq \omega$ i F prebrojivo kompletan ultrafilter nad skupom I, onda $\mathcal{A}^I_{/F} \simeq \mathcal{A}$.

Podsetimo se, ultrafilter F nad skupom I je prebrojivo kompletan ako i samo ako za svaku prebrojivu particiju $\{X_n : n \in \omega\}$ skupa I postoji $k \in \omega$ takvo da $X_k \in F$. Kada se to ima u vidu, dovoljno je dokazati da kanonsko utapanje h preslikava $\mathcal{A}$ na $\mathcal{A}^I_{/F}$.

Neka je $f_F \in A^I_{/F}$ i za svako $a \in A$, $X_a = \{i \in I : f(i) = a\}$. Familija $\{X_a : a \in A\}$ je prebrojiva particija skupa I. Zbog prebrojive kompletnosti ultrafiltra F, postoji $a_0 \in A$ takvo da $X_{a_0} \in F$. To znači da je $h(a_0) = f_F$, tj. kanonsko utapanje h preslikava $\mathcal{A}$ na $\mathcal{A}^I_{/F}$.

Primer 8. Ako je $\mathcal{A}$ konačan model jezika $\mathcal{L}$ i F proizvoljan ultrafilter nad I, onda $|A^I_{/F}| = |A|$.

Opštije, pretpostavimo da je $(\mathcal{A}_i : i \in I)$ familija konačnih modela jezika $\mathcal{L}$ i F ultrafilter nad skupom I.

Ako postoji $n \in \omega$ takvo da $\{i \in I : |A_i| = n\} \in F$, onda je $|A^I_{/F}| = |A|$.

Primer 9. Postoji familija funkcija $A \subseteq \omega^\omega$ kardinalnosti 2^ω koja zadovoljava sledeće uslove:

(a) ako $f \in A$, za svako $n \in \omega$, $f(n) < 2^n$,

(b) za sve $f, g \in A$, ako $f \leq g$, onda $|\{n \in \omega : f(n) = g(n)\}| < \omega$.

Za svaku funkciju $\varepsilon \in 2^\omega$, neka je $f_\varepsilon \in \omega^\omega$ funkcija takva da za svako $n \in \omega$, $f_\varepsilon(n) = \sum_{m<n} \varepsilon(m) \cdot 2^m$. Familija funkcija $A = \{f_\varepsilon : \varepsilon \in 2^\omega\}$ zadovoljava uslove (a) i (b).

Primer 10. Ako je $(\mathcal{A}_i : i \in I)$ familija konačnih modela jezika $\mathcal{L}$ i F ultrafilter nad I takav da za svako $n \in \omega$, $X_n = \{i \in I : |A_i| = n\} \notin F$, onda je $2^\omega \leq |A^I_{/F}|$.

Kako ni jedan od skupova X_n ne pripada ultrafiltru F, on mora biti prebrojivo nekompletan ultrafilter, a to znači da je F neglavni ultrafilter. Takođe, postoje proizvoljno veliki prirodni brojevi n takvi da X_n nije prazan. Od nepraznih skupova X_n napravimo particiju $\{I_n : n \in \omega\}$ skupa I koja zadovoljava uslove:

(a) za svako $n \in \omega$, $I_n \notin F$,

(b) ako $i \in I_n$, onda $|A_i| \geq 2^n$.

Pritom, za svako $i \in I$, postoji jedinstveno određen prirodan broj $n(i) \in \omega$ takav da $i \in I_{n(i)}$.

Za svako $i \in I$ neka je $(a_{i,k} : k \leq 2^{n(i)})$ niz različitih elemenata skupa A_i i neka je $A \subseteq \omega^\omega$ familija funkcija koja zadovoljava uslove prethodnog primera.

Za svako $f \in A$ definišimo funkciju $h_f \in \prod A_i$ tako da za svako $i \in I$, $h_f(i) = a_{i,f(n(i))}$. Za svako $i \in I$, $f(n(i)) < 2^{n(i)}$, pa $h_f(i)$ uvek postoji. Skup $\{h_f/F : f \in A\} \subseteq \prod A_i/F$ ima kardinalnost 2^ω.

Primer 11. Pretpostavimo da je $(\mathcal{A}_i : i \in \omega)$ prebrojiva familija konačnih modela jezika $\mathcal{L}$ i F ultrafilter nad ω. Ako postoji $n \in \omega$ takav da $\{i \in \omega : |A_i| = n\} \in F$, onda je $|A^I_{/F}| = n$, inače $|A^I_{/F}| = 2^\omega$.

Dakle, ultraproizvod prebrojive familije konačnih skupova je ili konačan ili kardinalnosti 2^ω. U slučaju familije skupova čiji svaki element ima kardinalnost ω, prebrojiva kompletnost ultrafiltra omogućava ocenu kardinalnosti njenog ultraproizvoda. Bez nekih dodatnih skupovno teoretskih pretpostavki, kardinalnost takvog ultraproizvoda se teško može tačno odrediti.

Primer 12. Neka je $\mathcal{A}$ model jezika $\mathcal{L}$ kardinalnosti $|A| = \omega$.

(a) Ako je F prebrojivo kompletan ultrafilter nad I, $|A^I/F| = \omega$.

(b) Ako je F prebrojivo nekompletan ultrafilter, $|A^I/F| \geq 2^\omega$.

Pritom, ako je $|I| = \omega$, onda $|A^I/F| = 2^\omega$.

Kako je tvrđenje (a) je očigledno, pretpostavimo da je F prebrojivo nekompletan ultrafilter. To znači da postoji particija $\{X_n, n \in \omega\}$ skupa I čiji elementi ne pripadaju ultrafiltru F. Za svako $i \in X_n$, $n \in \omega$, neka je B_i skup takav da $|B_i| = n$. Na osnovu ranijih primera, to znači da je $2^\omega \leq |\prod B_i/F| \leq |A^I/F|$.

Na osnovu prethodnih primera možemo zaključiti da ako su svi modeli familije $(\mathcal{A}_i : i \in I)$ beskonačni i F nekompletan ultrafilter na skupom I, onda je $|\prod A_i/F| \geq 2^\omega$. To znači da su ultraproizvodi, osim u trivijalnim slučajevima, uvek neprebrojivi modeli.

Aksiomatske klase

Po svojoj prirodi, ultraproizvodi su algebarska konstrukcija. Ipak, svojim nastankom i u primenama oni su više vezani za logiku nego za algebru. To se pre svega ogleda u teoriji modela teorije skupova i jednoj karakterizaciji elementarne ekvivalencije. U narednim razmatranjima ilustrovaćemo primenu konstrukcije ultraproizvoda na probleme aksiomatizacije standardnih matematičkih teorija.

Neka je $\mathcal{L}$ jezik. Sa $\mathrm{Mod}(\mathcal{L})$ označavamo klasu svih modela jezika $\mathcal{L}$. Klasu svih modela teorije Σ jezika $\mathcal{L}$ označavamo sa $\mathrm{Mod}(\Sigma)$.

Ako je $\mathcal{K}$ klasa modela jezika $\mathcal{L}$ i $\mathcal{K} = \mathrm{Mod}(\Sigma)$, teorija Σ je skup aksioma klase $\mathcal{K}$. Klasa modela $\mathcal{K}$ je aksiomatska ako postoji skup aksioma za $\mathcal{K}$. Kada je takav skup konačan, klasa $\mathcal{K}$ je konačno aksiomatska.

Za proizvoljnu klasu modela $\mathcal{K}$ jezika $\mathcal{L}$, sa $\mathrm{Th}(\mathcal{K})$ označavamo skup svih rečenica jezika $\mathcal{L}$ koje važe u svim modelima klase $\mathcal{K}$. Jasno, klasa $\mathcal{K}$ je aksiomatska ako i samo ako $\mathcal{K} = \mathrm{Mod}(\mathrm{Th}(\mathcal{K}))$.

Primer 1. Za svako $n \in \omega$ neka je $\varphi^{\geq n}$ sledeća rečenica:

$$\exists v_1 \cdots \exists v_n \, (v_1 \neq v_2 \wedge \cdots \wedge v_1 \neq v_n \wedge v_2 \neq v_3 \wedge \cdots v_{n-1} \neq v_n).$$

Za svaki model $\mathcal{A}$ jezika $\mathcal{L}$, $\mathcal{A} \models \varphi^{\geq n}$ ako i samo ako domen A sadrži bar n elemenata. Dakle, za svako $n \in \omega$, klasa $\mathcal{K}_{\geq n}$ svih modela jezika $\mathcal{L}$ koji sadrže bar n elemenata je konačno aksiomatska i $\mathcal{K}_{\geq n} = \mathrm{Mod}(\varphi^{\geq n})$.

Neka je $n \in \omega$. Ako sa φ^n označimo rečenicu $\varphi^{\geq n} \wedge \neg\varphi^{\geq n+1}$, onda $\mathcal{A} \models \varphi^n$ ako i samo ako domen A sadrži tačno n elemenata. Dakle, za svako $n \in \omega$, klasa $\mathcal{K}_n$ svih modela jezaika $\mathcal{L}$ sa tačno n elemenata je konačno aksiomatska.

Primer 2. Neka je $\Sigma = \{\varphi^{\geq n} : n \in \omega\}$. Tada $\mathcal{A} \models \Sigma$ ako i samo ako $\mathcal{A}$ je beskonačan model, odnosno, klasa $\mathcal{K}_{inf}$ beskonačnih modela jezika $\mathcal{L}$ je aksiomatska.

Skup aksioma Σ klase $\mathcal{K}_{inf}$ je beskonačan. U sledećim primerima dokazaćemo da klasa $\mathcal{K}_{inf}$ nije konačno aksiomatska.

Primer 3. Ako skup rečenica Σ ima proizvoljno veliki konačan model, onda Σ ima beskonačan model.

Pretpostavimo da je $(\mathcal{A}_n : n \in \omega)$ niz konačnih modela teorije Σ takav da za sve $m, n \in \omega$, ako $m < n$, onda $|A_m| < |A_n|$. Neka je F neglavni ultrafilter nad ω i $\mathcal{A}$ ultraproizvod $\prod \mathcal{A}_n / F$. Kako Σ važi u svakom $\mathcal{A}_n$, prema teoremi o ultraproizvodu, Σ važi u $\mathcal{A}$.

Po definiciji niza $(\mathcal{A}_n : n \in \omega)$, za svako $n \in \omega$, rečenica φ^n važi u najviše jednom modelu $\mathcal{A}_k$, međutim, kako je F neglavni ultrafilter, F ne sadrži jednoelementni ili prazan skup. Prema teoremi o ultraproizvodu, za sve $n \in \omega$, u $\mathcal{A}$ ne važi φ^n, odnosno. model $\mathcal{A}$ je beskonačan. $\square$

Prethodni primer pokazuje da klasa $\mathcal{K}_{fin}$ svih konačnih modela jezika $\mathcal{L}$ nije aksiomatska.

Primer 4. (a) Ako su $\mathcal{K}_1$ i $\mathcal{K}_2$ aksiomatske klase modela jezika $\mathcal{L}$, onda su $\mathcal{K}_1 \cap \mathcal{K}_2$ i $\mathcal{K}_1 \cup \mathcal{K}_2$ aksiomatske klase.

(b) Klasa $\mathcal{K}$ je konačno aksiomatska ako i samo ako klase $\mathcal{K}$ i $\mathcal{K}^c$ su aksiomatske.

Na osnovu činjenice da klasa $\mathcal{K}_{fin}$ svih konačnih modela jezika $\mathcal{L}$ nije aksiomatska i poslednjeg tvrđenja sledi da klasa $\mathcal{K}_{inf}$ svih beskonačnih modela jezika $\mathcal{L}$ nije konačno aksiomatska.

Primer 5. Neka su Σ_1 i Σ_2 teorije, a $\mathcal{K}_1$ i $\mathcal{K}_2$ klase modela jezika $\mathcal{L}$.

(a) Ako $\Sigma_1 \subseteq \Sigma_2$, onda $\mathrm{Mod}(\Sigma_2) \subseteq \mathrm{Mod}(\Sigma_1)$.

(b) Ako $\mathcal{K}_1 \subseteq \mathcal{K}_2$, onda $\mathrm{Th}(\mathcal{K}_2) \subseteq \mathrm{Th}(\mathcal{K}_1)$.

Primer 6. (a) Za svaku teoriju Σ jezika $\mathcal{L}$, $\Sigma \subseteq \mathrm{Th}(\mathrm{Mod}(\Sigma))$, a jednakost u ovoj relaciji važi ako i samo ako postoji klasa modela $\mathcal{K}$ takva da $\Sigma = \mathrm{Th}(\mathcal{K})$.

(b) Za svaku klasu modela $\mathcal{K}$ jezika $\mathcal{L}$, $\mathcal{K} \subseteq \mathrm{Mod}(\mathrm{Th}(\mathcal{K}))$, a jednakost u ovoj relaciji važi ako i samo ako postoji teorija Σ takva da $\mathcal{K} = \mathrm{Mod}(\Sigma)$.

Primer 7. Za svako $i \in I$, neka je $\mathcal{K}_i$ klasa modela jezika $\mathcal{L}$. Tada $\mathrm{Th}(\bigcup_{i\in I} \mathcal{K}_i) = \bigcap_{i\in I} \mathrm{Th}(\mathcal{K}_i)$.

Primer 8. Neka je Σ_i, $i \in I$ familija teorija jezika $\mathcal{L}$, onda

(a) $\mathrm{Mod}(\bigcup_{i\in I} \Sigma_i) = \bigcap_{i\in I} \mathrm{Mod}(\Sigma_i)$.

(b) Jednakost $\mathrm{Mod}(\bigcap_{i\in I} \Sigma_i) = \bigcup_{i\in I} \mathrm{Mod}(\Sigma_i)$ važi samo pod uslovom da je skup I konačan i da svaka od teorija Σ_i ima oblik $\Sigma_i = \mathrm{Th}(\mathcal{K}_i)$, za neku klasu modela $\mathcal{K}_i$ jezika $\mathcal{L}$.

Teorema 28. Klasa modela $\mathcal{K}$ je aksiomatska ako i samo ako $\mathcal{K}$ je zatvorena za elementarnu ekvivalenciju i ultraproizvode.

Dokaz: Pretpostavimo da je klasa $\mathcal{K}$ zatvorena za ultraproizvode i elementarnu ekvivalenciju. Ako je $\Sigma = \mathrm{Th}(\mathcal{K})$, tvrdimo da je Σ skup aksioma za klasu modela $\mathcal{K}$.

Neka je $\mathcal{A}$ model u kojem važi Σ i neka je $\mathrm{Th}(\mathcal{A}) = I$. Za svako $\varphi \in I$, rečenica $\neg\varphi$ nije dokaziva u Σ, pa postoji model $\mathcal{A}_\varphi \in \mathcal{K}$ u kojem važi φ.

Za proizvoljnu formulu $\varphi \in I$ neka je $I_\varphi = \{\psi \in I : \mathcal{A}_\psi \models \varphi\}$.

Familija $(I_\varphi : \varphi \in I)$ ima svojstvo konačnih preseka, pa postoji ultrafilter F nad skupom I koji proširuje familiju $(I_\varphi : \varphi \in I)$. Otuda sledi da je ultarproizvod $\prod \mathcal{A}_\varphi/F$ familije elemenata klase $\mathcal{K}$ elementarno ekvivalentan modelu $\mathcal{A}$, pa dakle model $\mathcal{A}$ pripada klasi $\mathcal{K}$. $\Box$

Teorema 29. Modeli $\mathcal{A}$ i $\mathcal{B}$ jezika $\mathcal{L}$ su elementarno ekvivalentni ako i samo ako model $\mathcal{B}$ može se elementarno utopiti u ultrastepen modela $\mathcal{A}$.

Dokaz: Neka je $\mathcal{A}^I_{/F}$ ultrastepen modela $\mathcal{A}$. Ako se model $\mathcal{B}$ može elementarno utopiti u $\mathcal{A}^I_{/F}$, onda je $\mathcal{B} \equiv \mathcal{A}^I_{/F}$, pa dakle $\mathcal{A} \equiv \mathcal{B}$.

Pretpostavimo da je $\mathcal{A} \equiv \mathcal{B}$. Neka je $b \in B^\beta$ numeracija skupa $\mathcal{B}$. Označimo sa I skup rečenica $\mathrm{Th}(\mathcal{B}, b)$ jezika $\mathcal{L}_\beta$.

Svaka rečenica $\varphi \in I$ sadrži konačan broj konstanti $c_{\gamma_1}, \ldots, c_{\gamma_k}$ jezika $\mathcal{L}_\beta$. Neka je φ^* formula jezika $\mathcal{L}$ dobijena iz φ zamenom tih konstanti promenljivim $v_{i_1}, \ldots, v_{i_k}$ koje se ne javljaju u φ. Kako u modelu $(\mathcal{B}, b)$ važi φ i kako je φ^* formula jezika $\mathcal{L}$ to

$$\mathcal{B} \models \exists v_{i_1} \cdots \exists v_{i_k}\, \varphi^*.$$

Kako je $\mathcal{A} \equiv \mathcal{B}$, $\mathcal{A} \models \exists v_{i_1} \cdots \exists v_{i_k}\, \varphi^*$. Otuda sledi da postoji numeracija $a_\varphi = (a_{\varphi\gamma} : \gamma < \beta)$ skupa A takva da $(\mathcal{B}, a_\varphi) \models \varphi$. Za svaku rečenicu $\varphi \in I$ moguće je odrediti niz $a_\varphi \in A^\beta$.

Neka je $I_\varphi = \{\psi \in I : (\mathcal{A}, a_\psi) \models \varphi\}$. Familija $(I_\varphi : \varphi \in I)$ ima svojstvo konačnih preseka i može se proširiti do ultrafiltra F nad skupom I. Tvrdimo da se $\mathcal{B}$ može elementarno utopiti u $\mathcal{A}^I_{/F}$.

Definišimo preslikavanje $h : B \to A^I_{/F}$ tako da $h(b_\gamma) = f_{\gamma F}$, za proizvoljno $\gamma < \beta$, gde je $f_\gamma \in A^I$ funkcija takva da za svako $\varphi \in I$, $f_\gamma(\varphi) = a_{\varphi\gamma}$.

Pretpostavimo da je ψ formula jezika $\mathcal{L}$ i $d \in B^\omega$ valuacija promenljivih u modelu $\mathcal{B}$. Treba dokazati da $\mathcal{B} \models_d \psi$ ako i samo ako $\mathcal{A}^I_{/F} \models_{h(d)} \psi$.

Neka je ψ^* rečenica jezika $\mathcal{L}_\beta$ koja se dobija iz ψ na sledeći način: za svako $k \in \omega$, ako je $d_k = b_\gamma$, sva slobodna javljanja promenljive v_k u formuli ψ zamene se konstantom c_γ. Tada, $\mathcal{B} \models_d \psi$ ako i samo ako $(\mathcal{B}, b) \models \psi^*$.

Ako je $f_\varphi = a_\varphi$, za sve $\varphi \in I$, na osnovu teoreme o ultraproizvodu i po definiciji, redom se dobija da važi:

$$\begin{aligned} (\mathcal{B}, b) \models \psi^* \quad &\Leftrightarrow \quad \psi^* \in I, \\ &\Leftrightarrow \quad I_{\psi^*} \in F, \\ &\Leftrightarrow \quad \{\varphi \in I : (\mathcal{A}, a_\varphi) \models \psi^*\} \in F, \\ &\Leftrightarrow \quad (\mathcal{A}^I/F, f_F) \models \psi^*. \end{aligned}$$

Kako je po definiciji, $h(b) = f_{/F}$ otuda sledi da $(\mathcal{B}, b) \models \psi^*$ ako i samo ako $(\mathcal{A}^I/F, h(b)) \models \psi^*$, što konačno znači da $\mathcal{B} \models_d \psi$ ako i samo ako $\mathcal{A}^I/F \models_{h(d)} \psi$, tj. preslikavanje h je elementarno utapanje. $\Box$

Primer 9. Elementarno ekvivalentni konačni modeli su izomorfni.

Ako je $n \in \omega$ kardinalnost modela $\mathcal{A}$, onda $\mathcal{A} \models \varphi^n$, pa zbog elementarne ekvivalencije, $\mathcal{B} \models \varphi^n$, tj. modeli $\mathcal{A}$ i $\mathcal{B}$ su iste kardinalnosti. Takođe, zbog elementarne ekvivalencije, model $\mathcal{A}$ može se elementarno utopiti u neki ultrastepen modela $\mathcal{B}$. Kako je model $\mathcal{B}$ konačan, svaki njegov ultrastepen je izomorfan sa $\mathcal{B}$. Zbog jednake kardinalnosti, model $\mathcal{A}$ je izomorfan sa $\mathcal{B}$.

Kako smo već napomenuli, jezik teorije grupa $\mathcal{L}_G = \{+, 0\}$ sadrži jedan binarni operacijski znak i jednu konstantu. Sa φ_G označavaćemo konjunkciju aksioma komutativnih grupa.

Primer 10. Klasa konačnih grupa, konačnih komutativnih grupa i klasa cikličnih grupa nisu aksiomatske.

Ako je $\mathcal{G} = (G, +, 0)$ grupa, red elementa $x \in G$ je najmanji prirodan broj n takav da $\underbrace{x + \cdots + x}_{n} = n \cdot x = 0$, ako takav $n \in \omega$ postoji. U suprotnom, element $x \in G$ je beskonačnog reda.

Primer 11. Za svaki prost broj $p \in \omega$, klasa komutativnih grupa u kojima su svi elementi reda p je aksiomatska. Njena aksioma je konjunkcija aksiome φ_G i rečenice $\forall x\,(p \cdot x = 0)$.

Nije teško dokazati da za svaki prost broj $p \in \omega$, bilo koje dve komutativne grupe iste kardinalnosti, u kojima je svaki element reda p, su izomorfne.

Primer 12. Komutativna grupa $\mathcal{G}$ je grupa bez torzije ako svaki element grupe $\mathcal{G}$ ima beskonačni red.

Za svako $n \geq 1$ neka je φ_n rečenica $\forall x\,(n \cdot x = 0 \rightarrow x = 0)$. Skup rečenica $\Sigma_G = \{\varphi_G\} \cup \{\varphi_n : n > 0\}$ je skup aksioma klase komutativnih grupa bez torzije.

Klasa komutativnuh grupa bez torzije nije konačno aksiomatska.

Primer 13. Komutativna grupa $\mathcal{G}$ je grupa sa deljenjem ako za svaki prirodan broj $n \in \omega$, važi $\mathcal{G} \models \forall x \exists y\,(n \cdot y = x)$.

Klasa komutativnih grupa sa delenjem nije konačno aksiomatska.

Primer 14. (a) Bilo koje dve neprebrojive komutativne grupe sa deljenjem i bez torzije su izomorfne.

Postoji neprebrojivo mnogo komutativnih grupa sa deljenjem i bez torzije čija je kardinalnost ω.

Jezik teorije polja $\mathcal{L}_F = \{+, \cdot, 0, 1\}$ sadrži dva binarna opreacijska simbola i dve konstante. Sa φ_F označavamo konjunkciju aksioma teorije polja. Klasa svih polja je klasa modela rečenice φ_F.

Polje $\mathcal{A}$ je polje karakteristike $p \in \omega$ ako je p najmanji prirodan broj takav da za svako $x \in A$, $\underbrace{x + \cdots + x}_{p} = p \cdot x = 0$.

Primer 15. (a) Karakteristika polja je prost broj. Za svaki prost broj $p \in \omega$, postoji polje karakteristike p.

(b) Za svaki prirodan broj $n \geq 1$, do na izomorfizam, postoji jedinstveno određeno polje karakteristike p kardinalnosti p^n.

Za svaki prirodan broj $p \in \omega$, označimo sa φ^p rečenicu

$$\forall x\,(p \cdot x = 0) \wedge \exists x\,((p-1) \cdot x \neq 0) \wedge \exists x\,((p-2) \cdot x \neq 0) \wedge \cdots \wedge \exists x\,(x \neq 0).$$

Za svaki prost broj $p \in \omega$, neka je φ_F^p rečenica $\varphi_F \wedge \varphi^p$. Model $\mathcal{A}$ jezika teorije polja zadovoljava φ_F^p ako i samo ako $\mathcal{A}$ je polje karakteristike p. Dakle, klasa polja date karakteristike p je konačno aksiomatska.

Polje $\mathcal{A}$ je polje karakteristike nula ako za svaki prost broj p, $\mathcal{A}$ nije karakteristike p. Neka je $\Sigma_F^0 = \{\neg\varphi^p : p \in \omega\} \cup \{\varphi_F\}$. Polje $\mathcal{A}$ je karakteristike nula ako i samo ako $\mathcal{A}$ je model za Σ_F^0.

Teorema 30. Klasa polja karakteristike nula nije konačno aksiomatska.

Dokaz: Pretpostavimo da postoji rečenica φ_F^0 jezika teorije polja takva da za svaki model jezika $\mathcal{L}_F$, imamo $\mathcal{A} \models \varphi_F^0$ ako i samo ako $\mathcal{A}$ je polje karakteristike nula.

Za svaki prost broj $p \in \omega$ neka je $\mathcal{A}_p$ polje karakteristike p. Jasno, u modelu $\mathcal{A}_p$ važi rečenica φ^p. Neka je F neglavni ultrafilter nad skupom prostih brojeva $P \subseteq \omega$ i neka je $\mathcal{A} = \prod \mathcal{A}_p/F$.

Za svako $p \in P$, $\mathcal{A}_p$ je model rečenice φ_F, pa prema teoremi o ultraproizvodu, $\mathcal{A}$ je model rečenice φ_F, tj. $\mathcal{A}$ je polje. Za svako $p \in P$, rečenica φ^p važi u tačno jednom faktoru $\mathcal{A}_p$. Kako je F neglavni ultrafilter, F ne sadrži jednoelementni skup, pa prema teoremi o ultraproizvodu, za svako $p \in P$, u modelu $\mathcal{A}$ ne važi rečenica φ^p.

Ovo poslednje znači da je $\mathcal{A}$ polje karakteristike nula, tj. $\mathcal{A} \models \varphi_F^0$. Međutim, kako je $\{p \in P : \mathcal{A}_p \models \varphi_F^0\} = \emptyset$, prema teoremi o ultraproizvodu, $\emptyset \in F$, što nije moguće. $\Box$

Polje $\mathcal{A}$ je algebarski zatvoreno polje ako svaki polinom sa koeficijentima u $\mathcal{A}$, stepena > 0, ima nulu u polju $\mathcal{A}$. Za svako $n \geq 2$ neka je

$$\theta_n = \forall x_1 \cdots \forall x_n\,(x_n \neq 0 \to \exists y\,(x_n y^n + \cdots + x_1 y + x_0 = 0).$$

Ako je $\Sigma_{CF} = \{\varphi_F\} \cup \{\theta_n : 2 \leq n < \omega\}$, polje $\mathcal{A}$ je algebarski zatvoreno ako i samo ako $\mathcal{A}$ je model za Σ_{CF}.

Primer 16. Svako polje ima algebarsko zatvorenje, tj. ako je $\mathcal{A}$ polje, onda postoji minimalno algebarski zatvoreno polje $\mathcal{A}^*$ koje sadrži $\mathcal{A}$.

Neka je $\mathcal{A}$ polje, Δ_A^+ pozitivni dijagram polja $\mathcal{A}$ i $\Sigma = \{\varphi_F\} \cup \Delta_A^+$. Prema teoremi o pozitivnom dijagramu, svaki model teorije Σ je proširenje polja $\mathcal{A}$. Neka je $I = A[x]$ skup svih polinoma stepena ≥ 1 sa koeficijentima u polju $\mathcal{A}$. Za svako $p \in I$ neka je $\mathcal{A}_p$ faktorizacijsko polje polinoma p, tj. najmanje proširenje polja $\mathcal{A}$ koje sadrži sve nule polinoma p.

Za svako $p \in I$ neka je $I_p = \{q \in I : p$ faktoriše u $\mathcal{A}_q\}$. Kako za proizvoljne $p_1, \ldots, p_n \in I$, $p_1 \cdots p_n \in I_{p_1} \cap \cdots \cap I_{p_n}$, familija $(I_p : p \in I)$ ima svojstvo konačnih preseka, što znači da se može proširiti do ultrafiltra F nad skupom I. Ako je $\mathcal{B} = \prod \mathcal{A}_p/F$, prema teoremi o ultraproizvodu, $\mathcal{B}$ je model za Σ, tj. $\mathcal{B}$ je proširenje polja $\mathcal{A}$.

Neka je $p(x) = x^n + a_1 x_{n-1} + \cdots + a_{n-1}x + a_n$ polinom nad poljem $\mathcal{A}$. Tvrdimo da $p(x)$ faktoriše u $\mathcal{B}$. Neka je φ rečenica

$$\exists y_1 \cdots \exists y_n \, (y_1 + \cdots + y_n = -a_1 \wedge \cdots \wedge y_1 \cdots y_n = (-1)^n a_n).$$

Rečenica φ važi tačno u onim modelima za Σ u kojima faktoriše polinom $p(x)$. Kako je $\{q \in I : \mathcal{A}_q \models \varphi\} = I_p \in F$, prema teoremi o ultraproizvodu, $\mathcal{B} \models \varphi$, odnosno, polinom $p(x)$ faktoriše u polju $\mathcal{B}$.

Dakle, polje $\mathcal{B}$ je ekstenzija polja $\mathcal{A}$ u kojoj faktoriše svaki normirani polinom sa koeficijentima iz $\mathcal{A}$. Neka je A^* skup svih elemenata polja $\mathcal{B}$ koji su algebarski nad poljem $\mathcal{A}$. Skup takvih elemenata čini polje i struktura $\mathcal{A}^*$ je algebarsko zatvorenje polja $\mathcal{A}$.

Da to dokažemo, pretpostavimo da je $p(x)$ normirani polinom nad poljem $\mathcal{A}^*$. Kao polinom nad poljem $\mathcal{B}$, polinom $p(x)$ faktoriše nad poljem $\mathcal{B}$, pa postoje $a_1, \ldots, a_n \in B$ takvi da je $p(x) = (x - a_1) \cdots (x - a_n)$. Kako su elementi $a_1, \ldots, a_n$ algebarski nad $\mathcal{A}^*$, oni moraju biti algebarski i nad poljem $\mathcal{A}$.

Za svako $i \in \{1, \ldots, n\}$ neka je $p_i(x)$ minimalni polinom elementa a_i nad poljem $\mathcal{A}$. Kako $p_i(x)$ faktoriše u polju $\mathcal{B}$, njegovi koreni pripadaju polju $\mathcal{B}$, a kako su ti koreni algebarski nad $\mathcal{A}$, oni pripadaju $\mathcal{A}^*$. Dakle $a_1, \ldots, a_n \in A^*$, tj. polinom $p(x)$ faktoriše u polju $\mathcal{A}^*$, pa je $\mathcal{A}^*$ algebarski zatvoreno polje.

Primer 17. Ako polje $\mathcal{A}$ nije algebarski zatvoreno, ultrafilter F, konstruisan u prethodnom primeru, nije glavni filter. Takođe, polje $\mathcal{B}$ nije algebarska ekstenzija polja $\mathcal{A}$, a ultrastepen $\mathcal{A}^I_{/F}$ je čista transendentna ekstenzija od $\mathcal{A}$.

Primer 18. Za svako $n \in \omega$ postoji polje $\mathcal{A}_n$, koje nije algebarski zatvoreno, u kojem faktorišu svi polinomi pozitivnog stepena $\leq n$.

Primer 19. Klasa algebarski zatvorenih polja nije konačno aksiomatska.

Pretpostavimo da postoji rečenica φ jezika teorije polja koja aksiomatizuje klasu algebarski zatvorenih polja karakteristike nula.

Za svako $n \in \omega$, neka je $\mathcal{A}_n$ polje koje nije algebarski zatvoreno u kojem faktoriše svaki polinom stepena $\leq n$. Neka je F neglavni ultrafilter nad ω i $\mathcal{A} = \prod \mathcal{A}_n/F$. Za svako $n \in \omega$, $\mathcal{A}_n$ je polje, pa prema teoremi o ultraproizvodu, $\mathcal{A}$ je takođe polje.

Za svako $n \geq 2$, skup $X_n = \{k \in \omega : \mathcal{A}_k \models \theta_n\}$ je neprazan i ima konačan komplement. Pritom, rečenica θ_n je jedna od aksioma teorije zatvorenih polja. Kako je F neglavni ultrafilter, $X_n \in F$, pa prema teoremi o ultraproizvodu, za svako $n \geq 2$, $\mathcal{A} \models \theta_n$. Dakle, $\mathcal{A}$ je algebarski zatvoreno polje, pa $\mathcal{A} \models \varphi$. Međutim, za svako $n \in \omega$, $\mathcal{A}_n \models \neg\varphi$, što nije moguće. $\Box$

Primer 20. Klasa algebarski zatvorenih polja karakteristike nula nije konačno aksiomatska. Slično, za svaki prost broj $p \in \omega$, klasa algebarski zatvorenih polja karakteristike p nije konačno aksiomatska.

Jezik parcijalnih uređenja je $\mathcal{L} = \{<\}$ i neka je φ_u rečenica jezika $\mathcal{L}$ koja opisuje striktna linearna uređenja.

Primer 21. Teorija gustog linearnog uređenja bez krajeva je konačno aksiomatska. Isto važi i za gusta linearna uređenja sa jednim, odnosno, dva kraja.

Aksioma klase gustih linearnih uređenja bez krajeva je konjunkcija rečenice φ_u i sledećih rečenica:

$$\varphi_1 = \forall x \forall y\, (x < y \to \exists z\, (x < z \land z < y))$$
$$\varphi_2 = \forall x\, (\exists y\, (y < x) \land \exists y\, (x < y)).$$

Linearno uređenje $\mathcal{P} = (P, <)$ je dobro uređenje ako svaki neprazan podskup skupa P ima najmanji element u uređenju $\mathcal{P}$.

Primer 22. Ako je $(\mathcal{P}_i, i \in I)$ familija dobrih uređenja i F prebrojivo kompletan ultrafilter nad skupom I, onda je $\mathcal{P} = \prod \mathcal{P}_i/F$ dobro uređenje.

Za svako $i \in I$, $\mathcal{P}_i \models \varphi_u$, pa prema Lošovoj teoremi, $\mathcal{P} \models \varphi_u$, tj. $\mathcal{P}$ je linearno uređenje i pretpostavimo da je $f_0/F >_F \cdots >_F f_n/F >_F \cdots$, beskonačan opadajući niz u P.

Za svako $n \in \omega$, $X_n = \{i \in I : f_n(i) > f_{n+1}(i)\} \in F$. Kako je F prebrojivo kompletan ultrafilter, skup $X = \bigcap_{n \in \omega} X_n$ pripada filtru F. To znači da skup X nije prazan.

Ako $i \in X$, niz $f_0(i) > \cdots > f_n(i) > \cdots$ je beskonačan opadajući niz u dobrom uređenju $\mathcal{P}_i$, što nije moguće.

Primer 23. Neka je $(a_n : n \in \omega)$ beskonačan striktno opadajući niz racionalnih brojeva. Za svako $n \in \omega$, neka je $P_n = \{a_0, \ldots, a_n\}$ i $\mathcal{P}_n =$

$(P_n, <)$, gde je $<$ uređenje racionalnih brojeva. Ultraproizvod $\mathcal{P} = \prod \mathcal{P}_n/F$ je dobro uređenje ako i samo ako F je glavni ultrafilter nad ω.

Da to dokažemo, pretpostavimo da je F neglavni ultrafilter nad ω. Za svako $k \in \omega$, definišimo funkciju f_k tako da za svako $n \in \omega$,

$$f_k(n) = \begin{cases} a_{n+1} & \text{ako} \quad n \leq k-1, \\ a_k & \text{ako} \quad k \leq n. \end{cases}$$

Niz $f_{0/F} > f_{1/F} > \cdots$ je beskonačan opadajući niz elemenata uređenja $\mathcal{P}$, pa ultraproizvod $\mathcal{P}$ nije dobro uređenje.

Obratno, ako pretpostavimo da je F glavni ultrafilter nad ω, onda za neko $k \in \omega$ važi $\mathcal{P} \cong \mathcal{P}_k$.

Otuda sledi da klasa dobrih uređenja nije aksiomatska.

Primer 24. Za svako $i \in I$, neka je $\mathcal{P}_i$ beskonačno dobro uređenje. Ako je F prebrojivo nekompletan ultrafilter nad skupom I, ultraproizvod $\mathcal{P} = \prod \mathcal{P}_i/F$ nije dobro uređenje.

Primer 25. Neka je F neglavni ultrafilter nad ω.

(a) Ultraproizvod $\mathcal{N}^* = \mathcal{N}^\omega/F$ je nestandarni model kompletne aritmetike kardinalnosti 2^ω.

(b) Model $\mathcal{N}^*$ sadrži 2^ω prostih brojeva.

Primer 26. Klase arhimedovskih polja, kompletnih uređenja, i Bulovih algebri koje su izomorfne algebrama svih podskupova nekog skupa nisu aksiomatske klase.

Kompletne teorije

U narednim razmatranjima govorićemo o kompletnim teorijama i pokušati da to svojstvo teorija delimično izrazimo modelsko-teorijskim sredstvima. Jednu takvu karakterizaciju kompletnih teorija smo implicitno i ranije spominjali.

Primer 1. Teorija je kompletna ako i samo ako svi njeni modeli su elementarno ekvivalentni.

Navedena karakterizacija nema stvarni značaj budući da njena primena u proveri kompletnosti neke teorije podrazumeva razmatranje beskonačnog skupa rečenica. Ni njena preformulacija pomoću elementarnih utapanja, nema bitno veći značaj u primenama.

Primer 2. Teorija Σ jezika $\mathcal{L}$ je kompletna ako i samo ako svaka dva modela teorije Σ mogu se elementarno utopiti u model teorije Σ.

Ako za svaka dva modela $\mathcal{A}$ i $\mathcal{B}$ teorije Σ postoji model $\mathcal{C}$ u koji se $\mathcal{A}$ i $\mathcal{B}$ mogu utopiti, onda su $\mathcal{A}$ i $\mathcal{B}$ elementarno ekvivalentni, pa je Σ kompletna teorija.

Prema teoremi o dijagramu, model $\mathcal{A}$ može se elementarno utopiti u model $\mathcal{C}$ ako i samo ako postoji ekspanzija modela $\mathcal{C}$ u jeziku $\mathcal{L}_\alpha$ koja je model dijagrama $\mathrm{Th}(\mathcal{A}, a) = \Delta_A$, za neku numeraciju $a \in A^\alpha$.

Neka su $\mathcal{A}$ i $\mathcal{B}$ modeli kompletne teorije Σ i $a \in A^\alpha$, $b \in B^\beta$ numeracije skupova A i B. Tvrdimo da postoji model $\mathcal{C}$ jezika $\mathcal{L}_{\alpha+\beta}$ takav da $(\mathcal{C}, a, b) \models \Delta_A \cup \Delta_B$.

Ako pretpostavimo suprotno, teorija $\Delta_A \cup \Delta_B$ sadrži konačan protivrečan skup rečenica. To znači da postoji rečenica $\varphi(\vec{a}) \in \Delta_A$ i rečenica $\psi(\vec{b}) \in \Delta_B$ takve da je $\{\varphi(\vec{a}), \psi(\vec{b})\}$ protivrečan skup, tj. $\varphi(\vec{a}) \vdash \neg\psi(\vec{b})$.

Zamenom konstanti jezika $\mathcal{L}_\beta$ u formuli $\psi(\vec{b})$ promenljivim koje se ne javljaju u $\varphi(\vec{a})$ dobijamo da $\varphi(\vec{a}) \vdash \forall\vec{x}\,\neg\psi(\vec{x})$. Kako $(\mathcal{A}, a) \models \varphi(\vec{a})$ to $(\mathcal{A}, a) \models \forall\vec{x}\,\neg\psi(\vec{x})$. Međutim, $\forall\vec{x}\,\neg\psi(\vec{x})$ je rečenica jezika $\mathcal{L}$, pa kako je Σ kompletna teorija, $\forall\vec{x}\,\neg\psi(\vec{x}) \in \Sigma$. Kako je $\mathcal{B}$ model teorije Σ, $\mathcal{B} \models \forall\vec{x}\,\neg\psi(\vec{x})$, što nije moguće.

Teorija Σ jezika $\mathcal{L}$ je kategorična ako su svaka dva modela teorije Σ izomorfna. Ako je κ kardinal, teorija Σ je κ- kategorična ako su svaka dva modela teorije Σ kardinalnosti κ izomorfna.

Primer 3. Teorija koja ima konačne i beskonačne modele nije kompletna. Kompletna teorija koja ima konačan model je kategorična.

Primer 4. (a) Teorija gustog linearnog uređenja bez krajeva je ω-kategorična.

(b) Teorija gustog linearnog uređenja bez krajeva nije 2^ω-kategorična.

Neka su $\mathcal{P}_1 = (P_1, <)$ i $\mathcal{P}_2 = (P_2, <)$ prebrojiva gusta linearna uređenja bez krajeva i $(a_n : n \in \omega)$, $(b_n : n \in \omega)$ numeracije skupova P_1 i P_2. Izomorfizam $f : P_1 \to P_2$ konstruiše na sledeći način:

Definišemo redom $f(a_0)$, $f^{-1}(b_0)$, $f(a_1)$, $f^{-1}(b_1), \ldots$ tako da u svakom koraku funkcija f čuva poredak. Za svako $n > 0$, ako vrednost $f(a_n)$ nije definisana, neka je $f(a_n) = b_k$, gde je $k \in \omega$ najmanji prirodan broj takav da funkcija f čuva poredak. Kako je funkcija f prethodno definisana za samo konačno mnogo $a \in P_1$ i kako je P_2 gusto linearno uređenje bez krajeva, takav prirodan broj k uvek postoji. Na isti način, za svako $n > 0$, definišemo vrednost $f^{-1}(b_n)$.

Neka je R je skup realnih brojeva i $R_0 = R - \{0\}$. Zbog kompletnosti realnih brojeva, uređenja $(R_0, \leq)$ i $(R, \leq)$ nisu izomorfna, tj. teorija gustog linearnog uređenja bez krajeva nije 2^ω kategorična.

Primer 5. Neka je Σ teorija u jeziku $\mathcal{L} = \{0, s\}$, gde je s unarna operacijska konstanta, koja sadrži sledeće rečenice:

$$\forall x\,(s(x) \neq 0) \wedge \forall x \forall y\,(s(x) = s(y) \to x = y),$$
$$\forall x\,(x \neq 0 \to \exists y\,(s(y) = x)),\ \text{i}\ \forall x\,(s^n(x) \neq x),\ \text{za svako}\ n > 0.$$

(a) Svi modeli teorije Σ su beskonačni. Model $\mathcal{M} = (\omega, 0, s)$ je model teorije Σ. Postoji prebrojiv model teorije Σ koji nije izomorfan sa $\mathcal{M}$.

(b) Ako je $\mathcal{A}$ neprebrojiv model teorije Σ kardinalnosti κ, $\mathcal{A}$ je izomorfan modelu čiji je tip uređenja $\omega + (\omega^* + \omega) \cdot \kappa$.

Dakle, teorija Σ nije ω-kategorična, ali jeste kategorična u svakom neprebrojivom kardinalu.

Teorema 31. Pretpostavimo da neprotivrečna teorija Σ ima samo beskonačne modele. Ako je Σ kategorična u nekom kardinalu $\kappa \geq \|\mathcal{L}\|$, onda je Σ kompletna teorija.

Dokaz: Dovoljno je dokazati da su svaka dva modela $\mathcal{A}$ i $\mathcal{B}$ teorije Σ elementarno ekvivalentna. Po pretpostavci, modeli $\mathcal{A}$ i $\mathcal{B}$ su beskonačni. Prema Skolemovoj teoremi, postoje modeli $\mathcal{A}'$ i $\mathcal{B}'$ kardinalnosti κ takvi da je $\mathcal{A} \equiv \mathcal{A}'$ i $\mathcal{B} \equiv \mathcal{B}'$. Kako je teorija Σ κ-kategorična, $\mathcal{A}' \cong \mathcal{B}'$. Otuda sledi da je $\mathcal{A}' \equiv \mathcal{B}'$, tj. $\mathcal{A} \equiv \mathcal{B}$. $\square$

Prethodna teorema je relativno jednostavan test kompletnosti teorija u predikatskom računu i to će biti ilustrovano u nekoliko sledećih primera.

Primer 6. Teorija gustog linearnog uređenja bez krajeva je kompletna.

Svi modeli ove teorije su beskonačni. Njena kompletnst sledi iz činjenice da su svaka dva prebrojiva gusta linearna uređenja bez krajeva izomorfna.

Primer 7. Teorija bezatomičnih Bulovih algebri je kompletna.

Primer 8. Neka je $p \in \omega$ prost broj. Teorija beskonačnih komutativnih grupa, u kojima je svaki element različit od neutralnog reda p, jeste kompletna teorija.

Ako je G grupa sa navedenom osobinom čija je kardinalnost κ i ako je X skup njenih generatora, onda i skup X mora biti kardinalnosti κ. Jednostavno se proverava da je grupa G izomorfna direktnoj sumi cikličnih grupa od kojih je svaka generisana jednim elementom skupa X.

Primer 9. Teorija beskonačnih komutativnih grupa sa deljenjem i bez torzije je kompletna.

Svaka beskonačna komutativna grupa sa deljenjem i bez torzije je izomorfna direktnoj sumi izomorfnih kopija aditivne grupe racionalnih brojeva. Otuda sledi da su u svakom neprebrojivom kardinalu bilo koje dve beskonačne komutativne grupe sa deljenjem i bez torzije izomorfne. Na primer, to znači da su aditivne grupe realnih i kompleksnih brojeva izomorfne.

Sa druge strane, ima prebrojivo mnogo neizomorfnih prebrojivih komutativnih grupa sa deljenjem i bez torzije. Na primer, otuda sledi da aditivna grupa racionalnih brojeva i aditivna grupa kompleksnih racionalnih brojeva nisu izomorfne.

Primer 10. Teorija prebrojivo mnogo različitih konstanti, odnosno, teorija jednakosti za beskonačne skupove je kompletna.

Primer 11. Teorija algebarski zatvorenih polja određene karakteristike je kompletna. Prema jednom klasičnom rezultatu, ova teorija je kategorična u svakom neprebrojivom kardinalu.

Primer 12. Za sve $n, p \in \omega$, ako je p prost broj ili nula, teorija n-dimenzionalnih vektorskih prostora nad algebarski zatvorenim poljem karakteristike p je kompletna.

Primer 13. Neka je Σ kompletna teorija jezika $\mathcal{L}$ i neka su $\Sigma_0 \supseteq \Sigma$ i $\Sigma_1 \supseteq \Sigma$ neprotivrečna proširenja teorije Σ u jeziku $\mathcal{L}_0$, odnosno, u jeziku $\mathcal{L}_1$. Ako sve individualne konstante jezika $\mathcal{L}_0$ pripadaju $\mathcal{L}$ i sve relacijske i operacijske konstante jezika $\mathcal{L}_2$ pripadaju jeziku $\mathcal{L}$, onda je $\Sigma_0 \cup \Sigma_1$ neprotivrečna teorija.

Pretpostavimo da je $\Sigma_0 \cup \Sigma_1$ protivrečna teorija. U tom slučaju postoje rečenice $\varphi_1, \ldots, \varphi_n \in \Sigma_1$, $n \geq 1$, za koje je skup rečenica $\Sigma_0 \cup \{\varphi_1, \ldots, \varphi_n\}$ protivrečan.

Neka je $\varphi = \varphi_1 \wedge \cdots \wedge \varphi_n$ i $c_1, \ldots, c_k$ sve individualne konstante jezika $\mathcal{L}_1$ koje se javljaju u rečenici φ, a koje ne pripadaju jeziku $\mathcal{L}$. Kako je $\Sigma_0 \cup \{\varphi\}$ protivrečan skup, $\Sigma_0 \vdash \neg\varphi$, odnosno, $\Sigma_0 \vdash \forall x_1 \cdots \forall x_k \, \neg\varphi(x_1, \ldots, x_n)$.

Po pretpostavci, Σ je kompletna, a Σ_0 neprotivrečna teorija, pa dakle važi $\Sigma \vdash \forall x_1 \cdots \forall x_k \, \neg\varphi(x_1, \ldots, x_n)$. Kako je $\Sigma_1 \supseteq \Sigma$, dobijamo da važi $\Sigma \vdash \forall x_1 \cdots \forall x_k \, \neg\varphi(x_1, \ldots, x_n)$, odnosno, $\Sigma_1 \vdash \neg\varphi$, što nije moguće.

Primer 14. Neka je Σ kompletna teorija u jeziku $\mathcal{L}$ i φ rečenica jezika $\mathcal{L}_1 \supseteq \mathcal{L}$ čije sve individualne konstante pripadaju jeziku $\mathcal{L}$. Ako je $\Sigma \cup \{\varphi\}$ neprotivrečna teorija i $\mathcal{A}$ model teorije Σ, onda je $\{\varphi\} \cup \mathrm{Th}(\mathcal{A})$ neprotivrečna teorija.

Primer 15. Neka je $\mathcal{A}$ model jezika $\mathcal{L}$ i $\mathcal{A}_1$ ekspanzija modela $\mathcal{A}$ na jezik $\mathcal{L}_1 \supseteq \mathcal{L}$. Ako je $\mathcal{B}$ elementarno proširenje modela $\mathcal{A}$, onda postoji elementarno proširenje $\mathcal{B}_1$ modela $\mathcal{B}$, čija redukcija na jezik $\mathcal{L}$ je elementarno proširenje modela $\mathcal{B}$.

Primer 16. Prepostavimo da je Σ kompletna teorija u jeziku $\mathcal{L}$, φ rečenica jezika $\mathcal{L}_1 \supseteq \mathcal{L}$, ψ rečenica jezika $\mathcal{L}_2 \supseteq \mathcal{L}$, $\mathcal{L}_1 \cap \mathcal{L}_2 = \mathcal{L}$ i pretpostavimo da sve individualne konstante koje se javljaju u rečenicama φ i ψ pripadaju jeziku $\mathcal{L}$. Ako su $\Sigma \cup \{\varphi\}$ i $\Sigma \cup \{\psi\}$ neprotivrečne teorije, onda je $\Sigma \cup \{\varphi, \psi\}$ neprotivrečna teorija.

Neka je $\mathcal{A}_0$ model teorije $\Sigma \cup \{\varphi\}$ i $\mathcal{A}_0^*$ njegova redukcija na jezik $\mathcal{L}$. Prema prethodnim primerima, teorija $\{\varphi\} \cup \mathrm{Th}(\mathcal{A}_0^*)$ je neprotivrečna i neka je $\mathcal{A}_1$ njen model u jeziku $\mathcal{L}_2$. Pritom, $\mathcal{A}_0^* \preceq \mathcal{A}_1^*$. Iz istih razloga, postoji model $\mathcal{A}_2$ jezika $\mathcal{L}_1$ takav da $\mathcal{A}_0 \preceq \mathcal{A}_2$ i pritom $\mathcal{A}_1^* \preceq \mathcal{A}_2^*$. Na taj način se usmeren niz modela $\mathcal{A}_0 \preceq \mathcal{A}_2 \preceq \cdots$ jezika $\mathcal{L}_1$, usmeren niz modela $\mathcal{A}_1 \preceq \mathcal{A}_3 \preceq \cdots$ jezika $\mathcal{L}_2$ i usmeren niz modela $\mathcal{A}_0^* \preceq \mathcal{A}_1^* \preceq \mathcal{A}_2^* \cdots$ jezika $\mathcal{L}$. Ako je $\mathcal{A}$ model jezika $\mathcal{L}_1 \cup \mathcal{L}_2$ čija redukcija na jezik $\mathcal{L}_1$ je unija prvog, redukcija na jezik $\mathcal{L}_2$ unija drugog, a redukcija na jezik $\mathcal{L}$ unija trećeg usmerenog niza modela, onda model $\mathcal{A}$ jeste model teorije $\Sigma \cup \{\varphi, \psi\}$.

Primetimo da se pretpostavka o individualnim konstantama može eliminisati iz prethodnog tvrđenja. Ako su $c_1, \ldots, c_m$ individualne konstante rečenice φ, i $d_1, \ldots, d_n$ individualne konstante rečenice ψ, koje se ne pripadaju jeziku *calL*, onda za formule $\varphi_1 = \exists x_1 \cdots \exists x_m\, \varphi$ i $\psi_1 = \exists x_1 \cdots \exists x_n\, \psi$ prethodno tvrđenje važi bez pretpostavke o konstantama.

Izlaganje osnova teorije modela završavamo dokazom teoreme interpolacije sredstvima ove teorije. Direktan dokaz je znatno komplikovaniji.

Primer 17. Teorema interpolacije: Ako su φ i ψ rečenice redom jezika $\mathcal{L}_1$, odnosno, $\mathcal{L}_2$ takve da važi $\vdash \varphi \to \psi$, $\not\vdash \neg\varphi$ i $\not\vdash \psi$, onda je $\mathcal{L}_1 \cap \mathcal{L}_2 \neq \emptyset$ i postoji rečenica θ jezika $\mathcal{L}_1 \cap \mathcal{L}_2$ takva da $\vdash \varphi \to \theta$ i $\vdash \theta \to \psi$.

Neka je $\mathcal{L} = \mathcal{L}_1 \cap \mathcal{L}_2$ i $\Sigma = \{\theta : \varphi \to \theta\}$ skup rečenica u $\mathcal{L}$. Pretpostavimo da je $\Sigma \cup \{\neg\psi\}$ neprotivrečan skup i neka je $\mathcal{A}$ njegov model u jeziku $\mathcal{L}_2$. U tom slučaju, ako je $\Gamma = \mathrm{Th}_{\mathcal{L}}(\mathcal{A})$, skup rečenica $\Gamma \cup \{\varphi\}$ je takođe neprotivrečan. U suprotnom, postojale bi rečenice $\varphi_1, \ldots, \varphi_n \in \Gamma$ takve da važi $\Gamma \vdash \neg(\varphi_1 \wedge \cdots \wedge \varphi_n)$, a to bi zanačilo da $\neg(\varphi_1 \wedge \cdots \wedge \varphi_n) \in \Sigma \subseteq \Gamma$ i $\varphi_1 \wedge \cdots \wedge \varphi_n \in \Gamma$, što nije moguće. Prema prethodnom primeru, skup $\Gamma \cup \{\varphi, \neg\psi\}$ je neprotivrečan, a to znači da mora biti $\not\vdash \varphi \to \psi$.

Kako je $\Sigma \cup \{\neg\psi\}$ protivrečan skup, postoje $\varphi_1, \ldots, \varphi_n \in \Sigma$, za koje važi $\vdash \varphi_1 \wedge \cdots \wedge \varphi_n \to \psi$. Jasno je da jezik $\mathcal{L}$ ne može biti prazan. U suprotnom, postojao bi model za φ i $\neg\psi$, što bi značilo da važi $\not\vdash \varphi \to \psi$.

Napomene

– Pojam induktivno definisanog formalnog sistema i pojam njegove induktivno definisane interpretacije javlja se eksplicitno dvadesetih godina ovog veka. Kako je osnovna ideja teorije modela dualizam sintakse i semantike, ova teorija predstavlja prototip platonističkog shvatanja matematike. Jezik predikatskog računa je sredstvo za izražavanje svojstava matematičkih struktura, a one same postoje nezavisno od toga kako matematika istražuje njihova svojstva.

– Koristeći normalne konjunktivne forme, stav potpunosti iskaznog računa dokazao je Emil Post 1921. godine. Nešto drugačijim sredstvima, isti rezultat dokazao je i Kalmar 1935. godine. Sikorskog i Helene Rašove iz 1951. godine [1].

– Prva verzija predikatskog računa, koju je formulisao Frege 1879. godine, značajno se razlikuje od verzije koju smo izložili. Osim razlika u notaciji, izboru aksioma i pravila izvođenja, Fregeova formulacija dozvoljavala je i kvantifikaciju preko predikatskih promenljivih. Uz ostale Fregeove pretpostavke, ta je teorija bila protivrečna.

– Modelsko-teorijsku definiciju istine ili semantiku predikatskog računa formulisao je Alfred Tarski 1935. godine [1]. Stav potpunosti predikatskog računa dokazao je Gedel u jednom radu iz 1930. godine. U istom radu za prebrojive jezike dokazani su prošireni stav potpunosti i stav kompaktnosti. Dokaz stava potpunosti za prebrojive jezike, u formi u kojoj je ovde izložen, nastao je 1951. godine u radu Rašove i Sikorskog [1]. Dokaz i sa svedočkim konstantama formulisao je Henkin 1949. godine, a opštu verziju stava kompaktnosti Maljcev 1936. godine [2].

– Da svaka neprotivrečna teorija u prebrojivom jeziku ima prebrojiv model dokazao je Skolem 1920. godine. Nešto ranije, 1915. godine, Levenhajm je dokazao verziju ove teoreme za slučaj samo jedne formule, odnosno, dokazao je da svaka konačno aksiomatska teorija ima prebrojiv model [2].

– Većinu modesko-teorijskih ideja formulisao je Tarski pedesetih godina ovog veka uključujući pre svega definiciju i karakterizaciju elementarnih podmodela [1]. Pojmove elementarnog utapanja i dijagrama definisao je Abraham Robinson 1949. godine [4].

– Prvu konstrukciju prebrojivog nestandardnog modela aritmetike definisao je Skolem 1934. godine. Na jedan sasvim posredan način, Lajbnic je verovao u egzistenciju nearhimedovskih proširenja uređenih polja. U kontekstu nestandardnih modela realnih brojeva, Abraham Robinson je 1960. godine oživeo Lajbnicove ideje u diferencijalnom i integralnom računu i zasnovao nestandardnu analizu [3]. Pokazalo se da su Lajbnicove pretpostavke o aktualnoj egzistenciji beskonačno malih i beskonačno velikih brojeva bile opravdane.

– Konstrukcija ultraproizvoda je implicitno prisutna u Gedelovim i Skolemovim radovima [1]. Prva eksplicitna formulacija u kontekstu teorije modela javlja se u jednom Lošovom radu iz 1955. godine [2].

– Većinu skupovno-teorijskih svojstava ultraproizvoda i karakterizaciju elementarne ekvivalencije, dokazali su Frejn, Morel i Skot 1962. godine [1].

– Pristup osnovama algebre sa modelsko-teorijskog stanovišta izložen je u knjizi Žarka Mijallovića Algebra I [5] i njen sadržaj predstavlja dobru osnovu za razumevanje materije koja je ovde izložena. Znatno potpuniji pregled rezultata savremene teorije modela izložen je u monografiji An Introduction to Model Theory istog autora [4].

Literatura

[1] Bell, J.L., Slomson, A.B. Models and Ultraproducts, North-Holland, Amsterdam, 1969.

[2] Chang, C.C., Keisler H.J. Model Theory, North-Holland, Amsterdam, 1973.

[3] Davis, M. Applied Nonstandard Analysis, John Wiley & Sons, New York, 1977.

[4] Sacks, G. Saturated Model Theory, Benjamin, Reding Mass., 1972.

[5] Mijajlović, Ž. Algebra I, Beograd, 1990.

[6] Mijajlović, Ž. An Introduction to Model Theory, Univer. of Novi Sad, Novi Sad, 1987.

Teorija skupova

Skup je osnovni matematički pojam i sva matematička tvrđenja izražavaju neka njegova svojstva. Ako bi formalizacija ovog pojma bila moguća, u eventualnoj formalnoj teoriji skupova moglo bi se formulisati sve što se u matematici može izraziti. Sve što je uopšte dokazivo moglo bi se i formalno dokazati. Sa stanovišta svakodnevne matematike, a i samo po sebi, ovo tvrđenje izgleda preterano ambiciozno. Međutim, kada to kažemo, uopšte ne mislimo da bi se matematika stvarno mogla svesti na mehaničko dokazivanje teorema, već da je načelno i do određenog stepena jedna takva formalizacija moguća.

Dakle, u teoriji skupova može se zasnovati matematika, ali se sama teorija skupova samo načelno bavi takvim zasnivanjem. Njen pravi predmet jeste jedan broj pitanja čija formalizacija nije u potpunosti ostvariva. Ona su po svom karakteru skupovno-teorijska i samo izuzetno direktno vezana za probleme svakodnevne matematike.

Aksiome teorija skupova izražavaju nekoliko očiglednih principa na kojima počiva svako matematičko rasuđivanje. Svako ko ima izvesno matematičko iskustvo podrazumeva da skupovi imaju sledeće osobine:

– jednaki skupovi imaju iste elemente,
– svaka familija skupova ima uniju,
– nad svakim skupom postoji skup svih njegovih podskupova,
– postoji beskonačan skup,
– slika skupa pri svakom preslikavanju je takođe skup,
– svi matematički objekti su skupovi.

Svi navedeni principi mogu se izraziti u predikatskom računu. Njihova formulacija u jeziku $\mathcal{L}_{ZF} = \{\in\}$, gde je $\in$ binarna relacijska konstanta, jeste *Cermelo-Frenkelova* teorija skupova. Ovu teoriju označavamo sa ZF.

Osim principa teorije ZF, u matematici se koristi i aksioma izbora. Iako sa ovim skupovno-teorijskim principom manipuliše veoma obazrivo i samo izuzetno ga koristi, većina matematičara ipak smatra nespornim da

– svaka familija nepraznih skupova ima funkciju izbora.

Aksioma izbora takođe ima jednostavnu formulaciju u jeziku $\mathcal{L}_{ZF}$. Teoriju ZF proširenu takvom formulacijom označavamo sa ZFC.

Sve elementarne formule jezika $\mathcal{L}_{ZF}$ su oblika $(x = y)$ ili $(x \in y)$, za neke individualne promenljive $x, y \in V$. Slično jednakosti, znak $\in$ istovremeno upotrebljavamo kao formalni simbol jezika $\mathcal{L}_{ZF}$ i kao neformalnu oznaku, ali je iz konteksta uvek jasno o kakvoj se upotrebi radi.

Formalno posmatrano, model jezika $\mathcal{L}_{ZF}$ je struktura $\mathcal{M} = (M, \varepsilon)$ u kojoj je ε binarna relacija nepraznog skupa M. Saglasno definiciji zadovoljenja, za sve $a, b \in M$,

$$\mathcal{M} \models (x \in y)[a, b] \text{ ako i samo ako } (a, b) \in \varepsilon.$$

Interpretacija jezika $\mathcal{L}_{ZF}$ se suštinski razlikuje od interpretacije drugih jezika. Kada formulišemo jezik teorije algebarski zatvorenih polja, jezik aritmetike ili bilo koji drugi jezik, pred sobom imamo jednu klasu struktura na koju se takav jezik odnosi. Ako to nije slučaj, odnosno, ako jezik nema *osnovnu interpretaciju*, njegove teorije se svode na puku igru simbolima lišenu svakog smisla. Međutim, opis takve interpretacije teorije skupova nije uopšte jednostavan.

Primer 1. (a) Uređenje realnih brojeva $\mathcal{R} = (R, <)$ jeste model jezika $\mathcal{L}_{ZF}$, ali relacija $x < y$ ni približno nema svojstva koja očekujemo da ima interpretacija predikata $\in$.

(b) Neka je ε binarna relacija na prirodnim brojevima takva da za sve $n, m \in \omega$, $n \, \varepsilon \, m$ ako i samo ako na n-tom mestu u binarnoj ekspanziji prirodnog broja m, računajući sa desna, javlja se cifra jedan.

Sa izuzetkom beskonačnosti, struktura $M = (\omega, \varepsilon)$ ima sva svojstva izražena u teoriji ZFC. Budući da verujemo u postojanje beskonačnih skupova, model $\mathcal{M}$ ne može biti osnovna interpretacija jezika $\mathcal{L}_{ZF}$.

Ne ulazeći do kraja u problem osnovne interpretacije, za sada ćemo reći samo to da u takvoj interpretaciji jezika $\mathcal{L}_{ZF}$, formula $x \in y$ ima značenje "x je element od y." Kako su svi matematički objekti skupovi, ako je x skup i $y \in x$, onda y mora biti skup. Takođe, ako je x skup, $y \in x$ i $z \in y$, onda z mora biti skup itd. Ako je $\mathcal{M}$ model jezika $\mathcal{L}_{ZF}$, njegov domen M mora imati navedeno svojstvo. On mora biti *skup u naslednom smislu*, pa u načelu naša osnovna interpretacija podrazumeva takve modele.

Primer 2. Ako pretpostavimo da je rekurzija legitimna u teoriji ZF, skupovi tipa $V_0 = \{\emptyset\}$, za svako $n \in \omega$, $V_n = P^n(\emptyset)$ ili $V_\omega = \bigcup_{n \in \omega} V_n$ su primeri skupova u naslednom smislu.

U načelu, formulacije svih matematičkih pojmova izrazive su u jeziku $\mathcal{L}_{ZF}$. Međutim, radi jednostavnijeg izlaganja, mi ćemo faktički uvek raditi u nekoj njegovoj definicionoj ekstenziji. Dakle, jezik $\mathcal{L}_{ZF}$ postepeno širimo novim predikatskim, operacijskim i individualnim konstantama. Pritom, nove simbole definišemo formulom jezika $\mathcal{L}_{ZF}$ tako da se definisani simboli uvek mogu eliminisati i sva tvrđenja dokaziva u proširenom jeziku dokazati u jeziku $\mathcal{L}_{ZF}$.

Ideja proširenja jezika simbolima definisanim njegovim rečenicama je sasvim opšta i odnosi se na svaki jezik u predikatskom računu. U narednim razmatranjima pretpostavljamo da je teorija ZF formulisana u jeziku $\mathcal{L}_{ZF}$ i ništa više od toga. Svi rezultati se mogu odnositi i na bilo koju teoriju predikatskog računa prvog reda.

Jedina specifičnost teorije ZF o kojoj treba voditi računa u ovom kontekstu jeste činjenica da ona, poput Peanove aritmetike sadrži i jednu shema aksiomu koja se sastoji od skupa rečenica jezika $\mathcal{L}_{ZF}$. Sa proširenjem jezika širi se i skup njegovih formula tako da se shema aksioma, kao skup rečenica, menja u odnosu na prvobitni jezik.

Neka je $\varphi(x_1, \ldots, x_n)$ formula jezika $\mathcal{L}_{ZF}$, i P relacijska konstanta dužine $n \in \omega$ koja ne pripada $\mathcal{L}_{ZF}$. Rečenica

$$\psi = \forall x_1 \cdots \forall x_n \, (\varphi(x_1, \ldots, x_n) \leftrightarrow P(x_1, \ldots, x_n))$$

je *definicija relacijske konstante* P u teoriji ZF.

Teorija $\mathrm{ZF}(P) = \mathrm{ZF} \cup \{\psi\}$ u jeziku $\mathcal{L}_{ZF} \cup \{P\}$ je *definiciono proširenje* teorije ZF. Formula φ je *definiciona formula* relacijske konstante P i označavamo je sa φ_P.

Ova definicija izgleda neprirodno utoliko što definicija nove relacijske konstante nema nikakve veze sa teorijom ZF. Ona je zapravo definisana u jeziku $\mathcal{L}_{ZF}$. To jeste tačno, ali samo kada se radi o predikatskim konstantama. U slučaju operacijske konstante, osim njene definicije u jeziku $\mathcal{L}_{ZF}$, neophodan je dokaz da takva definicija zaista odredjuje operaciju, a on se mora izvesti u okviru neke teorije. Isto važi i u slučaju definicije individualne konstante.

Ako je $\varphi(x_1, \ldots, x_n, y)$ formula jezika $\mathcal{L}_{ZF}$ i F operacijska konstanta dužine $n \in \omega$ koja ne pripada $\mathcal{L}_{ZF}$, rečenica

$$\psi = \forall x_1 \cdots \forall x_n \forall y \, (F(x_1, \ldots, x_n) = y \leftrightarrow \varphi(x_1, \ldots, x_n, y))$$

je definicija operacijskog simbola F u teoriji ZF ako

$$\mathrm{ZF} \vdash \forall x_1 \cdots \forall x_n \exists y \forall z \, (\varphi(x_1, \ldots, x_n, z) \leftrightarrow z = y).$$

Teorija $\mathrm{ZF}(F) = \mathrm{ZF} \cup \{\psi\}$ jezika $\mathcal{L}_{ZF} \cup \{F\}$ je definiciono proširenje teorije ZF. Definicionu formulu φ operacijskog slova F označavamo sa φ_F.

Neka je $\varphi(x)$ formula jezika $\mathcal{L}_{ZF}$ i c individualna konstanta koja ne pripada $\mathcal{L}_{ZF}$. Rečenica

$$\psi = \forall x\,(c = x \leftrightarrow \varphi(x))$$

je definicija konstante c u teoriji ZF ako

$$\mathrm{ZF} \vdash \exists y \forall z\,(\varphi(z) \leftrightarrow z = y).$$

Teorija $\mathrm{ZF}(c) = \mathrm{ZF} \cup \{\psi\}$ je definiciona ekstenzija teorije ZF u jeziku $\mathcal{L}_{ZF} \cup \{c\}$. Formula $\varphi(x)$ je definiciona formula konstante c, u oznaci $\varphi_c(x)$.

U opštem slučaju, radimo u teoriji $\Sigma = \mathrm{ZF}(S_1, .., S_n)$, odnosno, u nekom konačnom definicionom proširenju teorije ZF.

Teorema 1. Ako je teorija Σ, u jeziku $\mathcal{L}_\Sigma$, definiciono proširenje teorije ZF, za svaku formulu ψ jezika $\mathcal{L}_\Sigma$ postoji formula ψ^* jezika $\mathcal{L}_{ZF}$ takva da

$$\Sigma \vdash \forall x_1 \cdots \forall x_n\,(\psi(x_1, \ldots, x_n) \leftrightarrow \psi^*(x_1, \ldots, x_n)).$$

Dokaz: Za svaku formulu ψ jezika $\mathcal{L}_\Sigma$, indukcijom po složenosti formule ψ, definišemo formulu ψ^* jezika $\mathcal{L}_{ZF}$, a potom, indukcijom po složenosti formule ψ dokazujemo teoremu.

Za proizvoljne formule ψ i θ jezika $\mathcal{L}_\Sigma$ neka je

$$(\neg\psi)^* = \neg\psi^*,\ (\psi \to \theta)^* = \psi^* \to \theta^* \text{ i } (\exists x\,\psi)^* = \exists x\,\psi^*.$$

Ako je ψ elementarna formula, onda formulu ψ^* takođe definišemo indukcijom po složenosti formule ψ.

Pretpostavimo da formula ψ ima oblik $P(t_1, \ldots, t_n)$, gde je P relacijska konstanta i $t_1, \ldots, t_n$ termi jezika $\mathcal{L}_\Sigma$. Neka su $x_0, \ldots, x_n$ promenljive koje se ne javljaju u formuli ψ, onda je

$$\psi^* = \exists x_1 \cdots \exists x_n\,((x_1 = t_1)^* \wedge \cdots \wedge (x_n = t_n)^* \wedge \varphi_P(x_0, \ldots, x_n)).$$

Svaka formula $(x_i = t_i)$ je manje složenosti od formule ψ.

Pretpostavimo da formula ψ ima oblik $F(t_1, \ldots, t_n) = t$, gde je F operacijska konstanta i $t_1, \ldots, t_n, t$ termi jezika $\mathcal{L}_\Sigma$. Neka su $x_0, \ldots, x_n, x$ promenljive koje se ne javljaju u ψ, onda je

$$\begin{aligned}\psi^* = \exists x_1 \cdots \exists x_n \exists x\,((x_1 = t_1)^* \wedge \cdots \wedge (x_n = t_n)^* \\ \wedge (x = t)^* \wedge \varphi_F(x_0, \ldots, x_n, x)).\end{aligned}$$

Svaka od formula $(x_i = t_i)$ i $(x = t)$ ima manju složenost od formule ψ.

Neka je formula ψ oblika $c = t$, gde je c individualna konstanta, t term jezika $\mathcal{L}_\Sigma$ i neka je x promenljiva koja se ne javlja u formuli ψ, onda

$$\psi^* = \exists x\,((x = t)^* \wedge \varphi_c(x)).$$

Pritom, formula $(x = t)$ ima manju složenost od formule ψ.

Konačno, ako elementarna formula ψ ima oblik $(x = y)$ ili $(x \in y)$, gde su x i y promenljive predikatskog računa, onda $\psi^* = \psi$.

Relacija, $\Sigma \vdash \forall x_1 \cdots \forall x_n\,(\psi(x_1, \ldots, x_n) \leftrightarrow \psi^*(x_1, \ldots, x_n))$ dokazuje se indukcijom po složenosti formule ψ. Netrivijalni koraci su jedino elementarne formule, a oni se dokazuju na osnovu definicije formule ψ^*. $\square$

Neka je $\mathcal{L}^*$ definiciona ekstenzija jezika $\mathcal{L}$, Γ skup definicija novih konstanti jezika $\mathcal{L}^*$ i Σ teorija u jeziku $\mathcal{L}$. Sa $\Sigma^* = \Sigma \cup \Gamma$ označavamo definicionu ekstenziju teorije Σ. Jasno, teorija Σ^* je teorija u jeziku $\mathcal{L}^*$.

Primer 3. Neka je $\mathcal{L}^*$ definiciona ekstenzija jezika $\mathcal{L}$ i Γ skup definicija novih konstanti jezika $\mathcal{L}^*$.

Svaki model $\mathcal{A}$ jezika $\mathcal{L}$ ima tačno jednu ekspanziju $\mathcal{A}^*$ u jeziku $\mathcal{L}^*$ takvu da, za svaku rečenicu $\varphi \in \Gamma$, važi $\mathcal{A}^* \models \varphi$.

Ekspanzija $\mathcal{A}^*$ je *definiciona ekspanzija* modela $\mathcal{A}$.

Primer 4. Ako je Σ teorija u jeziku $\mathcal{L}$, onda za svaku formulu ψ jezika $\mathcal{L}^*$, postoji formula ψ^* jezika $\mathcal{L}$ takva da:

(a) za svaki model $\mathcal{A}$ jezika $\mathcal{L}$, za sve $a_1, \ldots, a_n \in A$, ako $\mathcal{A} \models \Sigma$, onda

$$\mathcal{A}^* \models \psi[a_1, \ldots, a_n] \text{ ako i samo ako } \mathcal{A} \models \psi^*[a_1, \ldots, a_n],$$

(b) Ako su $\mathcal{A}$ i $\mathcal{B}$ modeli jezika $\mathcal{L}$, onda $\mathcal{A} \equiv \mathcal{B}$ ako i samo ako $\mathcal{A}^* \equiv \mathcal{B}^*$.

Rezultat ovog primera značajan je u slučaju teorija jezika $\mathcal{L}$ koje, poput ZF ili PA, sadrže sheme aksioma. On pokazuje da se takve sheme mogu primenjivati i na formule proširenog jezika $\mathcal{L}^*$.

U slučaju definicionih ekstenzija jezika $\mathcal{L}_{ZF}$ najčešće upotrebljavamo terme oblika $t = \{y : \varphi\}$, gde je φ formula neke definicione ekstenzije jezika $\mathcal{L}_{ZF}$. Ako se takav term javlja u elementarnoj formuli oblika $(t = u)$, onda je $(t = u)^* = \exists z\,(\forall y\,(y \in z \leftrightarrow \varphi) \wedge z = u)$.

Slično, ako se term t javlja u elementarnoj formuli oblika $(u \in t)$, formula $(u \in t)^*$ je formula $\exists z\,(\forall y\,(y \in z \leftrightarrow \varphi) \wedge u \in z)$. Isto važi i u slučaju formule $t \in u$, za svaki term u jezika $\mathcal{L}_{ZF}$.

Neka su Σ i Σ' redom teorije jezika $\mathcal{L}$ i $\mathcal{L}'$. Ako je $\mathcal{L}'$ ekstenzija jezika $\mathcal{L}$ i $\Sigma \subseteq \Sigma'$, teorija Σ' je *konzervativna ekstenzija* teorije Σ ako za svaku rečenicu φ jezika $\mathcal{L}$,

$$\Sigma' \vdash \varphi \text{ ako i samo ako } \Sigma \vdash \varphi.$$

Dakle, teorija Σ i njena konzervativna ekstenzija Σ^* imaju iste posledice u jeziku $\mathcal{L}$. Na osnovu prethodne teoreme, sve uvedene konstante definicionih ekstenzija mogu se eliminisati. Medjutim, tek konzervativnost u potpunosti opravdava ovakvu vrstu ekstenzija. Sve što se dobije sredstvima proširenja, može se dobiti i u okviru osnovne teorije.

Teorema 2. Svaka definiciona ekstenzija je konzervativna.

Dokaz: Neka je Σ teorija u jeziku $\mathcal{L}$ i Σ^* njena definiciona ekstenzija u jeziku $\mathcal{L}^*$. Na osnovu prethodnog primera, svaki model $\mathcal{A}$ teorije Σ ima definicionu ekspanziju $\mathcal{A}^*$ koja je model teorije Σ^*. Otuda, ako je φ rečenica jezika $\mathcal{L}$, onda $\mathcal{A} \models \varphi$ ako i samo ako $\mathcal{A}^* \models \varphi$. Na osnovu stava potpunosti, $\Sigma \vdash \varphi$ ako i samo ako $\Sigma^* \vdash \varphi$. $\Box$

Konzervativnost definicionih ekstenzija dokazali smo pozivanjem na stav potpunosti, ali samo po sebi izgleda da on nije neophodan u dokazu takvog tvrđenja.

Primer 5. Ako je teorija Σ' jezika $\mathcal{L}'$ definiciona ekstenzija teorije Σ u jeziku $\mathcal{L}$, svaki dokaz formule φ jezika $\mathcal{L}$ u teoriji Σ' može se preraditi u dokaz formule φ u teoriji Σ.

Aksiome teorije skupova

Teorija ZF sastoji se od aksioma *ekstenzionalnosti, unije, partitivnog skupa, beskonačnosti, regularnosti* i jedne sheme aksioma koju ćemo nazivati *aksiomom zamene.* U našem pregledu pojaviće se kao aksiome i formalizacije nekih svojstava skupova koje se iz navedenih aksioma mogu dokazati. O njima govorimo samo radi jednostavnijeg izlaganja i eventualno iz istorijskih razloga.

U okviru pregleda samih aksioma, nastojaćemo da ilustrujemo deo matematike koji se u njihovom okviru može razviti. Bez preterane sistematičnosti u toj stvari, postupno uvodimo standardne matematičke pojmove i istovremeno nastojimo da razvijemo opšte skupovno-teorijske ideje na kojima se zasniva sama teorija skupova.

Aksioma ekstenzionalnosti izražava uverenje da su skupovi jednaki ako imaju iste elemente. U jeziku $\mathcal{L}_{ZF}$ ona je formulisana sledećom rečenicom:

$$\forall x \forall y\, (\forall z\, (z \in x \leftrightarrow z \in y) \rightarrow x = y).$$

Kako na osnovu aksioma jednakosti u predikatskom računu važi i suprotna implikacija

$$\vdash \forall x \forall y\, (x = y \rightarrow \forall u\, (u \in x \leftrightarrow u \in y)),$$

to znači da je $x = y$ ako i samo ako $\forall u\, (u \in x \leftrightarrow u \in y)$, za sve x, y. Dakle, skupovi su jednaki ako i samo ako imaju iste elemente ili istu ekstenziju.

Aksioma separacije je shema koja formalizuje skupovnu konstrukciju oblika $\{x : \varphi(x)\}$ u kojoj $\varphi(x)$ izražava neko svojstvo skupa x. U našem slučaju svojstvo φ je formula jezika $\mathcal{L}_{ZF}$.

Za svaku formulu φ, u kojoj y nije slobodna promenljiva, sledeća formula je aksioma teorije ZF:

$$\forall z \exists y \forall x\, (x \in y \leftrightarrow (x \in z \wedge \varphi(x))).$$

Aksioma separacije tvrdi da za svaku formulu φ i proizvoljan skup z, postoji podskup y svih njegovih elemenata koji zadovoljavaju svojstvo izraženo formulom φ. Pritom, u formuli φ mogu se javiti i parametri različiti od promenljive y. Kao shema, aksioma separacije je familija rečenica navedenog oblika indeksirana formulama $\varphi(x)$ jezika $\mathcal{L}_{ZF}$ u kojima promenljiva y nema slobodnih javljanja.

Primer 6. Prema aksiomi ekstenzionalnosti, za svaki skup z i svaku formulu $\varphi(x)$ u kojoj y nije slobodna promenljiva, skup $y = \{x \in z : \varphi\}$ je jedinstveno određen.

Primer 7. Ako je φ rečenica jezika $\mathcal{L}_{ZF}$, klasa svih objekata koji imaju svojstvo φ nije uvek skup.

Shema oblika $\exists y \forall x\, (x \in y \leftrightarrow \varphi)$ je protivrečna. Naime, ako je $\varphi = x \notin x$, onda na osnovu navedene sheme, postoji y takvo da $\forall x\, (x \in y \leftrightarrow x \notin x)$. Instanca ove formule $y \in y \leftrightarrow y \notin y$ je kontradikcija.

Zapravo, pretpostavka da za svaku formulu φ jezika $\mathcal{L}_{ZF}$ postoji skup svih objekata koji zadovoljavaju formulu φ je protivrečna. Specijalan slučaj ove konstatacije jeste upravo navedeni Raselov paradoks "skupa svih skupova koji nisu elementi samih sebe" [3].

Primetimo da postojanje skupa x koji zadovoljava relaciju $x \in x$ ne protivreči aksiomi separacije. Ona ne eliminiše mogućnost da se kao skup može javiti i objekt tipa $x = \{x\}$, koji intuitivno ne odgovara ovom pojmu.

Primer 8. Na osnovu teoreme predikatskog računa $\vdash \exists x\,(x = x)$, postoji bar jedan skup. Prema aksiomi separacije, za svaki skup z postoji skup $y = \{x \in z : x \neq x\}$. Kako postoji bar jedan skup, prema aksiomi ekstenzionalnosti, $\emptyset$ je jedinstven skup y takav da $\forall x\,(x \notin y)$.

Formula $\varphi_{\emptyset}(y) = \forall x\,(x \notin y)$ je definiciona formula konstante $\emptyset$, pa kako je zadovoljen uslov jedinstvenosti $\mathrm{ZF} \vdash \exists y \forall z\,(\varphi_{\emptyset}(z) \to z = y)$, mogli bismo reći da ćemo ubuduće raditi u definicionoj ekstenziji

$$\mathrm{ZF} \cup \{\forall y\,(y = \emptyset \leftrightarrow \varphi_{\emptyset}(y))\}.$$

Kada se ima u vidu mogućnost eliminacije definisanih simbola i konzervativnost definicionih ekstenzija, možemo reći da radimo u teoriji ZF.

Primer 9. Prema aksiomi separacije, važi $\vdash \neg\exists z \forall x\,(x \in z)$.

Na osnovu prethodnog primera, ne postoji skup svih skupova, odnosno, klasa svih skupova $V = \{x : x = x\}$ nije skup. Pritom, termin *klasa* upotrebljavamo u smislu kolekcije objekata koji zadovoljavaju određenu formulu φ. Zapravo, klasa $A = \{x : \varphi(x)\}$ izražava značenje formule φ i može se sa njom identifikovati. Na primer, klasu svih skupova V možemo identifikovati sa formulom $(x = x)$, klasu svih grupa sa formulom φ_G itd.

Primer 10. Prema aksiomi separacije, za proizvoljne skupove x i y, postoji skup z takav da $\forall u\,(u \in z \leftrightarrow (u \in x \wedge u \in y))$. Prema aksiomi ekstenzionalnosti takav z je jedinstven, tj. $z = x \cap y$. Na sličan način, za svaki neprazan skup x postoji $\bigcap x$. Za sve x, y postoji skup $x - y$. Takođe, može se definisati predikat $x \cap y = \emptyset$.

Aksioma dvočlanog skupa izražava činjenicu da za proizvoljne skupove x i y postoji skup $\{x, y\}$ čiji su elementi upravo skupovi x i y. Formuliše sledećom rečenicom jezika $\mathcal{L}_{ZF}$:

$$\forall x \forall y \exists z \forall u\,(u \in z \leftrightarrow (u = x \vee u = y)).$$

Zbog aksiome ekstenzionalnosti za date x i y, skup z čiju egzistenciju postulira aksioma dvočlanog skupa, jedinstveno je određen. To znači da se par skupova $\{x, y\}$ može definisati kao jedinstven skup z koji zadovoljava uslov $\forall u\,(u \in z \leftrightarrow (u = x \vee u = y))$.

Primer 11. Jednočlan skup $\{a\}$ je par $\{a, a\}$. Takođe, uređen par može se definisati kao skup $(a, b) = \{\{a\}, \{a, b\}\}$. Pritom, $(a, b) = (c, d)$ ako i samo ako $a = c$ i $b = d$.

Aksioma unije izražava činjenicu da za svaku familiju skupova postoji unija njenih elemenata. U jeziku $\mathcal{L}_{ZF}$ eormulisana je rečenicom

$$\forall x \exists y \forall z\, (z \in y \leftrightarrow \exists u\, (u \in x \wedge z \in u)).$$

Prema aksiomi ekstenzionalnosti, za svaki skup x, skup y čiju egzistenciju garantuje aksioma unije, jedinstveno je određen i označava se sa $\cup x$. Na primer, na osnovu aksiome dvočlanog skupa, za proizvoljne skupove x, y, $x \cup y = \cup\{x, y\}$ je skup.

Aksioma partitivnog skupa postulira egzistenciju skupa svih podskupova datog skupa. Izražava se sledećom rečenicom jezika $\mathcal{L}_{ZF}$:

$$\forall x \exists y \forall z\, (z \in y \leftrightarrow \forall u\, (u \in z \rightarrow u \in x)).$$

Na osnovu aksiome ekstenzionalnosti, za svaki skup x, skup y čiju egzistenciju tvrdi aksioma partitivnog skupa je jedinstveno određen i označava se sa $P(x)$. Skup $P(x)$ je skup svih podskupova skupa x ili partitivni skup skupa x.

Primer 12. Ne postoji skup x takav da je $P(x) \subseteq x$.

Da bismo pojednostavili formulacije, ubuduće ćemo koristiti sledeće oznake: $x \subseteq y$ za formulu $\forall x\, (z \in x \rightarrow z \in y)$, zatim $\exists x \in y\, \varphi$ za formulu $\exists x\, (x \in y \wedge \varphi)$ i $\forall x \in y\, \varphi$ za formulu $\forall x\, (x \in y \rightarrow \varphi)$.

Takođe, sa $\exists^* x\, \varphi$ označavamo formulu $\forall x \forall y\, (\varphi(x) \wedge \varphi(y) \rightarrow x = y)$, a sa $\exists! x\, \varphi$ formulu $\exists y \forall x\, (\varphi(x) \leftrightarrow x = y)$. U oba slučaja $\varphi(x)$ je formula u kojoj y nije slobodna promenljiva. Pritom, smisao formule $\exists^* x\, \varphi$ jeste da postoji najviše jedno x za koje važi formula φ, a smisao formule $\exists! x\, \varphi$ je da postoji tačno jedno x takvo da važi formula φ.

Primer 13. Koristeći aksiomu unije i partitivnog skupa može se definisati Dekartov proizvod $x \times y$ skupova x i y.

Neka je $x \times y = \{z : \exists u \exists v\ u \in x \wedge v \in y \wedge z = (u, v)\}$. Da bismo opravdali ovu definiciju, primetimo da je $x \times y \subseteq PP(x \cup y)$. Otuda, na osnovu aksioma unije, partitivnog skupa i separacije, proizvod $x \times y$ jeste skup, a na osnovu aksiome ekstenzionalnosti, jedinstveno je određen.

Primer 14. Na osnovu do sada izloženih aksioma teorije skupova, mogu se definisati i sledeći predikati:

(a) "r je n-arna relacija", gde je $n \in \omega$ proizvoljan prirodan broj,

(b) "$y = \mathrm{dom}(r)$" i "$y = \mathrm{codom}(r)$," gde je r binarna relacija.

Pritom, da su $\mathrm{dom}(r)$ i $\mathrm{codom}(r)$ zaista skupovi, sledi na osnovu relacija $\mathrm{dom}(r) \subseteq \cup \cup r$, odnosno $\mathrm{codom}(r) \subseteq \cup \cup r$.

Primer 15. Binarna relacija f je funkcija ako i samo ako za svako $z \in \mathrm{dom}(f)$ i sve $u, v \in \mathrm{codom}(f)$, $(z, u) \in f$ i $(z, v) \in f$ implicira $u = v$. Za svako $z \in \mathrm{dom}(f)$, jedinstven skup u takav da $(z, u) \in f$ označavamo sa $f(z)$.

Formulu koja u teoriji ZF odgovara predikatu "f je funkcija" označavamo sa $\mathrm{fun}(f)$. Ako važi $\mathrm{fun}(f)$, $x = \mathrm{dom}(f)$ i $\mathrm{codom}(f) \subseteq y$, koristimo uobičajenu oznaku $f : x \to y$.

Za svako $n \geq 1$, ako je $\mathrm{dom}(f) = x^n$, f je n-arna operacija skupa x.

Ako je $y = \mathrm{codom}(f)$, f je funkcija na skup y. Ako za sve $u, v \in \mathrm{dom}(f)$, $f(x) = f(y)$ implicira $x = y$, funkcija f je obostrano jednoznačna.

Funkcija g je proširenje funkcije f ako $f \subseteq g$. Restrikcija funkcije f na skup $x \subseteq \mathrm{dom}(f)$ je funkcija $f \upharpoonright x = \{(u, v) \in f : u \in x\}$.

Ako važi $\mathrm{fun}(f)$, $f[x] = \{v \in \mathrm{codom}(f) : \exists\, u \in x(f(u) = v)\}$, za svako $x \subseteq \mathrm{dom}(f)$. Za svako $x \subseteq \mathrm{codom}(f)$, $f^{-1}(x) = \{u \in \mathrm{dom}(f) : f(u) \in x\}$ je inverzna slika skupa x pri preslikavnju f.

Postoji skup svih funkcija iz x u y koji označavamo sa y^x. To sledi iz činjenice da je $y^x \subseteq P(x \times y)$.

Primer 16. Na osnovu do sada navedenih aksioma, za zadati skup x, mogu se formulisati pojmovi relacije ekvivalencije, particije i količnika s obzirom na određenu relaciju ekvivalencije skupa x.

Aksioma beskonačnosti posredno postulira egzistenciju beskonačnog skupa. Preciznije, kako nemamo definisan pojam konačnog skupa, u aksiomi beskonačnosti zapravo postuliramo egzistenciju induktivnog skupa. Ta činjenica izražava se sledećom rečenicom jezika $\mathcal{L}_{ZF}$:

$$\exists x\, (\emptyset \in x \land \forall y\, (y \in x \to y \cup \{y\} \in x)).$$

Neka je $\varphi_{ind}(x) = \emptyset \in x \land \forall y\, (y \in x \to y \cup \{y\} \in x)$. Svaki skup koji ima svojstvo $\varphi_{ind}(x)$ je *induktivan skup*. Na osnovu aksiome separacije, postoji najmanji induktivan skup

$$\omega = \bigcap \{x : \varphi_{ind}(x)\}.$$

Najmanji induktivan skup ω je skup *prirodnih brojeva*.

Koristićemo sledeću notaciju: $0 = \emptyset$, $1 = \{0\}$, $2 = \{0, 1\}$, itd. Ako $n \in \omega$, onda $n + 1 = n \cup \{n\}$.

Skup x je *tranzitivan* ako za svako $y \in x$, važi $y \subseteq x$. Zapravo, skup x je tranzitivan ako za sve y, z, $y \in z \land z \in x \to y \in x$, tj. ako je relacija $\in$ tranzitivna na skupu x.

Primer 17. (a) Ako je skup x induktivan, $\{y \in x : y \subseteq x\}$ je induktivan skup. Otuda sledi da je skup prirodnih brojeva ω tranzitivan i za svaki prirodan broj $n \in \omega$, $n = \{m \in \omega : m \in n\}$.

(b) Ako je skup x induktivan, $\{y \in x : y \text{ je tranzitivan}\}$ je induktivan skup. Dakle, svaki prirodan broj $n \in \omega$ je tranzitivan.

(c) Ako je skup x induktivan, $\{y \in x : y \text{ je tranzitivan i } y \notin y\}$ je induktivan skup. Otuda sledi da za svako $n \in \omega$, važi $n \notin n$, što znači da je relacija $\in$ je nerefleksivna na skupu ω. Takođe, za svako $n \in \omega$, važi $n \neq n + 1$.

Neka je $y \in x$. Skup y je $\in$-*minimalan element* skupa x ako ne postoji skup $z \in x$ takav da $z \in y$.

Na osnovu do sada izloženih aksioma, ne može se dokazati da svaki skup ima $\in$-minimalni element. Na primer, "skup" oblika $x = \{\{x\}\}$ nema element koji je minimalan u $\in$ smislu.

Primer 17. Ako je x induktivan skup, svaka familija tranzitivnih skupova $y \in x$ takvih da svaki neprazan $z \subseteq y$ ima $\in$-minimalni element, jeste induktivan skup.

Primer 19. (a) Svaki neprazan skup $x \subseteq \omega$ ima $\in$-minimalni element.

(b) Skup $\{y \in x : y = \emptyset \vee \exists z \in x \, y = \{z\} \cup z\}$ je induktivan, ako je x induktivan skup. Otuda sledi da za svako $n \neq 0$, postoji prirodan broj $m \in \omega$ takav da važi $n = m + 1$.

(c) Ako je $x \subseteq \omega$ takav da $0 \in x$ i za svako $n \in \omega$, $n \in x$ implicira $n + 1 \in x$, onda je $x = \omega$.

Neka je $n \in \omega$. Skup x ima n elemenata ako postoji obostrano jednoznačana funkcija f koja preslikava x na skup n. Skup x je *konačan* ako za neko $n \in \omega$, x ima n elemenata. Skup je *beskonačan* ako nije konačan.

Primer 20. (a) Skup x je konačan ako i samo ako svaki neprazan skup $y \subseteq P(x)$ ima $\subseteq$-minimalni element.

(b) Skup ω nije konačan, pa dakle postoji beskonačan skup.

Na osnovu prethodnih primera može se zaključiti da skup prirodnih brojeva ω zadovoljava sledeće uslove:

(a) skup ω je beskonačan,

(b) relacija $\in$ je dobro uredjenje na ω,

(c) svaki neprazan ograničen skup u ω ima najveći element.

Kasnije ćemo pokazati da ova tri uslova jedinstveno određuju prirodne brojeve. Dakle, u teoriji skupova jeste moguća karakterizacija strukture prirodnih brojeva izražen u Dedekindovoj teoremi.

Aksioma zamene intuitivno tvrdi da ako neke od elemenata datog skupa zamenimo proizvoljnim skupovima, svaki element jednim skupom, rezultat takve zamene jeste skup.

Slično aksiomi separacije, aksioma zamene je shema aksioma. Za svaku formulu $\varphi(x, y)$, u kojoj z nije slobodna promenljiva, sledeća rečenica je aksioma teorije ZF:

$$\forall u\, (\forall x \in u\, \exists^* y\, \varphi \to \exists z \forall y\, (y \in z \leftrightarrow \exists x \in u\, \varphi))$$

Aksioma separacije dakle tvrdi sledeće: ako formula $\varphi(x, y)$ na skupu u definiše parcijalnu funkciju, klasa svih slika elemenata skupa u pripada nekom skupu z. Pojednostavljeno rečeno, ako je preslikavanje definisano formulom jezika $\mathcal{L}_{ZF}$, onda je slika svakog skupa pri takvom preslikavanju takođe skup.

Ako formule shvatimo kao klase skupova, onda formula $\varphi(x, y)$ određuje klasu parova skupova $F = \{(x, y) : \varphi(x, y)\}$. Prema uslovu aksiome zamene, klasa F je funkcionalna, tj. za svaki skup x postoji najviše jedan skup, u oznaci $F(x)$, takav da par $(x, F(x))$ pripada klasi F. Aksioma zamene tvrdi da za svaki skup u, klasa $\{F(v) : v \in u\}$ jeste skup.

To znači da ako formula $\varphi(x, y)$ određuje funkcionalnu relaciju F i ako je $\mathrm{dom}(F)$ skup, onda je $\mathrm{codom}(F)$ takođe skup. U tom slučaju, zbog ekstenzionalnosti, skup $F[x]$ jedinstveno je određen.

Primer 21. Ako z nije slobodna promenljiva u formuli ψ, iz aksiome zamene sledi $\forall u \exists z \forall y\, (y \in z \leftrightarrow y \in u \wedge \psi)$. To zapravo znači da se aksioma separacije može izostaviti u teoriji skupova koja sadrži aksiomu zamene.

Neka je φ formula $(x = y) \wedge \psi$. U tom slučaju važi pretpostavka aksiome zamene, odnosno, važi $\forall x \in u\, \exists^* y\, \varphi$. Otuda, prema aksiomi zamene, dobijamo $\exists z \forall y\, (y \in z \leftrightarrow \exists x \in u\, \varphi)$. Zbog $\exists x \in u\, \varphi \leftrightarrow y \in u \wedge \psi$, konačno se dobija aksioma separacije $\exists z \forall y\, (y \in z \leftrightarrow y \in u \wedge \psi)$.

Primer 22. Slično aksiomi separacije, u teoriji skupova koja sadrži shemu zamene može se izostaviti i aksioma dvočlanog skupa, tj. može se dokazati da važi $\exists x \forall y\, (y \in x \leftrightarrow (y = u \vee y = v))$.

Po aksiomi partitivnog skupa, postoje $P(\emptyset) = 1$, $P(1) = 2$ i pritom važe sledeći uslovi: $0 \neq 1$, $x \in 1 \leftrightarrow x = 0$ i $x \in 2 \leftrightarrow x = 0 \vee x = 1$. Dakle, postoji bar jedan dvočlan skup 2. Otuda, na osnovu aksime zamene, pokazujemo da za proizvoljne skupove u i v postoji skup $\{u, v\}$.

Neka je $\varphi(z, y)$ formula $(z = 0 \wedge y = u) \vee (z = 1 \wedge y = v)$. Kako je $0 \neq 1$, to mora biti $\forall z \in 2\, \exists^* y\, \varphi(z, y)$, tj. važi pretpostavka aksiome zamene. Dakle, važi $\exists x \forall y\, (y \in x \leftrightarrow \exists z \in 2\, \varphi(z, y))$ što konačno znači da važi $\exists x \forall y\, (y \in x \leftrightarrow y = u \vee y = v)$.

Sa aksiomom zamene završava se spisak aksioma teorije ZF koji formalizuje relevantna matematička svojstva skupova. Sa izuzetkom aksiome izbora, pod tim podrazumevamo svojstva skupova na koja se svakodnevno pozivamo u svim oblastima matematike. Teorija ZF sadrži još jednu aksiomu, aksiomu regularnosti, koja prevashodno ima skupovno-teorijski smisao. U narednim razmatranjima radimo u teoriji ZF bez aksiome regularnosti koju označavamo sa ZF - Reg. Sva tvrđenja koja ćemo izložiti u narednima odeljcima, do uvođenja aksiome regularnosti, mogu se formulisati i dokazati u ovoj teoriji. Teorija ZF - Reg predstavlja formalizaciju teorije kaja se uobičajeno naziva naivnom teorijom skupova.

Ordinalni brojevi

U aritmetici, ideja brojanja izražena je principom matematičke indukcije. Kako smo ranije napomenuli, taj princip je u prirodnim brojevima ekvivalentan njihovom dobrom uređenju. U sledećem primeru pokazaćemo da u svakom dobrom uređenju važi princip matematičke indukcije što znači da dobro uređenje predstavlja skupovno-teorijsko uopštenje ideje brojanja.

Primer 1. Princip indukcije važi u svakom dobrom uređenju.

Neka je $(P, \leq, 0)$ dobro uređenje sa najmanjim elementom 0. Ako skup $E \subseteq P$ zadovoljava uslove

(a) $0 \in E$ i

(b) za svako $x \in P$, $\forall y < x\,(y \in E)$ implicira $x \in E$,

onda je $E = P$.

Pretpostavimo da je $E \neq P$. Neka je x najmanji element skupa $P - E$. Zbog (a), $x \neq 0$. Kako za sve $y < x$, $y \in E$, prema uslovu (b), $x \in E$, što nije moguće.

Proširivanje principa indukcije na sva dobra uređenja omogućava da se skup prirodnih brojeva proširi na transfinitan sistem koji uopštava ideju brojanja. To uopštenje izražava se u pojmu ordinalnih brojeva.

Skup x je tranzitivan ako je svaki element od x podskup skupa x. U jezuku $\mathcal{L}_{ZF}$ predikat "x je tranzitivan" definisan je formulom

$$\varphi_{tr}(x) = \forall y \in x\, \forall z \in y\, (z \in x).$$

Primer 2. (a) Skup x je tranzitivan ako i samo ako $\cup x \subseteq x$.

(b) Skup x je tranzitivan ako i samo ako $x \subseteq P(x)$.

Primetimo da je "skup" x oblika $x = \{x\}$ takođe tranzitivan.

Tranzitivan skup x je *ordinal* ako je relacija $\in$ dobro uređenje na x. U narednim razmatranjima pokazaćemo da se ovako definisan pojam ordinala u konačnom slučaju poklapa sa prirodnim brojevima. U beskonačnom slučaju on sasvim prirodno uopštava ideju brojanja.

Primer 3. Predikat "x je ordinal" može se izraziti formulom jezika $\mathcal{L}_{ZF}$.

Skup x ordinal ako i samo ako x je tranzitivan skup i dobro uređen relacijom $\in$. Predikat "relacija $\in$ je dobro uređenje skupa x" izrazićemo formulom jezika $\mathcal{L}_{ZF}$.

Predikati "x je parcijalno uređen relecijom $\in$", "x je linearno uređen relacijom $\in$" i "x je dobro uređen relacijom $\in$" su u jeziku $\mathcal{L}_{ZF}$ redom izraženi formulama:

$$
\begin{aligned}
&\varphi_{pu}(x) = \forall y \in x\,(y \notin y) \wedge \forall y, z, u \in x\,(y \in z \wedge z \in u \to y \in u),\\
&\varphi_{lu}(x) = \varphi_{pu}(x) \wedge \forall y, z \in x\,(y \in z \vee y = z \vee z \in y),\\
&\varphi_{du}(x) = \varphi_{lu}(x) \wedge \forall y \in x\,(y \neq \emptyset \to \exists z \in y\,(x \cap z = \emptyset)).
\end{aligned}
$$

To konačno znači da formula $\varphi_{on}(x) = \varphi_{tr}(x) \wedge \varphi_{du}(x)$ jezika $\mathcal{L}_{ZF}$ definiše predikat "x je ordinal". Klasa $On = \{x : \varphi_{on}(x)\}$ je klasa svih ordinala.

Ordinale označavamo malim grčkim slovima. Poredak među ordinalima definišemo tako da, $\alpha < \beta$ ako i samo ako $\alpha \in \beta$.

Primer 4. (a) Prirodan broj 0 je ordinal, odnosno, $On \neq \emptyset$.

(b) Ako je α ordinal i $\beta \in \alpha$, onda je β ordinal.

(c) Ako su α i β ordinali i $\alpha \subseteq \beta$, onda $\alpha \in \beta$.

(d) Ako su α i β ordinali, onda $\alpha \subseteq \beta$ ili $\beta \subseteq \alpha$.

U ovom primeru tvrđenje "0 je ordinal" treba shvatiti kao teoremu teorije ZF, odnosno, $ZF \vdash \varphi_{on}(0)$. Slično važi i za sva ostala tvrđenja u prethodnom i svim narednim primerima.

Primer 5. (a) Za sve $\alpha, \beta \in On$, $\alpha < \beta$ ili $\alpha = \beta$ ili $\alpha > \beta$, odnosno, relacija $<$ je linearno uređenje klase On.

(b) Za svaki ordinal α, važi $\alpha = \{\beta : \beta < \alpha\}$.

(c) Ako je C neprazna klasa ordinala, $\cap C$ je ordinal, $\bigcap C \in C$ i važi jednakost $\bigcap C = \inf C$. Svaki skup ordinala je dobro uređen relacijom $\in$.

(d) Ako je C neprazan skup ordinala, $\bigcup C$ je ordinal i $\bigcup C = \sup C$.

(e) Za svaki ordinal α, $\alpha \cup \{\alpha\}$ je ordinal i $\alpha \cup \{\alpha\} = \inf\{\beta : \alpha < \beta\}$.

Ordinal $\alpha + 1 = \alpha \cup \{\alpha\}$ je *naslednik* ordinala α. Ako α nije naslednik, ordinal α je *granični ordinal* i tada je $\alpha = \sup\{\beta : \beta < \alpha\}$.

Primer 6. Klasa On nije skup.

U suprotnom, $\sup On + 1$ bi bio ordinal, pa se tako dobija protivrečnost slična Raselovom paradoksu.

Primer 7. Ordinal α je granični ordinal ako i samo ako za svaki ordinal β, $\beta < \alpha$ implicira $\beta + 1 < \alpha$.

Potpunosti radi, pretpostavljamo da je $0 = \sup \emptyset$ granični ordinal. Posle ordinala 0, sledeći ordinal je skup prethodnih ordinala, odnosno, $1 = \{0\}$, pa redom imamo: $2 = \{0, 1\}, \ldots, n = \{0, 1, \ldots, n-1\}$.

Prvi beskonačan ordinal je $\omega = \{0, 1, \ldots, n, \ldots\}$. Istovremeno, ω je najmanji granični ordinal različit od 0 i definisan je formulom

$$\varphi_\omega(x) = \varphi_{ind}(x) \wedge \forall z\,(\varphi_{ind}(z) \rightarrow x = z \vee x \subseteq z),$$

gde je $\varphi_{ind}(x)$ instanca aksiome beskonačnosti.

Ordinal je $\omega + 1 = \omega \cup \{\omega\} = \{0, 1, \ldots, n, \ldots, \omega\}$ je naslednik ordinala ω, pa na sličan način, $\omega + n = \{0, 1, \ldots, \omega, \omega + 1, \ldots, \omega + (n-1)\}$ itd. Prvi granični ordinal veći od ω je $\omega + \omega = \sup\{\omega + n : n \in \omega\}$.

Kao uopštenje ideje brojanja, ordinalni brojevi čuvaju sva važna svojstva prirodnih brojeva. U ovom smislu ključna je činjenica da se teoreme indukcije i rekurzije prirodnih brojeva mogu uopštiti na ordinalne brojeve. Indukciju možemo uopštiti na transfinitnu indukciju i legitimno koristiti kao pravilo zaključivanja u teoriji ZF. Slično, u teoriji ZF legitimne su i definicije transfinitnom rekurzijom. Pre nego što pređemo na razmatranje ovih pitanja, dokazaćemo da se svako dobro uređenje može predstaviti ordinalom. U ovoj teoremi reprezentacije koristimo svojstva dobrih uređenja koja su izložena u sledećim primerima.

Primer 8. (a) Ako je f automorfizam dobrog uređenja $(P, \leq)$, onda za svako $x \in P$, važi $x \leq f(x)$.

(b) Jedini automorfizam dobrog uređenja je identitet.

(c) Ukoliko postoji, izomorfizam dobrih uređenja je jedinstven.

U dokazu tvrđenja (a) treba pokazati da je $D = \{x \in P : f(x) < x\}$ prazan skup. Na sličan način, u dokazu tvrđenja (b) treba pokazati da je $E = \{x \in P : f(x) \neq x\}$ prazan skup.

Ako su $f : \mathcal{P} \rightarrow \mathcal{G}$ i $g : \mathcal{P} \rightarrow \mathcal{G}$ izomorfizmi dobrih uređenja, kompozicija $h = f^{-1} \circ g$ je automorfizam uređenja $\mathcal{G}$. Zbog tvrđenja (b), automorfizam h je identitet, pa mora biti $f = g$.

Za svako $u \in P$, skup $P_u = \{x \in P : x < u\}$ je *inicijalni segment* dobrog uređenja $(P, \leq)$, određen elementom u.

Primer 9. (a) Ne postoji dobro uređen skup koji je izomorfan svom inicijalnom segmentu.

(b) Svaka dva dobra uređenja su ili izomorfna ili je jedno od njih izomorfno inicijalnom segmentu drugog.

Neka je $(P, \leq)$ parcijalno uređenje, $a \in P$ i $f : P \to P_a$ izomorfizam uređenja $\mathcal{P}$ na inicijalni segment P_a. Na osnovu prethodnog primera, važi $a \leq f(a)$, ali po pretpostavci, $f(a) \in P_a$, tj. $f(a) < a$, što nije moguće.

Teorema 3. Svaki dobro uređen skup je izomorfan ordinalu.

Dokaz: Neka je $\mathcal{P} = (P, \leq)$ dobro uređenje. Teoremu dokazujemo indukcijom u dobrom uređenju $\mathcal{P}$. Primetimo da, ukoliko uopšte postoji, prema prethodnim primerima, ordinal izomorfan uređenju $\mathcal{P}$ jedinstveno je određen.

Za svako $x \in P$, neka je α_x ordinal izomorfan inicijalnom segmentu P_x. Tvrdimo da za svako $x \in P$ postoji ordinal α_x.

U suprotnom, postojao bi najmanji element $x \in P$, za koji ne postoji ordinal α_x izomorfan sa P_x. To bi značilo da za svako $y < x$, inicijalni segment P_y izomorfan je ordinalu α_y. Prema principu indukcije na dobrom uređenju $\mathcal{P}$, P_x je izomorfan ordinalu, što nije moguće.

Na osnovu prethodnih primera, za svako $x \in P$, ordinal α_x je jedinstveno određen. Prema aksiomi zamene, $S = \{\alpha_x : x \in P\}$ je skup. Kao skup ordinala, S je dobro uređen relacijom $\in$. Treba dokazati da je S tranzitivan skup.

Pretpostavimo da je $\alpha \in \alpha_x$. Neka je $f : P_x \to \alpha_x$ odgovarajući izomorfizam i $y = f^{-1}(\alpha)$. Neposredno se proverava da je $f \restriction P_y$ izomorfizam inicijalnog segmenta P_y i ordinala α, tj. $\alpha \in S$. $\square$

Primer 10. *Princip transfinitne indukcije:* ako klasa $C \subseteq On$ zadovoljava uslove

(a) $0 \in C$,

(b) za svako α, ako $\alpha \in C$, onda $\alpha + 1 \in C$,

(c) ako je α granični ordinal, za svako $\beta < \alpha$, $\beta \in C$ implicira $\alpha \in C$,

onda je $C = On$.

U suprotnom, postojao bi $\alpha = \inf(On - C)$, pa bi se primenom jednog od navedenih uslova transfinitne indukcije morala dobiti kontradikcija.

U do sada razvijenim pojmovima teorije skupova može se kombinatornim sredstvima izložiti i veći deo aritmetike ordinala. Kako u nekim slučajevima takve definicije nisu sasvim očigledne, pre nego što razvijemo ovu aritmetiku formulisaćemo *teoremu transfinitne rekurzije.*

Transfinitna rekurzija

Neka je a proizvoljan skup. Za svako $n \in \omega$, sa a^n označavamo skup svih funkcija sa domenom n i vrednostima u skupu a. Svaka funkcija $f \in a^n$ je *niz* elemenata skupa a dužine n. Primetimo da se u odnosu na raniju definiciju uređenog para skupovi $a \times a$ i a^2 razlikuju, ali među njima postoji obostrano jednoznačna korespodencija. Za svaki skup a, $a^{<\omega} = \bigcup\{a^n : n \in \omega\}$ je skup svih konačnih nizova skupa a. Egzistenciju ovog skupa garantuju aksiome partitivnog skupa, unije i separacije.

Slično konačnim nizovima, za svaki ordinal α, definisan je skup a^α svih nizova elemenata skupa a dužine α. Niz $f \in a^\alpha$ je funkcija koja preslikava α u skup a. U opštem slučaju, funkcija f može biti zadata eksplicitno, odnosno, pravilom pomoću kojeg za svako $\beta < \alpha$ računamo vrednost $f(\beta)$ ili implicitno, jednim skupom uslova koji propisuju kako se izračunava $f(0)$ i kako se na osnovu vrednosti $f(\xi)$, $\xi < \beta$ izračunava vrednost $f(\beta)$.

Primer 1. (a) Neka je $f \in \omega^\omega$ niz prirodnih brojeva takav da za svako $n \in \omega$, $f(n) = 2 \cdot n^2 + n + 3$. Ako znamo da računamo, a kasnije ćemo videti da to u ZF zaista jeste tako, onda na osnovu vrenosti n, neposredno izračunavamo vrednost funkcije $f(n)$.

(b) Ako je a skup, $f(0) = a$ i za sve $n \in \omega$, $f(n+1) = \{f(n)\}$, onda vrednost $f(n)$ ne računamo neposredno, već na osnovu prethodno izračunate vrednosti niza f. U ovom primeru domen niza f je skup ω, ali nije odmah jasno šta je njegov kodomen. Bez aksiome zamene, nije moguće dokazati da skup vrednosti $\{a, \{a\}, \{\{a\}\}, \dots\}$ funkcije f zaista jeste skup. Polazeći od skupa a, ovaj skup se ne može dobiti primenom partitivnog skupa, unije ili separacije.

(c) Neka je $f \in \omega^\omega$ niz prirodnih brojeva takav da $f(0) = 1$, $f(1) = 1$ i za svako $n \in \omega$, $f(n+2) = f(n+1) + f(n)$.

U ovom primeru, takozvanog Fibonačijevog niza, vrednosti funkcije $f(n)$, za $n \geq 2$, računaju se na osnovu vrednosti $f(n-1)$ i $f(n-2)$.

Lako je zamisliti primere u kojima se vrednosti niza računaju na osnovu svih prethodno izračunatih vrednosti niza, ili konačnog broja vrednosti nekog drugog niza itd. Jasno je da spisak uslova koji implicitno definišu neku funkciju može biti vrlo dugačak i složen. U svakom takvom slučaju nije apriori jasno da li zadati uslovi uopšte određuju neku funkciju, a ako to jeste slučaj, da li je takva funkcija jedinstveno određena. Teorema rekurzije razrešava ovaj problem u jednoj prilično prirodnoj klasi slučajeva. Da bi se ona bolje razumela, u sledećim primerima izložene su njene varijante u slučaju prirodnih brojeva.

Primer 2. *Teorema rekurzije za prirodne brojeve*: Ako je a neprazan skup, $g : \omega \times a \to a$ funkcija i $x \in a$, postoji jedinstveno određen niz $f : \omega \to a$ koji zadovoljava uslove:

$$f(0) = x \text{ i za sve } n \in \omega,\ f(n+1) = g(n, f(n)).$$

Ako funkcija $f' : \omega \to a$ zadovoljava navedene uslove, onda $f(0) = f'(0)$ i za svako $n \in \omega$, $f(n+1) = g(n, f(n)) = g(n, f'(n)) = f'(n+1)$, tj. ukoliko postoji, niz f je jedinstveno određen.

Za svako $m \in \omega$, neka je $t_m : m+1 \to a$ funkcija takva da $t_m(0) = x$ i za sve $k < m$, $t_m(k+1) = g(k, t_m(k))$. Primetimo da za sve $n \in \omega$, $t_m \subseteq \omega \times a$. Neka je $f = \bigcup\{t_m : m \in \omega\}$. Jasno, $f \subseteq \omega \times a$.

Tvrdimo da je f funkcija, da je $\mathrm{dom}(f) = \omega$ i da f zadovoljava uslove teoreme.

Kako za sve $m, n \in \omega$, $m \leq n$ implicira $t_m \subseteq t_n$, neposredno dobijamo da je f zaista funkcija. Jasno je da $\mathrm{dom}(f) \subseteq \omega$, pa kako je $\omega \subseteq \bigcup_{m \in \omega} \mathrm{dom}(t_m) = \mathrm{dom}(f)$, mora biti $\mathrm{dom}(f) = \omega$.

Za svako $n \in \omega$, $t_n(0) = x$, pa mora biti $f(0) = x$ i

$$f(n+1) = t_{n+1}(n+1) = g(n, t_{n+1}(n)) = g(n, f(n)),$$

što znači da funkcije f zadovoljava uslove teoreme.

Primer 3. Za svaki skup a i svaku funkciju $g : a^{<\omega} \to a$, postoji funkcija $f : \omega \to a$ takva da za svako $n > 0$,

$$f(n) = g(f \upharpoonright n) = g(f(0), \ldots, f(n-1)).$$

Pritom, $f(0) = g(f \upharpoonright 0) = g(\emptyset)$.

Neka je $h_0 = \emptyset$ i za svako $n \in \omega$, $h_{n+1} = h_n \cup \{(n, g(h_n))\}$. Na osnovu prethodnog primera, niz $h : \omega \to a^{<\omega}$ je jedinstveno određen.

Neka je $f = \bigcup_{n \in \omega} h_n$, onda $f : \omega \to a$ i za svako $n \in \omega$, $f \upharpoonright n = h_n$. Pritom, za svako $n \in \omega$, $f(n) = h_{n+1}(n) = g(h_n) = g(f \upharpoonright n)$.

Definicija elementarnih aritmetičkih operacija podrazumeva varijantu teoreme rekurzije za prirodne u kojoj rekurzivno definisana funkcija može da sadrži jedan ili više parametara.

Primer 4. *Teorema rekurzije sa parametrima*: Ako su a i b proizvoljni skupovi, a $f : b \to a$ i $g : b \times \omega \times a \to a$ funkcije, onda postoji jedinstveno određena funkcija $h : b \times \omega \to a$ takva da za sve $x \in b$, $n \in \omega$

$$h(x, 0) = f(x) \text{ i } h(x, n+1) = g(x, n, h(x, n)).$$

Dokaz teoreme rekurzije sa parametrima se praktično ne razlikuje od dokaza njene obične verzije. U ovom slučaju, za svako $m \in \omega$ definiše se funkcija $t_m : b \times (m+1) \to a$ takva da za svako $x \in b$, $t_m(x, 0) = f(x)$ i za sve $k < m$, $t_m(x, k+1) = g(x, n, t_m(n))$, a parametar x provuče kroz čitav dokaz.

Primer 5. Koristeći teoremu rekurzije sa parametrima jednostavno se definiše aritmetika prirodnih brojeva.

(a) Za sve $x, y, z \in \omega$, neka je $f(x) = x$ i $g(x, y, z) = z + 1$. Polazeći od funkcija f i g, na osnovu teoreme rekurzije, *sabiranje prirodnih brojeva* definisano je sledećim relacijama:

$$x + 0 = x \text{ i za svako } y \in \omega,\ x + (y+1) = (x+y) + 1.$$

(b) Operaciju *množenja prirodnih brojeva* definišemo rekurzijom pomoću konstante $f(x) = 0$, za svako $x \in \omega$ i sabiranja:

$$x \cdot 0 = 0 \text{ i za sve } y \in \omega,\ x \cdot (y+1) = x \cdot y + y.$$

Ključni argument uopštenja rekurzije na sve ordinale jeste aksioma zamene. Ako formula $\varphi(x, y)$ jezika $\mathcal{L}_{ZF}$ definiše parcijalnu funkciju, na osnovu aksiome zamene, za svaki skup a, postoji skup b takav da za svako $x \in a$, $\varphi(x, y)$ ako i samo ako $y \in b$.

Ako sa f označimo klasu $\{(x, y) : \varphi(x, y)\}$, za svaki skup x, ukoliko postoji, $f(x)$ označavamo jedinstveno određen skup y takav da važi $\varphi(x, y)$. Klasu f shvatamo kao parcijalnu skupovnu operaciju definisanu formulom φ. Pritom, na osnovu aksiome zamene, za svaki skup a, $f[a] = \{y : \exists x \in a\, \varphi(x, y)\}$ je jedinstveno određen skup.

U daljim razmatranjima identifikujemo klase i formule, tj. pretpostavljamo da je svaku formulu $\varphi(\vec{x})$ određena klasa skupova $\{\vec{x} : \varphi\}$ i obratno, svaka klasa definisana je formulom jezika $\mathcal{L}$. Takođe, govorimo o odgovarajućim operacijama i relacijama definisanim na klasama.

Na primer, ako su $A = \{x : \varphi(x)\}$ i $B = \{x : \psi(x)\}$ klase skupova, onda jednakost $A = B$ podrazumeva rečenicu $\forall x\, (\varphi(x) \leftrightarrow \psi(x))$. Slično, klasa $A \cap B$ određena je konjunkcijom formula φ i ψ.

Klasa svih skupova je $V = \{x : x = x\}$. Kako je klasa ordinala $On \subseteq V$ definisana formulom $\varphi_{on}(x)$ jezika $\mathcal{L}_{ZF}$, klasa V nije skup. U suprotnom, prema aksiomi separacije i klasa On bi bila skup, a to nije moguće.

Primer 6. (a) Ako su x i y skupovi, onda postoji $x \cup y$, pa se unija može shvatiti kao klasa $\bigcup = \{(x, y, z) : x \cup y = z\}$, odnosno, kao binarna operacija $\bigcup : V \times V \to V$ na klasi svih skupova V.

(b) Slično važi i za operacije $x \cap y$, $x \times y$, $\{x\}$, $P(x)$ i x^y koje su uvek definisane. Operacije poput $\mathrm{dom}(f)$ i $\mathrm{codom}(f)$ su parcijalno definisane.

Primer 7. *Opšta teorema rekurzije za prirodne brojeve*: Ako je $g(x, y)$ skupovna operacija, za svaki skup a postoji jedinstveno određen niz $(f(n) : n \in \omega)$ takav da:

$$f(0) = a \text{ i za svako } n \in \omega,\ f(n+1) = g(n, f(n)).$$

Dokaz ovog tvrđenja sledi neposredno iz teoreme o transfinitnoj rekurziji. U sledećim primerima ilustrovane su neke njene posledice.

Primer 8. (a) Na osnovu teoreme rekurzije za prirodne brojeve, u dobrom uređenju $\mathcal{P}$ ne postoji niz $a_0 > a_1 > \cdots$, tj. u dobrom uređenju ne postoji beskonačan striktno opadajući niz.

Ako se pretpostavi aksioma izbora, ovaj uslov implicira da je $\mathcal{P}$ dobro uređenje.

(b) Takođe, na osnovu prethodne teoreme rekurzije, neposredno sledi da za svaki skup a, $S = \{a, \{a\}, \{\{a\}\}, \dots\}$ je skup.

(c) $\omega + \omega$ i $\{\omega, P(\omega), P(P(\omega)), \dots\}$ su skupovi.

Primer 9. (a) Postoji niz skupova $(V_n : n \in \omega)$ takav da $V_0 = \emptyset$ i za svaki prirodan broj $n \in \omega$, $V_{n+1} = P(V_n)$. Takođe, $V_\omega = \bigcup_{n \in \omega} V_n$ je skup.

(b) Skup V_ω je tranzitivan i za svako $x \in V_\omega$, skup x je konačan. Ako je $x \subseteq V_\omega$ konačan skup, onda $x \in V_\omega$.

(c) Ako $x, y \in V_\omega$, onda $\{x, y\} \in V_\omega$, $\bigcup x \in V_\omega$ i $P(x) \in V_\omega$. Ako je $a \in V_\omega$ i f funkcija na a takva da za svako $x \in a$, $f(x) \in V_\omega$, onda je $f[a] \in V_\omega$.

Ako je α granični ordinal, *granična vrednost* neopadajućeg niza ordinala $(\beta_\gamma : \gamma < \alpha)$ je $\lim_{\gamma \to \alpha} \beta_\gamma = \sup\{\beta_\gamma : \gamma < \alpha\}$.

Primer 10. Postoje proizvoljno veliki granični ordinali, tj. za svaki ordinal α, postoji granični ordinal $\beta > \alpha$.

Neka je α ordinal, $\alpha_0 = \alpha$ i za sve $n \in \omega$, $\alpha_{n+1} = \alpha_n + 1$. Ordinal $\beta = \lim_{n \to \omega} \alpha_n$ je granični ordinal veći od α.

Primer 11. Niz ordinala $(\gamma_\alpha : \alpha \in On)$ je *neprekidan* ako za svaki granični ordinal α, $\lim_{\beta \to \alpha} \gamma_\beta = \gamma_\alpha$. Svaki neprekidan rastući niz ordinala ima fiksnu tačku, tj. postoji ordinal α takav da $\alpha = \gamma_\alpha$.

Za svako $n \in \omega$ neka je $\alpha_{n+1} = \gamma_{\alpha_n}$. Ordinal $\alpha = \lim_{n \to \omega} \alpha_n$ je fiksna tačka niza $(\gamma_\alpha : \alpha \in On)$. Jasno, svaki takav niz ima beskonačno mnogo fiksnih tačaka.

Kako smo nagovestili, rekurzivne definicije su moguće i na ordinalima većim od ω, odnosno opštije, na klasi On svih ordinala.

Kako je priroda spomenutih varijanti teoreme transfinitne rekurzije bitno različita, svaku od njih dokazaćemo posebno.

Teorema 4. Ako je λ ordinal i $h : On \times V \to V$ skupovna operacija, postoji jedinstveno određena funkcija $f : \lambda \to V$ takva da za svako $\alpha \in \lambda$,

$$f(\alpha) = h(\alpha, f \restriction \alpha).$$

Pre nego što dokažemo teoremu, primetimo da ona nije dokaziva u teoriji ZF. U njoj je implicitno sadržan kvantifikator "za svako h", pri čemu h prolazi preko klasa, što u teoriji ZF nije moguće. Ako fiksiramo konkretnu skupovnu operaciju h, onda postoji formula $\varphi(x, y, z)$ jezika $\mathcal{L}_{ZF}$ koja definiše klasu h, tj. za svako $\alpha \in On$ i sve $x, y \in V$,

$$h(\alpha, x) = y \quad \Leftrightarrow \quad \varphi(\alpha, x, y)$$

Ako se to ima u vidu, smisao teoreme jeste da za zadatu formulu φ jezika $\mathcal{L}_{ZF}$, u teoriji ZF možemo dokazati da za svaki ordinal λ, postoji jedinstvena funkcija $f : \lambda \to V$ takva da za svako $\alpha \in \lambda$ važi $\varphi(\alpha, f \restriction \alpha, f(\alpha))$. Dakle, teorema se ne može dokazati u ZF, već predstavlja shemu koja za svaku konkretnu formulu daje teoremu teorije ZF.

Dokaz: Neka su $h : On \times V \to V$ i $\lambda \in On$ zadati. Koristeći samo aksiome teorije ZF, dokazaćemo da postoji jedinstveno određena funkcija $f : \lambda \to V$ takva da za sve $\alpha < \lambda$, $f(\alpha) = h(\alpha, f \restriction \alpha)$.

Neka je $\mu \leq \lambda$. Pretpostavimo da su $f_1 : \mu \to V$ i $f_2 : \mu \to V$ funkcije takve da za sve $\alpha < \mu$, $f_1(\alpha) = h(\alpha, f_1 \restriction \alpha)$ i $f_2(\alpha) = h(\alpha, f_2 \restriction \alpha)$. Tvrdimo da je $f_1 = f_2$.

Ako je $\mu = 0$, tvrđenje je trivijalno zadovoljeno. Pretpostavimo da je $\mu > 0$ i da za svako $\mu' < \mu$ važi $f_1 \restriction \mu' = f_2 \restriction \mu'$. Ako je μ granični ordinal, onda neposredno imamo da je $f_1 = f_2$. Neka je $\mu = \nu + 1$. Prema induktivnoj pretpostavci $f_1 \restriction \nu = f_2 \restriction \nu$, pa je $f_1(\nu) = h(\nu, f_1 \restriction \nu) = h(\nu, f_2 \restriction \nu) = f_2(\nu)$. To konačno znači da je

$$f_1 = (f_1 \restriction \nu) \cup \{(\nu, f_1(\nu))\} = (f_2 \restriction \nu) \cup \{(\nu, f_2(\nu))\} = f_2,$$

što dokazuje jedinstvenost funkcije f.

Neka je M klasa funkcija takva da

$$M = \{f : \exists \mu < \lambda \, (f : \mu \to V \wedge \forall \alpha \in \mu \, (f(\alpha) = h(\alpha, f \restriction \alpha))\}.$$

Da bismo dokazali teoremu, dovoljno je pokazati da postoji $f \in M$ takvo da važi $\mathrm{dom}(f) = \lambda$.

Primedba: Ako su funkcije $f, g \in M$ takve da $\mu = \mathrm{dom}(f)$, $\nu = \mathrm{dom}(g)$ i ako je $\mu < \nu$, na osnovu dokaza jedinstvenosti, mora biti $f = g \restriction \mu$.

Neka je $A = \{\mu : \exists f \in M\,(\mathrm{dom}(f) = \mu)\}$. Tvrdimo da $\lambda \in A$.

Pretpostavimo suprotno, onda $\lambda \in (\lambda + 1) - A$, pa skup $(\lambda + 1) - A$ nije prazan. Neka je μ njegov najmanji element. To znači da je $\mu \leq \lambda$, pa za svako $\nu < \mu$, postoji $f \in M$ takvo da je $\mathrm{dom}(f) = \nu$. Prema prethodnoj primedbi, za svako $\nu < \mu$, neka je $F(\nu)$ jedinstvena funkcija $f \in M$ takva da je $\mathrm{dom}(f) = \nu$. Prema aksiomi zamene, $F[\mu]$ je skup.

Neka je $f_0 = \bigcup F[\mu]$. Takođe, prema gornjoj primedbi, f_0 je funkcija i pritom, za svako $\nu < \mu$, važi $f_0 \restriction \nu = F[\nu]$. Otuda za sve $\nu < \mu$ imamo

$$\forall \alpha \in \nu\ f_0(\alpha) = h(\alpha, f_0 \restriction \alpha).$$

Ako je μ granični ordinal, onda $f_0 \in M$ i $\mathrm{dom}(f_0) = \mu$, suprotno pretpostavci o izboru ordinala μ. To znači da bi μ morao biti oblika $\mu = \nu + 1$.

U tom slučaju, ako je $f_0' = f_0 \cup \{(\nu, h(\nu, f_0 \restriction \nu))\}$, mora biti $f_0' \in M$ i $\mathrm{dom}(f_0') = \mu$, što takođe protivreči izboru ordinala μ. $\square$

Kao graničnu verziju prethodne teoreme, sada možemo formulisati opštu em teoremu rekurzije na ordinalima.

Teorema 5. Za svaku funkciju $h : On \times V \to V$ postoji jedinstveno određena funkcija $f : On \to V$ takva da za svako $\alpha \in On$, $f(\alpha) = h(\alpha, f \restriction \alpha)$.

U odnosu na prethodnu, ova teorema ne predstavlja ni shema teoremu čija je svaka instanca dokaziva u teoriji ZF. Opšta teorema rekurzije je metateorema o teoriji ZF, odnosno, metateorema o predikatskom računu prvog reda koja garantuje legitimnost rekurzivnih definicija u teoriji ZF. Precizno formulisana, teorema tvrdi da za svaku formulu $\varphi(x, y, z)$ jezika $\mathcal{L}_{ZF}$ koja zadovoljava uslov

$$\forall \alpha \in On\, \forall x \exists y \forall z\, (\varphi(\alpha, x, z) \leftrightarrow z = y),$$

postoji formula $\psi(x, y)$ takva da važi:

(a) $ZF \vdash \forall \alpha \in On\, \exists y \forall z\, (\psi(\alpha, z) \leftrightarrow z = y)$ i

(b) $ZF \vdash \forall \alpha \forall y\, (\psi(\alpha, y) \leftrightarrow \exists z\, (\mathrm{fun}(z) \wedge \mathrm{dom}(z) = \alpha) \wedge$
$\forall \xi \in \alpha\, \varphi(\xi, z \restriction \xi, z(\xi)) \wedge \varphi(\alpha, z, y))$.

Dokaz: Jedini način da dokažemo teoremu jeste da, polazeći od formule φ, eksplicitno konstruišemo formulu ψ. Zapravo, formula ψ je već data uslovom (b), odnosno, $\psi(\alpha, y)$ je sledeća formula:

$$\exists z\, (\mathrm{fun}(z) \wedge \mathrm{dom}(z) = \alpha) \wedge \forall \xi \in \alpha\, \varphi(\xi, z \restriction \xi, z(\xi)) \wedge \varphi(\alpha, z, y).$$

Izborom formule ψ, uslov (b) je trivijalno zadovoljen, pa ostaje da dokažemo uslov (a). Jednostavnosti radi, umesto o formulama govorićemo o klasama. Neka je $h : On \times V \to V$ zadato. Definišimo klasu f tako da

$$f = \{(\alpha, x) : \exists z(\mathrm{fun}(z) \wedge \mathrm{dom}(z) = \alpha) \wedge \\ \forall \xi \in \alpha \, (z(\xi) = h(\xi, z \upharpoonright \xi)) \wedge x = h(\alpha, z))\}.$$

Ako $(\alpha, x), (\alpha, x') \in f$, onda $x = x'$. Pretpostavimo da je α ordinal za koji ne postoji skup x takav da $(\alpha, x) \in f$. U tom slučaju postoji najmanji ordinal α sa takvim svojstom. Slično dokazu prethodne teoreme, lako se proverava da takva pretpostavka vodi do kontradikcije. Dakle, $f : On \to V$ je funkcija i za svako α, $f(\alpha) = h(\alpha, f \upharpoonright \alpha)$. Konačno, ako je $g : On \to V$ funkcija sa istim svojstvom, indukcijom po α dobija se da je $f(\alpha) = g(\alpha)$, za svako $\alpha \in On$. $\Box$

U narednim primerima, na osnovu opšte teoreme transfinitne rekurzije definisaćemo aritmetiku ordinalnih brojeva. Konstrukcije osnovnih operacija su znatno jednostavnije ako se u opštoj teoremi transfinitne rekurzije napravi razlika između graničnih ordinala i ordinala oblika naslednika.

Primer 12. Ako je a skup i $h_1, h_2 : On \times V \to V$ skupovne operacije, onda postoji jedinstveno određena funkcija $f : On \to V$ takva da:

(a) $f(0) = a$,
(b) $f(\alpha + 1) = h_1(\alpha, f(\alpha))$, za svako $\alpha \in On$,
(c) ako je $\alpha \neq 0$ granični ordinal, $f(\alpha) = h_2(\alpha, f \upharpoonright \alpha)$.

Definišimo skupovnu operaciju h tako da za svaki skup $x \in V$ i proizvoljan ordinal $\alpha \in On$,

$$h(\alpha, x) = \begin{cases} a & \text{ako } \alpha = 0, \\ h_1(\alpha, x) & \text{ako je } \alpha \neq 0, \ \mathrm{fun}(x) \\ & \text{i } \mathrm{dom}(x) = \alpha + 1, \\ h_2(\alpha, x) & \text{ako je } \alpha \neq 0 \text{ granični ordinal,} \\ & \mathrm{fun}(x) \text{ i } \mathrm{dom}(x) = \alpha, \\ \emptyset & \text{inače.} \end{cases}$$

Na osnovu teoreme transfinitne rekurzije, funkcija $f : On \to V$ definisana relacijom $f(\alpha) = h(\alpha, f \upharpoonright \alpha)$ zadovoljava uslove (a), (b) i (c).

Slično teoremi rekurzije za prirodne brojeve i transfinitna rekurzija se najčešće primenjuje u verziji za parametarima. Ona omogućava da rekurzivnu definiciju elementarnih operacija prirodnih brojeva proširimo na transfinitne ordinale. U sledećim primerima definisaćemo sabiranje, množenje i stepenovanje ordinala i izložiti osnovne osobine ovih operacija.

U teoremi rekurzije sa parametrima, razdvojićemo slučajeve ordinala naslednika i graničnih ordinala.

Primer 13. Ako su $h_1 : V \to V$ i $h_2, h_3 : V \times On \times V \to V$ skupovne operacije, postoji jedinstvena operacija $f : V \times On \to V$ takva da:

(a) $f(x, 0) = h_1(x)$,
(b) za svako $\alpha \in On$, $f(x, \alpha + 1) = h_2(x, \alpha, f_x(\alpha))$ i
(c) ako je $\alpha \neq 0$ granični ordinal, $f(x, \alpha) = h_3(x, \alpha, f_x \upharpoonright \alpha)$.

Pritom, za svaki skup x, $f_x \upharpoonright \alpha = \{(x, y, z) : \exists y \in \alpha\, (f(x, y) = z)\}$.

Primer 14. *Sabiranje ordinala* definisano je sledećim relacijama: za svaki ordinal β,

$$\begin{aligned} &\beta + 0 = \beta \\ &\beta + (\alpha + 1) = (\beta + \alpha) + 1, \text{ za svaki ordinal } \alpha, \\ &\beta + \alpha = \sup\{\beta + \gamma : \gamma < \alpha\}, \text{ ako je } \alpha \neq 0 \text{ granični ordinal.} \end{aligned}$$

Korektnost definicije sabiranja garantuje prethodna parametarska varijanta teoreme rekurzije. Suma ordinala dobija se transfinitnom rekurzijom iz sledećih operacija:

$$h_1(x) = x,\ h_2(x, \alpha, y) = y \cup \{y\} \text{ i } h_3(x, \alpha, y) = \sup(\text{codom}(y)).$$

Primer 15. Intuitivno, ako su α i β ordinali, njihova suma $\alpha + \beta$ je tip uređenja koji se dobija kada se ordinal α produži ordinalom β. Bez pozivanja na teoremu rekurzije, suma ordinala može se definisati na sledeći način:

Neka je $P = (\alpha \times \{0\}) \cup (\beta \times \{1\})$ i $<_P$ binarna relacija skupa P takva da za sve $\gamma, \delta < \max\{\alpha, \beta\}$ i sve $i, j \in \{0, 1\}$,

$$(\gamma, i) <_P (\delta, j) \text{ ako i samo ako } (i < j) \vee (i = j \wedge \gamma < \delta).$$

Kako je $\mathcal{P} = (P, <_P)$ dobro uređenje postoji jedinstveno određen ordinal, u oznaci $\alpha + \beta$, izomorfan sa $\mathcal{P}$.

Transfinitnom indukcijom se dokazuje da je navedena kombinatorna definicija sume ordinala ekvivalentna njenoj rekurzivnoj definiciji.

Primer 16. Ako su α, β i γ ordinali, onda:

(a) $\alpha < \beta$ ako i samo ako $\gamma + \alpha < \gamma + \beta$,
(b) $\alpha = \beta$ ako i samo ako $\gamma + \alpha = \gamma + \beta$,
(c) $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$.

Kako je $1 + \omega = \sup\{1 + n : n \in \omega\} = \omega$, a istovremeno, $\omega + 1 > \omega$, sabiranje ordinala nije komutativno.

Primer 17. Ako je $\alpha < \beta$, onda $\alpha + \gamma \leq \beta + \gamma$, relacija $\leq$ ne može se zameniti realcijom $<$. U opštem slučaju, iz $\alpha + \gamma = \beta + \gamma$ ne sledi $\alpha = \beta$.

Primer 18. (a) Za svaki ordinal α, postoje jedinstveno određeni granični ordinal β i prirodan broj $n \in \omega$ takvi da $\alpha = \beta + n$.

(b) Ako je $\alpha \leq \beta$, postoji jedinstven ordinal γ takav da $\alpha + \gamma = \beta$, a jednačina $\gamma + \alpha = \beta$ ima jedno, beskonačno mnogo ili uopšte nema rešenja.

(c) Postoji najmanji ordinal $\alpha > \omega$ takav da za sve $\beta < \alpha$, $\beta + \alpha = \alpha$.

Primer 19. *Množenje ordinala* definisano je sledećim relacijama: za svaki ordinal β,

$$\begin{aligned}
&\beta \cdot 0 = 0,\\
&\beta \cdot (\alpha + 1) = \beta \cdot \alpha + \beta, \text{ za svaki ordinal } \alpha,\\
&\beta \cdot \alpha = \sup\{\beta \cdot \gamma : \gamma < \alpha\} \text{ ako je } \alpha \neq 0 \text{ granični ordinal.}
\end{aligned}$$

Intuitivno, proizvod ordinala α i β je odrinal $\alpha \cdot \beta$ koji se sastoji od β kopija ordinala α. Pored rekurzivne definicije, množenje ordinala ima i prirodnu kombinatornu definiciju, tj. proizvod ordinala α i β može se definisati kao tip leksikografskog uređenja Dekartovog proizvoda $\alpha \times \beta$.

Ordinal $\alpha \cdot \beta$ je tip uređenja $(\alpha \times \beta, <^*)$ u kojem je poredak $<^*$ definisan tako da za sve $\gamma, \gamma^{'} < \alpha$ i sve $\delta, \delta^{'} < \beta$,

$$(\gamma, \delta) <^* (\gamma', \delta') \text{ ako i samo ako } (\gamma < \gamma^{'}) \vee (\gamma = \gamma^{'} \wedge \delta < \delta^{'}).$$

Nije teško proveriti da su kombinatorna i rekurzivna definicija množenja ordinala ekvivalentne.

Primer 20. (a) Slično sabiranju, množenje ordinala je asocijativno, ali nije komutativno. Na primer, $2 \cdot \omega = \sup\{2 \cdot n : n \in \omega\} = \omega$, a sa druge strane, $\omega \cdot 2 = \omega \cdot (1 + 1) = \omega + \omega$.

(b) Ordinal α je granični ako i samo ako postoji β takvo da $\alpha = \omega \cdot \beta$.

(c) Za sve $\alpha, \beta, \gamma \in On$, važi $\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$. Međutim, desna distributivnost množenja u odnosu na sabiranje ordinala ne važi.

Primer 21. Neka su α, β i γ ordinali. Ako $\gamma \neq 0$, onda:

(a) $\alpha < \beta$ ako i samo ako $\gamma \cdot \alpha < \gamma \cdot \beta$,

(b) $\alpha = \beta$ ako i samo ako $\gamma \cdot \alpha = \gamma \cdot \beta$,

(c) Ako $\alpha < \beta$, onda $\alpha \cdot \gamma \leq \beta \cdot \gamma$.

Relacija $\leq$ u tvrđenju (c) ne može se zameniti relacijom $<$. U opštem slučaju, iz $\alpha \cdot \gamma = \beta \cdot \gamma$ ne sledi $\alpha = \beta$.

Primer 22. *Stepenovanje ordinala* definisano je sledećim relacijama: za svaki ordinal β,

$$\begin{aligned}&\beta^0 = 1,\\ &\beta^{\alpha+1} = \beta^\alpha \cdot \beta, \text{ za svaki ordinal } \alpha,\\ &\beta^\alpha = \sup\{\beta^\gamma : \gamma < \alpha\}, \text{ ako je } \alpha \neq 0 \text{ granični ordinal.}\end{aligned}$$

Za razliku od sabiranja i množenja, kombinatorna definicija stepenovanja je prilično komplikovana i retko se koristi.

Naglašavamo da je $2^\omega = \sup\{2^n : n \in \omega\} = \omega$. Kao stepen ordinala, 2^ω treba jasno razlikovati od skupa 2^ω kao skupa svih funkcija iz ω u 2.

Primer 23. Ako su α, β i γ ordinali, onda $\alpha^\beta \cdot \alpha^\gamma = \alpha^{\beta+\gamma}$ i $(\alpha^\beta)^\gamma = \alpha^{\beta\cdot\gamma}$.

Primer 24. (a) Za svako α, postoji proizvoljno veliki ordinal β takav da $\alpha + \beta = \beta$. Postoji najmanji ordinal β takav da $\omega + \beta = \beta$.

(b) Za svako α, postoji proizvoljno veliki ordinal β takav da $\alpha \cdot \beta = \beta$. Postoji najmanji ordinal β takav da $\omega \cdot \beta = \beta$.

(c) Za svako α, postoji proizvoljno veliki ordinal β takav da $\alpha^\beta = \beta$. Postoji najmanji ordinal β takav da $\omega^\beta = \beta$.

Primer 25. Svaki ordinal α može se predstaviti u Kantorovom normalnom obliku: $\alpha = \omega^{\alpha_1} + \cdots + \omega^{\alpha_n}$, gde je $\alpha_1 \geq \cdots \geq \alpha_n$.

Za zadato α, odredimo α_1 kao najveći ordinal takav da $\omega^{\alpha_1} \leq \alpha$, a potom δ_1 takvo da $\omega^{\alpha_1} + \delta_1 = \alpha$. Isti postupak ponovimo sa δ_1 i odredimo najveći α_2 takav da $\omega^{\alpha_2} \leq \delta_1$ i δ_2 takvo da $\omega^{\alpha_2} + \delta_2 = \delta_1$. Kako je $\alpha > \delta_1 > \delta_2 > \cdots$, ovaj postupak završava se u konačno mnogo koraka, a kako je $\omega^0 = 1$, postupak se završava samo ako je $\delta_n = 0$.

Ova forma ordinala je veoma korisna u izučavanju prebrojivih ordinala manjih od Kantorovog ordinala ε_0, tj. najmanjeg ordinala takvog da $\omega^\varepsilon = \varepsilon$. Kantorova normalna forma za ε_0 je sam ε_0. Uopšte, ordinal α takav da $\omega^\alpha = \alpha$ je ε-ordinal.

Primetimo da je $\varepsilon_0 = \omega^{\omega^{\omega^{\cdot^{\cdot^{\cdot}}}}}$. Pritom, stepenovanje se vrši u ω koraka.

Kardinalni brojevi

Kao što je to bio slučaj u naivnoj teoriji skupova, za upoređivanje skupova po broju elemenata, ili po njihovoj veličini, koristimo obostrano jednoznačne funkcije. Za proizvoljne skupove x i y neka je $x \preceq y$ ako i samo ako postoji obostrano jednoznačna funkcija skupa x u skup y.

Intuitivno, ako $x \preceq y$, skup x ima manje elemenata od skupa y. Pritom, relacija $\preceq$ je parcijalno uređenje klase V.

Za proizvoljne skupove x i y, neka je $x \approx y$ ako i samo ako postoji obostrano jednoznačna funkcija skupa x na skup y. Intuitivno, ako je $x \approx y$, skupovi x i y su jednaki po veličini. Relacija $\approx$ je relacija ekvivalencije klase svih skupova V. Naglašavamo da su $x \preceq y$ i $x \approx y$ formule jezika $\mathcal{L}_{ZF}$.

Primer 1. Za sve x, y, ako $x \preceq y$ i $y \preceq x$, onda $x \approx y$.

Ovo tvrđenje se naziva Šreder-Bernštajnovom teoremom, a sredstvima teorije ZF dokazano je u poglavlju o Bulovim algebrama.

Veličinu konačnog skupa određujemo brojanjem. Ako se skup x može dobro urediti, onda postoji najmanji ordinal α takav da je $x \approx \alpha$. Pod ovim uslovom, brojanje je moguće i u slučaju beskonačnog skupa.

Ako se skup x može dobro urediti, *kardinalnost skupa* x, u oznaci $|x|$, je najmanji ordinal α takav da $\alpha \approx x$.

Za svaki ordinal α, kardinalnost $|\alpha|$ je definisana i $|\alpha| \leq \alpha$. Ordinal α je *kardinal* ako i samo ako $\alpha = |\alpha|$. Predikat "x je kardinal" može se izraziti formulom $\phi_{kard}(x)$ jezika $\mathcal{L}_{ZF}$.

Primer 2. (a) Za proizvoljne α i β, ako $|\alpha| \leq \beta \leq \alpha$, onda $|\beta| = |\alpha|$.
(b) Za svako $n \in \omega$, $n \not\approx n+1$.
(c) Za svako α, ako $\alpha \approx n$, onda $\alpha = n$.
(d) Ordinal ω i svi prirodni brojevi su kardinali.

Skup x je *konačan* ako je $|x| < \omega$. Skup je *beskonačan* ako nije konačan. Takođe, skup x je *prebrojiv* ako $|x| \leq \omega$, a u suprotnom, skup x je *neprebrojiv*.

Primer 3. Za svaki skup x, $x \preceq P(x)$ i nije $x \approx P(x)$.

Ako je $f : x \to P(x)$ funkcija, skup $y = \{z \in x : z \notin f(z)\}$ nije element kodomena funkcije f. U suprotnom, ako postoji $z \in x$ takvo da $f(z) = y$, onda $z \in y$ ako i samo ako $z \notin y$, što nije moguće.

Ovaj dokaz je star preko sto godina. Kantor je njime želeo da dokaže egzistenciju neprebrojivih skupova. Zanimljivo, on je bio u pravu, ne samo u pogledu samog rezultata, već i u smislu sredstava koja je u dokazu koristio. Bez aksiome o partitivnom skupu nije moguće dokazati da postoji neprebrojiv skup. Sistem aksioma teorije skupova, koji se dobija zamenom aksiome partitivnog skupa u teoriji ZF njenom negacijom, takođe je konzistentan, odnosno, postoji model teorije skupova u kojoj je ordinal ω jedini beskonačan kardinal.

Time što smo rekli da postoji neprebrojiv skup, nismo tvrdili da postoji skup kardinalnosti veće od ω. Bez aksiome izbora, ta činjenica nije sasvim očigledna.

Primer 4. Za svaki ordinal α postoji kardinal veći od α.
Pretpostavimo da je $\alpha \geq \omega$. Neka je

$$R = \{r \in P(\alpha \times \alpha) : r \text{ je dobro uređenje na } \alpha\}$$

Za svako $r \in R$ neka je α_r ordinal izomorfan dobrom uređenju (α, r). Prema aksiomi zamene, postoji skup $S = \{\alpha_r : r \in R\}$. Ako je $\kappa = \sup(S)$, onda je κ kardinal i $\kappa > \alpha$.

Primer 5. Neka je λ granični ordinal i $(\kappa_\xi : \xi < \lambda)$ strogo rastući niz beskonačnih kardinala. Ako je $\kappa = \lim_{\xi<\lambda} \kappa_\xi$, onda je κ kardinal.
Pretpostavimo da ordinal κ nije kardinal. To znači da postoji odrinal $\alpha < \kappa$ i funkcija $f : \alpha \to \kappa$ koja preslikava α na κ. Kako je $\kappa = \bigcup_{\xi<\lambda} \kappa_\xi$, zbog $\alpha < \kappa$, postoji $\xi < \lambda$ takvo da $\alpha < \kappa_\xi$. Definišimo funkciju $g : \alpha \to \kappa_\xi$ tako da za svako $\nu < \alpha$,

$$g(\nu) = \begin{cases} f(\nu) & \text{ako } f(\nu) \in \kappa_\xi, \\ 0 & \text{inače.} \end{cases}$$

Funkcija g preslikava α na κ_ξ, suprotno pretpostavci da je κ_ξ kardinal.

Ako je κ kardinal, κ^+ je najmanji kardinal veći od κ. Kardinal κ je *naslednik* ako postoji kardinal λ takav da $\kappa = \lambda^+$. Kardinal $\kappa > 0$ koji nije naslednik je *granični kardinal*.

Transfinitnom rekurzijom, na osnovu prethodnog primera, može se definisati strogo rastući niz kardinala $(\aleph_\alpha : \alpha \in On)$:

$$\begin{aligned}
&\aleph_0 = \omega, \\
&\aleph_{\alpha+1} = \aleph_\alpha^+, \text{ za svako } \alpha \in On, \\
&\aleph_\alpha = \sup\{\aleph_\beta : \beta < \alpha\}, \text{ ako je } \alpha \text{ granični ordinal.}
\end{aligned}$$

Svaki kardinal $\aleph_\alpha$ je ordinal. Kada o njemu govorimo kao o ordinalu, označavamo ga sa ω_α. Iako se radi o istoj stvari, koju smo označili na dva načina, ova razlika u oznakama biće značajna u aritmetici kardinala. Po definiciji niza $(\aleph_\alpha : \alpha \in On)$ kardinali čune pravu klasu.

Primer 6. (a) Za svako α, ordinal ω_α je kardinal.
(b) Za svaki beskonačan kardunal κ, postoji ordinal α takav da $\kappa = \omega_\alpha$.
(c) Ako $\alpha < \beta$, onda $\omega_\alpha < \omega_\beta$.
(d) Ordinal ω_α je granični kardinal ako i samo ako α je granični ordinal.

Bez aksiome izbora, nije jasno da li se svaki skup može dobro urediti. Pretpostavka da postoji skup koji se ne može dobro urediti ne protivreči teoriji ZF. Međutim, u teoriji ZF, svaki skup sadrži podskupove koji se mogu dobro urediti. Na primer, svaki skup sadrži konačan podskup.

Za svaki skup a neka je $h(a)$ najmanji ordinal α takav da, za svaki skup $x \subseteq a$ koji se može dobro urediti, $|x| < |\alpha|$. Ordinal $h(a)$ je *Hartogsov broj* skupa a. Dakle $h(a)$ je najmanji odrinal koji se ne može obostrano jednoznačno preslikati u skup a. Ako je α ordinal, onda $|\alpha| < |h(\alpha)|$, odnosno, $h(\alpha) = |\alpha|^+$.

Primer 7. Svaki skup a ima Hartogsov broj i $h(a)$ je kardinal.

Prema aksiomi zamene, postoji skup S svih ordinala koji su izomorfni nekom dobrom uređenju $r \in P(a \times a)$. Ako je $f : \alpha \to a$ obostrano jednoznačna funkcija koja preslikava ordinal α u skup a, neka je $r = \{(f(\nu), f(\xi)) : \nu < \xi < \alpha\}$. Kako je α izomorfan uređenju r, $\alpha \in S$. Dakle, skup S sadrži sve ordinale koji imaju istu kardinalnost kao podskupovi skupa a. Prema aksiomi separacije, $\{\alpha \in S : \exists x \subset a\, (\alpha \preceq x)\}$ je skup ordinala, pa ordinal $h(a)$ postoji. Ako je $|\alpha| = |h(a)|$ za neko $\alpha < h(a)$, onda postoji $x \subseteq a$ takvo da $x \approx h(a)$, pa dakle $h(a) < h(a)$, što nije moguće.

Ako je α ordinal, onda $|\alpha| < |h(\alpha)|$, odnosno, $h(\alpha) = |\alpha|^+$.

Sa Hartogsovim brojem, kao nekom vrstom ocene kardinalnosti skupova, u ovom smislu uglavnom se iscrpljuju mogućnosti teorije ZF.

Niz ordinala $(\alpha_\xi : \xi < \beta)$ je *kofinalan* u α ako je skup $\{\alpha_\xi : \xi < \beta\}$ neograničen u ordinalu α, odnosno, ako je $\sup\{\alpha_\xi : \xi < \beta\} = \alpha$.

Najmanji ordinal β za koji postoji rastući niz $(\alpha_\xi : \xi < \beta)$ koji je kofinalan u α je *kofinalnost* ordinala $\alpha > 0$ i označava se sa $\mathrm{cf}(\alpha)$. Ako je ordinal α naslednik, $\mathrm{cf}(\alpha) = 1$. Jasno, za svaki ordinal α, $\mathrm{cf}(\alpha) \leq \alpha$.

Na primer, kofinalnost ordinala ω_ω je ω, kofinalnost ordinala ω_{ω_1} je ordinal ω_1, a kofinalnost od $\omega_{\omega_1} + \omega_\omega$ je ordinal ω.

Primer 8. (a) Za svaki ordinal α, postoji striktno rastući niz ordinala $(\alpha_\xi : \xi < \mathrm{cf}(\alpha))$ kofinalan u ordinalu α.

(b) Ako je α granični ordinal i $(\alpha_\xi : \xi < \alpha)$ strogo rastući niz kofinalan u ordinalu β, onda je $\mathrm{cf}(\alpha) = \mathrm{cf}(\beta)$.

Neka je niz $(\delta_\xi : \xi < \mathrm{cf}(\alpha))$ kofinalan u α. Za svako $\xi < \mathrm{cf}(\alpha)$, neka je $\alpha_\xi = \max(\delta_\xi, \sup\{\alpha_\mu + 1 : \mu < \xi\})$. Na osnovu teoreme rekurzije, takav niz zaita postoji i kofinalan je u α.

Da dokažemo (b) Pretpostavimo da je α granični ordinal takav da postoji niz $(\alpha_\xi : \xi < \alpha)$ koji je kofinalan u β. Ako je niz $(\delta_\xi : \xi < \delta)$ kofinalan u α, onda je niz $(\alpha_{\delta_\xi} : \xi < \delta)$ kofinalan u β. Dakle, $\mathrm{cf}(\beta) \leq \mathrm{cf}(\alpha)$.

Ako je niz $(\gamma_\xi : \xi < \mathrm{cf}(\beta))$ kofinalan u β, za svako $\xi < \mathrm{cf}(\beta)$ neka je ε_ξ najmanji ν takav da $\alpha_\nu > \gamma_\xi$. Kako je $(\alpha_\xi : \xi < \alpha)$ striktno rastući niz, $(\varepsilon_\xi : \xi < \mathrm{cf}(\beta))$ je kofinalan u α, odnosno, $\mathrm{cf}(\alpha) \le \mathrm{cf}(\beta)$.

Na osnovu perthodnog primera, $\mathrm{cf}(\mathrm{cf}(\alpha)) = \mathrm{cf}(\alpha)$, za svaki ordinal α.

Ordinal β je *regularan* ako $\mathrm{cf}(\beta) = \beta$, a inače, ordinal β je *singularan*.

Ako je α granični ordinal, $\mathrm{cf}(\alpha)$ je regularan. Takođe, ako je α regularan ordinal, α je kardinal. Dakle, kofinalnost je uvek regularan kardinal.

Primer 9. (a) Postoje proizvoljno veliki singularni kardinali. Za svako α, kardinal $\aleph_{\alpha+\omega}$ je singularan. Njegova kofinalnost je ω.

(b) Ako je $\aleph_\alpha$ neprebrojiv granični kardinal, $\mathrm{cf}(\aleph_\alpha) = \mathrm{cf}(\alpha)$. Zapravo, $\aleph_\alpha$ je granica niza $(\aleph_\xi : \xi < \mathrm{cf}(\alpha))$.

(c) Postoji proizvoljno veliki singularni kardinal $\aleph_\alpha$ takav da $\aleph_\alpha = \alpha$. Dakle niz $(\aleph_\alpha :\in On)$ ima proizvoljno veliku fiksnu tačku koja je singularan kardinal.

Za svaki kardinal $\aleph_\beta$, neka je $\alpha_0 = \omega_\beta$ i za svako $n > 0$, $\alpha_{n+1} = \omega_{\alpha_n}$. Ako je $\alpha = \lim_{n\to\omega} \alpha_n$, onda niz $(\aleph_{\alpha_n} : n \in \omega)$ ima granicu $\aleph_\alpha$.

Kako je $\aleph_\alpha = \lim_{n\to\omega} \aleph_{\alpha_n} = \lim_{n\to\omega} \alpha_{n+1} = \alpha$. Budući da je njegova kofinalnost ω, kardinal $\aleph_\alpha$ je singularan.

Kako su svi neprebrojivi granični kardinali koje smo do sada naveli singularni, prirodno se postavlja pitanje da li uopšte postoji takav kardinal koji je regularan.

Primer 10. Ako je $\aleph_\alpha$ regularan neprebrojiv granični kardinal, $\aleph_\alpha = \alpha$.

Za svako α, $\mathrm{cf}(\aleph_\alpha) = \mathrm{cf}(\alpha)$, pa kako je kardinal $\aleph_\alpha$ regularan, mora biti $\aleph_\alpha = \alpha$. Kako je prva fiksna tačka niza $(\aleph_\alpha : \alpha \in On)$ singularan kardinal kofinalnosti ω, koji se dobija kao granična vrednost niza

$$(\aleph_0, \aleph_\omega, \aleph_{\omega_\omega}, \aleph_{\omega_{\omega_\omega}}, \dots,),$$

regularna fiksna tačka niza $(\aleph_\alpha : \alpha \in On)$, ukoliko uopšte postoji, morala bi biti jako veliki kardinal.

Regularan granični kardinal κ je *slabo nedostižan*. U teoriji ZFC ne može se dokazati egzistencija slabo nedostižnog neprebrojivog kardinala. Pretpostavka da je 2^ω slabo nedostižan kardinal, ne protivreči ZFC.

Kardinal ω je regularan i za svako $n < \omega$, $2^n < \omega$. Ako se pretpostavi aksioma izbora, to svojstvo može se definisati i u slučaju neprebrojivih kardinala. Regularan kardinal κ je *jako nedostižan* ako za svako $\lambda < \kappa$ $(2^\lambda < \kappa)$. Svaki jako nedostižan kardinal je slabo nedostižan.

Ako se pretpostavi aksioma izbora, za svako α, kardinal $\aleph_\alpha^+$ je regularan. Otvoren je problem da li se bez aksiome izbora može dokazati da postoji kardinal kofinalnosti veće od ω, odnosno, da li postoji regularan neprebrojiv kardinal $\aleph_\alpha$. Pretpostavka da kardinal $\aleph_1$ nije regularan ne protivreči teoriji ZF. Dakle, ordinal ω_1 može biti i prebrojiva unija prebrojivih skupova. Nekim topološkim osobinama ovog ordinala završićemo izlaganje svojstava kardinala u teoriji ZF. O njima ćemo kasnije govoriti u svetlu aksiome izbora.

Primer 11. Neka je na ordinalu ω_1 definisana topologija poretka. Kao topološki prostor ω_1 ima sledeće osobine:

(a) Skup $x \subseteq \omega_1$ je zatvoren ako i samo ako za svaki granični ordinal $\xi < \omega_1$, ako je $x \cap \xi$ neograničen skup u ξ, onda $\xi \in x$. Isto važi i u slučaju prostora $\omega_1 + 1$.

(b) Za svako $\alpha \in \omega_1$, α je izolovana tačka prostora ω_1 ako i samo ako ordinal α je naslednik.

(c) Prostori ω_1 i ω_1+1 su Hauzdorfovi. Prostor ω_1 je lokalno kompaktan, ali nije kompaktan. Prostor $\omega_1 + 1$ nije lokalno kompaktan.

Aksioma regularnosti

Sve do sada izložene aksiome deluju sasvim prirodno i za većinu matematičara samorazumljivo. Sa druge strane, aksioma regularnosti postulira jednu osobinu skupova koja prevashodno ima skupovno-teorijski značaj i koristi se u konstrukcijama modela teorije skupova.

Istorijski gledano, teorija ZF je nastala kao rezultat logičke analize jedne predstave o postepenoj, kumulativnoj izgradnji skupova u kojoj aksioma regularnosti ima ključnu ulogu. Ta predstava podrazumeva hijerarhiju skupova u kojoj se na prvom stupnju nalazi kolekcija zadatih objekata ili praelemenata, na drugom stupnju javljaju se skupovi praelemenata i svi elementi prvog stupnja itd. Prvobitno, teorija ZF je predstavljala opis svojstava ovako izgrađenih skupova, a kasnije se pokazalo da praelementi uopšte nisu potrebni, tj. da se svi matematički skupovi ovakvom konstrukcijom mogu dobiti iz praznog skupa.

Intuitivno, aksioma regularnosti eleminiše određene patološke objekte iz klase svih skupova. Ona obezbeđuje da se, u odnosu na relaciju $\in$, ne mogu pojaviti ciklusi oblika $x_0 \in x_1 \in \cdots \in x_n \in x_0$ ili beskonačni opadajući nizovi oblika $x_0 \ni x_1 \ni x_2 \ni \cdots$. U jeziku $\mathcal{L}_{ZF}$ formulisana je sledećom rečenicom:

$$\forall x\,(\exists y\,(y \in x) \to \exists y\,(y \in x \wedge \neg\exists z\,(z \in x \wedge z \in y))).$$

Za svaki neprazan skup x postoji $y \in x$ takav da $x \cap y = \emptyset$, odnosno, svaki neprazan skup u odnosu na relaciju $\in$ ima minimalni element.

Primer 1. Na osnovu aksiome regularnosti, važi $\vdash \neg\exists x\,(x \in x)$. Opštije, za svako $n \in \omega$, važi $\vdash \neg\exists x_0 \cdots \exists x_n\,(x_0 \in x_1 \wedge \cdots \wedge x_n \in x_0)$.

Prvo tvrđenje dobija se primenom aksiome regularnosti na skup $\{x\}$, a drugo, primenom na skup $\{x_0, \ldots, x_n\}$.

Kako smo nagovestili, sa aksiomom regularnosti, klasa svih skupova izgleda veoma prirodno i može se shvatiti kao *kumulativna hijerarhija* skupova koja se dobija polazeći od praznog skupa transfinitnom primenom operacije partitivnog skupa i unije. U takvoj hijerarhiji svaki skup ima rang, tj. nivo hijerarhije na kojem se prvi put pojavljuje. Stupnjevi hijerarhije indeksirani su ordinalima.

Primer 2. Za svaki skup x postoji najmanji tranzitivan skup, u oznaci $\mathrm{tr}(x)$, koji sadrži x. Skup $\mathrm{tr}(x)$ je *tranzitivno zatvorenje* skupa x.

Neka je $x_0 = x$. Za svaki prirodan broj $n \in \omega$, neka je $x_{n+1} = \cup x_n$. Tako definisan skup $\mathrm{tr}(x) = \cup_{n\in\omega} x_n$ je tranzitivan i sadrži x. Naime, ako $y \in \mathrm{tr}(x)$, postoji $n \in \omega$ takvo da $y \in x_n$. Otuda sledi da $y \subseteq \cup x_n = x_{n+1}$, tj. $\mathrm{tr}(x)$ je tranzitivan skup. Ako je a tranzitivan skup koji sadrži x, onda za svako $n \in \omega$, $x_n \subseteq a$, tj. $\mathrm{tr}(x) \subseteq a$.

Primer 3. Svaka neprazna klasa skupova sadrži $\in$-minimalni element.

Pretpostavimo da je C klasa skupova i $x \in C$. Ako $x \cap C = \emptyset$, skup x je $\in$-minimalni element u C. Ako je $x \cap C$ neprazan, neka je $y = \mathrm{tr}(x) \cap C$. Skup y nije prazan, pa prema aksiomi regularnosti, postoji $z \in y$ takav da $z \cap y = \emptyset$. Skup z je $\in$-minimalni element klase C. U suprotnom, ako $u \in z$ i $u \in C$, zbog $z \in \mathrm{tr}(x)$ i zbog tranzitivnosti skupa $\mathrm{tr}(x)$, mora biti $u \in \mathrm{tr}(x)$, tj. $u \in z \cap \mathrm{tr}(x) \cap C = z \cap y = \emptyset$.

Na osnovu teoreme rekurzije, definišemo familiju skupova $(V_\alpha, \alpha \in On)$:

$$\begin{aligned}
&V_0 = \emptyset,\\
&V_{\alpha+1} = P(V_\alpha),\ \text{za svaki ordinal } \alpha,\\
&V_\alpha = \textstyle\bigcup_{\gamma<\alpha} V_\gamma,\ \text{ako je } \alpha \text{ granični ordinal.}
\end{aligned}$$

Primer 4. (a) Za svaki ordinal α, skup V_α je tranzitivan i $\alpha \subseteq V_\alpha$.

(b) Ako je $\alpha < \beta$, onda $V_\alpha \subseteq V_\beta$.

Primer 5. Zbog aksiome regularnosti, za svaki skup x postoji α, $x \in V_\alpha$, tj. $V = \bigcup_{\alpha\in On} V_\alpha$ je klasa svih skupova.

Da to pokažemo, pretpostavimo da je C klasa svih skupova x koji nisu u V. Ako C nije prazna, C sadrži $\in$-minimalni element x. Za svako $z \in x$, $z \in V$, pa dakle $x \subseteq \bigcup_{\alpha \in On} V_\alpha$. Prema aksiomi zamene, postoji ordinal β takav da $x \subseteq \bigcup_{\alpha < \beta} V_\alpha$. Dakle $x \subseteq V_\beta$, tj. $x \in V_{\beta+1}$. To znači da je C prazna klasa, tj. da je V univerzum svih skupova.

Kako svaki skup x u kumulativnoj hijerarhiji pripada nekom V_α, postoji najmanji ordinal α, u oznaci $\mathrm{rang}(x)$, takav da $x \in V_{\alpha+1}$. Takav ordinal nazivamo *rangom* skupa x.

Primer 6 (a) Za sve x, y, ako $x \in y$, onda $\mathrm{rang}(x) < \mathrm{rang}(y)$.
(b) Za svaki skup x, $\mathrm{rang}(x) = \sup\{\mathrm{rang}(z) + 1 : z \in x\}$.

Na osnovu prethodnog primera možemo zaključiti da da aksioma regularnosti o skupovima kaže dve stvari: za svaki skup uvek postoji prvi nivo na kojem se on u univerzumu pojavljuje i drugo, svi njegovi elementi pojavljuju se na nižim nivoima hijerarhije.

Kako svaka neprazna klasa sadrži $\in$-minimalni element, pojam transfinitne indukcije koji smo definisali na klasi ordinala može se proširiti na proizvoljnu tranzitivnu klasu.

Primer 7. *Dokaz $\in$-indukcijom:* Neka je M tranzitivna klasa i $\varphi(x)$ formula jezika $\mathcal{L}_{ZF}$. Ako važi $\varphi(\emptyset)$ i za svako $x \in M$,

$$\forall y \in M\, (y \in x \rightarrow \varphi(y)) \rightarrow \varphi(x),$$

onda za svako $x \in M$ važi $\varphi(x)$.

Neka je C klasa svih $x \in M$ za koje ne važi $\varphi(x)$. Ako C nije prazna klasa, onda C sadrži $\in$-minimalni element z. Zbog tranzitivnosti klase M, primenom uslova $\in$-indukcije dobijamo kontradikciju.

Obostrano jednoznačno i na preslikavanje $f : M \rightarrow N$ tranzitivnih klasa M i N je izomorfizam, ako za sve $x, y \in M$, $x \in y$ ako i samo ako $f(x) \in f(y)$.

Primer 8. Ako je f izomorfizam tranzitivnih klasa M i N, onda $M = N$ i za svako $x \in M$, $f(x) = x$.

Tvrđenje dokazujemo $\in$-indukcijom, odnosno, dokazujemo da za svako $x \in M$, $f(x) = x$. Pretpostavimo da za sve $z \in x$, $f(z) = z$ i neka je $f(x) = y$.

Ako je $z \in x$, onda $z = f(z) \in f(x) = y$, pa je $x \subseteq y$. Obratno, neka je $u \in y$. Kako $y \in N$ to postoji $z \in M$ takvo da $f(z) = u$. Dakle $f(z) \in y$, tj. $f(z) \in f(x)$, pa mora biti $z \in x$. Po induktivnoj pretpostavci $f(z) = z$ što znači da $u \in x$. Dakle $y \subseteq x$.

Prethodni primer pokazuje da ne postoje različite izomorfne tranzitivne klase i da takve klase ne dopuštaju netrivijalne automorfizme. Na primer, univerzum svih skupova V nema netrivijalnih automorfizama.

Primer 9. (a) Za svako α, $\mathrm{rang}(\alpha) = \alpha$ i $V_\alpha \cap On = \alpha$.

(b) Ako $x \in V$, onda $\cup x$, $P(x)$ i $\{x\} \in V$, a rangovi ovih skupova su manji od $\mathrm{rang}(x) + \omega$.

Primer 10. Ako $x, y \in V$, onda $x \times y$, $x \cup y$, $x \cap y$, $\{x, y\}$, (x, y) i $x^y \in V$. Svi rangovi ovih skupova su manji od $\max(\mathrm{rang}(x), \mathrm{rang}(y)) + \omega$.

Primer 11. (a) Za svako $n \in \omega$, $|V_n| < \omega$ i $|V_\omega| = \omega$.

(b) Postoji skup a takav da $a \times a \subseteq a$.

Primer 12. Definišimo relaciju $\varepsilon \subseteq \omega^2$ tako da za sve $m, n \in \omega$,

$n \,\varepsilon\, m$ ako i samo ako "na n-tom mestu, računajući sa desna, u binarnoj ekspanziji broja m se javlja cifra 1".

Na primer $13 = 1101$, pa $0 \,\varepsilon\, 13$, $2 \,\varepsilon\, 13$, $3 \,\varepsilon\, 13$, a $\neg(1 \,\varepsilon\, 13)$ i $\neg(4 \,\varepsilon\, 13)$.

Kao modeli jezika $\mathcal{L}_{ZF}$, (ω, ε) i $(V_\omega, \in)$ su izomorfni.

Primer 13. U modelu $(V_\omega, \in)$ važe sve aksiome teorije ZF osim aksiome beskonačnosti. Zapravo, svaki element skupa V_ω je konačan skup.

Primer 14. (a) Ako je $\mathcal{L} \in V$ jezik predikatskog računa, rang skupa njegovih formula je manji od $\mathrm{rang}(\mathcal{L}) + \omega$. Ako je $\mathcal{A} \in V$ model jezika $\mathcal{L}$, $\mathrm{rang}(\mathcal{A}) < \mathrm{rang}(A) + \omega$.

(b) Ako se pretpostavi aksioma izbora, svaka grupa, topološki prostor ili bilo koja matematička struktura izomorfna je strukturi u klasi V.

Zanimljivo je da bez aksiome izbora ovo tvrđenje nije moguće dokazati. Onako kako su ovde definisane strukture celih $\mathcal{Z}$, racionalnih $\mathcal{Q}$ i realnih brojeva $\mathcal{R}$ pripadaju skupu $V_{\omega+\omega}$.

Zasnivanje matematike

Zasnivanje standardne matematike u okviru teorije ZF pre svega podrazumeva definiciju strukture prirodnih brojeva. Skup prirodnih brojeva ω definisali smo kao najmanji induktivan skup. Skup ω je beskonačan, relacija $<$ je dobro uredjenje na ω i svaki neprazan ograničen skup u ω ima najveći element. Sledeći primer pokazuje da ovi uslovi jedinstveno karakterišu prirodne brojeve.

Primer 1. Beskonačno dobro uređenje u kojem svaki neprazan skup ima najveći element, izomorfno je uredjenju prirodnih brojeva.

Neka je p najmani element u uređenju $\mathcal{P}$. Za proizvoljne $x \in P$ i $n \in \omega$, neka je $g(x,n)$ najmanji $y \in P$ takav da $x < y$. Na osnovu teoreme rekurzije, postoji jedinstveno određena funkcija $f : \omega \to P$ takva da $f(0) = p$ i za svako $n > 0$, $f(n+1) = g(x,n)$.

Za svako $n \in \omega$, $f(n) < f(n+1)$. Otuda sledi da za sve $m, n \in \omega$, $m < n$ implicira $f(m) < f(n)$, odnosno, funkcija f je obostrano jednoznačna. Ako je $P - \mathrm{codom}(f)$ neprazan skup, neka je $q \in P$ njegov najmanji element. Kako skup $\{r \in P : r < q\}$ ima gornje ograničenje, neka je $r \in P$ njegov najveći element. Po definiciji elementa r, postoji $n \in \omega$ takvo da $f(n) = r$. Kako je q najmanji element skupa P takav da $r < q$, po definiciji funkcije f mora biti $f(n+1) = q$, a to nije moguće.

Definicije sabiranja i množenja prirodnih brojeva u aksiomama aritmetike su rekurzivne, pa je struktura $\mathcal{N} = (\omega, +, \cdot, \leq, s, 0)$ koja zadovoljava aksiome navedene u uvodnom poglavlju jedinstveno određena.

Primer 2. (a) Neka je $\sim$ binarna relacija skupa $\omega \times \omega$ definisana tako da za sve $x, y, u, v \in \omega$, $(x,y) \sim (u,v)$ ako i samo ako $x + v = y + u$. Relacija $\sim$ je ekvivalencija.

Neka $[x,y]$ klasa ekvivalencije elementa (x,y). Količnik skupa $\omega \times \omega$ po relaciji $\sim$ označavamo sa Z. Tako dobijen skup Z je *skup celih brojeva*.

(b) Za svaki ceo broj $[x,y]$, ako $x \geq y$, onda $(x,y) \sim (x-y,0)$. Ako je $x < y$, onda $(x,y) \sim (0, y-x)$. Otuda sledi da svaki ceo broj sadrži jedinstven par oblika $(n,0)$, $n \in \omega$, ili $(0,n)$, $n > 0$. Dakle, skup celih brojeva je beskonačan prebrojiv skup.

(c) Za proizvoljne $x, y, u, v \in \omega$, neka je $[x,y] \leq [u,v]$ ako i samo ako $x + v \leq y + u$. Definicija relacije $\leq$ je korektna, a struktura $(Z, \leq)$ je linearno uređenje bez krajeva u kojem je svaki interval konačan.

Za svako $n > 0$, $[0,n] < [0,0] < [n,0]$ i preslikavanje $f : \omega \to Z$ definisano sa $f(n) = [n,0]$ je obostrano jednoznačno i čuva poredak prirodnih brojeva.

(d) Za sve $x, y, u, v \in \omega$, neka je $[x,y] + [u,v] = [x+u, y+v]$. Operacija $+$ je korektno definisana i struktura $(Z, +, \leq, 0)$ je uređena grupa. Pritom, za sve $x, y \in \omega$, $-[x,y] = [y,x]$.

(e) Za sve $x, y, u, v \in \omega$, neka je $[x,y] \cdot [u,v] = [xu + yv, xv + yu]$. Pritom, operacija $\cdot$ je korektno definisana.

Struktura $\mathcal{Z} = (Z, +, \cdot, \leq, 1)$ je *uređen prsten*, odnosno, zadovoljava sve aksiome uredjenih polja osim egzistencije inverznog elementa u odnosu na operaciju množenja. Svaki uređen prsten sadrži izomorfnu kopiju prstena celih brojeva.

Sa stanovišta teorije ZF, struktura $\mathcal{Z}$ je definabilna konstanta jezika $\mathcal{L}_{ZF}$.

Dakle, postoji formula $\varphi_Z(x)$ jezika $\mathcal{L}_{ZF}$ takva da $\forall x\,(Z = x \leftrightarrow \varphi_Z(x))$ i pritom, $ZF \vdash \exists x \forall y\,(\varphi_Z(y) \rightarrow y = x)$.

Primer 3. (a) Na skupu $P = Z \times (Z - \{0\})$ definišimo relaciju $\sim$ tako da za sve $(x, y), (u, v) \in P$, $(x, y) \sim (u, v)$ ako i samo ako $x \cdot v = y \cdot u$. Pritom, relacija $\sim$ je relacija ekvivalencije.

Označimo sa $[\frac{x}{y}]$ klasu ekvivalencije elementa $(x, y) \in P$. Količnik $Q = P_{/\sim}$ je skup *racionalnih brojeva*. Za sve $m, n \in \omega$, ako $m \neq n$, onda $[\frac{m}{1}] \neq [\frac{n}{1}]$, pa je skup racionalnih brojeva beskonačan prebrojiv skup.

(b) Za svako $[\frac{x}{y}] \in Q$, $[\frac{x}{y}] = [\frac{-x}{-y}]$, pa možemo pretpostaviti da je svaki racionalan broj predstavljen elementom $[\frac{x}{y}]$ u kome je $y > 0$.

Za sve $[\frac{x}{y}], [\frac{u}{v}] \in Q$, ako $y > 0$ i $v > 0$, neka je $[\frac{x}{y}] \leq [\frac{u}{v}] \in Q$ ako i samo ako $x \cdot v \leq y \cdot u$. Struktura $(Q, \leq)$ je gusto linearno uređenje bez krajeva.

(c) Neka je $[\frac{x}{y}] + [\frac{u}{v}] = [\frac{x \cdot v + y \cdot u}{y \cdot v}]$ i $[\frac{x}{y}] \cdot [\frac{u}{v}] = [\frac{x \cdot u}{y \cdot v}]$, za sve $[\frac{x}{y}], [\frac{u}{v}] \in Q$. Operacije $+$ i $\cdot$ su korektno definisane i struktura $\mathcal{Q} = (Q, +, \cdot, \leq, 0, 1)$ je uređeno polje racionalnih brojeva. Polje $\mathcal{Q}$ može se izomorfno utopiti u svako uređeno polje.

Neka je $\mathcal{P}$ linearno gusto uređenje bez krajeva. Skup $D \subseteq P$ je *gust u* $\mathcal{P}$ ako za sve $x, y \in P$, $x < y$, postoji $z \in D$ takvo da $x < z < y$. Kompletno gusto linearno uredjenje bez krajeva $\mathcal{S} \supseteq \mathcal{P}$ je *kompletiranje* uređenja $\mathcal{P}$ ako je skup P gust u uređenju $\mathcal{S}$.

Teorema 6. Svako linearno gusto uređenje bez krajeva ima jedinstveno kompletiranje. Ako su $\mathcal{S}_1$ i $\mathcal{S}_2$ kompletiranja uređenja $\mathcal{P}$, onda postji izomorfizam $f : S_1 \rightarrow S_2$ takav da za svako $p \in P$, $f(p) = p$.

Dokaz: Uređen par (A, B) disjunktnih nepraznih podskupova linearnog gustog uređenja bez krajeva $\mathcal{P}$ je *sečenje* ako $A \cup B = P$, za sve $a \in A$ i $b \in B$, $a < b$ i skup A nema najveći element. Neka je S skup svih sečenja u $\mathcal{P}$ i $(A_1, B_1) \leq (A_2, B_2)$ ako i samo ako $A_1 \subseteq A_2$.

Uređenje $\mathcal{S} = (S, \subseteq)$ je kompletno; ako je $\{(A_i, B_i) : i \in I\}$ ograničen skup u $\mathcal{S}$, onda je $(\bigcup_{i \in I} A_i, \bigcap_{i \in I} B_i)$ njegov supremum.

Neka su $\mathcal{P}_1$ i $\mathcal{P}_2$ kompletiranja uređenja $\mathcal{P}$. Za svako $x \in P_1$ neka je $S_x = \{p \in P : p < x\}$. Skup $S_x \subseteq P$ je ograničen, pa u P_2 postoji $f(x) = \sup S_x$.

Za svako $p \in P$, p je gornje ograničenje za S_p, pa $f(p) \leq p$. Ako je $x \in P_2$ takvo da $x < p$, zbog gustine skupa P, postoji $q \in P$ takvo da $x < q < p$. Dakle, x nije gornje ograničenje skupa S_p, pa mora biti $f(p) = p$.

Ako $x < y$, zbog gustine skupa P, postoje $p, q \in P$, $x < p < q < y$. Kako je p gornje ograničene za S_x i $q \in S_y$, to mora biti $f(x) \leq p < q \leq f(y)$. Obratno, ako $f(x) < f(y)$, onda $x < y$.

Neka je $g : P_1 \to P_2$ izomorfizam koji fiksira skup P. Za svako $x \in P_1$, ako $p \in S_x$, onda $p < x$, pa je $p = g(p) < g(x)$. Dakle, $g(x)$ je gornje ograničenje skupa S_x. Ako je $z < g(x)$ gornje ograničenje skupa S_x, kako je g izomorfizam, postoji $y \in P_1$ takvo da $z = g(y)$. To znači da je $y < x$, pa postoji $p \in P$ takvo da $y < p < x$. Kako $p \in S_x$ i $g(y) < g(p) = p$, to $z \in P_2$ nije gornje ograničenje za S_x, pa dakle $g(x) = \sup S_x$. $\square$

Kako je $\mathcal{Q}$ jedinstveno prebrojivo linearno gusto uređenje bez krajeva, na osnovu prethodne teoreme jedinstveno je određeno i njegovo kompletiranje $\mathcal{R}$. Uređenje $\mathcal{R}$ je realna prava ili *kontinuum*. Dakle, realna prava je kompletno gusto linearno uređenje bez krajeva u kojem je skup racionalnih brojeva svuda gust.

Sa stanovišta uredjenja, jedinstveno smo okarakterisali realne brojeve, ali nismo definisali i njihovu algebarsku strukturu. Samo po sebi uopšte nije jasno da postoji tačno jedna takva struktura saglasna sa postojećim uređenjem, čija je restrikcija na skup racionalnih brojeva identična strukturi uređenog polja $\mathcal{Q}$.

Struktura uređenog polja defiiše se na sečenjima racionalnih brojeva, a dokaz njene jedinstvenosti je neposredan. Dakle, u ZF - Reg, do na izomorfizam postoji jedinstveno kompletno uređeno polje.

U sledećem primeru izložićemo jednu čudnu konstrukciju pozitivnih realnih brojeva koja se neposredno izvodi nad prirodnim brojeva. Konstrukciju je definisao Kolmogorov analizirajući Euklidov postupak merenja duži.

Intuitivno, duž kojoj odgovara pozitivan realan broj r, premeri se jediničnom duži, zatim polovinom jedinične duži, trećinom itd. Tako se dobija niz $(n_1/1, n_2/2, n_3/3, \dots)$ koji aproksimira realan broj r.

Primer 4. Za sve $m, n \in \omega$, $n > 0$, neka je $\left[\frac{m}{n}\right]$ najveći prirodan broj k takav da je $k \cdot n \leq m$, tj. $\left[\frac{m}{n}\right]$ je celi deo količnika m/n.

Pozitivan realan broj je funkcija $r : \omega^+ \to \omega$ koja zadovoljava uslove:

(a) za sve $k, n > 0$, $r(n) = \left[\frac{r(kn)}{k}\right]$,

(b) za svako $n > 0$ postoji $k > 0$ takvo da $k \cdot r(n) < r(kn)$.

Skup pozitivnih realnih brojeva označavamo sa R^+, njegovu strukturu definišemo na sledeći način:

(c) Poredak $<$ definišemo tako da za sve $r, s \in R^+$,

$$r < s \ \Leftrightarrow \ \text{postoji } n > 0,\ r(n) < s(n).$$

(b) Sabiranje je definisano tako da za sve $r, s, t \in R^+$,

$$r + s = t \ \Leftrightarrow \ \text{za svako } n > 0,\ t(n) = \max_{k>0} \left[\frac{r(kn)+s(kn)}{k}\right].$$

(d) Proizvod realnih brojeva definisan je tako da za sve $r, s, t \in R^+$,

$$r \cdot s = t \;\; \Leftrightarrow \text{ za svako } n > 0,\, t(n) = \max_{k,k'>0} \left[\frac{r(kn) \cdot s(k'n)}{n \cdot k \cdot k'} \right].$$

Neposredno se proverava da, u odnosu na definisani poredak i operacije, R^+ zaista ima strukturu pozitivnih realnih brojeva. Na primer, ako je $k > 0$, funkcija $r_k(n) = kn - 1$, za sve $n > 0$, reprezentuje prirodan broj k.

Primer 5. Skup realnih brojeva je neprebrojiv.

U dokazu ovog tvrđenja, Kantor je upotrebio argument koji se uobičajeno naziva *dijagonalizacijom*. Pretpostavimo suprotno, tj. neka je $R = (c_0, \ldots, c_n, \ldots)$ prebrojavanje realnih brojeva. Odredićemo realan broj različit od svakog c_n.

Neka je $a_0 = c_0$ i $b_0 = c_k$, gde je k je najmanji prirodan broj takav da $a_0 < c_k$. Za svako $n \in \omega$, neka je $a_{n+1} = c_k$, gde k je najmanji prirodan broj takav da $a_n < c_k < b_n$. I konačno neka je $b_{n+1} = c_k$, gde je k najmanji prirodan broj takav da $a_{n+1} < c_k < b_n$. Ako je $a = \sup\{a_n : n \in \omega\}$, za svaki prirodan broj $k \in \omega$, mora biti $a \neq c_k$.

Kako su sečenja racionalnih brojeva podskupovi prebrojivog skupa $Q \times Q$, $R \preceq 2^\omega$. Da bismo pokazali da važi i suprtna nejednakost, neka je C skup realnih brojeva oblika $\sum_{n \geq 1} \frac{a_n}{3^n}$, gde je za svako $n \geq 1$, $a_n = 0$ ili $a_n = 2$. Skup C je zapravo Kantorov skup i $C \subseteq [0, 1]$. Po definiciji, $C \approx \{0, 2\}^\omega$, odnosno, $2^\omega \preceq R$. Dakle, sa stanošta teorije ZF, ukoliko skup realnih brojeva ima kardinalnost, $|R| = 2^{\aleph_0}$. I sledeće primere treba shvatiti na taj način.

Primer 6. (a) Ako je $A \subseteq R$ prebrojiv skup, onda je $|R - A| = 2^{\aleph_0}$.

(b) Skup iracionalnih brojeva je kardinalnosti $2^{\aleph_0}$. Skup svih beskonačnih skupova prirodnih brojeva je kardinalnosti $2^{\aleph_0}$.

Kako je $|R \times R| = 2^{\aleph_0}$, dovoljno je pokazati da ako je $A \subseteq R \times R$ prebrojiv, onda je $|(R \times R) - A| = 2^{\aleph_0}$. Ako je $P = \{x \in R : (x, y) \in A\}$, skup P mora biti prebrojiv, pa postoji $x \in R$ takvo da $x \notin P$. Ako je $X = \{x\} \times R$, onda $A \cap X = \emptyset$, pa $X \subseteq (R \times R) - A$ i $|X| = 2^{\aleph_0}$.

Gusto linearno uređenje $\mathcal{P}$ koje sadrži prebrojiv gust skup je *separabilno*. Ako je svaka familija disjunktnih otvorenih intervala najviše prebrojiva, uređenje $\mathcal{P}$ zadovoljava *uslov prebrojivih lanaca*.

Primer 7. Svako separabilno linearno uređenje zadovoljava uslov prebrojivih lanaca.

Realna prava je jedinstveno određeno, kompletno separabilno gusto linearno uređenje bez krajeva. Jasno, realna prava zadovoljava uslov prebrojivih lanaca, pa se prirodno postavlja pitanje:

– da li je kompletno gusto uređenje bez krajeva koje zadovoljava uslov prebrojivih lanaca, izomorfno realnoj pravoj?

Pozitivan odgovor na ovo pitanje naziva se Suslinovom hipotezom. Poznato je da se u teoriji ZFC ovaj problem ne može rešiti.

Aksioma izbora

Kao princip, aksiomu izbora koristili smo u više navrata. U odnosu na aksiome ZF ona se razlikuje utoliko što postulira egzistenciju određenog skupa koji istovremeno i ne definiše. Na primer, aksiome separacije, dvočlanog skupa, unije, partitivnog skupa, beskonačnog skupa i zamene eksplicitno definišu skupove čiju egzistenciju tvrde. Iz tih razloga, aksioma izbora ima posebno mesto u teoriji skupova i matematici uopšte. Zanimljivo je da većina matematičara samo ovaj skupovno-teorijski princip naziva aksiomom, a sve druge aksiome se u svakodnevnoj matematici uopšte i ne spominju. Aksiomu izbora u jeziku $\mathcal{L}_{ZF}$ izražavamo rečenicom:

$$\forall x\,(\forall y \in x\,(y \neq \emptyset) \rightarrow \exists f\,(\mathrm{fun}(f) \wedge \mathrm{dom}(f) = x \,\wedge\, \forall y \in x\, f(y) \in y))$$

Svaka familija nepraznih skupova x ima skup predstavnika u, odnosno, svaka takva familija ima funkciju izbora.

Aksiomu izbora, odnosno, prethodnu rečenicu predikatskog računa prvog reda, označavamo sa AC. Kasnije ćemo videti da je ona nezavisna od ostalih aksioma teorije ZF i da mnoga matematička tvrđenja nisu dokaziva u ZF bez pretpostavke AC. Proširenje ZF sa AC označavamo sa ZFC.

Kako smo već naglasili, većina matematičara od svih skupovno-teorijskih principa jedino koristi aksiomu izbora i jedino se na nju poziva. Pritom, najčešće se ne koristi ona sama, već neka od njenih ekvivalentnih verzija. U sledećim primerima navedeno je nekoliko takvih verzija, a odgovarajuća ekvivalencija dokazuje se uvek u teoriji ZF.

Primer 1. Aksioma izbora važi ako i samo ako za svaku familiju disjunktnih nepraznih skupova postoji funkcija izbora.

Ako je x familija nepraznih skupova, za svako $y \in x$ neka je $y^* = y \times \{y\}$. Prema aksiomi zamene, familija $x^* = \{y^* : y \in x\}$ je skup, a svi njegovi elementi su disjunktni i neprazni. Neka je $a \subseteq \cup x^*$ skup predstavnika familije x^*. Za svako $y \in x$, označimo sa $f^*(y)$ jedinstveni element skupa $a \cap y^*$. Pritom, za svako $y \in x$, $f^*(y)$ je uređen par i neka je $f(y)$ njegov prvi element. Očigledno, $f : x \rightarrow \cup x$ i f je funkcija izbora skupa x.

U nekim jednostavnim slučajevima, postojanje funkcije izbora može se dokazati i u teoriji ZF.

Primer 2. Familija jednočlanih skupova ima funkciju izbora. Isto važi i za svaku konačnu familiju nepraznih skupova. Sa druge strane, egzistencija funkcije izbora familije X se ne može dokazati čak ni uz pretpostavku da je svaki $x \in X$ konačan skup.

Primer 3. Aksioma izbora je ekvivalentna principu dobrog uređenja. Dakle, ako se pretpostavi AC, svaki skup može se dobro urediti.

Pretpostavimo aksiomu izbora. Neka je f funkcija izbora familije svih nepraznih podskupova skupa a. Neka je $a_0 = f(a)$ i za svako $\alpha > 0$ neka je $a_\alpha = f(a - \{a_\xi : \xi < \alpha\})$ ako $a - \{a_\xi : \xi < \alpha\}$ nije prazan. Neka je β najmanji ordinal takav da $a = \{a_\xi : \xi < \beta\}$. Niz $(a_\alpha : \alpha < \beta)$ je numeracija skupa a.

Obratno, pretpostavimo da se svaki skup može dobro urediti. Ako je a familija nepraznih skupova, uredimo linearno skup $\cup a$, pa za proizvoljan element $x \in a$, neka je $f(x)$ najmanji element skupa x.

Primer 4. Aksioma izbora je ekvivalentna Cornovoj lemi. Dakle, AC važi ako i samo ako svako parcijalno uređenje, u kojem svaki lanac ima gornje ograničenje, sadrži maksimalni element.

Pretpostavimo aksiomu izbora. Neka je $\mathcal{P}$ parcijalno uređenje u kojem svaki lanac ima gornje ograničenje i f funkcija izbora familije svih nepraznih podskupova skupa P. Neka je

$$p_\alpha = f(\{p \in P : p_\xi < p \text{ za sve } \xi < \alpha\}),$$

ako takav p_α postoji. Ako je $\alpha \neq 0$ granični ordinal, skup $\{p_\xi : \xi < \alpha\}$ je lanac u $\mathcal{P}$, pa prema pretpostavci, takav p_α postoji. Neka je β najmanji ordinal za koji ne postoji $p_{\beta+1} \in P$ takav da $p_\beta < p_{\beta+1}$. Dakle, p_β je maksimalni element uređenja $\mathcal{P}$.

Pretpostavimo da važi Cornova lema. Neka je a familija nepraznih skupova i $P = \{f : f \text{ je funkcija izbora familije } z \text{ i } z \subseteq a\}$. Kako svaka konačna familija ima funkciju izbora, skup P nije prazan. U parcijalnom uređenju $(P, \subseteq)$ svaki lanac L ima gornje ograničenje $\bigcup L$, pa prema Cornovoj lemi, P sadrži maksimalni element f koji je funkcija izbora familije a.

U teoriji ZFC, svaki skup x može se dobro urediti, odnosno, postoji ordinal α takav da je $x \approx \alpha$. Najmanji ordinal sa takvim svojstvom je kardinalnost skupa x. Dakle, u ZFC svaki skup ima kardinalnost. Podsetimo se, u teoriji ZF može se definisati pojam kardinala i razviti do određenog stepena, ali ne i govoriti o kardinalnosti svakog skupa.

Na primer, u teoriji ZF, ni za jedan ordinal α ne može se dokazati da skup $P(\omega_\alpha)$ zaista ima kardinalnost.

Zbir niza kardinala $(\kappa_\alpha : \alpha < \beta)$ je kardinal

$$\sum_{\alpha<\beta} \kappa_\alpha = |\bigcup_{\alpha<\beta}(\kappa_\alpha \times \{\alpha\})|.$$

U ovoj definiciji, kardinale κ_α možemo shvatiti i kao skupove, odnosno, $\sum_{\alpha<\beta} \kappa_\alpha = |\bigcup_{\alpha<\beta} A_\alpha|$, gde je $(A_\alpha : \alpha < \beta)$ proizvoljna familija disjunktnih skupova takvih da za svako $\alpha < \beta$, $|A_\alpha| = \kappa_\alpha$. Na osnovu aksiome izbora, ova definicija je korektna.

U specijalnom slučaju, zbir kardinala κ i λ definisan je kao kardinal $\kappa + \lambda = |(\kappa \times \{0\}) \cup (\lambda \times \{1\})|$.

Sabiranje kardinala je asocijativno i komutativno u opštem smislu, tj. poredak članova niza $(\kappa_\alpha : \alpha < \beta)$ je irelevantan za kardinalnost njegovog zbira.

Kardinalnost Dekartovog proizvoda $\prod_{\alpha<\beta} \kappa_\alpha$ je *proizvod niza kardinala* $(\kappa_\alpha : \alpha < \beta)$. Prema aksiomi izbora, ova definicija je korektna. Množenje kardinala je asocijativno i komutativno u istom smislu kao i sabiranje.

Za proizvoljne kardinale κ i λ, *stepen* κ^λ definišemo kao kardinalnost proizvoda $\prod_{\alpha<\lambda} \kappa$, odnosno $\kappa^\lambda = |\{f : f$ je funkcija λ u $\kappa\}|$. Za proizvoljne kardinale κ, λ i ν, $\kappa^\lambda \cdot \kappa^\mu = \kappa^{(\lambda+\mu)}$, $\kappa^\lambda \cdot \mu^\lambda = (\kappa \cdot \mu)^\lambda$ i $(\kappa^\lambda)^\mu = \kappa^{(\lambda\cdot\mu)}$,

Prethodne napomene pokazuju da aritmetika kardinala ima sva algebarska svojstva aritmetike konačnih kardinala. Međutim, one nisu u potpunosti svodljive jedna na drugu. U izvesnom smislu, kardinalna aritmetika je trivijalna, što pokazuje sledeći primer.

Teorema 7. Za svaki kardinal $\kappa \geq \aleph_0$, važi jednakost $\kappa \cdot \kappa = \kappa$.

Dokaz: Pretpostavimo suprotno. Neka je κ najmanji kardinal takav da $\kappa \cdot \kappa \neq \kappa$. To znači da za sve $\lambda < \kappa$, $\lambda \cdot \lambda = \lambda < \kappa$.

Neka je $P = \kappa \times \kappa$. To znači da je $|P| = \kappa \cdot \kappa > \kappa$. Za svako $\xi < \kappa$, neka je $P_\xi = \{(\alpha, \beta) \in P : \alpha + \beta = \xi\}$.

Ako $\xi \neq \gamma$, onda $P_\xi \cap P_\gamma = \emptyset$ i $P = \bigcup_{\xi<\kappa} P_\xi$, što znači da familija $(P_\xi : \xi < \kappa)$ čini particiju skupa P.

Za svako $\xi < \kappa$, neka je na P_ξ definisan leksikografski poredak $<_\xi$ i neka je $<_*$ ordinalna suma poredaka $(P_\xi, <_\xi)$. To zapravo znači da je $<_*$ dobro uređenje skupa P.

Neka je δ ordinal izomorfan uređenju $(P, <_*)$. Kako je $|P| > \kappa$, mora biti $\delta > \kappa$. Otuda sledi da postoji par $(\alpha_0, \beta_0) \in P$ za koji je inicijalni segment $P_{(\alpha_0,\beta_0)}$ uređenja $(P, <_*)$ jednak kardinalu κ.

Neka je $\xi_0 < \kappa$ takvo da $(\alpha_0, \beta_0) \in P_{\xi_0}$. To znači da je $\alpha_0 + \beta_0 = \xi_0$, pa mora biti $P_{(\alpha_0,\beta_0)} \subseteq (\xi_0 + 1) \times (\xi_0 + 1)$.

Kako je $\xi_0 + 1 < \kappa$, to mora biti $|\xi_0 + 1| < \kappa$, što konačno znači da je $|P_{(\alpha_0,\beta_0)}| < \kappa$, suprotno definiciji inicijalnog segmenta $P_{(\alpha_0,\beta_0)}$. $\square$

Iako se to relativno retko naglašava, prethodni primer spada u brojne varijante aksiome izbora.

Primer 5. Aksioma izbora važi ako i samo ako za svaki beskonačan kardinal κ, važi jednakost $\kappa^2 = \kappa$.

Primer 6. Bez aksiome izbora, dakle u ZF, postoji proizvoljno veliki kardinal β takav da $\beta^2 = \beta$.

Neka je α proizvoljan kardinal i $\beta = 2^{\alpha \cdot \aleph_0}$. Kako je $\alpha < 2^\alpha$, to mora biti $\alpha < 2^{\alpha \cdot \aleph_0} = \beta$. Pritom, $\beta^2 = (2^{\alpha \cdot \aleph_0})^2 = 2^{\alpha \cdot \aleph_0 \cdot 2} = 2^{\alpha \cdot \aleph_0} = \beta$.

Primer 7. Donja Skolemova teorema je ekvivalentna aksiomi izbora.

Pretpostavimo da je κ beskonačan kardinal, onda postoji kardinal $\lambda > \kappa$ takav da je $\lambda^2 = \lambda$. Neka je F binarna operacijska konstanta i φ sledeća rečenica jezika $\mathcal{L} = \{F\}$:

$$\begin{aligned}\varphi = \forall x \forall y \exists z \forall u\, (F(x,y) = u \leftrightarrow u = z) \land \\ \forall z \exists u \exists v \forall x \forall y\, (F(x,y) = z \leftrightarrow (x = u\ \land\ y = v)).\end{aligned}$$

Rečenica φ u modelu $\mathcal{A} = (\lambda, f)$ izražava činjenicu: "f je obostrano jednozanačna i na funkcija". Prema donjoj Skolemovoj, postoji model $\mathcal{B} = (B, g)$ kardinalnosti $|B| = \kappa$ u kojem važi rečenica φ, što znači da je $\kappa^2 = \kappa$.

Primer 8. Gornja Skolemova teorema je ekvivalentna aksiomi izbora.

Za dokaz ovog tvrđenja dovoljno je primetiti da, u ZF, postoji obostrano jednoznačna funkcija f koja preslikava $\omega \times \omega$ na ω. Na primer, sledeći polinom nabraja parove prirodnih brojeva: za proizvoljne $m, n \in \omega$,

$$p(m,n) = \tfrac{1}{2}[(m+n)^2 + 3m + n].$$

To znači da rečenica φ, definisana u prethodnom primeru, ima prebrojiv model. Prema gornjoj Skolemovoj teoremi, φ ima model svake beskonačne kardinalnosti.

Primer 9. Ako je κ beskonačan kardinal, onda skup svih ordinala kardinalnosti κ ima kardinalnost κ^+.

Primer 10. Unija prebrojive familije prebrojivih skupova je prebrojiva. Opštije, za svaku familiju S, $|\bigcup S| \leq |S| \cdot \sup\{|x| : x \in S\}$.

Pretpostavimo da je $\kappa = |S|$ i $\lambda = \sup\{|x| : x \in S\}$. Prema aksiomi izbora, familija S, a i svaki od njenih elemenata, može se dobro urediti.

Neka je $S = \{S_\alpha : \alpha < \kappa\}$ i za svako $\alpha < \kappa$, $S_\alpha = \{x_{\alpha\beta} : \beta < \lambda_\alpha\}$, $\lambda_\alpha \leq \lambda$. Preslikavanje $(\alpha, \beta) \mapsto x_{\alpha\beta}$ je projekcija $\kappa \times \lambda$ na $\bigcup S$, tj. $|\bigcup S| \leq \kappa \cdot \lambda$.

Specijalno, unija $\aleph_\alpha$ skupova, od kojih je svaki kardinalnosti $\aleph_\alpha$, ima kardinalnost $\aleph_\alpha$. Takođe, iz prethodnog rezultata sledi da za svako α, kardinal $\aleph_{\alpha+1}$ je regularan kardinal.

Primer 11. (a) Neka su κ i λ kardinali i za svako $\alpha < \lambda$, $\kappa_\alpha = \kappa$. Tada je $\sum_{\alpha<\lambda} \kappa_\alpha = \lambda \cdot \kappa$.

(b) Neka je λ beskonačan kardinal i za svako $\alpha < \lambda$, $\kappa_\alpha > 0$, onda je $\sum_{\alpha<\lambda} \kappa_\alpha = \lambda \cdot \sup_{\alpha<\lambda} \kappa_\alpha$.

(c) Ako je $\lambda \leq \sup_{\alpha<\lambda} \kappa_\alpha$, onda $\sum_{\alpha<\lambda} \kappa_\alpha = \sup_{\alpha<\lambda} \kappa_\alpha$.

Na osnovu ovih rezultata, singularni kardinal κ je kardinal predstavljiv kao suma $\kappa = \sum_{\alpha<\lambda} \kappa_\alpha$ u kojoj je $\lambda < \kappa$ i svaki $\kappa_i < \kappa$.

Primer 12. (a) Neka je λ beskonačan kardinal i $(\kappa_\alpha > 0 : \alpha < \lambda)$ neopadajući niz kardinala, onda je

$$\prod_{\alpha<\lambda} \kappa_\alpha = (\sup_{\alpha<\lambda} \kappa_\alpha)^\lambda.$$

(b) Skup $\omega! = \{f \in \omega^\omega : f$ je "1-1" i "na" $\}$ ima kardinalnost 2^ω. Pritom, $\omega!$ se može shvatiti kao $\prod_{0<n<\omega} n$.

Primer 13. (a) Za svaki kardinal κ, ako je λ beskonačan kardinal i $2 \leq \kappa \leq \lambda$, onda $\kappa^\lambda = 2^\lambda$.

(b) Ako je κ beskonačan kardinal $(\kappa^+)^\kappa = 2^\kappa$.

Da bi se dokažalo tvrđenje (a), dovoljno je dokazati nejednakost $\kappa^\lambda \leq 2^\lambda$. Kako je λ beskonačan kardinal i $\kappa \leq \lambda$, $\kappa \cdot \lambda = \lambda$. Neka je $f : \lambda \times \kappa \to \lambda$ obostrano jednoznačna i "na" funkcija.

Za svaku funkciju $h : \lambda \to \kappa$, $h \subseteq \kappa \times \lambda$, pa neka je $G(h) = f[h]$. To znači da je $G(h) \subseteq \lambda$, tj. $G : \kappa^\lambda \to P(\lambda)$ je obostrano jednoznačna funkcija. Pritom, u ovom slučaju, sa κ^λ označili smo skup svih funkcija iz λ u κ. Otuda sledi da je $\kappa^\lambda = |\kappa^\lambda| \leq |P(\lambda)| = 2^\lambda$.

Kardinal κ^+ je regularan, pa ako $(\kappa^+)^\kappa$ shvatimo kao skup svih funkcija iz κ u κ^+, $(\kappa^+)^\kappa \subseteq \bigcup_{\alpha<\kappa^+} \alpha^\kappa$. Otuda se redom dobija

$$|(\kappa^+)^\kappa| \leq \sum_{\alpha<\kappa^+} |\alpha^\kappa| = \sum_{\alpha<\kappa^+} |\alpha|^\kappa = \kappa^+ \cdot \kappa^\kappa = \kappa^+ \cdot 2^\kappa = 2^\kappa,$$

što dokazuje tvrđenje (b).

U prethodnim dokazima, izraz κ^λ javljao se kao oznaka stepena kardinala i istovremeno, kao oznaka skupa svih funkcija iz λ u κ, ali je iz konteksta bilo jasno u kom smislu je on bio upotrebljen.

Za beskonačan kardinal λ, tvrđenje (a) daje potpun odgovor o ponašanju stepena κ^λ za sve vrednosti $\kappa \leq \lambda$. Za $\kappa > \lambda$, ponašanje stepena je mnogo kompleksnije i o njemu se u ZFC ne može reći monogo više od onoga što je rečeno u tvrđenju (b). Na primer, $2^{\aleph_0}$ jeste kardinal, pa za neki ordinal α, $2^{\aleph_0} = \aleph_\alpha$, ali se u teoriji ZFC ova jednačina ne može rešiti.

Iako je pokušavao da dokaže i suprotno, Kantor je izgleda verovao da je $2^{\aleph_0} = \aleph_1$. Kako je $2^{\aleph_0}$ kardinalnost skupa R realnih brojeva, odnosno, kontinuuma, pretpostavka $2^{\aleph_0} = \aleph_1$ se uobičajeno naziva *hipotezom kontinuuma*

Skup 2^ω može se definisati u teoriji ZF, pa je 2^ω konstanta konačnog definicionog proširenja jezika $\mathcal{L}_{ZF}$. Isto važi i za predikate $\mathrm{Fin}(x)$ ako i samo ako "x je konačan skup", $\mathrm{Preb}(x)$ ako i samo ako "x je prebrojiv skup" i "$x \approx y$". Stoga, hipotezu kontinuuma možemo izraziti rečenicom

$$CH = \forall x\,((x \subseteq 2^\omega \wedge \neg \mathrm{Fin}(x)) \rightarrow (\mathrm{Preb}(x) \vee x \approx 2^\omega)).$$

Rečenica CH formulisana je u definicionom proširenju jezika $\mathcal{L}_{ZF}$. Kada eliminišemo sve uvedene konstante, dobijamo ekvivalentnu formulaciju rečenice CH u jeziku $\mathcal{L}_{ZF}$. Zapravo, ta rečenica predstavlja formulaciju hipoteze kontinuuma u jeziku teorije ZF. Kantorov problem kontinuuma sada možemo shvatiti kao problem dokazivosti rečenice CH u teoriji ZF, odnosno ZFC ili bilo kojoj teoriji Σ u jeziku $\mathcal{L}_{ZF}$.

Nije sasvim jasno koliko je ovakva preformulacija Kantorovog problema opravdana. Sigurno, on sam ga nije tako shvatao. Iako po formulaciji sasvim jednostavan, problem kontinuuma je decenijama mobilisao značajne napore većine matematičara. O tome kako je rešen i da li je uopšte rešen, govorićemo i kasnije. Prethodno ćemo izložiti svojstva kardinala 2^ω koja se mogu dokazati u teoriji ZFC. Granicu do koje ova teorija rasvetljava problem kontinuuma i aritmetiku kardinala određuje sledeća teorema.

Kenihova Lema: Ako su $(\kappa_\alpha : \alpha < \beta)$ i $(\lambda_\alpha : \alpha < \beta)$ nizovi kardinala takvi da za svako $\alpha < \beta$, $\kappa_\alpha < \lambda_\alpha$, onda je

$$\textstyle\sum_{\alpha<\beta} \kappa_\alpha < \prod_{\alpha<\beta} \lambda_\alpha.$$

Dokaz: Neka je $(a_\alpha : \alpha < \beta)$ familija skupova takva da za svaki ordinal $\alpha < \beta$, $|a_\alpha| = \lambda_\alpha$. Dovoljno je dokazati da za proizvoljnu familiju skupova $(b_\alpha : \alpha < \beta)$, ako $b_\alpha \subseteq \prod_{\alpha<\beta} a_\alpha = a$ i $|b_\alpha| \leq \kappa_\alpha$, onda $\bigcup_{\alpha<\beta} b_\alpha \neq a$.

Za svako $\alpha < \beta$, neka je $x_\alpha = \{f(\alpha) : f \in b_\alpha\}$. Kako je $|x_\alpha| < |a_\alpha|$, neka je $f \in a$ takvo da za svako $\alpha < \beta$, $f(\alpha) \in (a_\alpha - x_\alpha)$. Dakle, za svaki ordinal $\alpha < \beta$, $f \notin b_\alpha$, tj. $\bigcup_{\alpha<\beta} b_\alpha \neq a$. $\square$

Primer 14. Ako je κ beskonačan kardinal, onda $\kappa < \mathrm{cf}(2^\kappa)$.

Svaki niz kardinala $(\kappa_\alpha < 2^\kappa : \alpha < \kappa)$, na osnovu Kenihove leme zadovoljava nejednakost $\Sigma_{\alpha<\kappa}\kappa_\alpha < \prod_{\alpha<\kappa}(2^\kappa)^\kappa = 2^\kappa$.

Primer 15. Ako je κ beskonačan kardinal, $\kappa < \kappa^{\mathrm{cf}(\kappa)}$.

Za $\alpha < \mathrm{cf}(\kappa)$, neka su $\kappa_\alpha < \kappa$ takvi da $\kappa = \sum_{\alpha<\mathrm{cf}(\kappa)} \kappa_\alpha$. Na osnovu Kenihove leme, $\kappa = \sum_{\alpha<\mathrm{cf}(\kappa)} \kappa_\alpha < \prod_{\alpha<\mathrm{cf}(\kappa)} \kappa = \kappa^{\mathrm{cf}(\kappa)}$.

Prema prethodnom primeru $2^{\aleph_0}$ ne može biti kardinal kofinalnosti ω, što znači da je $2^{\aleph_0} \neq \aleph_\omega$, odnosno, $2^{\aleph_0} \neq \aleph_{\omega+\omega}$ itd. Pretežno, to je sve što se u teoriji ZFC može reći o problemu kontinuuma.

Modeli teorije skupova

Sve aksiome teorije ZF važe u modelu $(V, \in)$, pa dakle ZF je neprotivrečna teorija. Međutim, ovaj "dokaz" neprotivrečnosti teorije ZF samo izražava naše uverenje da teorija skupova u kojoj se može zasnovati čitava matematika nije protivrečna. Klasa V nije skup, pa dakle u pravom smislu te reči, $(V, \in)$ nije model teorije ZF. Jedan od ključnih problema zasnivanja matematike je problem neprotivrečnosti teorije ZF. Eksplicitno formulisan to je problem "da li postoji dokaz kontradikcije iz pretpostavki ZF", odnosno, da li postoji konačan niz rečenica $\varphi_1, \ldots \varphi_{n-1}, \varphi \wedge \neg\varphi$ jezika $\mathcal{L}_{ZF}$ u kojem su rečenice $\varphi_1, \ldots, \varphi_{n-1}$ aksiome teorije ZF ili njihove posledice.

Ovako postavljena, neprotivrečnost teorije ZF ima čisto kombinatorni karakter, pa izgleda da se taj problem može rešiti u elementarnom računu sa konačnim nizovima. Po svemu sudeći, Hilbert je verovao u postojanje upravo takvog dokaza "da opšte prihvaćene metode matematike uzete u svojoj ukupnosti ne dovode do kontradikcije". Međutim, prema Gedelovoj teoremi nepotpunosti, takav dokaz nije moguć čak ni kada se u metateoriji pretpostave sredstva izražena u teoriji ZFC.

Kako klasa V, kao osnovna interpretacija jezika $\mathcal{L}_{ZF}$ nije model u pravom smislu te reči, ključna ideja u dokazima neprotivrečnosti je Gedelov stav potpunosti. Za proizvoljnu teoriju Σ jezika $\mathcal{L}_{ZF}$, u klasi V definisaćemo interpretaciju u kojoj važe sve rečenice teorije Σ. Na primer, ako je CH formulacija hipoteze kontinuuma u jeziku $\mathcal{L}$, definisaćemo jednu interpretaciju u kojoj važi ZF + CH i drugu, u kojoj važi $ZF + \neg CH$, a da pritom uopšte ne odgovorimo na pitanje da li u našoj glavnoj interpretaciji V važi hipoteza CH ili njena negacija.

Smisao takvog rezultata jeste da pretpostavke teorije ZF ne dokazuju niti opovrgavaju hipotezu kontinuma i on je u principu prihvatljiv i sa platonističkog i sa formalističkog stanovišta. U prvom slučaju, on pokazuje da rečenice teorije ZF ne izražavaju sva svojstva skupova koja važe u matematičkom svetu. Sa formalističkog stanovišta, on pokazuje da se u formalizaciciji principa naše metateorije, dakle u ZF ili u ZFC, može dokazati rečenica

$$\mathrm{Con}(ZF) \rightarrow\ \mathrm{Con}(ZF + CH),$$

u kojoj $\mathrm{Con}(ZF)$ označava formalizaciju rečenice "ZF je neprotivrečna teorija" u jeziku $\mathcal{L}_{ZF}$.

Ako pretpostavimo da naša metateorija sadrži principe koji su neophodni da bi se dokazao stav potpunosti, iz neprotivrečnosti teorije ZF sledi da postoji model $\mathcal{A} = (A, \varepsilon)$ jezika $\mathcal{L}_{ZF}$ takav da $\mathcal{A} \models ZF$. Kao uređen par, model $\mathcal{A}$ je skup, tj. $\mathcal{A} \in V$, pa sve objekte koje smo do sada definisali, kao i njihova svojstva, možemo interpretirati u modelu $\mathcal{A}$. Na primer, u modelu $\mathcal{A}$ postoje skupovi prirodnih i realnih brojeva, ordinal ω^ω i kardinal ω_1, odnosno, u njemu su definisani klasa On, niz kardinal $(\aleph_\alpha : \alpha \in On)$ itd. Svi navedeni objekti ne moraju biti identični sa odgovarajućim objektima univerzuma V. U sledećim primerima ilustrovaćemo kako u modelima teorije ZF izgledaju prirodni brojevi.

Primer 1. Ako je ZF neprotivrečna teorija, ZF ima prebrojiv model. Međutim, u teoriji ZF dokazali smo da "u univerzumu V postoji neprebrojivo mnogo skupova".

Navedena "protivrečnost" naziva se Skolemovim paradoksom. Ipak, ona je samo prividna budući da rečenica koja izražava neprebrojivost univerzuma zaista važi u prebrojivom modelu teorije ZF.

Pretpostavimo da je ZF neprotivrečna teorija. Kako je jezik $\mathcal{L}_{ZF}$ prebrojiv, na osnovu Skolemove teoreme, teorija ZF ima prebrojiv model $\mathcal{A} = (A, \varepsilon)$. Neka je $\varphi(x) = \neg\exists y\,(\mathrm{fun}(y) \wedge \mathrm{mono}(y) \wedge \mathrm{dom}(y) = x \wedge \mathrm{codom}(x) \subseteq \omega)$ formula koja u teoriji ZF formalizuje predikat "ne postoji funkcija koja obostrano jednoznačno preslikava skup x u skup prirodnih brojeva ω".

Kako smo ranije dokazali $ZF \vdash \exists x\,\varphi(x)$, pa postoji skup $a \in A$ za koji važi $\mathcal{A} \models \varphi(x)[a]$. Skup $a^A = \{z \in A : z\,\varepsilon\,a\} \subseteq A$ je najviše prebrojiv, pa postoji funkcija $f \in V$ koja obostrano jednoznačno preslikava a^A na skup prirodnih brojeva ω.

Kako svaki skup pripada klasi V, za svako $a \in A$, važi $\mathcal{A} \models (x = x)[a]$, tj. interpretacija V^A klase V u modelu $\mathcal{A}$ jeste skup A. Kako je $V^A = A$, otuda ne sledi da $f \in A$. Jer, po definiciji zadovoljenja, smisao relacije $\mathcal{A} \models \varphi(x)[a]$ jeste da ne postoji $f \in A$ takvo da $\mathrm{fun}^A(f)$, $\mathrm{mono}^A(f)$, $\mathrm{dom}^A(f) = a$ i

$\mathrm{codom}^A(x) \subseteq^A \omega^A$, odnosno, skup $a \in A$ je $(\text{neprebrojiv})^A$. Slobodnije rečeno, posmatran iz univerzuma V, skup a^A je prebrojiv, a posmatran u samom modelu $\mathcal{A}$, skup a^A nije prebrojiv.

Kada se ima u vidu gornja Skolemova teorema, slika iz prethodnog primera može se potpuno preokrenuti. Spolja gledano, skupovi u modelu teorije ZF mogu biti neprebrojivi, a prebrojivi sa stanovišta samog modela.

Primer 2. Ako je teorija ZF neprotivrečna, postoji model $\mathcal{B}$ za ZF čiji je skup prirodnoh brojeva ω^B neprebrojiv u V.

Neka je $\mathcal{L}' = \mathcal{L}_{ZF} \cup \{\omega\}$ definiciono proširenje jezika $\mathcal{L}_{ZF}$. Proširimo $\mathcal{L}'$ sa ω_1 novih konstanti. U tako dobijenom jeziku definišimo skup rečenica:

$$\Sigma = ZF \cup \{c_\alpha \in \omega : \alpha \in \omega_1\} \cup \{c_\alpha \neq c_\beta : \alpha \neq \beta \text{ i } \alpha, \beta \in \omega_1\}.$$

Po pretpostavci, ZF je neprotivrečna teorija, pa svaki konačan skup rečenica $\Sigma_0 \subseteq \Sigma$ ima model. Prema stavu kompaktnosti, teorija Σ ima model. Neka je $\mathcal{B} = (B, \varepsilon, \omega^B)$ redukcija modela teorije Σ na jezik $\mathcal{L}'$. Kao i ranije, ω^B je interpretacija konstante ω u modelu $\mathcal{B}$. Po konstrukciji, skup $\{a \in B : a \varepsilon \omega^B\}$ je neprebrojiv, međutim, ω^B je prebrojiv^B. To zapravo znači da prirodni brojevi u modelu $\mathcal{B}$ nisu standardni prirodni brojevi.

Prethodni primeri na prvi pogled protivreče i činjenici da se u teoriji ZF može dokazati jedinstvenost strukture prirodnih brojeva. Naime, prirodni brojevi ω^A i ω^B sigurno nisu izomorfni. Međutim, ako se Dedekindova teorema o jedinstvenosti prirodnih brojeva definiše rečenicom jezika $\mathcal{L}_{ZF}$, onda njen smisao u modelu $\mathcal{A}$ teorije ZF jeste da su u modelu $\mathcal{A}$ bilo koje dve strukture prirodnih brojeva izomorfne.

Svi sintaksni i semantički pojmovi jezika $\mathcal{L}_{ZF}$ mogu se formalno izraziti u jeziku $\mathcal{L}_{ZF}$ i sva njegova svojstva dokaziva su u teoriji ZF.

Sintaksnu i semantičku strukturu $\mathcal{L}_{ZF}$ definišemo na isti način kao u slučaju strukture prirodnih, racionalnih ili realnih brojeva. U sledećim primerima, strukturu jezika $\mathcal{L}_{ZF}$ opisaćemo do stepena u kojem je moguće formalizovati metamatematičku relaciju zadovoljenja.

Za svaku formulu φ jezika $\mathcal{L}_{ZF}$, *kod formule* φ je skup $\ulcorner\varphi\urcorner$ koji definišemo indukcijom po njenoj složenosti:

(a) $\ulcorner v_m = v_n \urcorner = (0, m, n)$, za sve $m, n \in \omega$,
(b) $\ulcorner v_m \in v_n \urcorner = (1, m, n)$, za sve $m, n \in \omega$,
(c) $\ulcorner \varphi \to \psi \urcorner = (2, \ulcorner\varphi\urcorner, \ulcorner\psi\urcorner)$,
(d) $\ulcorner \neg\varphi \urcorner = (3, \ulcorner\varphi\urcorner)$,
(e) $\ulcorner \exists v_n\, \varphi \urcorner = (4, n, \ulcorner\varphi\urcorner)$, za svako $n \in \omega$.

Na osnovu teoreme rekurzije, definišemo skup F kodova svih formula jezika $\mathcal{L}_{ZF}$. Neka je $F_0 = 2 \times \omega \times \omega$ i za svako $n \geq 0$

$$F_{n+1} = F_n \cup (\{2\} \times F_n \times F_n) \cup (\{3\} \times F_n) \cup (\{4\} \times \omega \times F_n).$$

Primer 3. Ako je $F = \bigcup_{n \in \omega} F_n$, za svaku formulu φ jezika $\mathcal{L}_{ZF}$, u teoriji ZF važi $\ulcorner \varphi \urcorner \in F$.

Ako je φ formula jezika $\mathcal{L}_{ZF}$ i $x \in a^\omega$ valuacija promenljivih u skupu a, u jeziku $\mathcal{L}_{ZF}$ definišemo relaciju "formula φ važi u modelu $(a, \in_a)$ za valuaciju x". Pritom, sa $\in_a$ označili smo restrikciju relacije $\in$ na skup a, odnosno, relacija $\in_a$ je skup $\{(x, y) \in a^2 : x \in y\}$.

Ako je $x \in a^\omega$ valuacija promenljivih, $n \in \omega$ i $y \in a$, sa $x(n/y)$ označavamo valuaciju $(x - \{(n, x(n))\}) \cup \{(n, y)\}$.

Primer 4. U teoriji ZF može se definisati funkcija f koja, svakom kodu formule φ jezika $\mathcal{L}_{ZF}$, pridužuje skup valuacija za koje formula φ važi u modelu $(a, \in_a)$.

Za svako $k \in \omega$ definisaćemo funkciju $f_k : F_k \to P(a^\omega)$. Funkcija f čija se egzistencija tvrdi je $f = \bigcup_{k \in \omega} f_k$. Ako je $k = 0$, za sve $m, n \in \omega$,

(a) $f_0(0, m, n) = \{x \in a^\omega; x(m) = x(n)\}$,
(b) $f_0(1, m, n) = \{x \in a^\omega; x(m) \in x(n)\}$.

Za svako $k \geq 0$, ako je funkcija f_k definisana, onda za sve $u, v \in F_k$ i svako $n \in \omega$,

(c) $f_{k+1}(2, u, v) = (a^\omega - f_k(u)) \cup f_k(v)$,
(d) $f_{k+1}(3, u) = a^\omega - f_k(u)$,
(e) $f_{k+1}(4, n, u) = \{x \in a^\omega; \exists z \in a\, (x(n/z) \in f_k(u))\}$.

Na osnovu teoreme rekurzije, smisao prethodnog tvrđenja jeste da postoji formula $\varphi(x, y)$ jezika $\mathcal{L}_{ZF}$ takva da $ZF \vdash \forall a \exists f\, \varphi(a, f)$. Na osnovu prethodnog dokaza,

$$\begin{aligned}
\varphi(a, f) \quad = \quad & \mathrm{fun}(f) \wedge (\mathrm{dom}(f) = F) \\
& \wedge \forall m \forall n\, (f(0, m, n) = \{x \in a^\omega; x(m) = x(n)\} \\
& \wedge f(1, m, n) = \{x \in a^\omega; x(m) \in x(n)\} \\
& \wedge \forall u \in F\, \forall v \in F\, (f(2, u, v) = (a^\omega - f(u)) \cup f(v) \\
& \wedge f(3, u) = a^\omega - f(u) \\
& \wedge f(4, n, u) = \{x \in a^\omega; \exists z \in a\, x(n/z) \in f(u)\})).
\end{aligned}$$

Formula $\varphi(a, f)$ definiše skup valuacija za koji formula sa datim kodom važi u modelu $(a, \in_a)$. Za sve a, v, z neka je $s(a, v) = z$ ako i samo ako važi $\forall f\, (\varphi(a, f) \to f(v) = z)$.

Ako $v \in F$, onda je $s(a,v)$ skup svih valuacija $x \in a^\omega$ koje zadovoljavaju formulu v u modelu $(a, \in_a)$.

Sada se u jeziku $\mathcal{L}_{ZF}$ može definisati formulu

$$\mathrm{Sat}(x,v,a) = v \in F \wedge x \in s(a,v).$$

Primer 5. Formula $\mathrm{Sat}(x, \ulcorner\varphi\urcorner, a)$ u teoriji ZF formalizuje predikat "x zadovoljava formulu φ u modelu $(a, \in_a)$".

Za sve $m, n \in \omega$ i proizvoljne formule φ, ψ jezika $\mathcal{L}_{ZF}$, u teoriji ZF može se dokazati da za svaki skup a i svaku valuaciju $x \in a^\omega$,

(a) $\mathrm{Sat}(x, \ulcorner v_m = v_n\urcorner, a) \leftrightarrow x(m) = x(n)$,
(b) $\mathrm{Sat}(x, \ulcorner v_m \in v_n\urcorner, a) \leftrightarrow x(m) \in x(n)$,
(c) $\mathrm{Sat}(x, \ulcorner\varphi \to \psi\urcorner, a) \leftrightarrow \mathrm{Sat}(x, \ulcorner\varphi\urcorner, a) \to \mathrm{Sat}(x, \ulcorner\psi\urcorner, a)$,
(d) $\mathrm{Sat}(x, \ulcorner\neg\varphi\urcorner, a) \leftrightarrow \neg\mathrm{Sat}(x, \ulcorner\varphi\urcorner, a)$,
(e) $\mathrm{Sat}(x, \ulcorner\exists v_n\, \varphi\urcorner, a) \leftrightarrow \exists y \in a\, \mathrm{Sat}(x(n/y), \ulcorner\varphi\urcorner, a)$.

Primer 6. Ako je φ formula sa slobodnim promenljivim $v_0, \ldots v_n$, u teoriji ZF može se dokazati da za svaki skup a i svaku valuaciju $x \in a^\omega$ važi

$$\mathrm{Sat}(x, \ulcorner\varphi\urcorner, a) \leftrightarrow \varphi^a(x(0), \ldots, x(n)),$$

gde je φ^a formula koja se dobija relativizacijom svih kvantifikatora formule φ na skup a. To znači da se svaki kvantifikator $\exists x$ zameni sa $\exists x \in a$.

Primer 7. Ako je $\mathrm{Ist}(v,a) = \forall x \in a^\omega\, \mathrm{Sat}(x,v,a)$, onda za svaku rečenicu φ, u teoriji ZF može se dokazati da ako je $a \neq \emptyset$, $\mathrm{Ist}(\ulcorner\varphi\urcorner, a) \leftrightarrow \varphi^a$.

U teoriji ZF, formula $\mathrm{Ist}(\ulcorner\varphi\urcorner, a)$ izražava istinitost rečenice φ u modelu $(a, \in_a)$. Dakle, u teoriji ZF može se formulisati istina modela $(a, \in_a$). Međutim, ne postoji formula $\mathrm{Lis}(x)$ koja izražava logičke istine čitavog univerzuma V. To bi značilo da za svaku rečenicu φ važi $ZF \vdash \varphi \leftrightarrow \mathrm{Lis}(\urcorner\varphi\ulcorner)$, što u rekurzivno aksiomatskoj teoriji kakva je i ZF nije moguće. Ovaj rezultat izložen je u okviru teorije izračunljivosti.

Primer 8. U teoriji ZF može se definisati formula koja formalizuje elementarne podmodele. Ako je

$$\mathrm{Epm}(a,b) = a \subseteq b \wedge \forall v \in F\, \forall x \in a^\omega\, \mathrm{Sat}(x,v,a) \leftrightarrow \mathrm{Sat}(x,v,b).$$

formula $\mathrm{Epm}(a,b)$ izražava činjenicu da je $(a, \in_a)$ elementarni podmodel modela $(b, \in_a)$. Pritom, za svaku formulu φ jezika $\mathcal{L}_{ZF}$, čije su slobodne promenljive $v_0, \ldots v_n$, u teoriji ZF može se dokazati

$$\mathrm{Epm}(a,b) \to \forall v_0 \in a \cdots \forall v_n \in a\, (\varphi^a \leftrightarrow \varphi^b).$$

Primer 9. Ako pretpostavimo aksiomu izbora, dakle u teoriji ZFC, može se dokazati formalna varijanta donje Skolemove teoreme:

$$\forall x \subseteq b(\omega \leq |x| \leq |b| \to \exists a \subseteq b\,(\mathrm{Epm}(a,b) \wedge x \subseteq a)).$$

Formalizacija sintaksne strukture jezika $\mathcal{L}_{ZF}$ je znatno jednostavnija od formalizacije njegove semantike. Skup formula F smo definisali. Formalizacijom pravila izvođenja, može se definisati formula $\mathrm{Pr}(s,x,y)$ jezika $\mathcal{L}$ čiji je smisao "x je dokaz formule y u teoriji s", pritom, x je konačan niz kodova elemenata skupa F, $y \in F$ i $s \subseteq F$ skup kodova teorije Σ u jeziku $\mathcal{L}_{ZF}$. Za svaki skup rečenica Σ neka je

$$\mathrm{Con}(s) = \neg\exists x\, \mathrm{Pr}(s,x,\ulcorner 0=1 \urcorner).$$

Rečenica $\mathrm{Con}(s)$ u teoriji ZF formalizuje neprotivrečnost teorije Σ. Takođe, ako je s skup kodova teorije Σ, rečenica

$$\mathrm{Mod}(a,s) = \forall v \in s\, \mathrm{Ist}(v,a)$$

u teoriji ZF formalizuje važenje teorije Σ u modelu $(a, \in_a)$, odnosno, formula $\mathrm{Mod}(a,s)$ važi ako i samo ako $(a, \in_a)$ je model teorije čiji je skup kodova $s \subseteq F$.

Nije teško uveriti se da sve teoreme o kojima smo govorili u okviru teorije modela možemo formalizovati u ZF. Ako su dokazive metamatematičkim sredstvima koja se mogu izraziti u ZF, sve takve teoreme mogu se i formalno dokazati u ZF. Posebno, u slučaju stava potpunosti koristili smo jednu varijantu principa izbora.

Kada se radi o teorijama u prebrojivom jeziku $\mathcal{L}_{ZF}$, aksioma izbora može se eliminisati iz njegovog dokaza. Naime, svi objekti jezika $\mathcal{L}_{ZF}$, njegova sintaksa i semantika, mogu se kodirati konačnim nizovima prirodnih brojeva, a stav potpunosti za teorije u jeziku $\mathcal{L}_{ZF}$ može se dokazati sredstvima aritmetike. Kako se u teoriji ZF mogu izraziti sva aritmetička tvrđenja, otuda sledi da

$$ZF \vdash \forall s \subseteq F\,(\mathrm{Con}(s) \leftrightarrow \exists a\, \mathrm{Mod}(a,s)).$$

Ovo poslednje zapravo znači da svaka konstrukcija modela teorije ZF, sredstvima same ZF i aksiome izbora, a mi drugih sredstava u metateoriji za sada nemamo, istovremeno znači i dokaz rečenice $\mathrm{Con}(ZF)$ u teoriji ZF. Međutim, na osnovu Gedelove teoreme nepotpunosti, koja će biti dokazana u okviru teorije izračunljivosti, u bilo kojoj neprotivrečnoj rekurzivnoj teoriji tako nešto nije moguće.

Na osnovu prethodnih razmatranja sledi da u teoriji skupova možemo govoriti samo o relativnoj neprotivrečnosti. U tom smislu, kada govorimo o modelu teorije skupova irelevantno je da li se radi o modelu u pravom smislu te reči ili o strukturi oblika $\mathcal{M} = (M, \varepsilon)$ čiji domen M može biti i prava klasa. Uz pretpostavku neprotivrečnosti teorije u jeziku $\mathcal{L}_{ZF}$, na osnovu stava potpunosti, takav model može se uvek relativizovati na hipotetički model odgovarajuće teorije.

Neka je $\mathcal{M} = (M, \varepsilon)$ struktura jezika $\mathcal{L}_{ZF}$, u kojoj domen M može biti i prava klasa. Ako je $\varepsilon = (M^2 \cap \in)$, $\mathcal{M}$ je *standardni model* jezika $\mathcal{L}_{ZF}$. Kako je u standardnom modelu relacija ε isto što i pripadnost, samu klasu M nazivamo modelom jezika $\mathcal{L}_{ZF}$.

Ako je M tranzitivna klasa, $(M, \in)$ je *tranzitivan model*. I u slučaju tranzitivnih modela, umesto o modelu $(M, \in)$, prosto govorimo o modelu M jezika $\mathcal{L}_{ZF}$.

Ako je M klasa, *relativizaciju* φ^M formule φ na klasu M definišemo indukcijom po složenosti formule φ:

(a) $(x = y)^M$ i $(x \in y)^M$ su redom formule $x = y$ i $x \in y$,
(b) $(\varphi \to \psi)^M$ i $(\neg\varphi)^M$ su formule $\varphi^M \to \psi^M$ i $\neg\varphi^M$,
(c) $(\exists x\, \varphi)^M$ je formula $\exists x \in M\, \varphi^M$.

Dakle, relativizacija formule φ na klasu M je zapravo formula koja se dobija relativizacijom svih kvantifikatora formule φ na klasu M.

Primer 10. (a) Relativizacija formule $(x \subseteq y)$ na klasu M je formula

$$\forall z \in M\, (z \in x \to z \in y),$$

odnosno, $(x \subseteq y)^M$ je formula $x \cap M \subseteq y$. Ako je M tranzitivna klasa, za svako $x \in M$, $x \cap M = x$, pa dakle, za sve $x, y \in M$,

$$(x \subseteq y)^M \quad \Leftrightarrow \quad x \subseteq y.$$

(b) Ako se aksioma partitivnog skupa $\forall x \exists y \forall z\, (z \subseteq x \to z \in y)$ relativizuje na klasu M, dobija se formula:

$$\forall x \in M\, \exists y \in M\, \forall z \in M\, (z \cap M \subseteq x \to z \in y).$$

Ako je M tranzitivna klasa, za svako $z \in M$, $z \cap M = z$, pa je aksioma partitivnog skupa relativizovana na klasu M sledeća formula:

$$\forall x \in M\, \exists y \in M\, \forall z \in M\, (z \subseteq x \to z \in y).$$

Ako je $M = \{x : \theta(x)\}$, relativizaciju formule φ na klasu M označavamo sa φ^θ. To znači da je $(\exists x\, \varphi)^\theta$ formula $\exists x\, (\theta(x) \wedge \varphi^\theta)$.

Ako je φ rečenica jezika $\mathcal{L}_{ZF}$, φ važi u klasi M ako i samo ako φ^M. Ako φ važi u M, kažemo da je M model formule φ i upotrebljavamo uobičajenu oznaku $M \models \varphi$.

Primer 11. (a) Ako parafraziramo prethodni primer, formula $x \subseteq y$ važi u klasi M ako i samo ako $x \cap M \subseteq y$.

(b) Ako je M tranzitivan model, za sve $x, y \in M$, $(x \subseteq y)^M$ je formula $x \subseteq y$, pa aksioma partitivnog skupa važi u modelu M ako i samo ako

$$\forall x \in M\, \exists y \in M\, (P(x) \cap M \subseteq y).$$

Neka je Σ teorija i φ rečenica jezika $\mathcal{L}_{ZF}$. Rečenica φ je *relativno neprotivrečna* u odnosu na teoriju Σ ako neprotivrečnost teorije Σ implicira neprotivrečnost teorije $\Sigma \cup \{\varphi\}$.

Primer 12. Neka je Σ teorija i φ rečenica jezika $\mathcal{L}_{ZF}$. Ako postoji formula $\theta(x)$ jezika $\mathcal{L}$ koja zadovoljava sledeće uslove:

(a) $\Sigma \vdash \exists x\, \theta(x)$,
(b) $\Sigma \vdash \psi^\theta$, za sve $\psi \in \Sigma$,
(c) $\Sigma \vdash \varphi^\theta$,

onda je rečenica φ relativno neprotivrečna u odnosu na teoriju Σ.

Ako je rečenica ψ valjana, $(\exists x\, \theta(x) \to \psi^\theta)$ je takođe valjana rečenica. Ako je $\Sigma \cup \{\varphi\}$ protivrečna teorija, postoje rečenice $\psi_1, \ldots, \psi_n \in \Sigma$ takve da je $\psi_1 \wedge \cdots \wedge \psi_n \to \neg\varphi$ valjana rečenica. Otuda sledi da je

$$\exists x\, \theta(x) \to (\psi_1^\theta \wedge \cdots \wedge \psi_n^\theta \to \neg\varphi^\theta)$$

valjana rečenica. Sukcesivnom primenom uslova tvrđenja, dobijamo da važi $\Sigma \vdash \neg\varphi^\theta$, odnosno, Σ je protivrečna teorija.

Neka su Σ i Σ' teorije u jeziku $\mathcal{L}_{ZF}$. Klasa M je model teorije Σ' u teoriji Σ ako za svaku rečenicu $\varphi \in \Sigma'$, $\Sigma \vdash \varphi^M$.

Teorema 8. Ako su Σ i Σ' teorije u jeziku $\mathcal{L}_{ZF}$ takve da u teoriji Σ možemo dokazati da Σ' ima model, onda neprotivrečnost teorije Σ implicira neprotivrečnost teorije Σ'.

Dokaz: Ako je Σ' protivrečna teorija, onda se u Σ' može dokazati $\varphi \wedge \neg\varphi$. Kako se po pretpostavci teoreme, u teoriji Σ može dokazati da je M model teorije Σ', to bi značilo da se u Σ može dokazati $\varphi^M \wedge \neg\varphi^M$. $\square$

Kao prvu ilustraciju dokaza relativne neprotivrečnosti teorija u jeziku $\mathcal{L}_{ZF}$ izložićemo dokaz relativne neprotivrečnosti aksiome regularnosti u odnosu na ostale aksiome teorije ZF. Kako smo ranije naglasili, aksioma regularnosti ekvivalentna je činjenici da svaki skup pripada nekom nivou hijerarhije $(V_\alpha : \alpha \in On)$. Dakle, aksioma regularnosti Reg je formula $\forall x \,\mathrm{Reg}(x) = \forall x \exists \alpha\, (x \in V_\alpha)$.

Teorema 9.

Aksioma regularnosti je relativno neprotivrečna u odnosu na ostale aksiome teorije ZF.

Dokaz: Treba dokazati da je aksioma regularnosti relativno neprotivrečna u odnosu na teoriju ZF - Reg. S obzirom na rezultat prethodnog primera, treba pokazati da:

(a) ZF - Reg $\vdash \exists x \,\mathrm{Reg}(x)$,

(b) ZF - Reg $\vdash \varphi^{\mathrm{Reg}}$, za svaku aksiomu teorije ZF - Reg,

(c) ZF - Reg $\vdash (\forall x \,\mathrm{Reg}(x))^{\mathrm{Reg}}$.

Kako je klasa $V = \bigcup_{\alpha \in On} V_\alpha$ definisana rekurzijom u ZF - Reg, to znači da je V model teorije ZF definisan u teoriji ZF - Reg.

Kako je $0 \in V_1$, postoji x takvo da $\mathrm{Reg}(x)$, tj. ZF - Reg $\vdash \exists x \,\mathrm{Reg}(x)$.

Pokazaćemo da se relativizacija aksiome zamene i aksiome regularnosti na formulu $\mathrm{Reg}(x)$ mogu dokazati u ZF - Reg. Ostale aksiome se dokazuju primenom svojstava hijerarhije V_α koja su ranije dokazana.

Neka je $\varphi(x, y)$ formula jezika $\mathcal{L}_{ZF}$. Treba pokazati da, na osnovu pretpostavke $\mathrm{Reg}(u) \wedge \forall x \in u\, (\mathrm{Reg}(x) \to \exists^* y\, (\mathrm{Reg}(y) \wedge \varphi^{\mathrm{Reg}}))$, u teoriji ZF - Reg može se dokazati

$$\exists z\, (\mathrm{Reg}(z) \wedge \forall y\, (\mathrm{Reg}(y) \to (y \in z \leftrightarrow \exists x \in u\, (\mathrm{Reg}(x) \wedge \varphi^{\mathrm{Reg}})))).$$

Pretpostavimo da važi $\mathrm{Reg}(u)$. Otuda sledi da za svako $x \in u$, $\mathrm{Reg}(x)$, pa dakle $\forall x \in u\, \exists^* y\, (\mathrm{Reg}(y) \wedge \varphi^{\mathrm{Reg}})$.

Na osnovu aksiome zamene, postoji z takvo da

$$\forall y\, (y \in z \leftrightarrow \exists x \in u\, (\mathrm{Reg}(y) \wedge \varphi^{\mathrm{Reg}})).$$

U opštem slučaju, za svaki skup x važi $\forall y \in x \,\mathrm{Reg}(y) \to \mathrm{Reg}(x)$. Otuda, na osnovu prethodne relacije dobija se da važi $\mathrm{Reg}(z)$.

Iz istih razloga važi $\forall y\, (\mathrm{Reg}(y) \to (y \in z \leftrightarrow \exists x \in u\, \varphi^{\mathrm{Reg}}))$. Kako po pretpostavci važi $\mathrm{Reg}(u)$, zbog tranzitivnosti skupova oblika V_α, mora biti $\exists x \in u\, \varphi^{\mathrm{Reg}} \leftrightarrow \exists x \in u\, (\mathrm{Reg}(x) \wedge \varphi^{\mathrm{Reg}})$, pa konačno dobijamo

$$\forall y\, (\mathrm{Reg}(y) \to (y \in z \leftrightarrow \exists x \in u\, (\mathrm{Reg}(x) \wedge \varphi^{\mathrm{Reg}}))).$$

Uz uslov Reg(z), ovo poslednje zapravo znači da važi konsekvens aksiome zamene relativizovan na formulu Reg(x).

Proverićemo još i samu aksiomu regularnosti. U teoriji ZF - Reg treba dokazati da ako Reg(x) i $x \neq 0$, onda

$$\exists y \in x\,(\mathrm{Reg}(y) \land \forall z\,(\mathrm{Reg}(z) \land z \in y \to z \notin x)).$$

Neka je α najmanji rang svih elemenata skupa x i $y \in x$ takav da rang(y) $= \alpha$. Zbog tranzitivnosti skupova V_λ, važi Reg(y). Ako $z \in y$, onda rang(z) $< \alpha$, pa dakle, $z \notin x$. $\Box$

Za razliku od relativne neprotivrečnosti aksiome regularnosti u odnosu na ostale aksiome teorije ZF, relativna neprotivrečnost aksiome izbora ili hipoteze kontinuuma zahteva nešto jača sredstva od relativizacije. Pre nego što razvijemo takva sredstva, u sledećim primerima ilustrovaćemo specifičan položaj hipoteze o nedostižnom kardinalu u odnosu na teoriju ZFC. Naime, pokazaćemo da egzistencija nedostižnog kardinala nije dokaziva u teoriji ZFC, ali i više od toga, ne može se dokazati ni relativna neprotivrečnost egzistencije nedostižnog kardinala u odnosu na teoriju ZFC.

Primer 13. Ako je α granični ordinal, u V_α važe sve aksiome teorije ZF osim, eventualno, aksiome zamene. Pritom, ako važi aksioma izbora, onda u V_α važi AC.

Primer 14. Ako je κ nedostižan kardinal, V_κ je model teorije ZFC.

Kako je κ granični ordinal, osim aksiome zamene, sve aksiome teorije ZFC važe u V_κ. Za dokaz da u V_κ važi aksioma zamene dovoljno je pokazati da za svaku funkciju f, ako $\mathrm{dom}(f) \in V_\kappa$ i $\mathrm{codom}(f) \subseteq V_\kappa$, onda $f \in V_\kappa$.

Kako je κ nedostižan kardinal, $|V_\kappa| = \kappa$, pa za svako $x \in V_\kappa$, $|x| < \kappa$. Ako je f funkcija sa domenom $x \in V_\kappa$ i vrednostima u V_κ, onda $|f[x]| \leq |x| < \kappa$, pa kako je κ regularan kardinal, postoji $\alpha < \kappa$ takvo da $f[x] \subseteq V_\alpha$, što znači da $f \in V_\kappa$.

Primer 15. U teoriji ZFC ne može se dokazati egzistencija nedostižnog kardinala.

Ako je κ nedostižan kardinal, V_κ je model za ZFC, pa za svaki ordinal α, u V_κ važi "α je nedostižan kardinal" ako i samo ako α je zaista nedostižan kardinal. Otuda, ako je κ najmanji nedostižan kardinal,

$$V_\kappa \models \text{"ne postoji nedostižan kardinal"}.$$

Ako ne postoji nedostižan kardinal, onda je klasa V model teorije ZFC u kojem ne postoji nedostižan kardinal. Dakle, u teoriji ZFC ne može se dokazati egzistencija nedostižnog kardinala.

U sledećim primerima, formalizaciju rečenice "κ je nedostižan kardinal" u jeziku $\mathcal{L}_{ZF}$ označavaćemo sa $\mathrm{Nek}(\kappa)$.

Primer 16. Ne može se dokazati relativna neprotivrečnost egzistencije nedostižnog kardinala u odnosu na teorije ZFC.

Pretpostavimo da neprotivrečnost teorije ZFC implicira neprotivrečnost teorije $\mathrm{ZFC} + \exists\kappa\,\mathrm{Nek}(\kappa)$.

Na osnovu prethodnih primera i zbog stava potpunosti,

$$\mathrm{ZFC} + \exists\kappa\,\mathrm{Nek}(\kappa) \vdash \mathrm{Con}(\mathrm{ZFC}).$$

Ako ZFC nije protivrečna teorija, onda

$$\mathrm{ZFC} \vdash \mathrm{Con}(\mathrm{ZFC}) \to \mathrm{Con}(\mathrm{ZFC} + \exists\kappa\,\mathrm{Nek}(\kappa))$$

što konačno znači da

$$\mathrm{ZFC} + \exists\kappa\,\mathrm{Nek}(\kappa) \vdash \mathrm{Con}(\mathrm{ZFC} + \exists\kappa\,\mathrm{Nek}(\kappa)).$$

To bi značilo da se sredstvima rekurzivno aksiomatske teorije može dokazati njena sopstvena neprotivrečnost, što prema Gedelovoj teoremi nepotpunosti nije moguće.

Kasnije ćemo videti da hipoteza $\neg\exists\kappa\,\mathrm{Nek}(\kappa)$ jeste relativno neprotivrečna u odnosu na teoriju ZFC.

Ključni argument u dokazu relativne neprotivrečnosti i nezavisnosti aksiome izbora i hipoteze kontinuuma je *apsolutnost* skupovno-teorijskih pojmova.

Formula $\varphi(x_1, \ldots, x_n)$ jezika $\mathcal{L}_{ZF}$ je *apsolutna za model* M ako za proizvoljne $a_1, \ldots, a_n \in M$ važi

$$\varphi^M(a_1, \ldots, a_n) \;\;\Leftrightarrow\;\; \varphi(a_1, \ldots, a_n).$$

Primer 17. (a) Formula jezika $\mathcal{L}_{ZF}$, u kojoj su svi kvantifikatori ograničeni, apsolutna je za tranzitivne modele.

(b) Ako je formula φ u teoriji Σ ekvivalentna formuli sa ograničenim kvantifikatorima, φ je apsolutna za tranzitivne modele teorije Σ.

Neka je φ formula jezika $\mathcal{L}_{ZF}$ u kojoj su svi kvantifikatori ograničeni. Tvrđenje (a) dokazujemo indukcijom po složenosti formule φ. Jedini netrivijalan slučaj jeste formula oblika $\varphi = \exists x \in y\, \psi(x, y)$.

Pretpostavimo da važi φ^M, onda $\exists x \in M(x \in y \wedge \psi^M)$. Kako po induktivnoj pretpostavci ψ^M ako i samo ako ψ, to mora biti $\exists x \in y\, \psi(x, y)$, tj. važi formula φ.

Obratno, pretpostavimo da važi $\exists x \in y\, \psi(x, y)$. Zbog tranzitivnosti modela M, imamo $x \in M$. Po induktivnoj pretpostavci ψ^M ako i samo ako ψ, pa dakle važi $\exists x\, (x \in M \wedge x \in y \wedge \psi^M)$, tj. važi φ^M.

Primer 18. U tranzitivnim modelima važi aksioma ekstenzionalnosti.

Ovo tvrđenje sledi neposredno iz činjenice da se ekstenzionalnost izražava formulom u kojoj su svi kvantifikatori ograničeni:

$$(\forall z \in x\, (z \in y) \wedge \forall z \in y\, (z \in x)) \rightarrow x = y.$$

Primer 19. Formalizacije sledećih predikata u jeziku $\mathcal{L}_{ZF}$ su apsolutne za tranzitivne modele:

(a) $x = \{u, v\} \quad \Leftrightarrow \quad (u \in x) \wedge (v \in x) \wedge \forall z \in x\, (z = u \vee z = v)$.

(b) $x = (u, v) \quad \Leftrightarrow \quad \exists y \in x\, \exists z \in x\, (y = \{u\} \wedge z = \{u, v\}) \wedge \forall y \in x\, (y = \{u\} \vee y = \{u, v\})$.

(c) $x \subseteq y \quad \Leftrightarrow \quad \forall z \in x\, (z \in y)$.

Apsolutnost navedenih formula neposredno sledi iz ograničenosti svih kvantifikatora koji se u njima javljaju.

Definisani operacijski simboli i konstante jezika $\mathcal{L}_{ZF}$, su apsolutni za M ako su njihove definicione formule apsolutne za klasu M.

Ako je $A = \{x : \varphi(x)\}$ klasa skupova, sa A^M označavamo odgovarajuću klasu u modelu M, tj.

$$A^M = \{x \in M : \varphi^M(x)\}.$$

Za proizvoljnu klasu M, $V^M = M$ i $\emptyset^M = \emptyset$. Na osnovu apsolutnosti ordinala za tranzitivne klase, koju će mo dokazati u narednim primerima, ako je M tranzitivna klasa, $On^M = On \cap M$. Pritom, ako je M prava klasa, $On^M = On$, a ako je M skup, onda je On^M najmanji ordinal α takav da $\alpha \notin M$.

Ako je M tranzitivna klasa i $\varphi(x, y)$ formula jezika $\mathcal{L}_{ZF}$ takva da

$$\forall x \in M\, \forall y \in M\, \forall z \in M\, (\varphi^M(x, y) \wedge \varphi^M(x, z) \rightarrow y = z),$$

onda formula $\varphi(x, y)$ u modelu M određuje funkciju f^M takvu da za sve $x, y \in M$, $f^M(x) = y$ ako i samo ako $\varphi^M(x, y)$. Dakle, funkcija f je apsolutna za M ako:

(a) za svako $x \in M$, $f^M(x) \in M$, tj. f^M je funkcija u M,

(b) definiciona formula $\varphi(x, y)$ je apsolutna za M.

Apsolutnost skupovnih operacija poput $\cup x$, $P(x)$ ili tranzitivnog zatvorenja skupa X, tretiraćemo posebno.

Ako je $\varphi(x, y)$ formula jezika $\mathcal{L}_{ZF}$, $f(x) = \{y : \varphi(x, y)\}$ je *skupovna operacija*. U tranzitivnoj klasi M, za svako $x \in M$, neka je

$$f^M(x) = \{y \in M : \varphi^M(x, y)\}.$$

U opštem slučaju, za $x \in M$, ne mora biti $f^M(x) \in M$. Skupovna operacija f je apsolutna za M ako

(a) za svako $x \in M$, $f^M(x) \subseteq M$,

(b) definiciona formula φ je apsolutna za M.

Kada je zadovoljen uslov $f^M(x) \in M$, kažemo da je operacija f definisana u M. Postoje skupovne operacije koje su definisane u M, ali nisu apsolutne. U opšem slučaju, operacije koje zadovoljavaju uslov (b), odnosno, operacije čija je definiciona formula apsolutna za M, zadovoljavaju uslov $f^M(x) = f(x) \cap M$, za svako $x \in M$. Na primer, $P^M(x) = P(x) \cap M$.

Primer 20. Formalizacije sledećih predikata u jeziku $\mathcal{L}_{ZF}$ su apsolutne za tranzitivne modele:

(a) "x je prazan skup" $\Leftrightarrow$ $\forall y \in x\, (y \neq y)$,

(b) "x je tranzitivan skup" $\Leftrightarrow$ $\mathrm{tran}(x)$ $\Leftrightarrow$ $\forall y \in x\, (y \subseteq x)$,

(c) "x je ordinal" $\Leftrightarrow$ $\mathrm{tran}(x) \wedge \forall u \in x\, \forall v \in x\, (u \in v \vee v \in u \vee u = v)$
$\wedge\, \forall u \in x\, \forall v \in x\, \forall w \in x\, (u \in v \wedge v \in w \to u \in w)$,

(d) "x je granični ordinal" $\Leftrightarrow$ x je ordinal $\wedge\, \forall u \in x\, \exists v \in x\, (u \in v)$,

(e) "x je prirodan broj" $\Leftrightarrow$ x je ordinal $\wedge$ (x nije gran. ordinal $\vee$ $x = 0$)
$\wedge \forall u \in x\, (u = 0 \vee u$ nije granični ordinal$)$,

(f) $x = \omega$ $\Leftrightarrow$ x je gran. ordinal $\wedge$ $(x \neq 0) \wedge \forall u \in x\, u$ je prirodan broj.

Primer 21. Formalizacije sledećih predikata u jeziku $\mathcal{L}_{ZF}$ su apsolutne za tranzitivne modele:

(a) $x \times y = z$ $\Leftrightarrow$ $\forall u \in z\, \exists v \in x\, \exists w \in y\, (u = (v, w)) \wedge$
$\forall v \in x\, \forall w \in y\, \exists u \in z\, (u = (v, w))$,

(b) $x - y = z$ $\Leftrightarrow$ $\forall u \in z\, (u \in x \wedge u \notin y) \wedge \forall u \in x\, (u \notin y \to u \in z)$

(c) $x \cap y = z$, $y = \cup x$,

(d) $y \in \mathrm{dom}(x)$ $\Leftrightarrow$ $\exists z \in x\, \exists u \in z\, \exists v \in u\, (z = (y, v))$,

(e) $\forall y \in \mathrm{dom}(x)\, \varphi$ $\Leftrightarrow$ $\forall z \in x\, \forall u \in z\, \forall y, v \in u\, (z = (y, v) \to \varphi)$, gde je φ formula u kojoj su svi kvantifikatori ograničeni.

Tvrđenja (e) važi i u slučaju egzistencijalnog kvantifikatora. Takođe, tvrđenja (d) i (e) važe u slučaju formule $\mathrm{codom}(x)$.

Primer 22. Formalizacije sledećih predikata u jeziku $\mathcal{L}_{ZF}$ su apsolutne za tranzitivne modele:

(a) "x je relacija" $\;\Leftrightarrow\;$ $\forall y \in x\, \exists u \in \mathrm{dom}(x)\, \exists v \in \mathrm{codom}(x)\, (y = (u, v))$,

(b) "f je funkcija" $\;\Leftrightarrow\;$ f je relacija $\wedge\ \forall x \in \mathrm{dom}(f)\, \forall y, z \in \mathrm{codom}(f)$
$(\exists u \in f\, u = (x, y)\ \wedge\ \exists v \in f\, v = (x, z) \to y = z)$,

(c) $\mathrm{mono}(f)$ $\;\Leftrightarrow\;$ $\mathrm{fun}(f) \wedge \forall x, y \in \mathrm{dom}(f)\, \forall z \in \mathrm{codom}(f)$
$(\exists u \in f\, (x, z) = u\ \wedge\ \exists v \in f\, (y, z) = v \to y = x)$,

(d) $g = f \restriction x$ $\;\Leftrightarrow\;$ $\mathrm{fun}(f)\ \wedge\ g \subseteq f\ \wedge\ \forall y \in \mathrm{dom}(g)$,
$(y \in x)\ \wedge\ \forall y \in x\, (y \in \mathrm{dom}(g) \to y \in \mathrm{dom}(f))$.

Primer 23. U opštem slučaju, pojam kardinala nije apsolutan za tranzitivne modele. Na primer, poznato je da sledeće formule nisu apsolutne za tranzitivne modele: $y = P(x)$, $|x| = |y|$, "α je kardinal", $\beta = \mathrm{cf}(\alpha)$ i "α je regularan kardinal".

Primer 24. (a) Ako je M tranzitivan model, za sve $x, y \in M$,

$$M \models |x| \leq |y| \ \ \Rightarrow\ \ |x| \leq |y|.$$

(b) Ako je M tranzitivan model, za svako $\alpha \in M$,

$$\alpha \text{ je kardinal} \ \ \Rightarrow\ \ M \models \alpha \text{ je kardinal}.$$

Formula $|x| \leq |y|$ ima oblik $\exists f\, \varphi(x, y, f)$, gde je $\varphi(x, y, f)$ formalizacija predikata "f je obostrano jednoznačna funkcija sa domenom x i kodomenom $\subseteq\ y$". Na osnovu prethodnih primera, formula $\varphi(x, y, f)$ je apsolutna za tranzitivne modele, pa ako $M \models |x| \leq |y|$, onda postoji $f \in M$ takvo da $M \models \varphi(x, y, f)$. Zbog apsolutnosti, f zaista jeste obostrano jednoznačna funkcija skupa x u skup y, pa zaista važi formula $|x| \leq |y|$.

U jeziku $\mathcal{L}_{ZF}$, predikat "α je kardinal" izaražava se sledećom formulom $\neg\exists f\, (\exists \beta \in \alpha \wedge \varphi(\alpha, \beta, f)$. Ako $\alpha \in M$ i ako u M ne važi formula "α je kardinal", onda postiji $f \in M$ takvo da $M \models \exists \beta < \alpha \wedge \varphi(\alpha, \beta, f)$. Zbog apsolutnosti, to znači da α nije kardinal.

Primer 25. Ako je $\varphi(x, x_1, \ldots x_n)$ formula jezika $\mathcal{L}_{ZF}$ sa ograničenim kvantifikatorima i M standardni model, onda za sve $x_1, \ldots, x_n \in M$,

$$\text{(a) } M \models \exists x\, \varphi(x, x_1, \ldots, x_n) \ \ \Rightarrow\ \ \exists x\, \varphi(x, x_1, \ldots, x_n),$$
$$\text{(b)} \forall x\, \varphi(x, x_1, \ldots x_n) \ \ \Rightarrow\ \ M \models \forall x\, \varphi(x, x_1, \ldots x_n).$$

Primer 26. Neka je M tranzitivan model teorije ZF i $g : V \to V$ operacija koja je apsolutna za M. Ako za svako $\alpha \in On$, $f(\alpha) = g(f \restriction \alpha)$, onda je funkcija f apsolutna za model M i $\mathrm{dom}(f) = On^M$.

Dakle, pod navedenim uslovima, funkcija f definisana rekurzijom je apsolutna za tranzitivne modele. Funkcija f definisana je tako da za svako α i svaki skup y, $y = f(\alpha)$ ako i samo ako $\exists z\, \varphi(z, \alpha, y)$, gde je

$$\varphi(z, \alpha, y) = \mathrm{fun}(z) \wedge \mathrm{dom}(z) = \alpha \wedge \forall \xi < \alpha\, z(\xi) = g(z \restriction \xi) \wedge y = g(z)$$

Kako je M tranzitivan model za ZF, operacija $S(x, y) = x \restriction y$ apsolutna za M i definisana u M, zbog ograničenosti svih kvantifikatora koji se u njoj javljaju, formula $\varphi(x, \alpha, y)$ apsolutna za M.

Otuda, ako $y = f^M(\alpha)$, postoji $x \in M\, \varphi(x, \alpha, y)$, pa dakle $y = f(\alpha)$. To znači da je f^M funkcija u modelu M.

Treba još pokazati da, ako $\alpha \in M$ i $y = f(\alpha)$, onda $y \in M$ i $y = f^M(\alpha)$. Na osnovu teoreme rekurzije, ako je g zadato, za svako α postoji funkcija x definisana na α takva da za sve $\xi < \alpha$, $x(\xi) = g(x \restriction \xi)$. Kako je M model za ZF, u M važi $\exists x\, \varphi(x, \alpha, y)$, pa ako je $y = g(x)$, onda $y = f^M(\alpha) = f(\alpha)$.

Primer 27. (a) Neka je M tranzitivan model za ZF i g operacija apsolutna za M takva da za svako $x \in M$, $g(x) \in M$. Ako je funkcija f definisana na ω takva da $f(0) = a_0$ i za sve $n \geq 0$, $f(n+1) = g(f(n))$, onda $f \in M$.

(b) Operacije sabiranja i množenja ordinala su apsolutne za tranzitivne modele teorije ZF.

Primer 28. (a) Tranzitivno zatvorenje $\mathrm{tr}(x)$ je apsolutna operacija za tranzitivne modele teorije ZF.

(b) Predikat "x je konačan skup" je apsolutan za tranzitivne modele teorije ZF.

Ako je M tranzitivan model za ZF, onda je $V_\omega \subseteq M$, pa su konačni skupovi apsolutni za M.

Primer 29. (a) Ako je M tranzitivan model, $P^M(x) = P(x) \cap M$, za svako $x \in M$, ali operacija $P(x)$ nije apsolutna za tranzitivne modele ZF.

(b) Ako je M tranzitivan model za ZF, operacija $f(\alpha) = V_\alpha$ je definisana u M i za svaki ordinal α, $V_\alpha^M = V_\alpha \cap M$.

Relacija $V_\alpha^M = V_\alpha \cap M$ dokazuje se transfinitnom indukcijom. U graničnom slučaju koristimo apsolutnost operacije $\cup x$.

Primer 30. (a) Ako je α granični ordinal, u V_α važe sve aksiome ZF osim aksioma zamene i beskonačnosti.

(b) Ako je $\alpha > \omega$, u V_α važi aksioma beskonačnosti.

Model teorije ZF u pravom smislu te reči, čiji je domen skup, nije moguće konstruisati sredstvima teorije ZF. Međutim, za svaki konačan skup

$\varphi_1, \ldots, \varphi_n$ aksioma teorije ZF, u teoriji ZF može se dokazati da postoji tranzitivan skup M u kojem važe aksiome $\varphi_1, \ldots, \varphi_n$.

Drugačije rečeno, za svaku formulu φ, ako φ važi u univerzumu svih skupova, onda svaki skup ima proširenje u kojem važi φ. Dakle ne postoji svojstvo univerzuma koje ga razlikuje od proširenja njegovih elemenata. Iz tog razloga, ova činjenica naziva se *teoremom refleksije*.

Na prvi pogled može se pomisliti da iz teoreme refleksije sledi neprotivrečnost ZF. Ako svaki konačan skup aksioma teorije ZF ima model, prema stavu kompaktnosti to bi trebalo da znači da ZF ima model.

Međutim, teorema refleksije tvrdi samo da za svaki konačan skup aksioma $\varphi_1, \ldots, \varphi_n$ teorije ZF,

$$\mathrm{ZF} \vdash \exists a \, \mathrm{Mod}(\ulcorner \varphi_1 \wedge \cdots \wedge \varphi_n \urcorner, a).$$

Ako je $F_{ZF} \subseteq F$ skup kodova aksioma teorije ZF, stav kompaktnosti mogao bi se primeniti samo pod uslovom da važi

$$ZF \vdash \forall s \subseteq F_{ZF} \, (\mathrm{Fin}(s) \to \exists a \, \mathrm{Mod}(\ulcorner \textstyle\bigwedge_{\ulcorner \varphi \urcorner \in s} \varphi \urcorner, a)).$$

Ako iz činjenice da niz formula $\varphi_1, \ldots, \varphi_n$ sadrži formulu φ sledi da on sadrži i sve potformule formule φ, onda ćemo reći da je niz $\varphi_1, \ldots, \varphi_n$ *zatvoren za potformule*.

Primer 31. Ako je $\varphi_1, \ldots, \varphi_n$ niz formula zatvoren za potformule, za svaku klasu M, sledeći uslovi su ekvivalentni:

(a) Formule $\varphi_1, \ldots, \varphi_n$ su apsolutne za M i

(b) Ako je φ_i oblika $\exists x \, \varphi_j(x, x_1, \ldots, x_n)$, onda za sve $x_1, \ldots, x_n \in M$,

$$\exists x \, \varphi_j(x, x_1, \ldots, x_n) \to \exists x \in M \, \varphi_j(x, x_1, \ldots, x_n).$$

Da uslov (a) implicira (b) sledi neposredno iz pretpostavke o apsolutnosti formula φ_i i zatvorenosti datog niza za potformule. Neka su $a_1, \ldots, a_k \in M$ takvi da važi pretpostavka $\exists x \, \varphi_j(x, a_1, \ldots, a_k)$ uslova (b). Na osnovu uslova (a) redom se dobija:

$$\begin{array}{rcl} \exists x \, \varphi_j(x, a_1, \ldots, a_k) & \Leftrightarrow & \varphi_i(a_1, \ldots, a_k), \\ & \Leftrightarrow & \varphi_i^M(a_1, \ldots, a_k), \\ & \Leftrightarrow & \exists x \in M \, \varphi_j^M(x, a_1, \ldots, a_k), \\ & \Leftrightarrow & \exists x \in M \, \varphi_j(x, a_1, \ldots, a_k). \end{array}$$

Obratna implikacija dokazuje se indukcijom po složenosti formula φ_i. Pretpostavimo da važi uslov (b) i da sve formule manje složenosti od φ_i zadovoljavaju uslov (a). Ako je φ_i elementarna formula, oblika $\varphi_i = \varphi_j \wedge \varphi_k$ ili $\varphi_i = \neg \varphi_j$, uslov (a) za formulu φ_i dobija se neposredno po induktivnoj pretpostavci.

Pretpostavimo da je φ_i oblika $\exists x\, \varphi_j(x, x_1, \dots x_k)$. Za sve $a_1, \dots, a_k \in M$,

$$\begin{array}{rcl} \varphi_i^M(a_1, \dots a_k) & \Leftrightarrow & \exists x \in M\, \varphi_j^M(x, a_1, \dots a_k), \\ & \Leftrightarrow & \exists x \in M\, \varphi_j(x, a_1, \dots a_k), \\ & \Leftrightarrow & \exists x\, \varphi_j(x, a_1, \dots a_k), \\ & \Leftrightarrow & \varphi_i(x, a_1, \dots a_n). \end{array}$$

Pritom smo koristili definiciju relativizacije, apsolutnost formule φ_j i primenili uslov (b).

Teorema 10. Za proizvoljne formule $\varphi_0, \dots, \varphi_n$ jezika $\mathcal{L}_{ZF}$ u kojima su sve slobodne promenljive neke od promenljivih $x_1, \cdots, x_n$, u teoriji ZF može se dokazati da za svako α, postoji $\beta > \alpha$ takvo da za sve $x_1, \dots x_n \in V_\beta$,

$$(\varphi_1 \leftrightarrow \varphi_1^{V_\beta}) \wedge \cdots \wedge (\varphi_n \leftrightarrow \varphi_n^{V_\beta}).$$

Dokaz: Možemo pretpostaviti da je niz formula $\varphi_0, \dots, \varphi_n$ zatvoren za potformule. Za svako $i \leq n$, definišimo funkciju $F_i : On \to On$ na sledeći način:

Ako je φ_i oblika $\exists x\, \varphi_j(x, x_1, \dots, x_k)$, neka je

$$G(x_1, \dots, x_n) = \begin{cases} 0 & \text{ako } \neg \exists x\, \varphi_j, \\ \text{najmanji } \eta\ \exists x \in V_\eta\, \varphi_j & \text{ako } \exists x\, \varphi_j. \end{cases}$$

Za svako ξ, neka je $F_i(\xi) = \sup\{G_i(x_1, \dots, x_k) : x_1, \dots, x_k \in V_\xi\}$. Prema aksiomi zamene, takav supremum uvek postoji. Ako formula φ_i nije oblika $\exists x\, \varphi_j$, neka je $F_i(\xi) = 0$.

Na osnovu prethodnog primera, ako je β granični ordinal takav da za svako $i \leq n$, $\forall \xi < \beta\, (F_i(\xi) < \beta)$, formule $\varphi_0, \dots, \varphi_n$ su apsolutne za V_β, tj. za sve $a_1, \dots, a_k \in V_\beta$,

$$\varphi_i(a_1, \dots, a_k) \leftrightarrow \varphi_i^{V_\beta}(a_1, \dots, a_k).$$

Tvrdimo da za svaki ordinal α postoji granični ordinal $\beta > \alpha$ koji zadovoljava navedeni uslov.

Neka je $\beta_0 = \alpha$ i za svako $m \in \omega$

$$\beta_{m+1} = \max\{\beta_m + 1, F_1(\beta_m), \dots, F_n(\beta_m)\}.$$

Neka je $\beta = \sup\{\beta_m : m \in \omega\}$. Po konstrukciji, β je granični ordinal i $\beta > \alpha$. Za svako $i \leq n$, $\xi < \xi'$ implicira $F_i(\xi) \leq F_i(\xi')$. Kako je β granični ordinal, ako $\xi < \beta$, postoji $m \in \omega$ takvo da $\xi < \beta_m$, što konačno znači da je $F_i(\xi) \leq F_i(\beta_m) \leq \beta_{m+1} < \beta$. $\square$

Primer 32. Teorija ZF nije konačno aksiomatska.

Kako se u tranzitivnim modelima predikatski simbol $\in$ interpretira pripadnošću i kako je u odnosu na takve modele veliki broj svojstava skupova apsolutan, tranzitivne modele smatramo prirodnim interpretacijama jezika $\mathcal{L}_{ZF}$.

U tom smislu značajno je da za svaki model $\mathcal{M} = (M, \varepsilon)$ u kojem važe aksiome ekstenzionalnosti i regularnosti, postoji jedinstveno određen tranzitivan model $\mathcal{N} = (N, \epsilon)$ izomorfan modelu $\mathcal{M}$.

Teorema 11. Za svaki model $\mathcal{M}$ jezika $\mathcal{L}_{ZF}$, u kome važe aksiome ekstenzionalnosti i regularnosti, postoji jedinstveno određen tranzitivan model $\mathcal{N}$ izomorfan sa $\mathcal{M}$ i odgovarajući izomorfizam je jedinstveno određen.

Dokaz: Pretpostavimo da u (M, ε) važi ekstenzionalnost i regularnosti. Za svako $x \in M$ neka je $f(x) = \{f(y) : y \in M \wedge (y \,\varepsilon\, x)\}$ i neka je $N = \{f(x) : x \in M\}$. Tvrdimo da je $\mathcal{M} \cong (N, \in)$

Po definiciji funkcije f, za sve $x, y \in M$, $y \varepsilon x$ implicira $f(y) \in f(x)$. Takođe, iz same definicije sledi da je N tranzitivna klasa.

Pretpostavimo da f nije obostrano jednoznačna funkcija. Kako u modelu $\mathcal{M}$ važi aksioma regularnosti, neprazna klasa

$$A = \{x \in M : \exists y \in M \, (x \neq y \wedge f(x) = f(y))\}$$

ima minimalni element $a \in A$ u odnosu na relaciju ε. Neka je $b \in A$ takvo da $a \neq b$. Kako u modelu $\mathcal{M}$ važi aksioma ekstenzionalnosti, moguća su dva slučaja: za neko $x \in M$, $(x \,\varepsilon\, a)$ i $\neg(x \,\varepsilon\, b)$ ili postoji $y \in M$, $\neg(y \,\varepsilon\, a)$ i $(y \,\varepsilon\, b)$.

U prvom slučaju, $f(x) \in f(a) = f(b)$, pa za neko $u \,\varepsilon\, b$, $f(x) = f(u)$ i pritom $x \neq u$, tj. $x \in A$, što protivreči izboru skupa a. Na isti način proverava se i druga mogućnost.

Jedinstvenost izomorfizma f sledi iz činjenice da tranzitivni modeli dopuštaju samo trivijalan automorfizam. $\Box$

Primer 33. Ako je $\mathcal{M} = (M, \in)$ model jezika $\mathcal{L}_{ZF}$ u kojem važi aksioma ekstenzionalnosti, postoji tranzitivan model $\mathcal{N} = (N, \in)$ izomorfan modelu $\mathcal{M}$ i odgovarajući izomorfizam je jedinstveno određen. U ovom slučaju, jedinstvenost izomorfizma dokazuje se indukcijom po rangu.

Neka je u netranzitivnan skup na kojem važi aksioma ekstenzionalnosti. Za svako $x \in u$, u opštem slučaju $x \cap u$ je pravi podskup skupa x. U suprotnom, ako za sve $x \in u$, $x = x \cap u$, skup u bi bio tranzitivan. Ako je $f : u \to v$ $\in$-izomorfizam na tranzitivan skup v, onda za svako $x \in u$, $f[x] = f[x] \cap v$. U skupu $f[x]$ sada nema elemenata koji nisu u $f[x] \cap v$. Iz tog razloga, model $\mathcal{N}$ nazivamo *tranzitivnim kolapsom* modela $\mathcal{M}$.

Primer 34. (a) Ako je ZF neprotivrečna teorija, formalizacija predikata "x je prebrojiv skup" nije apsolutna za tranzitivne modele teorije ZF.

(b) Konstanta $P(\omega)$, a time i operacija $P(x)$, nije apsolutna za tranzitivne modele teorije ZF.

Dokaz ovog tvrđenja može se dobiti formalizacijom argumenta koji se javlja u Skolemovom paradoksu. Intuitivno, ako je ZF neprotivrečna teorija, prema Skolemovoj teoremi, postoji prebrojiv model (a, ε) teorije ZF i postoji $a_0 \in a$ takvo da $(a, \varepsilon) \models \neg\text{preb}[a_0]$, gde je $\text{preb}(x)$ formalizacija predikata "x je prebrojiv skup".

Kako u modelu (a, ε) važe aksiome ekstenzionalnosti i regularnosti, njegov tranzitivni kolaps $(a^*, \in)$ je model za ZF. Ako je $a_0^* = \{x \in a : x \,\varepsilon\, a_0\}$, onda $(a^*, \in) \models \neg\text{preb}[a_0^*]$. Apsolutnost predikata $\text{preb}(x)$ značila bi da skup $a_0^* \subseteq a$ nije prebrojiv, što nije moguće.

Formalno, ako pretpostavimo da je predikat $\text{preb}(x)$ apsolutan za tranzitivne modele teorije ZF, onda postoji konačna konjunkcija φ aksioma teorije ZF takva da za svaki tranzitivan skup a i svako $x \in a$,

$$\varphi^a \to (\text{preb}^M(x) \leftrightarrow \text{preb}(x)).$$

Slično, ako je ψ konačna konjunkcija aksioma teorije ZF koje su dovoljne za dokaz Kantorove teoreme $\exists z\, \neg\text{preb}(z)$, onda za svaki tranzitivan skup $a \neq \emptyset$,

$$\psi^a \to (\exists z\, \neg\text{preb}(z))^a.$$

Ako je $\theta(x) = \text{tranz}(x) \;\wedge\; |x| = \omega \wedge\; \varphi^x \;\wedge\; \psi^x$, onda

$$\theta(x) \to (\exists z\, \neg\text{preb}(z))^x.$$

Prema teoremi refleksije, formula $\varphi \wedge \psi$ je apsolutna za model V_β, za neki ordinal β. Ako pretpostavimo aksiomu izbora, prema primeru u kojem smo formalizovali Skolemovu teoremu, za svaki prebrojiv skup $y \subseteq V_\beta$, postoji prebrojiv $x \supseteq y$ takav da $\text{Epm}(x, V_\beta)$. Kako u V_β važe aksiome ekstenzionalnosti i regularnosti, prebrojiv model $(x, \in_x)$ ima tranzitivan kolaps $(a, \in_a)$ koji je elementarno ekvivalentan sa V_β. Skup a je prebrojiv, tranzitivan i važe formule φ^a i ψ^a, pa dakle važi rečenica $\exists x\, \theta(x)$.

Kako $\theta(x) \to (\exists z\, \neg\text{preb}(z))^x$, važi $\exists x\, (\theta(x) \;\wedge\; \exists z \in x\, \neg\text{preb}^x(z))$.

Ako važi $\theta(x)$, skup x je neprazan, tranzitivan i važi φ^x, što znači da za svako $z \in x$, $\text{preb}^x(z)$ ako i samo ako $\text{preb}(z)$, pa dakle dobijamo da važi rečenica $\exists x\, (\theta(x) \;\wedge\; \exists z \in x\, \neg\text{preb}(z))$.

Takođe, ako važi $\theta(x)$, onda je x tranzitivan skup kardinalnosti ω, što konačno znači da važi $\exists x\,(|x| = \omega \ \wedge \ \exists z \subseteq x\,\neg\mathrm{preb}(z))$, pa je ZFC protivrečna teorija. Kako je ZFC relativno neprotivrečna u odnosu na ZF, otuda sledi i da je teorija ZF protivrečna.

Konstruktibilni skupovi

Kardinalnost skupa $P^M(\omega)$ u tranzitivnom modelu M teorije ZF koji zadovoljava CH je minimalna, pa ukoliko uopšte postoji takav model, operacija $P(x)$ morala bi biti jako restriktivna. U tom smislu, najprirodnije je da partitivni skup $P(a)$ shvatimo kao familiju definabilnih podskupova skupa a. Ako je a beskonačan skup, budući da formula jezika $\mathcal{L}_{ZF}$ ima samo prebrojivo mnogo, tako shvaćena konstrukcija partitivnog skupa drastično bi se razlikovala od odgovarajuće konstrukcije u klasi V i nije uopšte jasno da li ona ima sva svojstva izražena aksiomama teorije ZF.

Neka je a proizvoljan skup. Skup $b \subseteq$ je *definabilan* podskup skupa a ako postoji formula $\varphi(x, x_1, \ldots, x_n)$ jezika $\mathcal{L}_{ZF}$ takva da

$$b = \{x \in a : \exists a_1, \cdots, a_n \in a\ (a, \in_a) \models \varphi[x, a_1, \cdots a_n]\}.$$

Na prvi pogled, ova definicija nema smisla budući da formula koja definiše skup b nije formula jezika $\mathcal{L}_{ZF}$. Međutim, ako se izraz $(a, \in_a) \models \varphi$ shvati kao oznaka formalizacije relacije zadovoljenja u jeziku $\mathcal{L}_{ZF}$, skup b je zaista definisan formulom ovog jezika, a u tom slučaju njegovu egzistenciju garantuje aksiomi separacije.

Sa $D(a)$ označavamo skup svih definabilnih podskupova skupa a.

Primer 1. Skup $D(a)$ definabilnih podskupova skupa a može se formalno izraziti na sledeći način:

$$\begin{aligned} y \in D(a) \quad \Leftrightarrow \quad & y = \emptyset \ \vee \ y \subseteq a \ \wedge \\ & \exists v \in F\ \exists x \in a^\omega\ y = \{z \in a : \mathrm{Sat}(x(0/z), v, a)\}. \end{aligned}$$

Dakle, ako $a \neq \emptyset$, skup $D(a)$ sadrži sve podskupove skupa a koji su u modelu $(a, \in_a)$ definisani kodom $v \in F$ formule jezika $\mathcal{L}_{ZF}$, sa valuacijom parametara $x \in a^\omega$ u skupu a.

Teorema 12. Za svaku formulu φ jezika $\mathcal{L}$, čije su slobodne promenljive neke od promenljivih $v_0, \ldots, v_n$, u teoriji ZF može se dokazati da za svaki neprazan skup a i sve $a_1, \ldots, a_n \in a$,

$$y = \{z \in a : \varphi^a(z, a_1, \ldots, a_n)\} \quad \Rightarrow \quad y \in D(a).$$

Dokaz: Ako je $y = \{z \in a : \varphi^a(z, a_1, \ldots, a_n)\}$, za neke $a_1, \ldots, a_n \in a$, definišimo valuaciju $x \in a^\omega$ tako da

$$x(k) = \begin{cases} a_k & \text{ako } k \leq n, \\ 0 & \text{ako } n < k. \end{cases}$$

Za svako $z \in a$, $\mathrm{Sat}(x(0/z), \ulcorner\varphi\urcorner, a) \leftrightarrow \varphi^a(z, a_1, \ldots, a_n)$, pa kako je relacija $\ulcorner\varphi\urcorner \in F$ dokazivo u ZF, mora biti $y \in D(a)$.

Kako svaka formula sadrži konačan broj slobodnih promenljivih, valuacije uvek možemo shvatiti na način kako su definisane u prethodnom primeru, odnosno, kao nizove $x \in a^\omega$ čiji su svi elementi, počev od nekog $n \in \omega$, jednaki nuli. To zapravo znači da su svi sintaksni i semantički objekti jezika $\mathcal{L}_{ZF}$ kodirani konačnim nizovima prirodnih brojeva.

Primer 2. Svaki skup a zadovoljava sledeće uslove:

(a) $D(a) \subseteq P(a)$,

(b) ako je a tranzitivan skup, $a \subseteq D(a)$,

(c) za svako $x \subseteq a$, $|x| < \omega$ implicira $x \in D(a)$,

(d) ako pretpostavimo AC, $a \geq \omega$ implicira $|D(a)| = |a|$.

Na osnovu definicije, jasno je da $D(a) \subseteq P(a)$. Ako se prethodni primer primeni na formulu $x \in y$, onda za svako $y \in a$, $\{x \in a : x \in y\} \in D(a)$. Kada je a tranzitivan skup, to znači da za svako $y \in a$, $y \in D(a)$.

Zbog apsolutnosti predikata "x je konačan skup" za tranzitivne modele teorije ZF, ako $x \subseteq a$ zaista jeste konačan skup, onda (x je konačan skup)^a, pa prema prethodnoj teoremi $x \in D(a)$.

Za svako $x \in a$, $\{x\} \in D(a)$, pa je $|a| \leq |D(a)|$. Na osnovu aksiome izbora, ako je $|a| \geq \omega$, $|\bigcup_{n\in\omega} a^n| = |a|$, pa kako je skup F kodova formula jezika $\mathcal{L}_{ZF}$ prebrojiv, $|D(a)| \leq |a|$.

Transfinitnom rekurzijom definišemo niz skupova $(L_\alpha, \alpha \in On)$ tako da:

$$\begin{aligned} &L_0 = \emptyset, \\ &L_{\alpha+1} = D(L_\alpha), \text{ za svaki ordinal } \alpha, \\ &L_\alpha = \textstyle\bigcup_{\beta<\alpha} L_\beta, \text{ za svaki granični ordinal } \alpha. \end{aligned}$$

Neka je $L = \bigcup_{\alpha\in On} L_\alpha$. Elemente klase L nazivaćemo konstruktibilnim skupovima. Dakle, skup x je *konstruktibilan* ako postoji $\alpha \in On$ takav da $x \in L_\alpha$. Predikat "x je konstruktibilan skup" označavamo sa $L(x)$.

Većina rezultata koji se mogu dokazati za skupove oblika V_α važe i u slučaju skupova L_α, što je ilustrovano u sledećim primerima.

Primer 3. Za svako $\alpha < \beta$, $L_\alpha \subseteq L_\beta$ i $L_\alpha \subseteq L_\beta$.

Ako je $\alpha < \beta$, po definiciji $L_\alpha \subseteq L_\beta$. Da dokažemo $L_\alpha \in L_\beta$ dovoljno je dokazati da važi $L_\alpha \in D(L_\alpha)$, za svaki ordinal α. Ako je $L_\alpha = \emptyset$, onda $L_\alpha \in \{\emptyset\} = D(L_\alpha)$.

Ako je $L_\alpha \neq \emptyset$, onda $L_\alpha = \{x \in L_\alpha : (x = x)^{L_\alpha}\}$, pa na osnovu prethodne teoreme, $L_\alpha \in D(L_\alpha)$.

Primer 4. Za svaki ordinal α, L_α je tranzitivan skup.

Ako je $v \in L_\alpha$, onda za neko $\beta < \alpha$, $v \in D(L_\beta)$, što znači da je $v \subseteq L_\beta$. Dakle, za svako $u \in v$, $u \in L_\beta$, tj. prema prethodnom primeru $u \in L_\alpha$.

Prema definiciji skupova tipa L_α, ako $x \in L$, najmanji ordinal α za koji $x \in L_\alpha$ mora biti naslednik, pa stoga za svako $x \in L$, konstruktibilni rang skupa x je najmanji ordinal $\lambda(x)$ za koji je $x \in L_{\alpha+1}$.

Primer 5. (a) Za svaki ordinal α, $L_\alpha = \{x \in L : \lambda(x) < \alpha\}$.

(b) Za svaki ordinal α, $\alpha \in L$ i $\lambda(\alpha) = \alpha$.

(c) Za svaki ordinal α, $L_\alpha \bigcap On = \alpha$.

(d) Za svaki ordinal α, $L_\alpha \in L_{\alpha+1}$.

Ako $x \in L$ i $\lambda(x) < \alpha$, onda $x \subseteq L_{\lambda(x)+1}$, pa $x \in L_{\lambda(x)+1} \subseteq L_{alpha}$, tj. važi tvrđenje (a). Primetimo da konstruktibilni podskupovi skupa L_α nisu obavezno elementi skupa $L_{\alpha+1}$. Prema tvrđenju (b), u slučaju ordinala to jeste slučaj. Kako (b) sledi neposredno iz (c), ostaje da dokažemo tvrđenje (c).

Ako je α granični ordinal ili nula, tvrđenje (c) je trivijalno zadovoljeno, pa stoga pretpostavimo da je $\alpha = \beta + 1$ i da važi $L_\beta \bigcap On = \beta$.

Kako je $L_\beta \subseteq L_\alpha \subseteq P(L_\beta)$, imamo $\beta \subseteq L_\alpha \bigcap On \subseteq \alpha$, pa treba još dokazati $\beta \in L_\alpha$. Kako smo ranije pokazali, postoji formula $\varphi(x)$ sa ograničenim kvantifikatorima takva da za svaki skup x,

$$\varphi(x) \quad \Leftrightarrow \quad \text{"}x \text{ je ordinal"} \; .$$

Kako su formule sa ograničenim kvantifikatorima apsolutne za tranzitivne skupove, $\beta = L_\beta \bigcap On = \{x \in L_\beta : \varphi^{L_\beta}(x)\}$. Otuda se dobija da važi $\beta \in D(L_\beta)$, pa na osnovu prethodne teoreme, $\beta \in L_\alpha$.

Konačno, $L_\alpha = \{x \in L_\alpha : (x = x)^{L_\alpha}\}$, pa dakle $L_\alpha \in D(L_\alpha)$. Na osnovu prethodne teoreme, to znači da je $L_\alpha \in L_{\alpha+1}$, što dokazuje tvrđenje (d).

Primer 6. Operacija $D(a)$ i formule $x = L_\alpha$, $x \in L_\alpha$ su apsolutne za tranzitivne modele teorije ZF.

Dokazaćemo apsolutnost definicione formule $u = D(a)$, a apsolutnost formula $x = L_\alpha$ i $x \in L_\alpha$ sledi iz apsolutnosti unije, operacije $D(a)$ i apsolutnosti rekurzije za tranzitivne modele teorije ZF.

Formalizacija predikata $u = D(a)$ u jeziku $\mathcal{L}_{ZF}$ je sledeća formula:

$$\begin{aligned} u = D(a) \quad \Leftrightarrow \quad & \emptyset \in u \ \wedge \ \forall y \in u \, [y \neq \emptyset \to y \subseteq a \\ & \wedge \exists v \in F \ \exists x \in a^{\omega} \ (y = \{z \in a : \mathrm{Sat}(x(0/z), v, a)\})] \\ & \wedge \ \forall v \in F \ \forall x \in a^{\omega} \ (\{z \in a : \mathrm{Sat}(x(0/z), v, a)\} \in u). \end{aligned}$$

Kako je skup F definisan rekurzijom i kako je $\mathrm{Sat}(x, v, a)$, apsolutna za tranzitivne modele ZF, formula $u = D(a)$ je apsolutna.

Za razliku od skupova V_α, skup $L_{\alpha+1}$ ne sadrži sve podskupove od L_α. Bez nekih dodatnih skupovno-teorijskih pretpostavki ne možemo tvrditi da su klase V i L jednake.

Primer 7. (a) Svaki konačan podskup od L_α pripada $L_{\alpha+1}$.
(b) Za svako $n \in \omega$, $L_n = V_n$ i $L_\omega = V_\omega$.
(c) Ako važi AC, za svako $\alpha \geq \omega$, $|L_\alpha| = |\alpha|$.

Dokazaćemo tvrđenje (c). Neka je $\alpha \geq \omega$. Kako je $\alpha \subseteq L_\alpha$, $|\alpha| \leq |L_\alpha|$. Obratnu nejednakost dokazujemo transfinitnom indukcijom.

Ako je $\alpha \geq \omega$ granični ordinal, onda $L_\alpha = \bigcup_{\beta<\alpha} L_\beta$. Prema induktivnoj pretpostavci, za svako $\beta < \alpha$, $|L_\beta| \leq |\alpha|$, pa kako je L_α unija $|\alpha|$ skupova kardinalnosti $\leq |\alpha|$, na osnovu aksiome izbora, $|L_\alpha| \leq |\alpha|$.

Ako je $\alpha \geq \omega$ i $\alpha = \beta + 1$, onda $|\alpha| = |\beta| = |L_\beta|$, pa kako je $L_\alpha = D(L_\beta)$, uz pretpostavku aksiome izbora važi $|L_\alpha \leq |\alpha|$. Napominjemo da se ovo tvrđenje može dokazati i bez aksiome izbora.

Na osnovu prethodnog primera, ako je $\omega < \alpha < \omega_1$, skup L_α je prebrojiv. Sa druge strane, za takve ordinale α, skup V_α je daleko od toga da bi mogao biti prebrojiv. Ima mnogo razloga za sumnju u pretpostavku da su svi podskupovi skupa ω konstruktibilni. Međutim, u teoriji ZFC ta sumnja ne može se dokazati. U odnosu na ZFC, nije protivrečno pretpostaviti da $P(\omega)$ nije konstruktibilan skup, ali je neprotivrečna i pretpostavka da su svi skupovi konstruktibilni.

Primer 8. Ako se pretpostavi aksioma izbora, za svaki ordinal $\alpha > \omega$,

$$|V_\alpha| = |L_\alpha| \quad \Leftrightarrow \quad \alpha = 2^{\aleph_\alpha}.$$

U dokazu relativne neprotivrečnosti hipoteze kontinuuma koristićemo teoremu refleksije sa klasu L. Isto kao u slučaju klase V, za svaki skup $x \in L$ i svako svojstvo klase L izraženo rečenicom jezika $\mathcal{L}_{ZF}$, postoji skup $ysupseteqx$ sa istim svojstvom. U dokazima teoreme refleksije, za klase V i L, nema praktično nikakve razlike.

Zapravo, ova teorema važi u svakoj klasi M koja zadovoljava sledeće uslove:

(a) Za svaki ordinal α, M_α je skup,
(b) $\alpha < \beta$ implicira $M_\alpha \subseteq M_\beta$,
(c) $M_\beta = \bigcup_{\alpha<\beta} M_\alpha$, ako je β granični ordinal,
(d) $M = \bigcup_{\alpha\in On} M_\alpha$.

Teorema 13. Ako su $\varphi_0, \ldots, \varphi_n$ formule jezika $\mathcal{L}_{ZF}$, u kojima su sve slobodne promenljive neke od promenljivih $x_1, \cdots, x_n$, u teoriji ZF može se dokazati da za svaki ordinal α, postoji $\beta > \alpha$ takvo da za sve $x_1, \ldots x_n \in L_\beta$,

$$(\varphi_1^L \leftrightarrow \varphi_1^{L_\beta}) \wedge \cdots \wedge (\varphi_n^L \leftrightarrow \varphi_n^{L_\beta}).$$

Dokaz: Ne umanjujući opštost možemo pretpostaviti da je niz formula $\varphi_0, \ldots, \varphi_n$ zatvoren za potformule. Slično dokazu teoreme refleksije za klasu V, koristimo činjenicu da za svaki ordinal α, model L_α je elementarni podmodel modela L u odnosu na nizove formula zatvorene za potformule:

Ako je $\varphi_1, \ldots, \varphi_n$ niz formula zatvoren za potformule, tvdrimo da su sledeći uslovi ekvivalentni:

(a) Za svaku formulu $\varphi_i(x_1, \ldots, x_k)$, $i = 1, \ldots, n$, čije su slobodne promenljive neke od promenljivuh $x_1, \ldots, x_k$, za svaki ordinal α i proizvoljne $a_1, \ldots, a_k \in L_\alpha$,

$$\varphi_i^L(a_1, \ldots, a_k) \;\;\Leftrightarrow\;\; \varphi_i^{L_\alpha}(a_1, \ldots, a_k).$$

(b) Ako je φ_i formula oblika $\exists x\, \varphi_j(x, x_1, \ldots, x_k)$, onda za proizvoljne $a_1, \ldots, a_k \in L_\alpha$

$$\exists x \in L\, \varphi_j^L(x, a_1, \ldots, a_k) \;\;\Rightarrow\;\; \exists x \in L_\alpha\, \varphi_j^L(x, a_1, \ldots, a_k)).$$

Neka je α ordinal i $a_1, \ldots, a_k \in L_\alpha$ takvi da važi pretpostavka tvrđenja (b), tj. $\exists x \in L\, \varphi_j^L(x, a_1, \ldots, a_k)$. Na osnovu (a), redom se diboja:

$$\begin{aligned}
\exists x \in L\, \varphi_j^L(x, a_1, \ldots, a_k) \;\;&\Leftrightarrow\;\; \varphi_i^L(a_1, \ldots, a_k),\\
&\Leftrightarrow\;\; \varphi_i^{L_\alpha}(a_1, \ldots, a_k),\\
&\Leftrightarrow\;\; \exists x \in L_\alpha\, \varphi_j^{L_\alpha}(x, a_1, \ldots, a_k),\\
&\Leftrightarrow\;\; \exists x \in L_\alpha\, \varphi_j^L(x, a_1, \ldots, a_k).
\end{aligned}$$

Obratna implikacija dokazuje se indukcijom po složenosti formula φ_i. Pretpostavimo da važi uslov (b) i da sve formule manje složenosti od φ_i zadovoljavaju uslov (a). Ako je φ_i elementarna formula, oblika $\varphi_i = \varphi_j \wedge \varphi_k$ ili $\varphi_i = \neg\varphi_j$, uslov (a) za formulu φ_i dobija se po induktivnoj pretpostavci.

Ako je φ_i formula oblika $\exists x\, \varphi_j(x, x_1, \ldots x_k)$, onda za sve $a_1, \ldots, a_k \in L_\alpha$,

$$\begin{aligned}
\varphi_i^{L_\alpha}(a_1, \ldots a_k) &\Leftrightarrow \exists x \in L_\alpha\, \varphi_i^{L_\alpha}(x, a_1, \ldots a_k), \\
&\Leftrightarrow \exists x \in L_\alpha\, \varphi_j^{L}(x, a_1, \ldots a_k), \\
&\Leftrightarrow \exists x \in L\, \varphi_j^{L}(x, a_1, \ldots a_k), \\
&\Leftrightarrow \varphi_i^{L}(x, a_1, \ldots a_n).
\end{aligned}$$

Vratimo se dokazu teoreme refleksije za klasu L. Za svako $i \leq n$, definišimo funkciju $F_i : On \to On$ na sledeći način:

Ako je φ_i oblika $\exists x\, \varphi_j(x, x_1, \ldots, x_k)$, neka je

$$G(x_1, \ldots, x_n) = \begin{cases} 0 & \text{ako } \neg\exists x \in L\, \varphi_j^L, \\ \text{najmanji } \eta,\ \exists x \in L_\eta\, \varphi_j^L & \text{ako } \exists x \in L\, \varphi_j^L. \end{cases}$$

Za svako ξ, neka je $F_i(\xi) = \sup\{G_i(x_1, \ldots, x_k) : x_1, \ldots, x_k \in L_\xi\}$. Prema aksiomi zamene, takav supremum uvek postoji. Ako formula φ_i nije oblika $\exists x\, \varphi_j$, neka je $F_i(\xi) = 0$.

Ako je β granični ordinal takav da za svako $i \leq n$, $\forall \xi < \beta\, (F_i(\xi) < \beta)$, onda formule $\varphi_0, \ldots, \varphi_n$ zadovoljavaju uslov (b), odnosno, to znači da važi uslov (a), pa za svako $i = 1, \ldots, n$ i proizvoljne $x_1, \ldots x_k \in L_\beta$,

$$\varphi_i^{L_\beta} \ \Leftrightarrow\ \varphi_i^L.$$

Tvrdimo da za svako α, postoji granični ordinal $\beta > \alpha$ koji zadovoljava navedeni uslov.

Neka je $\beta_0 = \alpha$ i $\beta_{m+1} = \max\{\beta_m + 1, F_1(\beta_m), \ldots, F_n(\beta_m)\}$, za sve $m \in \omega$. Neka je $\beta = \sup\{\beta_m : m \in \omega\}$. Po konstrukciji, ordinal β je granični i $\beta > \alpha$.

Za sve $i \leq n$, $\xi < \xi'$ implicira $F_i(\xi) \leq F_i(\xi')$. Otuda, ako $\xi < \beta$, onda postoji $m \in \omega$ takvo da $\xi < \beta_m$, što konačno znači da je $F_i(\xi) \leq F_i(\beta_m) \leq \beta_{m+1} < \beta$. $\square$

Teorema 14. Klasa L je model teorije ZF.

Dokaz: Treba dokazati da se sve relativizacije aksioma teorije ZF na klasu L mogu dokazati u ZF. Osim u slučaju aksiome separacije i zamene, principijelnih teškoća u proveravanju aksioma nema. Klasa L je i konstruisana tako da one budu zadovoljene. Stoga, dokazaćemo aksiomu separacije.

Neka je $\varphi(x)$ formula jezika $\mathcal{L}_{ZF}$ u kojoj z nije slobodna promenljiva. Formula $\varphi(x)$ moguće sadrži i slobodne promenljive različite od x koje tretiramo kao parametre.

U teoriji ZF treba dokazati da za svaki skup u važi

$$\exists z \in L\, \forall x \in L\, (x \in z \leftrightarrow \varphi^L \wedge x \in u).$$

Pretpostavimo da $u \in L$ i neka je $z = \{x \in u : \varphi^L\}$. Ako je α ordinal takav da $u \in L_\alpha$, prema teoremi refleksije za klasu L, postoji $\beta > \alpha$ takvo da za svako $x \in L_\beta$, $(\varphi^L \leftrightarrow \varphi^{L_\beta})$. Kako je $\alpha < \beta$, $L_\alpha \subseteq L_\beta$, pa dakle imamo da $u \in L_\beta$. Zbog tranzitivnosti skupa L_β, otuda sledi da je

$$z = \{x \in L_\beta : (x \in u \wedge \varphi)^{L_\beta}\}.$$

Skup z definisan je formulom relativizovanom na L_β, pa po definiciji skupova L_α, mora biti $z \in L_{\beta+1}$, što konačno znači da $z \in L$. $\square$

Tvrđenje da su svi skupovi konstruktibilni naziva se *aksiomom konstruktibilnosti*. Izražava se rečenicom $\forall x \exists \alpha\; x \in L_\alpha$ i označava sa $V = L$. Budući da je familija $(L_\alpha : \alpha \in On)$ definisana rekurzijom, aksioma konstruktibilnosti je zaista rečenica jezika $\mathcal{L}_{ZF}$.

Teorema 15. (a) Niz $(L_\alpha : \alpha \in On)$ je apsolutan za tranzitivne modele teorije ZF.

(b) Ako tranzitivan model M teorije ZF sadrži sve ordinale, predikat "x je konstruktibilan skup" je apsolutan za M i pritom $L^M = L$.

Dokaz: Neka je M tranzitivan model teorije ZF. Kako formula $x \in D(y)$ sadrži samo ograničene kvantifikatore, za svako $a \in M$, važi $D^M(a) = D(a)$ i kako je rekurzija apsolutne za tranzitivne modele teorije ZF, na osnovu definicije niza $(L_\alpha : \alpha \in On)$ sledi da za svako $\alpha \in M$, $L_\alpha^M = L_\alpha$, tj. važi tvrđenje (a).

Ako model M sadrži ordinale, niz $(L_\alpha^M : \alpha \in On)$ je definisan u M. Otuda, na osnovu apsolutnosti, za svaki skup x redom imamo

$$x \in L \;\Leftrightarrow\; \exists \alpha\, (x \in L_\alpha) \;\Leftrightarrow\; \exists \alpha\, (x \in L_\alpha^M) \;\Leftrightarrow\; x \in L^M,$$

što dokazuje tvrđenje (b). $\square$

Na osnovu tvrđenja (b), ako tranzitivan model M teorije ZF sadrži ordinale, onda $L \subseteq M$. Dakle, klasa L je najmanja tranzitivna prava klasa koja je model teorije ZF. Iz istog razloga dobija se i sledeća teorema.

Teorema 16. Aksioma $(V = L)$ je neprotivrečna u odnosu na teoriju skupova ZF.

Dokaz: Ako je $x \in L$, u modelu L važi "x je konstruktibilan skup". Kako je L model teorije ZF, na osnovu prethodne teoreme, to znači da u modelu L važi aksioma konstruktibilnosti. $\square$

Rezultati izloženi u prethodne dve teorema važe u odgovarajućem obliku i kada tranzitivan model M teorije ZF nije prava klasa i biće izloženi u sledećim primerima.

Primer 9. Za svaki skup x skup, neka je $\mathrm{On}(x) = x \cap On$. Ako je x tranzitivan skup, $\mathrm{On}(x)$ je najmanji ordinal koji ne pripada x.

Primer 10. Postoji konačna konjunkcija φ aksioma teorije ZF takva da za svaki tranzitivan skup M,

$$\varphi^M \quad \Rightarrow \quad L_{\mathrm{On}(M)} = L^M \text{ i } L^M \subseteq M.$$

Neka φ konjunkcija aksioma teorije ZF koje su dovoljne da se dokaže nepostojanje najvećeg ordinala i neka je M tranzitivan skup.

Ako pretpostavimo da važi φ^M, onda je $\mathrm{On}(M)$ granični ordinal, pa mora biti $L_{\mathrm{On}(M)} = \bigcup_{\alpha\in M} L_\alpha$.

Kako je $L^M = \{x \in M : \exists \alpha \in M\, (x \in L_\alpha)^M\}$, zbog apsolutnosti niza $(L_\alpha : \alpha \in On)$, imamo $L^M = \bigcup_{\alpha\in M} L_\alpha$, tj. $L_{\mathrm{On}(M)} = L^M$ i jasno, $L^M \subseteq M$.

Primer 11. Postoji konačna konjunkcija ψ aksioma teorije $ZF+(V = L)$ takva da, za svaki tranzitivan skup M, ako važi ψ^M, onda $M = L_{\mathrm{On}(M)}$.

U odnosu na konjunkciju φ iz prethodnog primera, konačna konjunkcija ψ sadrži i aksiomu konstruktibilnosti.

Primer 12. Ako teorija ZF nije protivrečna, onda ZF ima prebrojiv *minimalni model*.

Po pretpostavci, postoji tranzitivan model za ZF. Na osnovu prethodnog primera, postoji ordinal ξ za koji je L_ξ model Teorije ZF. Neka je ξ_0 najmanji takav ordinal. Model L_{ξ_0} ne sadrži pravi podmodel u kojem važi ZF.

Na osnovu Skolemove teoreme, postoji prebrojiv model za ZF. Njegov tranzitivni kolaps je prebrojiv model za ZF i sadrži L_{ξ_0}.

Primer 13. Ne postoji tranzitivan model teorije $ZF + (V \neq L)$.

Treba dokazati da ne postoji tranzitivan model M teorije ZF takav da u ZF važi $V \neq L^M$. Pretpostavimo suprotno, tj. neka je $M = \{x : \varphi(x)\}$ tranzitivan model za ZF u kojem važi $V \neq L$.

Ako je $N' = \{x \in L_{\xi_0} : \varphi^{L_{\xi_0}}(x)\}$ i N tranzitivni kolaps modela N', onda je N model za ZF u kome važi $V \neq L$. Kako je L_{ξ_0} minimalni model za ZF, mora biti $N = L_{\xi_0}$, tj. u N važi $V = L$, što nije moguće.

Ovaj rezultat pokazuje da se metoda tranzitivnih modela ne može koristiti u dokazu relativne neprotivrečnosti hipoteze $V \neq L$ u odnosu na teoriju ZF. Stoga, dokaz nezavisnosti aksiome konstruktibilnosti se zasniva na bitno drugačijoj ideji.

Teorema 17. U teoriji $ZF + (V = L)$ može se dokazati AC.

Dokaz: Rekurzijom po $\alpha \in On$ definisaćemo dobro uređenje $(L_\alpha, <_\alpha)$. Na osnovu aksiome konstruktibilnosti, za svaki skup x, postoji α takvo da $x \subseteq L_\alpha$, pa je $<_\alpha$ dobro uređenje skupa x.

Neka je $<_0 = \emptyset$ i za svaki granični ordinal α, $<_\alpha = \bigcup_{\beta<\alpha} <_\beta$.

Ako je $\alpha = \beta + 1$, uređenje $<_\beta$ proširujemo do dobrog uređenja $<_{\beta+1}$. Pretpostavimo da je $(\varphi_0, \varphi_1 \dots)$ numeracija svih formula jezika $\mathcal{L}_{ZF}$. Po definiciji, $x \in L_{\beta+1}$ ako postoji formula φ u $\mathcal{L}_{ZF}$ i $a_1, \dots, a_n \in L_\beta$ takvi da

$$x = \{y \in L_\beta : L_\beta \models \varphi(y, a_1, \dots, a_n)\}.$$

Za sve $x, y \in L_{\beta+1}$, $x \neq y$, ako $x, y \in L_\beta$ i $x <_\beta y$, onda $x <_{\beta+1} y$ ili ako $x \in L_\beta$ i $y \notin L_\beta$, onda $x <_{\beta+1} y$ i konačno, preostaje slučaj $x, y \in L_{\beta+1} - L_\beta$.

U poslednjem slučaju, postoje formule φ_i, φ_j koje definišu redom elemente $x, y \in L_{\beta+1} - L_\beta$. Ako je $i < j$, onda $x <_{\beta+1} y$ ili ako je $i = j$, onda postoji $n \geq 1$ i različiti nizovi $(x_1, \dots x_n)$, $(y_1, \dots y_n)$ elemenata iz L_β koji, kao vrednosti parametara u formuli φ_i, definišu redom elemente x i y. Ako u leksikografskom poretku $(x_1, \dots x_n) < (y_1, \dots y_n)$, onda $x <_{\beta+1} y$. $\square$

Teorema 18. U teoriji ZF + $(V = L)$ može se dokazati CH.

Dokaz: Pretpostavimo da je svaki skup konstruktibilan. Trvdimo da se tada može dokazati $P(L_\omega) \subseteq L_{\omega_1}$, tj. svaki podskup prirodnih brojeva je konstruisan na nekom prebrojivom nivou hijerarhije $(L_\alpha : \alpha \in On)$.

Ako to dokažemo, onda $P(\omega) \subseteq P(L_\omega) \subseteq L_{\omega_1}$, pa kako zbog $V = L$ važi aksioma izbora, imamo $2^\omega \leq |L_{\omega_1}| = \omega_1$, tj. važi hipoteza kontinuuma.

Neka je φ konačna konjunkcija aksioma ZF + $(V = L)$ koja sadrži aksiomu ekstenzionalnosti, takva da za svaki tranzitivan skup M,

$$\varphi^M \ \Rightarrow \ M = L_{\mathrm{On}(M)}.$$

Pretpostavimo da je $a \in P(L_\omega)$. Kako uz pretpostavku $V = L$ važi aksioma izbora, $|L_\omega \cup \{a\}| = \omega$. Na osnovu teoreme refleksije za klasu L, postoji $\alpha > \omega$ takvo da $(L_\omega \cup \{a\}) \subseteq L_\alpha$ i φ^{L_α}.

Kako konjunkcija φ sadrži aksiomu ekstenzionalnosti, koristeći Skolemovu teoremu i tranzitivni kolaps, dobijamo prebrojiv tranzitivan model M takav da $(L_\omega \cup \{a\}) \subseteq M$.

Skupovi L_α su apsolutni za tranzitivne modele, pa u modelu M važi φ^{L_α}. Kako su svi skupovi konstruktibilni, to znači da važi φ^M.

Otuda sledi da je $M = L_{\mathrm{On}(M)}$, a kako je M prebrojiv, $|L_{\mathrm{On}(M)}| < \omega_1$. To konačno znači da $a \in L_{\mathrm{On}(M)} \subseteq L_{\omega_1}$. $\square$

Konačno možemo zaključiti da ako teorija ZF nije protivrečna, onda je neprotivrečna i teorija ZF + AC + CH.

Primer 14. Poretkom koji je definisan na skupovima L_α određen je *kanonski poredak* svih konstruktibilnih skupova.

Ako je $\lambda(x)$ konstruktibilni rang skupa x, onda za sve $x, y \in L$,

$$x <_L y \;\Leftrightarrow\; \lambda(x) < \lambda(y) \vee (\lambda(x) = \lambda(y) \wedge x <_{\lambda(x)+1} y).$$

Primer 15. Restrikcija kanonskog poretka na skup konstruktibilnih realnih brojeva $R^L = R \cap L$ ima tip uređenja ω_1^L.

Primer 16. (a) Ako je κ slabo nedostižan kardinal, $L_\kappa = V_\kappa^L$

(b) L_κ je model teorije ZFC + $(V = L)$.

Dokaz je isti kao u slučaju modela V_κ. Treba samo primetiti da ako je κ regularan kardinal, onda (κ je regularan kardinal)^L. Slično, ako je κ slabo nedostižan kardinal, onda (κ je slabo nedostižan kardinal)^L.

Primer 17. Neka je $\mathrm{Snk}(\kappa)$ rečenica čiji je smisao "κ je slabo nedostižan kardinal". Ako je ZF neprotivrečna teorija, onda je neprotivrečna i teorija ZFC + CH + $\neg\exists\kappa\,\mathrm{Snk}(\kappa)$.

Na osnovu prethodnog primera, $M = \{x \in L : \forall\kappa\,(\mathrm{Snk}(\kappa)^L \to x \in L_\kappa)\}$ je model teorije ZFC + CH + $\neg\exists\kappa\,\mathrm{Snk}(\kappa)$.

Nezavisnost hipoteze kontinuma

Ako je rečenica $\neg\varphi$ relativno neprotivrečna u odnosu na teoriju Σ jezika $\mathcal{L}_{ZF}$, kažemo da je rečenica φ je *nezavisna* od teorije Σ.

Tehnički posmatrano, u dokazima relativne neprotivrečnosti AC ili CH ili Reg, polazeći od tranzitivnog modela M teorije ZF, formulom jezika $\mathcal{L}_{ZF}$ u modelu M definisali smo podmodel N u kojem važi odgovarajuća hipoteza. Egzistencija minimalnog modela teorije ZF pokazuje da se relativizacijom ne mogu dobiti modeli teorije ZF u kojima bi se potvrdila nezavisnost aksiome izbora ili hipoteze kontinuuma. Ukoliko uopšte postoje, takvi modeli bi se morali bitno razlikovati od tranzitivnih modela.

Metoda kojom se dokazuje nezavisnost hipoteza teorije skupova je u izvesnom smislu suprotna metodi tranzitivnih modela. Polazeći od prebrojivog tranzitivnog modela $\mathcal{M}$ teorije ZFC, konstruiše se njegovo proširenje $\mathcal{N}$, koje je takođe model za ZFC i u kojem ne važi CH ili neka druga skupovno-teoretska hipoteza. Samo proširenje podseća na algebarske konstrukcije poput ekstenzija polja ili slobodnih struktura, ali se u ovom slučaju odgovarajuća kongruencija koja obezbeđuje da širenjem nismo pokvarili polaznu strukturu znatno suptilnije definiše.

Intuitivno, ako je $\mathcal{M}$ prebrojiv tranzitivan model teorije ZFC, model u kojem ne važi CH dobija se proširivanjem modela $\mathcal{M}$ sa $\geq \aleph_2$ skupova prirodnih brojeva.

Pretpostavimo da je $x \in \omega$ jedan takav skup prirodnih brojeva. Zamislićemo skup x kao simbol koji treba opisati sredstvima modela $\mathcal{M}$. Kako očekujemo da $x \notin M$, to onda znači da se skup x ne može opisati formulom jezika $\mathcal{L}_{ZF}$. U suprotnom, ako bi postojala formula $\varphi(x)$ za koju je $x = \{n \in \omega : \varphi(n)\}$, to bi na osnovu aksiome separacije značilo da $x \in M$. Dakle, sredstvima teorije ZFC, odnosno njenog modela $\mathcal{M}$, novi skup prirodnih brojeva $x \notin M$ može se samo parcijalno opisati.

Ključna ideja Koenovog dokaza nezavisnosti hipoteze kontinuuma sastoji se u tome da je parcijalan opis novih elemenata dovoljan, odnosno, da skup x, kojim proširujemo model $\mathcal{M}$, može biti zadat kolekcijom njegovih aproksimacija.

Konačne nizove $P = \bigcup_{n\in\omega} 2^n$, uključujući i prazan niz, nazivaćemo *uslovima*. Uslov $p \in P$ shvatamo kao informaciju da li skup x sadrži određen prirodan broj. Ako je n-ti član niza $p \in P$ jednak 1, uslov p *forsira* formulu $n \in x$, a ako je n-ti član 0, uslov p forsira formulu $n \notin x$.

Primer 1. Ako je $p = (0,1,0,1,1)$, na osnovu uslova p znamo da $0 \notin x$, $1 \in x$, $2 \notin x$, $3 \in x$ i $4 \in x$. Pritom, za $n \geq 5$, uslov p ne daje nikavu informaciju o tome da li $n \in x$ ili $n \notin x$.

Dakle, ako važi uslov $p = (0,1,0,1,1)$, onda $0 \notin x \wedge 1 \in x$ i ovu relaciju označavamo sa $p \Vdash 0 \notin x \wedge 1 \in x$. Kažemo da uslov $p \in P$ *forsira* rečenicu $0 \notin x \wedge 1 \in x$ proširenog jezika $\mathcal{L}_{ZF} \cup \{x\}$.

Univerzum skupova koji se dobija proširivanjem modela $\mathcal{M}$ skupom x mora da sadrži skupove, čiju egzistenciju garantuju aksiome ZFC, koji nastaju skupovnim konstrukcijama nad skupom x i elementima modela $\mathcal{M}$. Na primer, to su skupovi poput $\omega - x$, $\omega \times x$ ili x^2. Pritom, svaki uslov nosi određenu količinu informacija i o takvim skupovima.

U opštem slučaju, činjenicu da informacija koju nosi uslov $p \in P$, determiniše važenje rečenice $\varphi(x)$, označavamo sa $p \Vdash \varphi(x)$. Intuitivno, ovu relaciju shvatamo kao uslovno tvrđenje: ako je skup x opisan uslovom p, onda x ima svojstvo $\varphi(x)$.

U prethodnom primeru to znači da važi $(0,1,0,1,1) \Vdash (1,3) \in x^2$ i $(0,1,0,1,1) \Vdash \{1,2\} \notin P(x)$. Kako skup x nije element modela $\mathcal{M}$, stanovnici tog sveta ne znaju da li je $1 \in x$, $2 \notin x$ i $3 \in x$, pa ne mogu odlučiti da li je $(1,3) \in x^2$, odnosno, da li je $\{1,2\} \notin P(x)$. Međutim, ako su inteligentna bića, stanovnici sveta $\mathcal{M}$ ipak znaju neka svojstva idelanog skupa x. Na primer, znaju da skup x nije konačan i da se razlikuje od svakog skupa prirodnih brojeva u njihovom svetu $\mathcal{M}$.

Primer 2. (a) Za svako $p \in P$, važi $p \Vdash$ "x nije konačan skup".

(b) Za svako $a \subseteq \omega^M$ i svako $p \in P$, važi $p \Vdash (a \neq x)$.

Pretpostavimo da uslov $p = (0,1,0)$ forsira rečenicu čiji je smisao "skup x ima tačno 3 elementa". Ako je $q = (0,1,0,1,1,1)$, onda $q \supseteq p$ i q nosi više informacija o skupu x, pa dakle q forsira rečenicu "skup x ima tačno 3 elementa". Međutim, uslov q forsira da skup x ima četiri elementa, što nije moguće. Jasno je da za svako $p \in P$, uvek možemo napraviti uslov $q \supseteq p$ koji forsira da skup x sadrži bilo koji broj elemenata.

Pretpostavimo da uslov $p = (0,1,0)$ forsira $a = x$, za neko $a \subseteq \omega^M$. Kako je $\mathcal{M}$ tranzitivan model, $a \in M$, pa dakle znamo da li $3 \in a$ ili $3 \notin a$. Ako $3 \in a$, stavimo $q = (0,1,0,0)$. Kako $q \supseteq p$ nosi više informacija o skupu x, uslov q forsira $a = x$, što nije moguće zbog $q \Vdash 3 \notin x$.

Elemente uređenja $\mathcal{P}$ nazivaćemo uslovima. Uslovi $p, q \in P$ su *saglasni* ako postoji $r \in P$ takav da $r \leq p$ i $r \leq q$.

Skup $D \subseteq P$ je gust u uređenju $\mathcal{P}$ ako za svako $p \in P$, postoji $q \in D$ takvo da $q \leq p$. Neprazan skup $F \subseteq P$ je filter u uređenju $\mathcal{P}$ ako:

(a) za sve $q \in P$, $p \leq q$ i $p \in F$ implicira $q \in F$,

(b) ako $p, q \in F$, onda postoji $r \in F$ takvo da $r \leq p$ i $r \leq q$.

Skup uslova $G \subseteq P$ je *generički* nad modelom $\mathcal{M}$ ako zadovoljava uslove:

(a) G je filter u uređenju $\mathcal{P}$,

(b) za svaki gust skup $D \subseteq P$, ako $D \in M$, onda $G \cap D \neq \emptyset$.

Primer 3. Pretpostavimo da je $\mathcal{M}$ prebrojiv tranzitivan model za ZFC. Neka je $P = \bigcup_{n\in\omega} 2^n$ skup svih konačnih binarnih nizova i $(P, <)$ uređenje takvo da za $p, q \in P$, $q < p$ ako i samo ako $q \supseteq p$.

Ako je $G \subseteq P$ generički skup uslova u modelu $\mathcal{M}$, onda je $f = \bigcup G$ funkcija, $\mathrm{dom}(f) = \omega$ i $f \notin M$.

Kako je G filter u uređenju $\mathcal{P}$, to $f = \bigcup G$ zaista jeste funkcija.

Za svako $n \in \omega$, skup $D_n = \{p \in P : n \in \mathrm{dom}(p)\}$ je gust u uređenju $\mathcal{P}$ i $D_n \in M$. Kako je G generički skup uslova, $G \cap D_n \neq \emptyset$, pa postoji $p \in D_n$, $p \subseteq f$, tj. $n \in \mathrm{dom}(f)$.

Neka je $g \in 2^\omega$ funkcija koja pripada $\mathcal{M}$ i $D_g = \{p \in P : p \not\subseteq g\}$. Skup D_g je gust u uređenju $\mathcal{P}$, pa kako $D_g \in M$ imamo $G \cap D_g \neq \emptyset$, što konačno znači da je $f \neq g$.

Funkcija $f \in 2^\omega$ definisana u prethodnom primeru, jedinstveno određuje skup $x \subseteq \omega$ takav da $x \notin M$. Ukoliko uopšte postoji, generički skup uslova proširuje model $\mathcal{M}$ novim elementom x.

Neka je $\mathcal{M}$ prebrojiv tranzitivan model za ZFC i $\mathcal{D}$ familija podskupova uređenja $\mathcal{P}$. Filter $G \subseteq P$ je $\mathcal{D}$-*generički* nad modelom $\mathcal{M}$, ako za svaki gust skup $D \in \mathcal{D}$, $G \in M$ implicira $G \cap D \neq \emptyset$.

Sledeća varijanta teoreme o egzistenciji ultrafiltra koji kompletan za prebrojive familije supremuma, obezbeđuje egzistenciju generičkih skupova nad prebrojivim tranzitivnim modelima teorije ZFC.

Primer 4. Neka je $\mathcal{D}$ prebrojiva familija gustih skupova uređenja $\mathcal{P}$. Za svako $p \in P$, postoji $\mathcal{D}$-generički filter G u $\mathcal{P}$ takav da $p \in G$.

Neka je $(D_n : n \in \omega)$ numeracija familije $\mathcal{D}$. Neka je $p_0 = p$ i za svako $n \geq 1$, neka je $p_n \in P$ takvo da $p_n \leq p_{n-1}$ i $p_n \in D_n$.

Skup $G = \{q \in P : \text{ postoji } n \in \omega, q \geq p_n\}$ je $\mathcal{D}$-generički filter u $\mathcal{P}$ i pritom $p \in G$.

Primer 5. Neka je P skup svih konačnih nizova prebrojivih ordinala u prebrojivom tranzitivnom modelu $\mathcal{M}$ teorije ZFC. Za sve $p, q \in M$, neka je $q < p$ ako i samo ako $q \supseteq p$. Jasno, $\mathcal{P} = (P, <)$ je parcijalno uređenje i pritom $\mathcal{P} \in M$.

Neka je $G \subseteq P$ generički skup nad $\mathcal{M}$. Kako je G filter, $f = \bigcup G$ je funkcija. Za svako $n \in \omega$, skup $D_n = \{p \in P : n \in \mathrm{dom}(p)\}$ je gust u $\mathcal{P}$. Slično, za svako $\alpha < \omega_1^M$, skup $E_\alpha = \{p \in P : \alpha \in \mathrm{codom}(p)\}$ je gust u $\mathcal{P}$. Dakle, za svako $n \in \omega$, $G \cap D_n \neq \emptyset$ i za svako $\alpha \in \omega_1^M$, imamo $G \cap E_\alpha \neq \emptyset$. To znači da je $\mathrm{dom}(f) = \omega$ i $\mathrm{codom}(f) = \omega_1^M$.

Model $\mathcal{M}$ je zatvoren za operaciju unije, pa kako $f = \bigcup G$ i $f \notin M$, skup G ne pripada modelu $\mathcal{M}$. To pokazuje da u svakom tranzitivnom modelu $N \supseteq M$, koji sadrži G, ordinal ω_1^M postaje prebrojiv. Obično se kaže da je u takvom modelu kardinal ω_1^M kolabirao na ω.

Eventualni dokaz nezavisnosti hipoteze kontinuuma podrazumeva konstrukciju proširenja $\mathcal{N} \supseteq \mathcal{M}$ prebrojivog tranzitivnog modela $\mathcal{M}$ teorije ZFC u kojem skup $P(\omega)$ ima bar $\aleph_2^M$. U takvom modelu N važiće $\neg$CH ako kardinal $\aleph_2^M$ nije kolabirao u $\mathcal{N}$, odnosno, ako je $\aleph_2^M = \aleph_2^N$. Dakle, u dokazu nezavisnosti ključne su tri stvari:

(a) Proširivanjem prebrojivog tranzitivnog modela $\mathcal{M}$ teorije ZF generičkim skupom uslova G nad $\mathcal{M}$ dobija se model $\mathcal{M}[G]$ teorije ZFC. Generički skup G je element modela $\mathcal{M}[G]$ i klasa ordinala u $\mathcal{M}[G]$ je On^M. Ako je $\mathcal{N} \supseteq \mathcal{M}$ tranzitivan model teorije ZF takav da $G \in N$, onda $\mathcal{M}[G] \subseteq \mathcal{N}$.

(b) Ako je $\mathcal{M}$ prebrojiv tranzitivan model teorije ZFC, postoji parcijalno uređenje $\mathcal{P} \in M$ i generički skup uslova $G \subseteq P$ takav da model $\mathcal{M}[G]$ sadrži funkciju koja preslikava ω_2^M na skup 2^ω.

(c) U prebrojivom tranzitivnom modelu $\mathcal{M}$ teorije ZFC, može se definisati jezik $\mathcal{L}_G$ koje sadrži individualnu konstantu c_G, kao ime za generički skup i za svako $a \in M$, individualnu konstantu c_a, kao ime elementa $a \in M$. Formulama jezika $\mathcal{L}_G$ može se definisati konstanta svakog potencijalnog elementa generičkog proširenja $\mathcal{M}[G]$. Ako je $\mathcal{P} \in M$ parcijalno uređenje i $G \subseteq P$ generički skup uslova nad $\mathcal{M}$, u modelu $\mathcal{M}$ može se definisati forsing relacija $\Vdash$ između uslova u $\mathcal{P}$ i rečenica jezika $\mathcal{L}_G$ koja predstavlja uopštenje relacije zadovoljenja modela $\mathcal{M}[G]$.

Ne ulazeći u detalje dokaza odgovarajućih preciznih formulacija stavova (a) i (c), pokazaćemo kako izgleda skup uslova koji u generičkom modelu forsira $2^{\aleph_0} \geq \aleph_2$.

Primer 6. Neka je $\mathcal{M}$ prebrojiv tranzitivan model teorije ZFC i $\mathcal{P} \in M$ skup svih funkcija p čiji je domen dom(p) konačan podskup od $\omega_2^M \times \omega$, kodomen codom$(p) \subseteq \{0, 1\}$, a poredak $<$ definisan tako da za sve $p, q \in P$, $p < q$ ako i samo ako $p \supseteq q$.

Kako je model $\mathcal{M}$ prebrojiv, postoji generički skup uslova $G \subseteq P$ nad $\mathcal{M}$ i neka je $f = \bigcup G$. Istim argumentima kao u prethodnim primerima, dokazuje se da je f funkcija sa domenom dom$(f) = \omega_2^M \times \omega$.

Za svako $\alpha < \omega_2^M$, neka je $f_\alpha : \omega \to \{0, 1\}$ funkcija definisana tako da za svako $n \in \omega$,

$$f_\alpha(n) = f(\alpha, n).$$

Za svako $g \in M$, skup $D_\alpha = \{p \in P : \exists n \; p(\alpha, n) \neq g(n)\}$ je gust u uređenju $\mathcal{P}$, pa dakle za svako $\alpha < \omega_2^M$, imamo $f_\alpha \neq g$, tj. svaka od funkcija f_α ne pripada modelu $\mathcal{M}$.

Ako je $\alpha \neq \beta$, skup $D = \{p \in P : \exists n\, p(\alpha, n) \neq p(\beta, n)\,\}$ je gust u $\mathcal{P}$, pa je $G \cap D \neq \emptyset$. To znači da je $\alpha \mapsto f_\alpha$ obostrano jednoznačno preslikavanje kardinala ω_2^M u skup 2^ω. Ukoliko kardinal ω_2^M nije kolabirao, u modelu $\mathcal{M}$ ne važi hipoteza kontinuuma.

Kantor je problem kontinuuma postavio u sasvim različitom kontekstu od onog u kojem je on sagledan u Gedelovim i Koenovim rezultatima. Oni su zapravo rešili jedan formalno-kombinatorni problem, koji Kantor uopšte nije imao u vidu. Pokazali su da u spisku dokaza iz hipoteza ZF nema dokaza za rečenice CH, AC ili $\neg CH$ i $\neg AC$, odnosno, da teorija ZF nije kompletna teorija. Matematika nije kombinatorna simbolička igra. Njena tvrđenja izražavaju svojstva određene objektivne realnosti, pa sa stanovišta te realnosti, kontinuum hipoteza važi ili ne važi. Ako se prihvati realističko gledište, ovi rezultati samo pokazuju nedostatke teorije ZF, a nikako ne predstavljaju rešenje problema kontinuuma ili problema izbora.

Iako dovoljno jake da se u njima mogu izraziti praktično svi značajni matematički principi, teorije ZF i ZFC ipak nemaju odgovor na jedan broj važnih i prirodnih pitanja, bar kada su one same u pitanju. Iz tih razloga, veruje se da one ipak ne iscrpljuju sva relativno jednostavna svojstva koja karakterišu skupove kao "realne" matematičke objekte.

Proširenje Lebegove mere

Posle Koenovih rezultata, metod forsinga upotrebljen je u analizi velikog broja principa, koji predstavljaju neku vrstu kandidata kojim bi se opravdano mogla proširiti teorija ZF. U sledećim primerima ilustrovan je problem egzistencije mere, koji je u ovom smislu bio veoma inspirativan i predstavljao izvor niza pretpostavki koje su nezavisne od teorije ZF. Međutim, kako se sve takve pretpostavke odnose na egzistenciju velikih kardinala, većih od najmanjeg nedostižnog kardinala, za većinu matematičara one se po svojoj prirodi bitno razlikuju od ostalih aksioma teorije ZF.

Za svaki neprazan skup S, realno vrednosna funkcija μ definisana na $P(S)$ je σ-aditivna *mera* na S ako zadovoljava sledeće uslove:

(a) $\mu(\emptyset) = 0$, $\mu(S) = 1$,

(b) ako su $x \subseteq y$, $\mu(x) \leq \mu(y)$,

(c) za svako $x \in S$, $\mu(\{x\}) = 0$,

(d) $\mu(\bigcup_{n\in\omega} x_n) = \sum_{n\in\omega} \mu(x_n)$, za svaku familiju $(x_n : n \in \omega)$ međusobno disjunktnih podskupova skupa S.

Jasno je da, na osnovu uslova (b), mera nema negativne vrednosti, tj. za svako $x \subseteq S$, $\mu(x) \geq 0$. U specijalnom slučaju, na osnovu uslova (d), odnosno, na osnovu σ-aditivnosti, sledi da je mera *aditivna funkcija*: ako su $x, y \subseteq S$ disjunktni skupovi, $\mu(x \cup y) = \mu(x) + \mu(y)$.

Opštije, ako je $\mathcal{B}$ proizvoljna σ-algebra skupova, mera na $\mathcal{B}$ je realno vrednosna funkcija μ definisana na B koja zadovoljava uslove $(a), \cdots, (d)$.

Paradigma ideje mere jeste Lebegova mera. Definisana je kao mera na σ-kompletnoj algebri merljivih skupova realnih brojeva koja je *invarijantna* u odnosu na izometrije realne prave:

(e) Ako je $x \subseteq R$ merljiv skup i $y = \{z + r : z \in x\}$, za neko $r \in R$, onda važi $\mu(x) = \mu(y)$.

Primer 1. U odnosu na inkluziju kao uređenje, neka je M maksimalan podskup intervala $[0, 1]$ takav da za sve $x, y \in M$, ako $x \neq y$, $(x - y) \notin Q$. Skup M nema Lebegovu meru.

Za svako $q \in Q$, neka je $M_q = \{x + q : x \in M\}$. Svi skupovi oblika M_q su međusobno disjunktni i $[0, 1] \subseteq \bigcup_{q \in Q \cap [0,1]} M_q \subseteq [0, 2]$, pa skup M ne može biti merljiv.

Primer 2. Ako je skup $x \subseteq [0, 1]$ takav da x i x^c ne sadrže perfektan skup, onda skup x nema Lebegovu meru.

Ovo tvrđenje je posledica činjenice da svaki skup pozitivne Lebegove mere sadrži zatvoren podskup pozitivne mere.

Postojanje nemerljivih skupova realnih brojeva može se shvatiti kao posledica uslova invarijantnosti. Stoga, prirodno se postavlja pitanje da li Lebegova mera ima proširenje, koje eventualno nije invarijantno, u kojem su svi podskupovi intervala $[0, 1]$ merljivi. Pozitivan odgovor na ovo pitanje negira hipotezu kontinuuma i ima drastične posledice po kardinalnost skupa realnih brojeva.

Teorema 19. Ako postoji mera na $2^{\aleph_0}$, ne važi kontinuum hipoteza.

Dokaz: Pretpostavimo da važi $2^{\aleph_0} = \aleph_1$. Neka je μ mera na ω_1 i neka je $I = \{x \subseteq \omega_1 : \mu(x) = 0\}$ ideal skupova mere nula. Na osnovu definicije mere, ideal I ima sledeća svojstva:

(a) Za svako $x \in \omega_1$, $\{x\} \in I$,

(b) Ako za svako $n \in \omega$, $x_n \in I$, onda $\bigcup_{n \in \omega} x_n \in I$,

(c) Ne postoji neprebrojiva familija $\mathcal{S}$, međusobno disjunktnih podskupova skupa ω_1, takva da za sve $x \in S$, $x \notin I$.

Pretpostavimo da je $\mathcal{S}$ familija podskupova ordinala ω_1 takva da za sve $x \in S$, $x \notin I$. Za svako $n \in \omega$, neka je $\mathcal{S}_n = \{x \in \mathcal{S} : \mu(x) \geq \frac{1}{n+1}\}$. Kako je $\mu(\omega_1) = 1$, svaka familija $\mathcal{S}_n$ je konačna, pa kako je $\mathcal{S} = \bigcup_{n\in\omega} \mathcal{S}_n$, familija $\mathcal{S}$ je najviše prebrojiva, odnosno, važi tvrđenje (c).

Konstruisaćemo matricu $(a_{\alpha n} : \alpha \in \omega_1, n \in \omega)$, podskupova ordinala ω_1, koja zadovoljava sledeće uslove:

(d) Za svako $n \in \omega$, $\alpha \neq \beta$ implicira $a_{\alpha n} \cap a_{\beta n} = \emptyset$,

(e) Za svako $\alpha \in \omega_1$, skup $\omega_1 - \bigcup_{n\in\omega} a_{\alpha n}$ je najviše prebrojiv.

Za svaki ordinal $\xi < \omega_1$, izaberimo funkciju $f_\xi : \omega \to \omega_1$ tako da važi $\xi \subseteq \text{codom}(f_\xi)$ i za sve $\alpha < \omega_1$, $n \in \omega$, neka je

$$a_{\alpha n} = \{\xi < \omega_1 : f_\xi(n) = \alpha\}.$$

Ako $\xi \in a_{\alpha n} \cap a_{\beta n}$, onda $f_\xi(n) = \alpha$ i $f_\xi(n) = \beta$, pa važi uslov (d).

Ako za svako $n \in \omega$, $\xi \notin a_{\alpha n}$, onda $\alpha \notin \text{codom}(f_\xi)$, pa dakle $\xi < \alpha$. To znači da matrica $(a_{\alpha n} : \alpha \in \omega_1, n \in \omega)$ zadovoljava uslov (e).

Neka je $\alpha < \omega_1$ fiksiran. Na osnovu uslova (e) i (b), svi skupovi oblika $a_{\alpha n}$, $n \in \omega$, ne pripadaju idealu I jer, ω_1 je unija skupova $a_{\alpha n}$ i najviše prebrojivog skupa, koji prema (a) i (b) pripada idealu I.

Otuda sledi da za svako $\alpha < \omega_1$, postoji $n_\alpha \in \omega$ takvo da $a_{\alpha n_\alpha} \notin I$. Kako postoji neprebrojivo mnogo ordinala $\alpha < \omega$, mora postojati $n \in \omega$ takvo da je $\{\alpha : n_\alpha = n\}$ neprebrojiv skup.

Konačno, prema uslovu (d) $\mathcal{S} = \{a_{\alpha n} : n_\alpha = n\}$ je neprebrojiva familija međusobno disjunktnih podskupova od ω_1 takva da za svako $a_{\alpha n} \in \mathcal{S}$, važi $a_{\alpha n} \notin I$, što prema uslovu (c) nije moguće. $\Box$

Zanimljivo, bez ikakvih teškoća ovaj dokaz može se preraditi u dokaz sledećeg tvrđenja: ako postoji mera na $2^{\aleph_0}$, onda postoji slabo nedostižan kardinal $\kappa \leq 2^{\aleph_0}$.

Teorema 20. Ako postoji mera na kardinalu β, postoji slabo nedostižan kardinal $\kappa \leq \beta$.

Dokaz : Pretpostavimo da je κ najmanji kardinal za koji postoji ideal I nad κ koji zadovoljava uslove:

(a) Za svako $x \in \kappa$, $\{x\} \in I$,

(b) Ako za svako $n \in \omega$, $x_n \in I$, onda $\bigcup_{n\in\omega} x_n \in I$,

(c) Ne postoji neprebrojiva familija $\mathcal{S}$, međusobno disjunktnih podskupova skupa κ, takva da za sve $x \in S$, $x \notin I$.

Za svako $\lambda < \kappa$, ako $x_\eta \in I$ za sve $\eta < \lambda$, onda je $\bigcup_{\eta<\lambda} x_\eta \in I$.

Pretpostavimo da postoji $\lambda < \kappa$ i familija $x_\eta \in I$, $\eta < \lambda$, međusobno disjunktnih skupova takva da $\bigcup_{\eta<\lambda} x_\eta \notin I$.

Ako je $J = \{y \subseteq \lambda : \bigcup_{\eta\in y} x_\eta \in I$, skup J je ideal na $\lambda < \kappa$ i zadovoljava uslove (a), (b) i (c), suprotno definiciji kardinala κ.

Otuda sledi da za svako $x \subseteq \kappa$, ako $|x| < \kappa$, onda $x \in I$, što znači da je κ regularan kardinal.

Po definiciji slabo nedostižnog kardinala, treba još dokazati da je κ granični kardinal. Pretpostavimo suprotno, tj. da je ν ordinal takav da $\kappa = \aleph_{\nu+1}$.

Za svaki $\xi < \kappa$, izaberimo funkciju f_ξ na ω_ν tako da $\xi \subseteq \mathrm{codom}(f_\xi)$. Za svako $\alpha < \omega_{\nu+1}$ i svako $\eta < \omega_\nu$, neka je

$$a_{\alpha\eta} = \{\xi < \kappa : f_\xi(\eta) = \alpha\}.$$

Kao u dokazu prethodne teoreme, matrica $(a_{\alpha\eta} : \alpha < \omega_{\nu+1}, \eta < \omega_\nu)$ zadovoljava uslove tipa (c) i (d):

(d') Za svako $\eta \in \omega_\nu$, $\alpha \neq \beta$ implicira $a_{\alpha n} \cap a_{\beta n} = \emptyset$,

(e') Za svako $\alpha \in \omega_{\eta+1}$, $|\omega_{\nu+1} - \bigcup_{\eta\in\omega_\nu} a_{\alpha\eta}| \leq \aleph_\nu$.

Isto kao u dokazu prethodne teoreme, za svako $\alpha < \omega_{\nu+1}$, postoji $\eta < \omega_\nu$ takvo da $a_{\alpha\eta} \notin I$. Tako se dobija familija $\mathcal{S}$ međusobno disjunktnih elemenata, koji ne pripadaju idealu I, kardinalnosti $\aleph_{\nu+1}$, što prema uslovu (c) nije moguće. $\Box$

Na osnovu prethodne teoreme, ako postoje beskonačni merljivi skupovi, njihova kardinalnost veća je od slabo nedostižnog kardinala, pa takva pretpostavka implicira neprotivrečnost teorije ZFC. Jedan broj matematičara veruje u postojanje takvih kardinala.

Primer 3. Ako je $(x_i : i \in \omega)$ familija gustih otvorenih skupova realnih brojeva, presek familije $(x_i : i \in \omega)$ je gust skup u R.

Ako je $x = \bigcap_{i\in\omega} x_i$, skup x ima neprazan presek sa svakim otvorenim intervalom I realnih brojeva. Naime, ako je $((p_k, q_k) : k \in \omega)$ numeracija svih racionalnih otvorenih intervala, neka je $I_0 = I$ i za svako $n \in \omega$, $I_{n+1} = (p_k, q_k)$, gde je $k \in \omega$ najmanji prirodan broj takav da je zatvoreni interval $[p_k, q_k] \subseteq I_n \cap x_n$. Kako je $x_0 \cap \cdots \cap x_n \neq \emptyset$, za svako $n \in \omega$ i ako je $a = \lim_{k\to\infty} q_k$, onda $a \in x \cap I$.

Neposredna posledica ovog tvrđenja jeste da skup racionalnih brojeva nije presek prebrojive familije otvorenih skupova realnih brojeva.

Primer 4. (a) Svaki perfektan skup ima kardinalnost $2^{\aleph_0}$.

(b) Svaka familija $F_0 \supseteq F_1 \supseteq \cdots \supseteq F_\alpha \supseteq \cdots, \alpha < \beta$ strogo opadajućih zatvorenih skupova realnih brojeva je najviše prebrojiva.

(c) Svaki skup realnih brojeva ima najviše prebrojiv skup izolovanih tačaka.

(d) Ako je F neprebrojiv zatvoren skup realnih brojeva, postoje perfektan skup P i prebrojiv skup S takvi da važi $F = P \cup S$.

Dakle, svaki zatvoren skup je ili prebrojiv ili ima kardinalnost $2^{\aleph_0}$, što znači da za zatvorene skupove realnih brojeva važi hipoteza kontinuuma.

Primer 5. Ako se pretpostavi aksioma izbora, postoji skup realnih brojeva kardinalnosti $2^{\aleph_0}$ koji ne sadrži perfektan podskup.

Izlaganje svojstava mere u svetlu teorije modela teorije skupova završavamo rezultatom koji pokazuje kako bi matematika mogla izgledati ukoliko se nekad potvrdi postojanje nedostižnog kardinala:

– Pretpostavimo da postoji nedostižan kardinal. Onda postoji model teorije ZF + $\neg$AC u kojem je svaki skup realnih brojeva merljiv i svaki neprebrojiv skup sadrži perfektan podskup.

Sa jednim brojem suptilnih detalja u odnosu na dokaz nezavisnosti hipoteze kontinuuma, može se dokazati nezavisnost aksiome izbora. Prebrojiv tranzitivan model teorije ZF moguće je proširiti "novim" skupom realnih brojeva, tako da generičko proširenje ne sadrži dobro uređenje tog skupa. Time se dobija model u kojem važi negacija aksiome izbora.

Paradoksalni skupovi

Iako ne rešava sva pitanja o kardinalima, aksioma izbora ipak omogućava definiciju i kakvu takvu aritmetiku kardinala. U ostalim oblastima matematike ona takođe ima značajne posledice. Neke od tih posledica smo već razmotrili. Teoremu o ultrafiltru, stav potpunosti, proširenje homomorfizma Bulovih algebri, egzistenciju algebarski zatvorenog polja i Skolemove teoreme dokazali smo pozivajući se na neku varijantu ovog principa. Od značajnijih matematičkih rezultata u ovom smislu svakako treba spomenuti i Han-Banahovu teoremu, Nilsen-Šrajerovu teoremu o podgrupama slobodne grupe, teoremu Tihonova o proizvodu kompaktnih prostora itd.

Međutim, u zasnivanjima teorije mere, u prvoj polovini ovog veka, pozivanjem na aksiomu izbora, dobijen je čitav niz rezultata koji protivreče geometriskoj intuiciji. Neki od njih izgledali su tako da je jedan broj matematičara ozbiljno posumnjao u legitimnost ovog principa.

Primer takvog rezultata je razlaganje jedinične lopte na konačan broj delova od kojih se, kretanjima u prostoru, mogu sklopiti dve jedinične lopte.

Ako je X proizvoljan skup, *slobodna grupa* generisana skupom X je grupa $\mathcal{F}(X)$ takva da za svaku grupu $\mathcal{G}$ i svaku funkciju $f : X \to G$, postoji jedinstveno određen homomorfizam $g : F(X) \to G$ koji proširuje funkciju f.

Nad proizvoljnim skupom X, postoji slobodna grupa generisana skupom X. Ona se sastoji se od svih reči nad slovima iz skupa X svedenih po zakonima grupe. Slobodnu grupu generisanu sa dva elementa označavaćemo sa $\mathcal{F}$.

Primer 1. Ako su a i b generatori grupe $\mathcal{F}$, svaki njen element $g \in F$ može se predstaviti u obliku

$$g = a^{k_1} b^{l_1} \cdots a^{k_n} b^{l_n},$$

gde su k_i i l_i celi brojevi Pritom, samo k_1 i l_n mogu biti jednaki nuli i jedinični element 1 grupe $\mathcal{F}$ ne može se predstaviti na takav način.

Zapravo, grupa $\mathcal{F}$ se sastoji od svih svedenih reči, u smislu aksioma teorije grupa, sastavljenih od slova a i b.

Primer 2. Grupa rotacija $\mathcal{SO}_3$ prostora $\mathcal{R}^3$, sa osama rotacije koje prolaze kroz koordinatni početak, sadrži podgrupu izomorfnu grupi $\mathcal{F}$.

Da bismo to pokazali, primetimo da se grupa $\mathcal{SO}_3$ može predstaviti ortogonalnim matricama reda 3×3 sa determinantom jednakom jedinici. Neka je ϕ rotacija oko prave $x = z$, $y = 0$ za ugao π i neka je ψ rotacija oko z-ose za ugao $\frac{2\pi}{3}$. Rotacije ϕ i ψ predstavljene su matricama

$$\phi = \begin{pmatrix} 0 & 0 & 1 \\ 0 & -1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \text{ i } \psi = \begin{pmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} & 1 \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

i pritom je $\phi^2 = 1$ i $\psi^3 = 1$. Neka je $a = \psi\phi\psi$ i $b = \phi\psi\phi\psi\phi$. Grupa $\mathcal{F}$ generisana rotacijama a i b je slobodna grupa.

Pretpostavimo suprotno. Tada postoji $n > 0$ i celi borjevi $k_1, \ldots, k_n$; $l_1, \ldots, l_n$, različiti od nule, takvi da je

$$1 = a^{k_1} b^{l_1} \cdots a^{k_n} b^{l_n}.$$

Imajući u vidu definicije rotacija a i b, jedinični element može se predstaviti u obliku $1 = \phi^s \psi^{r_1} \phi \psi^{r_2} \phi \cdots \psi^{r_m}$ za neke $r_1, \ldots, r_{m-1} \in \{1, 2\}$, $r_m \in \{0, 1, 2\}$ i $s \in \{0, 1\}$. U matričnoj reprezentaciji, ovaj proizvod ni za jednu kombinaciju brojeva $s, r_1, \ldots, r_m$, $m > 0$, nije jednak jediničnoj matrici. Dakle, grupa generisana elementima a i b je slobodna.

Teorema 21. Hauzdorfov paradoks: Na jediničnoj sferi S prostora $\mathcal{R}^3$ postoji skup $E \subseteq S$ koji zadovoljava sledeće uslove:

(a) četiri kopije skupa E pokrivaju S i

(b) S sadrži beskonačno mnogo dijunktnih kopija skupa E.

Naglašavamo da se kopije skupa E, o kojima se govori u teoremi, dobijaju rotacijama prostora $\mathcal{R}^3$. Taj skup zaista ima začuđujuća svojstva. Ako skup E rotiramo na jedan način, u četiri koraka pokrijemo čitavu sferu. Sa druge strane, na sferi se rotacijama može rasporediti beskonačno mnogo disjunktnih kopija skupa E.

Dokaz: Neka su rotacije $a, b \in SO_3$ takve da je grupa generisana sa a, b slobodna grupa $\mathcal{F}$. Prema prethodnom primeru takve rotacije grupe $\mathcal{S}O_3$ zaista postoje. Na sferi S definišemo relaciju ekvivalencije $\sim$ tako da za sve $x, y \in S$,

$$x \sim y \quad \Leftrightarrow \quad \text{postoji } f \in F,\ y = f(x).$$

Svaka klasa ekvivalencije je prebrojiva. Neka je C unija svih klasa koje sadrže bar jednu fiksnu tačku nekog neidentičkog preslikavanja iz $\mathcal{F}$. Kako svako takvo preslikavanje ima tačno dve fiksne tačke i kako je grupa $\mathcal{F}$ prebrojiva, skup C je takođe prebrojiv.

Prema aksiomi izbora, neka je $H \subseteq S$ skup koji sadrži po jednog predstavnika svake od klasa ekvivalencije. Svaka tačka $x \in S \backslash C$ ima jedinstvenu reprezentaciju oblika $x = f_x(y)$, gde je $f_x \in F$ i $y \in H$.

Neka je $U \subseteq F$ skup svih reči koje počinju sa a^k, $k \neq 0$ i neka je

$$E = \{x \in S \backslash C : f_x \in U\}.$$

Za sve $m \neq n$, skupovi $b^m E$ i $b^n E$ su disjunktni, tj važi tvrđenje (b).

Kako je $U \cup aU = F$ to je $S \backslash C \subseteq E \cup aE$. Skup C je prebrojiv. Kako je grupa $\mathcal{S}O_3$ neprebrojiva, postoji rotacija $r \in SO_3$ takva da je $C \cap rC = \emptyset$. Otuda je $rC \subseteq E \cup aE$, tj. $C \subseteq r^{-1}E \cup r^{-1}aE$, pa dakle

$$S \subseteq E \cup aE \cup r^{-1}E \cup r^{-1}aE,$$

što dokazuje tvrđenje (a). $\Box$

Hauzdorf je znao za ovaj fenomen. Pronašao je slobodnu podgrupu u grupi izometrija prostora i njen paradoksalan efekat na sferi. Praktično, bio je samo na korak od glavnog rezultata. Taj korak napravili su Banah i Tarski zahvaljujući jednoj varijanti Šreder-Bernštajnove teoreme.

Teorema 22. Ako su $f : A \to B$ i $g : B \to A$ obostrano jednoznačne funkcije, postoje particije $A_1, A_2 \subseteq A$ i $B_1, B_2 \subseteq B$ takve da

$$f[A_1] = B_1 \text{ i } g[B_2] = A_2.$$

Dokaz: Na paru skupova (A, B) definišimo *graf* Γ tako da za proizvoljne $x \in A$, $y \in B$, x i y su povezane tačke grafa Γ ako i samo ako $y = f(x)$ ili $x = g(y)$. Kako su f i g injektivna preslikavanja, svaka *povezana komponenta grafa* Γ je ciklus ili beskonačna putanja u jednom ili oba pravca. Za svaku komponentu C grafa Γ, $f[C \cap A] = C \cap B$ ili $g[C \cap B] = C \cap A$. Neka je

$$A_1 = \bigcup\{C \cap A : C \text{ komponenta u } \Gamma \text{ i } f[C \cap A)] = C \cap B\},$$

onda skupovi $A_2 = A \backslash A_1$, $B_1 = f(A_1)$ i $B_2 = g^{-1}(A_2)$ zadovoljavaju uslov teoreme. $\Box$

Skupovi $A, B \subseteq R^3$ su *razloživo jednaki* u prostoru R^3 ako postoje particije $A_1, \ldots, A_n \subseteq A$, $B_1, \ldots, B_n \subseteq B$ i elementi $g_1, \ldots, g_n \subseteq G_3$ grupe izometrija $\mathcal{G}_3$ takvi da za svako A_i, $g_i(A_i) = B_i$.

Razloživu jednakost skupova A i B označavamo sa $A \sim_n B$. Pritom, prirodan broj $n \geq 1$ označava broj elemenata particije s obzirom na koju se realizuje razloživa jednakost skupova A i B.

Korak koji je nedostajao Hauzdorfu u dokazu paradoksalne dekompozicije lopte je sledeća neposredna posledica Kantor-Bernštajnove teoreme:

Primer 4. Ako su $A_1 \subseteq A$ i $B_1 \subseteq B$ skupovi tačaka prostura R^3, onda za proizvoljne $m, n \geq 1$, $A \sim_m B_1$ i $A_1 \sim_n B$ implicira $A \sim_{m+n} B$.

Razloživa jednakost $A \sim_m B_1$ i inkluzija $B_1 \subseteq B$ određuju obostrano jednoznačnu funkciju $f : A \to B$, a razloživa jednakost $B \sim_n A_1$ i inkluzija $A_1 \subseteq A$ obostrano jednoznačnu funkciju $g : B \to A$.

Na osnovu Šreder-Bernštajnove teoreme, efekat funkcije g na elemente m-particije skupa A je $(m+n)$-particija u A, a efekat funkcije f na elemente n-particije u B, $(m+n)$-particija skupa B. Ove particije određuju $(m+n)$-razloživu jednakost skupova A i B.

Primer 5. Jediničan lopta se može razložiti na jedanaest delova od kojih se kretanjem u prostoru mogu sklopiti dve jedinične lopte.

Neka je E skup čije četiri kopije pokrivaju sferu S. Ako je B jedinična lopta, $E^* = \bigcup\{xE : 0 < x \leq 1\}$ i t translacija prostora R^3 takva da $0 \in tE^*$, onda je $B \subseteq E^* \cup aE^* \cup r^{-1}E^* \cup r^{-1}aE^* \cup tE^*$.

Neka je $A_1, \ldots, A_5$ particija jedinične lopte B određena prethodnim pokrivanjem i neka je B_1 jedinična lopta disjunktna sa B.

Prema svojstvu (b), deset disjunktnih kopija skupa E se rotacijama može rasporediti na sferu S, tj. deset disjunktnih kopija skupa E^* može se rotacijama i translacijama smestiti u loptu B. Ako u svaku od tih deset kopija rasporedimo redom kopije skupova $A_1, \ldots, A_5, A_1, \ldots, A_5$, onda

$$B \subseteq B \cup B_1 \ \text{ i } \ A_1^{'} \cup \cdots \cup A_5^{'} \cup A_1^{''} \cup \cdots \cup A_5^{''} \subseteq B.$$

Kako je $A_1^{'} \cup \cdots \cup A_5^{'} \cup A_1^{''} \cup \cdots \cup A_5^{''} \sim_{10} B \cup B_1$ i $B \sim_1 B$, prema posledici Kantor-Bernštajnove teoreme, $B \sim_{11} B \cup B_1$. $\square$

Ako je $n \geq 3$, paradoksalna razlaganja n-dimenzionalne jedinične lopte su moguća budući da u tim slučajevima grupa izometrija $\mathcal{G}_n$ prostora $\mathcal{R}^n$ sadrži slobodnu podgrupu. Primeri takvog razlaganja zapravo pokazuju da Lebegova mera prostora R^n, $n \geq 3$, nema proširenje koje je aditivno i invarijantno na $P(R^n)$.

U slučaju prostora R^2, grupa izometrija $\mathcal{G}_2$ ne sadrži slobodnu podgrupu, pa postoji aditivna invarijantna mera μ na $P(R^2)$ koja proširuje Lebegovu meru u ravni. Kako ovaj rezultat sledi na osnovu Han-Banahove teoreme, budući da se Han-Banahova teorema dokazuje pozivanjem na aksiomu izbora, efekat aksiome izbora u ravni je potpuno suprotan efektu koji ima u prostoru. Ona u ravni ne dozvoljava paradoksalna razlaganja, a u prostoru na njoj počiva paradoksalna dekompozicija jedinične lopte.

Završavajući izlaganje o teoriji skupova, vratićemo se na pitanje smisla matematičkih iskaza. Sa jedne strane, interpretirana u prebrojivim tranzitivnim modelima, teorija ZFC podseća na neku vrstu kombinatorne igre, ali kada se ima u vidu interpretacija njenih principa u prostorima sa jakom geometrijom, ipak se opravdano postavlja Hilbertovo pitanje: kakav je stvarni sadržaj matematičkih iskaza. Na kraju, da li se jedinična lopta stvarno može razložiti na pet delova, od kojih se mogu sklopiti dve takve lopte ili se samo radi o interpretativnoj zloupotrebi finitističkih objekata lišenih svakog smisla.

Napomene

– Kantor je prvi matematičar koji se sistematski bavio problemom zasnivanja pojma skupa. Uočio je značaj obostrano jednoznačnih preslikavanja, definisao pojmove kardinalnih i ordinalnih brojeva, dobrog uređenja i inicirao istraživanja topologije realne prave. Njega su pre svega interesovali beskonačni skupovi tako da je već 1878. godine imao formulisan problem kontinuuma.

– Sa izuzetkom aksiome zamene, aksiome teorije skupova o kojima smo do sada govorili formulisao je Cermelo 1908. U jednoj gruboj verziji aksiomu zamene definisao je Frenkel 1922. godine tako da se danas ova teorija uobičajeno naziva Cermelo-Frenkelovom teorijom skupova. Međutim, preciznu verziju ove aksiome u predikatskom računu prvog reda formulisao je Skolem 1922. godine.

- Kantor je definisao i delom razvio teoriju dobro uređenih skupova. Definisao je pojam transfinitne indukcije. Ideja da se ordinali definišu kao skupovi manjih ordinala nastala je 1923. godine u radovima Fon Nojmana i Cermela [2].

– Aksiomu regularnosti definisao je Mirimanov 1917. godine. Ideju kumulativne hijerarhije skupova, pojam ranga i dokaz njene relativne neprotivrečnosti formulisao je Fon Nojman 1929. godine [2].

– Pojam kardinalnog broja definisao je Kantor. Takođe, njemu je bio poznat i niz $\aleph_\alpha$, $\alpha \in On$. Regularnost kardinala definisao je Hauzdorf i postavio pitanje egzistencije regularnih graničnih kardinala. Osim klasičnog Kenihovog rezultata iz 1905. godine, veći deo aritmetike kardinala u okviru teorije ZFC razradio je Tarski [2].

- Aksiomu izbora formulisao je Cermelo i koristio je u dokazu principa dobrog uređenja 1904. godine. Fenomene paradoksalnih razlaganja uočio je Hauzdorf 1914. godine [5].

– Relativnu neprotivrečnost hipoteze kontinuuma, aksiome izbora i aksiome konstruktibilnosti dokazao je Gedel 1938. godine. U opširnoj monografiji iz 1940. godine [4] navedena je jedna detaljna konstrukcija klase L, kao i dokaz da u L važe hipoteza kontinuuma i aksioma izbora.

– Ideja apsolutnosti prvi put se javlja u spomenutoj Gedelovoj monografiji, koja obuhvata i opsežna istraživanja tranzitivnih modela. Pojam tranzitivnog kolapsa definisao je Mostovski [2], a teoremu refleksije dokazali su Levi 1960. i Montegju 1961. godine [4].

– Nezavisnost hipoteze kontinuuma i aksiome izbora dokazao je Koen 1963. godine metodom koji se uobičajeno naziva forsing. Tim metodom dokazan je čitav niz rezultata nezavisnosti u teoriji skupova, a on i danas ima ključnu ulogu u ovoj teoriji. U originalnom formalističkom pristupu, ovaj metod izložen je u monografiji [4].

– Matricu oblika (ω_1, ω) definisao je Ulam 1930. godine i dokazao da na ω_1 ne postoji netrivijalna σ-aditivna mera [2]. Uz pretpostavku postojanja nedostižnog kardinala, model teorije ZF u kojem svaki skup realnih brojeva ima Lebegovu meru konstruisao je Robert Solovej 1970, godine [2].

– U radu iz 1924. godine, u kojem su otkrili paradoksalnu dekompoziciju lopte, Banah i Tarski nisu precizirali broj delova dovoljan za takvu dekompoziciju [1]. Kasnije, 1929. godine fon Nojman je dokazao da se ona može izvršiti sa devet delova, 1945. godine Serpinski je izveo konstrukciju u kojoj je bilo dovoljno osam delova i konačno, 1947. godine, Robinson [5] je dokazao da je pet minimalan broj delova neophodan za paradoksalnu dekompoziciju jedinične lopte.

Literatura

[1] Banach, S., Tarski, A. Sur la decomposition des ensembles de point en partiesrespectivement congruents, Fund. Math.6 (1924), 236-239.

[2] Jech, T. Introduction to Set Theory, Academic Press, New York, 1978.

[3] Kron, A. Elementarna teorija skupova, Mat. Inst., Beograd, 1992.

[4] Kunen, K. Set Theory, North-Holland, Amstedram, 1980.

[5] Laczkovich, M. Equidecomposability of sets, invariant measures, and paradoxes, Rend. Inst. Math. Univ. di Trieste, Vol XXIII (1991), 145-176.

Teorija izračunljivosti

Osnovni pojam, prisutan u svim idejama koje će se javljati u daljim razmatranjima, jeste pojam efektivne procedure. Pod takvom procedurom podrazumevamo čisto mehanički proces koji se korak po korak izvodi nad konačnim skupom podataka. Svaki korak u proceduri nedvosmisleno je definisan, izvodi se u konačnom vremenu i u ograničenom delu fizičkog prostora.

Postoji mnogo primera efektivnih procedura i navedena definicija prilično dobro odgovara svakodnevnoj upotrebi ovog pojma. Međutim, u ovom kontekstu, nas prevashodno interesuju granice efektivnosti, odnosno, problemi u kojima je neophodno dokazati neefektivnost određenih procedura. Slično pojmu dokaza, za naše potrebe neophodan je precizan matematički pojam efektivnosti.

Na primer, pomoću istinosnih tablica, u konačno mnogo koraka može se utvrditi da li data formula iskaznog računa pripada klasi tautologija. Ali kako smo ranije napomenuli, to nije slučaj i sa rečenicama predikatskog računa. Problem njihovog univerzalnog važenja nije efektivnan. Sa stanovišta efektivnosti, iskazni i predikatski račun su bitno različiti. U čemu se ta razlika sastoji i kako se ona može izraziti matematičkim sredstvima?

Intuicija izračunljivosti je po prirodi aritmetička, pa odgovor na ovo pitanje i jeste aritmetizacija. Efektivnost podrazumeva aritmetičku jednostavnost. Kada se matematičke teorije interpretiraju u aritmetici, ukoliko se u ovom smislu uopšte razlikuju, njihova razlika u efektivnosti morala bi se pojaviti u klasama aritmetičkih funkcija u kojima su interpretirane. Stoga, matematičko zasnivanje ideje efektivnosti prevashodno podrazumeva njenu aritmetičku formulaciju. Kako se u prirodnim brojevima mogu kodirati svi konačni diskretni objekti, svaka efektivna procedura može se aritmetički izrazititi kao funkcija definisana na prirodnim brojevima.

Kao matematički objekt, klasu efektivno izračunljivih funkcija definišemo u klasi funkcija prirodnih brojeva. Pritom, funkcija f je *funkcija prirodnih brojeva* ako $\mathrm{dom}(f) \subseteq \omega^n$ i $\mathrm{codom}(f) \subseteq \omega$, za neki prirodan broj $n \geq 1$. Ovom definicijom, osim totalnih obuhvaćene su i parcijalno definisane funkcije uključujući i praznu funkciju. U oznakama koristimo izraze oblika $f(x_1, \ldots, x_n)$, a jednakost takvih izraza shvatamo kao jednakost funkcija. Saglasno takvoj notaciji, svi aritmetički izrazi su funkcije.

Rekurzivne funkcije

Nepodeljeno je mišljenje savremenih matematičara da intuitivnu ideju efektivnosti u potpunosti determiniše klasa $\mathcal{R}$ *rekurzivnih funkcija*. To uverenje izražava se *Čerčovom tezom*:

– Svaka intuitivno izračunljiva funkcija je rekurzivna.

Zapravo, kako se samo po sebi podrazumeva da su rekurzivne funkcije intuitivno izračunljive, u Čerčovoj tezi tvrdi se da je klasa $\mathcal{I}$ intuitivno definisanih izračunljivih funkcija jednaka klasi $\mathcal{R}$ rekurzivnih funkcija.

U ovoj hipotezi je čudno to što ona jedan nematematički pojam, klasu intuitivno izračunljivih funkcija, izjednačava sa konkretnim matematičkim objektom – klasom rekurzivnih funkcija. Ne ulazeći u eventualno dublji smisao koji Čerčova teza ima, mi ćemo je za sada shvatiti kao matematičku definiciju efektivne procedure. Dakle, efektivna je svaka procedura koja se može opisati rekurzivnom funkcijom.

Sve funkcije prirodnih brojeva sa kojima se svakodnevno susrećemo su rekurzivne. Međutim, standardne aritmetičke funkcije pripadaju nešto užoj klasi takozvanih primitivno rekurzivnih funkcija, tako da definicija spomenute klase prirodno prethodi definiciji klase rekurzivnih funkcija. Kako se pojam rekurzije može mnogo opštije definisati, njegov specijalan slučaj na prirodnim brojevima naziva se primitivnom rekurzijom, pa je tako nastao uobičajeni naziv klase primitivno rekurzivnih funkcija. U daljim razmatranjima, pod rekurzijom podrazumevamo primitivnu rekurziju.

Klasa *primitivno rekurzivnih funkcija* je najmanja klasa $\mathcal{P}$ koja sadrži *osnovne funkcije* i zatvorena je za supstituciju i primitivnu rekurziju. Pritom, osnovne su sledeće funkcije:

(a) konstanta nula: za svako $x \in \omega$, $0(x) = 0$,
(b) funkcija naslednika: za svako $x \in \omega$, $s(x) = x + 1$ i
(c) sve projekcije: za svako $x \in \omega^n$, $U_i^n(x_1, \dots, x_n) = x_i$, $1 \leq i \leq n$.

Supstitucija: Ako su $g_1(\vec{x}), \dots, g_m(\vec{x})$, $\vec{x} \in \omega^n$ i $h(\vec{y})$, $\vec{y} \in \omega^m$, primitivno rekurzivne funkcije, onda je funkcija

$$f(x_1, \dots, x_n) = h(g_1(\vec{x}), \dots, g_m(\vec{x}))$$

primitivno rekurzivna. Kažemo da je funkcija $f(\vec{x})$ dobijena supstitucijom funkcija $g_1(\vec{x}), \dots, g_m(\vec{x})$ u funkciju $h(\vec{y})$.

Rekurzija: Ako su $f(\vec{x})$ i $g(\vec{x}, y, z)$, $\vec{x} \in \omega^n$, primitivno rekurzivne funkcije, sledeća funkcija je primitivno rekurzivna:

$$h(\vec{x}, 0) = f(\vec{x})$$
$$h(\vec{x}, y+1) = g(\vec{x}, y, h(\vec{x}, y)).$$

Funkcija $h(\vec{x}, y)$ dobijena je rekurzijom iz funkcija $f(\vec{x}$ i $g(\vec{x}, y, z)$. Kada je $n = 0$, funkcija f je konstanta. Na osnovu opšte teoreme rekurzije, funkcija $h(\vec{x}, y)$ postoji i jedinstveno je određena.

Drugačije rečeno, funkcija f je primitivno rekurzivna ako postoji niz funkcija $f_1, \ldots, f_n$ takav da $f_n = f$ i za sve $i \leq n$, f_i je osnovna funkcija ili se f_i može dobiti primenom supstitucije ili rekurzije na neke od funkcija $f_1, \ldots, f_{i-1}$. Izračunavanje vrednosti takvih funkcija svodi se na izračunavanje baznih funkcija i primenu pravila supstitucije i rekurzije. Intuitivno, svaka od ovih operacija je efektivna.

Na primer, rekurzivna definicija sabiranja $h(x, y) = x + y$ je

$$h(x, 0) = x,$$
$$h(x, y+1) = h(x, y) + 1,$$

odnosno, $h(x, y)$ se dobija rekurzijom iz funkcije $f(x) = x$ i funkcije $g(x, y, z) = z + 1$, tj. rekurzijom iz osnovnih funkcija $U_1^1(x)$ i $s(x)$. Izvođenje funkcije h je niz funkcija: $f = U_1^1, U_3^3, s, g, h$. Sasvim neposredno, ovaj niz podseća na dokaz u iskaznom ili predikatskom računu.

Po definiciji, sve bazne funkcije su *totalne*, a kako supstitucija i rekurzija čuvaju to svojstvo, sve primitivno rekurzivne funkcije su totalne.

Primer 1. (a) Množenje prirodnih brojeva $h(x, y) = x \cdot y$ je primitivno rekurzivna funkcija. Dobija se rekurzijom iz konstante $f(x) = 0$ i sabiranja $g(x, y, z) = z + x$.

(b) Eksponencijalna funkcija $g(x, y) = x^y$ i faktorijel $h(x) = x!$ su primitivno rekurzivne funkcije.

Primer 2. Sledeća funkcija je primitivno rekurzivna:

$$x \dot{-} y = \begin{cases} x - y & \text{ako } x \geq y, \\ 0 & \text{ako } x < y. \end{cases}$$

U sledećim primerima naveden je jedan broj primitivno rekurzivnih funkcija koje su značajne u kasnijim izlaganjima. Poređane su uglavnom tako da rekurzivnost svake od njih, sledi iz rekurzivnosti prethodnih. Njihov izbor opredeljen je potrebama dokaza osnovne teoreme o jednakosti klasa izračunljivih i rekurzivnih funkcija.

Primer 3. Koristeći ranije navedene primere, lako je dokazati da su i sledeće funkcije primitivno rekurzivne:

(a) $|x-y| = (x \dot{-} y) + (y \dot{-} x)$,

(b) $\mathrm{sg}(x) = \begin{cases} 1 & \text{ako } x \neq 0, \\ 0 & \text{ako } x = 0. \end{cases}$

(c) $\overline{\mathrm{sg}}(x) = 1 \dot{-} \mathrm{sg}(x)$,

(d) $\min(x,y) = x \dot{-} (x \dot{-} y)$ i $\max(x,y) = x \dot{-} (y \dot{-} x)$,

(e) $\mathrm{rm}(x,y) = \begin{cases} \text{ostatak delenja } x \text{ sa } y & \text{ako } y \neq 0, \\ x & \text{ako } y = 0. \end{cases}$

(f) $\mathrm{qt}(x,y) = \begin{cases} \text{količnik delenja } x \text{ sa } y & \text{ako } y \neq 0, \\ 0 & \text{ako } y = 0. \end{cases}$

Relacija $R \subseteq \omega^n$ je *primitivno rekurzivna* ako njena karakteristična funkcija c_R pripada klasi $\mathcal{P}$. Pritom,

$$c_R(x_1, \ldots, x_n) = \begin{cases} 1 & \text{ako } R(x_1, \ldots, x_n), \\ 0 & \text{ako } \neg R(x_1, \ldots, x_n). \end{cases}$$

Skup $A \subseteq \omega$ je *primitivno rekurzivan* ako njegova karakteristična funkcija c_A pripada klasi $\mathcal{P}$.

Primer 4. (a) Predikati "$x = y$" i "$x \leq y$" su primitivno rekurzivni.

(b) Predikat $D(x,y)$ ako i samo ako "x je deljiv sa y" je primitivno rekurzivan. Pretpostavljamo da važi $D(0,0)$ i za sve $x \neq 0$, nije $D(x,0)$.

Primer 5. (a) Ako su predikati $P(x)$ i $Q(x)$ primitivno rekurzivni, predikati "nije $P(x)$", "$P(x)$ ili $Q(x)$" i "$P(x)$ i $Q(x)$" su primitivno rekurzivni.

(b) Neka je $\vec{x} \in \omega^n$, $n \geq 1$. Ako su $g_1(\vec{x}), \ldots, g_m(\vec{x})$ primitivno rekurzivne funkcije i $R_1(\vec{x}), \ldots, R_m(\vec{x})$ primitivno rekurzivni, međusobno disjunktni predikati takvi da $\bigcup_{i=1}^m R_i = \omega^n$, sledeća funkcija je primitivno rekurzivna:

$$f(\vec{x}) = \begin{cases} g_1(\vec{x}) & \text{ako } R_1(\vec{x}), \\ \cdots & \cdots \\ g_m(\vec{x}) & \text{ako } R_m(\vec{x}) \end{cases}$$

Primer 6. (a) Ako je funkcija $f(\vec{x}, y)$ primitivno rekurzivna, ograničena suma $\sum_{z<y} f(\vec{x}, z)$ i i ograničeni proizvod $\prod_{z<y} f(\vec{x}, z)$ su primitivno rekurzivne funkcije.

(b) Ako su funkcije $f(\vec{x}, y)$ i $g(\vec{x}, z)$ primitivno rekurzivne, ograničena suma $\sum_{y<g(\vec{x},z)} f(\vec{x}, y)$ i ograničeni proizvod $\prod_{y<g(\vec{x},z)} f(\vec{x}, y)$ su primitivno rekurzivne funkcije.

Za svako $\vec{x} \in \omega^n$, $y \in \omega$ i svaku funkciju $f(\vec{x}, y)$, neka je

$$\mu z < y\,(f(\vec{x},z)=0) = \begin{cases} \text{najmanji } z<y \text{ ta-} \\ \text{kav da } f(\vec{x},z)=0 & \text{ako takav } z \text{ postoji,} \\ \\ y & \text{inače.} \end{cases}$$

Funkcija $\mu z < y\,(f(\vec{x},z)=0)$ dobijena je ograničenom minimizacijom funkcije $f(\vec{x},y)$, odnosno, predikata $f(\vec{x},y)=0$. Operator $\mu z < y$ je operator *ograničene minimizacije*.

Primer 7. (a) Ako je funkcija $f(\vec{x},y)$ primitivno rekurzivna, funkcija $g(\vec{x},y) = \mu z < y\,(f(\vec{x},z)=0)$ je primitivno rekurzivna, tj. klasa $\mathcal{P}$ je zatvorena za primenu ograničenog μ-operatora.

Ovo tvrđenje sledi iz činjenice da se ograničena minimizacija može predstaviti na sledeći način:

$$\mu z < y\,(f(\vec{x},z)=0) = \textstyle\sum_{v<y}(\prod_{u\le v}\mathrm{sg}(f(\vec{x},u))).$$

(b) Ako su $f(\vec{x},y)$ i $h(\vec{x},\vec{u})$ primitivno rekurzivne funkcije, na osnovu pravila supstitucije, $g(\vec{x},\vec{u}) = \mu z < h(\vec{x},\vec{u})\,(f(\vec{x},z)=0)$ je primitivno rekurzivna funkcija.

Primer 8. Ako je $R(\vec{x},y)$ primitivno rekurzivan predikat,

(a) funkcija $g(\vec{x},y) = \mu z < y\,R(\vec{x},z)$ je primitivno rekurzivna,

(b) predikati $\forall z < y\,R(\vec{x},z)$ i $\exists z < y\,R(\vec{x},z)$ su primitivno rekurzivni.

Ako predikate identifikujemo sa njihovim karakterističnim funkcijama, poslednji rezultat pokazuje da je klasa primitivno rekurzivnih funkcija zatvorena za ograničenu kvantifikacju.

Primer 9. Ako je $d(x,y)$ karakteristična funkcija predikata "x je deljiv sa y", funkcija

$$q(x) = \begin{cases} \sum_{y\le x} d(x,y) & \text{ako } x>0, \\ \\ 1 & \text{ako } x=0. \end{cases}$$

je primitivno rekurzivna. Zapravo, funkcija $q(x)$ izračunava broj delitelja prirodnog broja x.

Primer 10. Karakteristična funkcija skupa $P = \{0,2,3,5,\dots\}$ prostih brojeva je primitivno rekurzivna. Funkcija $p_x =$ "x-ti prost broj" je primitivno rekurzivna.

Primitivno rekurzivna funkcija $c_p(x) = \overline{\mathrm{sg}}(|q(x)-2|)$ je karakteristična funkcija skupa P prostih brojeva.

Kako smo to već naznačili, u samoj definiciji skupa P prostih brojeva, $p_0 = 0$ i za svaki prirodan broj $x \in \omega$,

$$p_{x+1} = \mu z \leq (p_x! + 1)\, (p_x < z \text{ i } c_p(z) = 1).$$

Za svaki prirodan broj $x \in \omega$ postoje jedinstveno određeni prirodni brojevi $n, y_1, \ldots, y_n \in \omega$, takvi da je $x = p_1^{y_1} \cdots p_n^{y_n}$.

Kako svaki prirodan broj ima jedinstvenu faktorizaciju po stepenima rastućeg niza prostih brojeva, stepen y-tog prostog broja u faktorizaciji broja x može se primitivno rekurzivno odrediti, tj. funkcija

$$(x)_y = \begin{cases} \text{stepen } p_y \text{ u faktori-} \\ \text{zaciji broja } x & \text{ako } x, y > 0 \\ \\ 0 & \text{ako } x = 0 \text{ ili } y = 0 \end{cases}$$

je primitivno rekurzivna. To sledi iz činjenice da se funkcija $(x)_y$ može predstaviti na sledeći način: $(x)_y = \mu z < x\, (d(x, p_y^{z+1}) = 0)$.

Rekurzivnost funkcije $(x)_y$ je posebno značajna budući da ona omogućava kodiranje nizova prirodnih brojeva:

Svaki niz prirodnih brojeva $s = (a_1, \ldots, a_n) \in \omega^n$, $n \geq 1$, može se kodirati prirodnim brojem

$$b = p_1^{a_1+1} \cdots p_n^{a_n+1}.$$

S druge strane, dužina $l(b)$ niza s kodiranog prirodnim brojem $b \in \omega$ je

$$l(b) = \mu z < b\, ((b)_{z+1} = 0),$$

a njegovi elementi su $a_i = (b)_i \dot{-} 1$, za sve $i = 1, \ldots, l(s)$.

Primer 11. (a) Svaki polinom je primitivno rekurzivna funkcija.

(b) Kantorov polinom $\pi(x, y) = \frac{1}{2}(x^2 + 2xy + y^2 + 3x + y)$ je obostrano jednoznačna funkcija ω^2 na ω. Ako je $\pi(x, y) = \langle x, y \rangle$, inverzne funkcije $\pi_1(\langle x, y \rangle) = x$ i $\pi_2(\langle x, y \rangle) = y$ su primitivno rekurzivne.

Za svako $n \geq 2$, funkcija $\langle x_1, \ldots, x_{n+1} \rangle = \langle \langle x_1, \ldots, x_n \rangle, x_{n+1} \rangle$ je primitivno rekurzivna i obostrano jednoznačna, odnosno, kodira nizove prirodnih brojeva dužine $(n + 1)$.

Primer 12. (a) Za sve $x, y \in \omega$, neka je $f(x, y) = 2^x \cdot (2y+1) - 1$. Funkcija $f(x, y)$ obostrano jednoznačno preslikava skup ω^2 na ω.

(b) Njene inverzne funkcije $f_1(x) = (x + 1)_1$ i $f_2(x) = \frac{1}{2}(\frac{x+1}{2^{f_1(x)}} - 1)$ su primitivno rekurzivne.

Primer 13. Ako su funkcije $f(x), f'(x)$ i $g(x, y, z), g'(x, y, z)$ primitivno rekurzivne, funkcije $h(x, y)$ i $h'(x, y)$ definisane relacijama

$$h(x,0) = f(x), \quad h(x,y+1) = g(h(x,y), h'(x,y), x),$$
$$h'(x,0) = f'(x), \quad h'(x,y+1) = g'(h(x,y), h'(x,y), x).$$

su primitivno rekurzivne funkcije.

Primer 14. (a) Funkcija $f(x) = [\sqrt{x}\,]$, "najveći prirodan broj $\leq \sqrt{x}$" i funkcija $\mathrm{exc}(x) = x - [\sqrt{x}\,]$ su primitivno rekurzivne.

(b) Neka je $f(y)$ totalna funkcija i za svako $x \in \omega$, neka je $g(x) = f^x(0)$. Funkcija $g(x)$ dobijena je *iteracijom* funkcije $f(y)$. Svaka iteracija primitivno rekurzivne funkcije je primitivno rekurzivna.

(c) Klasa primitivno rekurzivnih funkcija je najmanja klasa koja sadrži osnovne funkcije, funkciju $\mathrm{exc}(x)$ i zatvorena je za supstituciju i iteraciju.

Klasa $\mathcal{E}$ *elementarnih funkcija* je najmanja klasa funkcija koja, pored osnovnih funkcija, sadrži funkcije $x+y$, $|x-y|$, $x \cdot y$, $\mathrm{qt}(x,y)$ i zatvorena je za supstituciju, konačne sume i konačne proizvode, odnosno, ako je $f(\vec{x}, y) \in \mathcal{E}$ elementarna funkcija, onda su $\sum_{z<y} f(\vec{x}, z)$ i $\prod_{z<y} f(\vec{x}, z) \in \mathcal{E}$ elementarne funkcije.

Primer 15. Sve funkcije koje smo do sada naveli su elementarne.

Primer primitivno rekurzivne fukcije koja nije elementarna je iteracija eksponencijalne funkcije $s(x,y)$:

$$s(x,o) = x, s(x,1) = x^x, s(x,2) = x^{x^x}, s(x,3) = x^{x^{x^x}}, \ldots .$$

Primer 16. Neka je $s(x,0) = x$ i za sve $y \in \omega$, $s(x,y+1) = x^{s(x,y)}$. Za svaku elementarnu funkciju $f(x_1, \ldots, x_n)$, postoji prirodan broj $y \in \omega$ takav da za sve $x_1, \ldots, x_n \in \omega$,

$$\max(x_1, \ldots, x_n) > 0 \;\Rightarrow\; f(x_1, \ldots, x_n) < s(\max(x_1, \ldots, x_n), y).$$

Dakle, funkcija $s(x,y)$ je primitivno rekurzivna i raste brže od svake elementarne funkcije, tj. $s \notin \mathcal{E}$.

Na osnovu dosadašnjih razmatranja, izgleda kao da klasa primitivno rekurzivnih funkcija sadrži sve intuitivno izračunljive funkcije. Međutim, svako izvođenje primitivno rekurzivne funkcije je konačan niz sastavljen od konačnog broja baznih funkcija i konačnog broja primena supstitucije i rekurzije, pa se skup primitivno rekurzivnih funkcija može efektivno numerisati. Ako je $(f_n : n \in \omega)$ efektivna numeracija svih unarnih primitivno rekurzivnih funkcija, funkcija $g(x) = f_x(x) + 1$ ne može biti primitivno rekurzivna jer, za svako $n \in \omega$, $g \neq f_n$. Ipak, funkcija g jeste intuitivno izračunljiva. Za svako $x \in \omega$, vrednost $g(x)$ može se dobiti po sledećoj proceduri: "odredi se f_x i izračuna $f_x(x) + 1$".

Ovaj argument može se primeniti na svaku klasu totalnih funkcija, pa dakle klasa svih intuitivno izračunljivih funkcija nužno sadrži parcijalno definisane funkcije. Samo u takvoj klasi funkcija, ne može se sprovesti argument dijagonalizacije. U proizvoljnoj efektivnoj numeraciji unarnih primitivno rekurzivnih funkcija $(f_n : n \in \omega)$, neka je

$$g(x) = \begin{cases} f_x(x) + 1 & \text{ako je vrednost } f_x(x) \text{ definisana,} \\ \text{nedefinisano} & \text{inače.} \end{cases}$$

Kako su funkcije parcijalno definisane, prethodni argument više nije korektan. Nije tačno da za svako $x \in \omega$, $g \neq f_x$ jer, $f_x(x)$ ne mora biti definisano. Kada se ima u vidu intuitivna ideja izračunljivosti, parcijalno definisane funkcije izgledaju sasvim prirodno. Za svaku mehaničku proceduru izračunavanja, lako je zamisliti okolnosti u kojima se ona nikada ne završava.

Klasa $\mathcal{R}$ *rekurzivnih funkcija* je najmanja klasa funkcija prirodnih brojeva koja sadrži osnovne funkcije i zatvorena je za supstituciju, rekurziju i minimizaciju. Pritom, minimizacija je definisana na sledeći način:

Minimizacija: Za svako $\vec{x} \in \omega^n$, $\in \omega$ i svaku funkciju $f(\vec{x}, y)$, neka je

$$\mu y\,(f(\vec{x}, y) = 0) = \begin{cases} \text{najmanji } y \text{ takav da} & \\ \text{za sve } z \leq y,\ f(\vec{x}, z) & \text{ako takav } y \text{ postoji,} \\ \text{postoji i } f(\vec{x}, y) = 0 & \\ & \\ \text{nedefinisano} & \text{inače.} \end{cases}$$

Funkcija $\mu y\,(f(\vec{x}, y) = 0)$ dobijena je neograničenom minimizacijom funkcije $f(\vec{x}, y)$, odnosno, predikata $f(\vec{x}, y) = 0$. Ako je funkcija $f(\vec{x}, y)$ rekurzivna, funkcija $\mu y\,(f(\vec{x}, y) = 0)$ je takođe rekurzivna.

Intuitivno, postupak izračunavanja vrednosti funkcije $\mu y\,(f(\vec{x}, y) = 0)$ je sledeći: izračunavamo vrednosti $f(\vec{x}, 0)$, $f(\vec{x}, 1), \ldots$, sve dok se ne dobije prvi prirodan broj z takav da $f(\vec{x}, z) = 0$ i tada je $\mu y\,(f(\vec{x}, y) = 0) = z$.

Predikat $R(\vec{x})$ je rekurzivan ili *odlučiv* ako je njegova karakteristična funkcija $c_R(\vec{x})$ rekurzivna. Slično, skup $A \subseteq \omega$ je *rekurzivan* ako je karakteristična funkcija $c_A(x)$ rekurzivna.

Primer 17. Ako je $R(\vec{x}, y)$ odlučiv predikat, $g(\vec{x}) = \mu y\, R(\vec{x}, y)$ je rekurzivna funkcija.

Zapravo, $g(\vec{x}) = \mu y\,(\overline{\mathrm{sg}}(c_R(\vec{x}, y)) = 0)$.

Po definiciji, $\mathcal{P} \subseteq \mathcal{R}$, ali kako su praktično sve poznate funkcije primitivno rekurzivne, nije odmah jasno da li klasa $\mathcal{R}$ stvarno sadrži funkciju koja ne pripada klasi $\mathcal{P}$. U trivijalnom smislu, to je tačno jer, polazeći od totalne izračunljive funkcije, primenom μ-operatora može se dobiti parcijalno definisana rekurzivna funkcija.

Primer 18. Neka je $f(x,y) = |x - y^2|$. Primenom neograničene minimizacije dobija se funkcija $g(x) = \mu y\,(f(x,y) = 0)$ koja nije totalna. Ako je x kvadrat prirodnog broja, $g(x) = \sqrt{x}$, a ako to nije slučaj, vrednost $g(x)$ ne postoji.

Mnogo složeniji problem predstavlja egzistencija totalne rekurzivne funkcije koja nije primitivno rekurzivna. Primer takve funkcije je *Akermanova funkcija*. Ona pokazuje da u klasi totalnih primitivno rekurzivnih funkcija nije moguće definisati operator neograničene minimizacije. Definisana je sledećim relacijama: za sve $x, y \in \omega$,

$$\begin{aligned}
&f(0,y) = y + 1,\\
&f(x+1,0) = f(x,1),\\
&f(x+1,y+1) = f(x, f(x+1,y)).
\end{aligned}$$

Primer 19. Postoji jedinstveno određena fukcija $f(x,y)$ koja zadovoljava prethodne uslove.

Skup uslova koji određuje funkciju $f(x,y)$ podseća na neku vrstu dvojne rekurzije i samo po sebi uopšte nije jasno da li je neprotivrečan. Međutim, indukcijom po $x \in \omega$, sa indukcijom po $y \in \omega$ u induktivnom koraku, dokazuje se da:

– za sve $x, y \in \omega$, $x > 0$, vrednost funkcije $f(x,y)$ određena je konačnim skupom $\{f(u,v) : u \leq x \text{ i } v < y\}$ njenih prethodno izračunatih vrednosti.

Akermanova funkcija spada u klasu takozvanih brzo rastućih funkcija. Teško je verovati da konkretan računar u razumnom vremenu može izračunati vrednost $f(7,1)$. Po jednoj definiciji mere brzine rasta aritmetičkih funkcija, njena brzina jednaka je Kantorovom ordinalu ε_0. Zapravo, primitivna nerekurzivnost Akermanove funkcije posledica je njenog brzog rasta; ona raste brže od svake primitivno rekurzivne funkcije.

Primer 20. Akermanova funkcija ima sledeće osobine: za sve $x, y \in \omega$,

(a) $y < f(x,y)$, $f(x,y) < f(x,y+1)$,
(b) $f(x,y+1) \leq f(x+1,y)$, $f(x,y) < f(x+1,y)$,
(c) $f(1,y) = y + 2$ i $f(2,y) = 2y + 3$.

Primer 21. Akermanova funkcija $f(x,y)$ zadovoljava sledeće uslove:

(a) Za proizvoljne $x_1, \ldots, x_n \in \omega$ postoji $x \in \omega$ takvo da za svaki prirodan broj $y \in \omega$, važi nejednakost $\sum_{i=1}^{n} f(x_i, y) \leq f(x,y)$.

(b) Za svaku primitivno rekurzivnu funkciju $g(x_1, \ldots, x_n)$, postoji $x \in \omega$ takvo da za sve $x_1, \ldots, x_n \in \omega$, $g(x_1, \ldots, x_n) < f(x, x_1 + \cdots + x_n)$,

Tvrđenje se dokazuje na osnovu svojstava funkcije $f(x, y)$ navedenih u prethodnom primeru. Pritom, tvrđenje (a) se prvo dokazuje za slučaj $n = 2$, kada je $x = \max(x_1, x_2) + 4$.

Rekurzija koja se javlja u definiciji Akermanove funkcije znatno je jača od osnovne varijante rekurzije. Formalno, to sledi i iz činjenice da $f(x, y)$ nije primitivno rekurzivna funkcija. Međutim, neposredan dokaz rekurzivnosti Akermanove funkcije je veoma težak. Kasnije, na osnovu jednog posebnog oblika teoreme rekurzije, izložićemo značajno jednostavniji dokaz.

Primer 22. Postoji rekurzivna funkcija koja zadovoljava sledeće uslove:

$$f(0, y) = y + 1,\ f(1, y) = y + 2,\ f(x + 2, 0) = f(x + 1, 1),$$
$$f(x + 2, y + 1) = f(x + 1, f(x + 1, f(x + 2, y))).$$

Prvobitno, Gedel i Klini razmatrali su klasu $\mathcal{R}_0$ takozvanih *μ-rekurzivnih funkcija.* Klasa $\mathcal{R}_0$ je najmanja klasa koja sadrži osnovne funkcije i zatvorena je za supstituciju, rekurziju i primenu μ-operatora, pod uslovom da ova primena kao rezultat ima totalnu funkciju. Klasa totalnih rekurzivnih funkcija ipak ne sadrži sve intuitivno izračunljive funkcije. Postoji parcijalno definisana rekurzivna funkcija koja nema proširenje do totalne rekurzivne funkcije. Glavni nedostatak ove klase funkcija je u tome što ona sama nije efektivna. Klasa $\mathcal{R}_0$ nema efektivno kodiranje, pa u njoj ne važe ključne teoreme opšte teorije izračunljivosti, odnosno, za nju se takva teorija uopšte i ne može razviti. Na primer, za ovu klasu ne važi teorema o univerzalnoj funkciji, jedna od osnovnih teorema bez koje ova teorija praktično nije moguća. Takođe, sam predikat "f je totalna izračunljiva funkcija" nije odlučiv; za zadati indeks rekurzivne funkcije ne može se efektivno utvrditi da li je ona totalna.

Idealni računar

Osim aritmetizacije, u zasnivanjima teorije efektivnosti značajno mesto ima ideja da se izračunavanje shvati kao determinisana procedura koja se izvršava, po utvrđenom programu i korak po korak, nad konačnim matematičkim objektima. Paradigmu ovakvih ideja pretstavlja *idealni računar.* On se od realnog razlikuje samo u tome što, makar potencijalno, nema nikakva ograničenja na memorijski prostor i veličinu ulaznih podataka.

Idealni računar ima niz registara $R_1, R_2, \dots, R_n, \dots$ koji u svakom trenutku redom sadrže prirodne brojeve $r_1, r_2, \dots, r_n, \dots$. Računar je sposoban da interpretira i izvodi određene *instrukcije* koje odgovaraju jednostavnim kalkulacijama sa prirodnim brojevima. Konačan niz takvih instrukcija je *program*. Računar prepoznaje i izvršava sledeće instrukcije:

(a) Za svako $n \geq 1$, instrukciju $Z(n)$ računar izvršava tako što u registar R_n unosi 0, a sve druge registre ostavlja nepromenjenim. Instrukciju tipa $Z(n)$ nazivamo *nula instrukcijom*.

(b) Za svako $n \geq 1$, instrukciju $S(n)$ računar izvršava tako što sadržaj registra R_n uvećava za 1, a sve druge registre ostavlja nepromenjenim. Instrukcija tipa $S(n)$ je *instrukcija naslednika*.

(c) Za sve $m, n \geq 1$, instrukciju $T(m, n)$ računar izvršava tako što u registar R_n unosi broj r_m, odnosno sadržaj registra R_m, a sve druge registre, uključujući i R_m, ostavlja nepromenjenim. Instrukcija $T(m, n)$ je *instrukcija prenosa*.

(d) Za sve $m, n, q \geq 1$, instrukciju $J(m, n, q)$ računar izvršava na sledeći način: ako su sadržaju registara R_m i R_n jednaki, računar prelazi na izvršavanje q-te instrukcije u datom programu, a ako su sadržaji registara R_m i R_n različiti, računar prelazi na izvršavanje sledeće instrukcije u nizu instrukcija datog programa. Instrukcija tipa $J(m, n, q)$ je *instrukcija prelaza*.

Izračunavanje po programu $P = (I_1, \dots, I_s)$, za *početnu konfiguraciju* $(r_1, r_2, \dots)$ sadržaja registara, izvršava se na sledeći način:

Izračunavanje počinje izvršavanjem instrukcije I_1. Kada izvrši instrukciju I_k računar prelazi na izvršavanje *sledeće instrukcije*:

– ako I_k nije instrukcija prelaza, sledeća instrukcija je I_{k+1},

– ako je $I_k = J(m, n, q)$ i $r_m = r_n$, sledeća instrukcija je I_q, a ako je $r_m \neq r_n$, sledeća instrukcija je I_{k+1}.

Ukoliko sledeća instrukcija u programu ne postoji, izračunavanje se završava, a konfiguracija sadržaja registara je *završna konfiguracija*.

Ako je P program i $(a_1, a_2, \dots)$ početna konfiguracija, odgovarajuće izračunavanje označavamo sa $P(a_1, a_2, \dots)$.

Sa $P(a_1, a_2, \dots)\downarrow$ označavamo izračunavanje $P(a_1, a_2, \dots)$ koje se završava, a sa $P(a_1, a_2, \dots)\uparrow$, označavamo da se odgovarajuće izračunavanje koje se nikada ne završava.

U toku svakog izračunavanja samo konačan broj sadržaja registara je različit od nule. Svaka početna konfiguracija ima oblik $(a_1, \dots, a_n, 0, 0, ..)$ pa izračunavanje $P(a_1, a_2, \dots)$ označavamo sa $P(a_1, \dots, a_n)$ ili sa $P(\vec{a})$.

Izračunavanje $P(a_1, \dots, a_n)$ *konvergira* prirodnom broju $a \in \omega$, u oznaci $P(a_1, \dots, a_n) \downarrow a$, ako $P(a_1, \dots, a_n) \downarrow$ i sadržaj registra R_1 u završnoj konfiguraciji je broj a.

Program P *izračunava* funkciju f ako za sve $a_1, \dots, a_n, a \in \omega$

$$P(\vec{a}) \downarrow a \quad \Leftrightarrow \quad \vec{a} \in \mathrm{dom}(f) \text{ i } f(\vec{a}) = a.$$

Funkcija f je *izračunljiva* ako postoji program koji izračunava f. Klasu izračunljivih funkcija označavamo sa $\mathcal{I}$.

Primer 1. Neka je $(x, y, 0, \dots)$ početna konfiguracija i P program koji se sastoji od sledećih instrukcija:

$$I_1 = J(3,2,5),\ I_2 = S(1),\ I_3 = S(3) \text{ i } I_4 = J(1,1,1).$$

Izračunavanje $P(x, y)$ izvršava se tako što u svakom koraku sadržaje registara R_1 i R_3 uvećavamo za 1 sve dok se ne izjednače sadržaji registara R_2 i R_3. Završna konfiguracija je $(x+y, y, y, 0, \dots)$, a rezultat izračunavanja $P(x, y)$ je sadržaj prvog registra $x+y$. Za proizvoljne $x, y \in \omega$, izračunavanje $P(x, y)$ se završava, tj. program P određuje totalnu funkciju.

Kada se program P primeni na konfiguraciju (x, y, z), ako je $z \leq y$, završna konfiguracija je $(x + y - z, y, y)$, a ako je $z > y$, izračunavanje $P(x, y, z)$ nikada se ne završava. U ovom slučaju program P izračunava parcijalno definisanu funkciju.

Neka je P program i $n \geq 1$ prirodan broj. Za proizvoljne prirodne brojeve $a_1, \dots, a_n \in \omega$ neka je

$$f_p^n(a_1, \dots, a_n) = \begin{cases} \text{jedinstven } a \text{ takav da} \\ P(a_1, \dots, a_n) \downarrow a & \text{ako } P(a_1, \dots, a_n) \downarrow, \\ \\ \text{nedefinisano} & \text{ako } P(a_1, \dots, a_n) \uparrow. \end{cases}$$

Dakle, za svaki prirodan broj $n \geq 1$, program P određuje n-arnu izračunljivu fukciju f_p^n. Sa druge strane, izračunljiva funkcija nema jedinstveno određen program.

Primer 2. Ako je f izračunljiva funkcija, postoji beskonačno mnogo programa za izračunavanje funkcije f.

Ako je Q program koji se iz programa P dobija dodavanjem instrukcije $J(1,1,2)$ ispred ostalih instrukcija programa P, za svako $n \geq 1$, programi P i Q izračunavaju istu funkciju, tj. $f_p^n = f_q^n$.

Obrnut problem, da li dva programa izračunavaju istu funkciju, značajno je složeniji i o njemu će kasnije biti više reči.

Osnovni rezultat ovog poglavlja jeste jednakost klasa izračunljivih i rekurzivnih funkcija. Sa jedne strane, neophodno je izvršavanja programa idealnog računara predstaviti rekurzivnim funkcijama i sa druge, pokazati da klasa izračunljivih funkcija sadrži osnovne funkcije i zatvorena je za supstituciju, rekurziju i minimizaciju. Da bismo to postigli, neophodno je do određenog stepena razviti ideju idealnog računara.

Slično realnom računaru i na idealnom se javlja potreba da rezultat primene određenog programa trajno ili privremeno sačuvamo i po potrebi koristimo za izračunavanje po nekom drugom programu. Da bi se to ostvarilo, neophodno je da se programi prerade u odgovarajuću formu.

Program $P = (I_1, \ldots, I_s)$ je u *standardnoj formi* ako svaka njegova instrukcija prelaza $J(m, n, q)$ zadovoljava uslov $q \leq s + 1$. Sasvim je jasno da svaki program P ima standardnu formu P^*. Pritom, za sve $a_1, \ldots, a_n, a \in \omega$, $P(a_1, \ldots, a_n) \downarrow a$ ako i samo ako $P^*(a_1, \ldots, a_n) \downarrow a$. Stoga, uvek pretpostavljamo da su programi zadati u standardnoj formi.

Ako programi P i Q sadrže redom $s, t \geq 1$ instrukcija, njihova *kompozicija* je program $PQ = (I_1, \ldots, I_s, I_{s+1}, \ldots, I_{s+t})$ koji se sastoji od instrukcija $I_1, \ldots, I_s$ programa P i instrukcija $I_{s+1}, \ldots, I_{s+t}$ programa Q. Pritom, svaka instrukcija prelaza $J(m, n, q)$ programa Q, zamenjena je instrukcijom $J(m, n, s + q)$.

Intuitivno, svako izračunavanje po programu PQ sastoji se od izračunavanja po programu P, na čiju se završnu konfiguraciju izvršava izračunavanje po programu Q.

Kako je program P konačan niz instrukcija, postoji najmanji prirodan broj $n_p \geq 1$ takav da, za sve $n > n_p$, registri R_n ostaju nepromenjeni tokom izračunavanja po programu P. Prirodan broj n_p je *dubina programa* P. Ako je $n_p \in \omega$ dubina programa P, registre R_n, za $n > n_p$, možemo koristiti kao memorijski prostor.

Često je u toku nekog izračunavanja neophodno izvršiti program P nad podacima $a_1, \ldots, a_n$ koji su smešteni u registrima $R_{l_1}, \ldots, R_{l_n}$ i rezultat eventualno sačuvati u nekom datom registru. Da bi se to postiglo, naredbama $T(l_1, 1), \ldots, T(l_n, n)$ podatke $a_1, \ldots, a_n$ prebacujemo u prvih n registara, naredbama $Z(n + 1), \ldots, Z(n_p)$ oslobađamo registre neophodne za izvršavanje programa P, izvršavamo izračunavanje po programu P i konačno, instrukcijom $T(1, l)$, rezultat izračunavanja memorišemo u registru R_l. Program ove procedure označavamo sa $P[l_1, \ldots, l_n \to l]$.

Teorema 1. Svaka rekurzivna funkcija je izračunljiva.

Dokaz: Klasa $\mathcal{I}$ sadrži osnovne funkcije. Konstanta 0 izračunava se po programu $Z(1)$, funkcija s po programu $S(1)$, a funkcija U_i^n po programu $T(i,1)$.

Tvrdimo da je klasa $\mathcal{I}$ je zatvorena za supstituciju. Pretpostavimo da se funkcija $h(\vec{x})$ dobija supstitucijom izračunljivih funkcija $g_1(\vec{x}), \dots, g_k(\vec{x})$ u izračunljivoj funkciji $f(y_1, \dots, y_k)$.

Neka su $F, G_1, \dots, G_k$ programi za izračunavanje funkcija $f, g_1, \dots, g_k$. Intuitivno, program za izračunavanje funkcije h je sledeći:

Za početnu konfiguraciju $(x_1, \dots, x_n, 0, 0)$, podatke $x_1, \dots, x_n$ čuvamo u registrima kojima se tokom izvršavanja programa $G_1, \dots, G_k$ i F neće menjati. Neka je $m = \max\{n, k, n_p, n_{g_1}, \dots, n_{g_k}\}$. Podatke $x_1, \dots, x_n$ čuvamo redom u registrima $R_{m+1}, \dots, R_{m+n}$.

Vrednosti $g_1(\vec{x}), \dots, g_k(\vec{x})$ izračunavamo po programima $G_1, \dots, G_k$ i smeštamo redom u registre $R_{m+n+1}, \dots, G_{m+n+k}$. Za tako izračunate vrednosti, po programu F izračunavamo vrednost $h(\vec{x})$.

Dakle, funkciju h izračunavamo po programu H koji je kompozicija sledećih programa:

$$\begin{aligned}&T(1, m+1), \dots, T(n, m+n), G_1[m+1, \dots, m+n \to m+n+1], \cdots,\\ &G_k[m+1, \dots, m+n \to m+n+k], F[m+n+1, \dots, m+n+k \to 1].\end{aligned}$$

Klasa $\mathcal{I}$ izračunljivih funkcija zatvorena je za rekurziju. Neka su $f(\vec{x})$ i $g(\vec{x}, y, z)$ izračunljive funkcije. Funkcija $h(\vec{x}, y)$ koja se dobija rekurzijom iz funkcija f i g je izračunljiva funkcija.

Neka je $\vec{x} = (x_1, \dots, x_n)$ i F, G redom programi za izračunavanje funkcija f i g. Takođe, neka je $m = \max\{n+2, n_f, n_g\}$.

Intuitivno, ako je $(x_1, \dots, x_n, y, 0, 0, \dots)$ početna konfiguracija, vrednosti $x_1, \dots, x_n, y$ čuvamo u registrima $R_{m+1}, \dots, R_{m+n}, R_{m+n+1}$. Registar R_{m+n+2} koristimo kao brojač koraka izračunavanja, a u registar R_{m+n+3} smeštamo vrednost $h(\vec{x}, k)$ u k-tom koraku izračunavanja.

Izračunavanje počinjemo izvršavanjem programa F i dobijenu vrednost $h(\vec{x}, 0)$ i smeštamo u registar R_{m+n+3}. Ako je $y \neq 0$, po programu G izračunavamo vrednosti $h(\vec{x}, 1), \dots, h(\vec{x}, k)$, sve dok se k ne izjednači sa y. Program H za izračunavanje funkcije h je sledeći:

$$\begin{aligned}&T(1, m+1), \dots, T(n+1, m+n+1),\\ &F[1, \dots, n \to m+n+3], I_q = J(m+n+1, m+n+2, p),\\ &G[m+1, \dots, m+n, m+n+2, m+n+3 \to m+n+3],\\ &S(m+n+2), J(1,1,q), I_p = T(m+n+3, 1).\end{aligned}$$

Konačno, klasa $\mathcal{I}$ izračunljivih funkcija zatvorena je za minimizaciju. Pretpostavimo da je funkcija $g(\vec{x}) = \mu y\,(f(\vec{x}, y) = 0)$ dobijena minimizacijom izračunljive funkcije $f(\vec{x}, y)$, $\vec{x} \in \omega^n$. Neka je F program za izračunavanje funkcije $f(\vec{x}, y)$ i $m = \max\{n, n_f\}$.

Intuitivno, vrednosti $\vec{x}$ čuvamo u registrima $R_{m+1}, \ldots, R_{m+n}$, u registru R_{m+n+1} brojimo korake izračunavanja, vrednosti funkcije $f(\vec{x}, k)$ izračunavamo po programu F i upoređujemo sa sardžajem registra R_{m+n+2} koji uvek ima vrednost 0. Eventualno, kada se tokom ovog izračunavanja prvi put dobije da je $f(\vec{x}, k) = 0$, vrednost funkcije $g(\vec{x})$ jednaka je prirodnom broju $k \in \omega$, pa u tom slučaju sadržaj registra R_{m+n+1} prenosimo u registar R_1. Dakle, program G za izračunavanje funkcije g sledeći:

$$\begin{aligned}
&T(1, m+1), \ldots, T(n, m+n),\\
&F[m+1, \ldots, m+n+1 \to m+n+3],\\
&J(m+n+3, m+n+2, q),\\
&S(m+n+1), J(1,1,p), I_q = T(m+n+1, 1).
\end{aligned}$$

Prva instrukcija u programu $F[m+1, \ldots, m+n+1 \to m+n+3]$ označena je sa I_p. To konačno znači da je svaka rekurzivna funkcija izračunljiva na idealnom računaru. $\Box$

Dokaz obratnog tvrđenja, da je svaka izračunljiva funkcija rekurzivna, pretpostavlja kodiranje izračunljivih funkcija. Preciznije, za svaku izračunljivu funkciju f_p^n, pomoću rekurzivnih funkcija, za zadatu početnu konfiguraciju $(a_1, \ldots, a_n, 0, 0, \ldots)$ može se potpuno opisati procedura izvršavanja programa P. Da bismo to postigli, konfiguracije i programe kodiramo različitim primitivno rekurzivnim funkcijama.

Za kodiranje konfiguracija koristimo funkciju: za svako $a \in \bigcup_{n>0} \omega^n$, ako je $a = (a_1, \ldots, a_n)$, broj $c(a) = 2^{a_1+1} \cdot 3^{a_2+1} \cdots p_n^{a_n+1}$ je kod niza a.

Obratno, ako je zadat prirodan broj $b \in \omega$, primitivno rekurzivna funkcija $\mathrm{l}(b) = \mu z < y\,((b)_{z+1} = 0)$ određuje dužinu niza $a \in \omega^{\mathrm{l}(b)}$ kodiranog prirodnim brojem b, a njegovi elementi su $a_i = (b)_i \dot{-} 1$, $1 \leq i \leq \mathrm{l}(b)$.

Ključna ideja teorije izračunljivosti jeste efektivna numeracija klase $\mathcal{R}$ rekurzivnih funkcija. U realizaciji takve numeracije koristimo kodiranje programa idealnog računara.

Nula instrukcije $Z(n)$ kodiramo prirodnim brojem $4(n-1)$, a instrukcije naslednika $S(n)$ sa $4(n-1)+1$, za svako $n \in \omega$. Instrukcije prenosa $T(m,n)$ kodiramo sa $4\langle m-1, n-1\rangle + 2$ i konačno, a instrukcije prelaza $J(m,n,q)$ kodiramo sa $4\langle\langle m-1, n-1\rangle, q-1\rangle + 3$, za sve $m, n, q \in \omega$. Na taj način, za svaku instrukciju I, efektivno je određen kod $\beta(I)$.

Ako je zadat prirodan broj x, primitivno rekurzivna funkcija $\mathrm{rm}(x, 4)$ određuje tip instrukcije. U zavisnosti od vrednosti ostatka, dakle po slučajevima, pomoću inverznih funkcija Kantorove kodirajuće funkcije, određujemo $I_x = \beta^{-1}(x)$, odnosno instrukciju I_x čiji je kod $x \in \omega$.

Ako je $P = I_1, \ldots, I_s$ program i $\tau : \bigcup_{n>0} \omega^n \to \omega$ kodiranje konačnih nizova, prirodan broj $\gamma(P) = \tau(\beta(I_1), \ldots, \beta(I_n))$ je *kod programa* P.

U ovom slučaju koristimo sledeće kodiranje: za svako $a \in \bigcup_{n>0} \omega^n$, ako je $a = (a_1, \ldots, a_n)$, $\tau(a) = \sum_{k=1}^{n} 2^{a_1+\cdots+a_k+k-1} - 1$.

Funkcija τ je obostrano jednoznačna. Izračunavanje vrednosti $\tau^{-1}(x)$ zasniva se na činjenici da svaki prirodan broj ima jedinstvenu reprezentaciju po rastućim stepenima broja dva.

Za zadato $x \in \omega$, postoje jedinstveni $0 \le b(x,1) < \cdots < b(x, d(x))$ takvi da je $x + 1 = 2^{b(x,1)} + \cdots + 2^{b(x,d(x))}$.

Funkcija $d(x)$ je primitivno rekurzivna. Ona određuje dužinu niza kodiranog prirodnim brojem $x \in \omega$.

Za svako $z \in \omega$, ako je $z = 0$ ili $z > d(x)$, neka je $b(x, z) = 0$. Na taj način dobija se totalna funkcija $b(x, z)$ koja je primitivno rekurzivna.

Konačno, članovi niza čiji je kod prirodan broj $x \in \omega$, određeni su primitivno rekurzivnom funkcijom:

$$
\begin{aligned}
&a(x, z) = b(x, z) \text{ ako } z = 0 \text{ ili } z = 1,\\
&a(x, z+1) = (b(x, z+1) \dot{-} b(x, z)) \dot{-} 1, \text{ za sve } z > 1.
\end{aligned}
$$

Na taj način, za zadato $x \in \omega$, dobijen je niz kodova instrukcija programa $P = \gamma^{-1}(x)$ koji je kodiran prirodnim brojem x. Za svaki član z niza $\tau^{-1}(x)$, u zavisnosti od vrednosti $\mathrm{rm}(z, 4)$, pomoću primitivno rekurzivne funkcije, određujemo instrukciju kodiranu sa $z \in \omega$.

Po definiciji kodiranja instrukcija β, ako $\mathrm{rm}(z, 4) = 0$, prirodan broj z kodira instrukciju oblika $Z(u(z))$, gde je $u(z) = \mathrm{qt}(z, 4) + 1$, a ako je $\mathrm{rm}(z, 4) = 1$, broj z kodira instrukciju $S(u(z))$.

Ako je $\mathrm{rm}(z, 4) = 2$, prirodan broj z kodira instrukciju prenosa oblika $T(u_1(z), u_2(z))$, gde je $u_1(z) = \pi_1(\mathrm{qt}(z, 4)) + 1$ i $u_2(z) = \pi_2(\mathrm{qt}(z, 4)) + 1$.

Konačno, ako je $\mathrm{rm}(z, 4) = 2$, instrukcija kodirana prirodnim brojem x je instrukcija prelaza oblika $J(v_1(z), v_2(z), v_3(z))$, gde je

$$
\begin{aligned}
v_1(z) &= \pi_1(\pi_1(\mathrm{qt}(z, 4)) + 1,\\
v_2(z) &= \pi_2(\pi_1(\mathrm{qt}(z, 4)) + 1,\\
v_3(z) &= \pi_2(\mathrm{qt}(z, 4)) + 1.
\end{aligned}
$$

Po definiciji, sve funkcije kojima se dekodiraju instrukcije su primitivno rekurzivne, pa je funkcija β^{-1} primitivno rekurzivna.

Za svako $e \in \omega$, sa P_e označavamo program $\gamma^{-1}(e)$. Po definiciji kodiranja γ, ako je $e_1 \neq e_2$, programi P_{e_1} i P_{e_2} su različiti, tj. $(P_e : e \in \omega)$ je efektivna numeracija programa idealnog računara bez ponavljanja.

U sledećim primerima naveden je jedan broj funkcija koje omogućavaju da se tok izračunavanja na idealnom računaru u potpunosti opiše primitivno rekurzivnim funkcijama. Takvim funkcijama prvo opisujemo izvršavanje instrukcija, a potom, čitavo izračunavanje po programu P, za početnu konfiguraciju $(x_1, \ldots, x_n)$, opisano je primitivno rekurzivnom funkcijom. Minimizacijom tako dobijene funkcije dobija se funkcija $f_p^n(\vec{x})$ definisana programom P što pokazuje da je svaka izračunljiva funkcija rekurzivna.

Primer 3. Sledeće funkcije su primitivno rekurzivne:

(a) $\mathrm{ln}(e) =$ "broj instrukcija programa P_e" ,

(b) $\mathrm{in}(e, j) = \begin{cases} \text{kod } j\text{-te instrukcije u } P_e & \text{ako } 1 \leq j \leq \mathrm{ln}(e) \\ 0 & \text{ako } \mathrm{ln}(e) < j \end{cases}$

Treba razlikovati redni broj instrukcije u programu P od njenog koda. Na osnovu definicije kodiranja programa, za svako $x \in \omega$, $\mathrm{ln}(x) = \mathrm{d}(x+1)$. Iz istog razloga, $\mathrm{in}(x, z) = a(x, z)$, pa su navedene funkcije primitivno rekurzivne.

U sledećem primeru opisujemo primenu instrukcije sa datim kodom na konfiguraciju koja je takođe zadata svojim kodom.

Primer 4. (a) Kod konfiguracije $\mathrm{nula}(c, n)$, koja se dobija primenom nulte instrukcije $Z(n)$ na konfiguraciju čiji je kod prirodan broj c, je primitivno rekurzivna funkcija.

Funkcija $\mathrm{nula}(c, n)$ je primitivno rekurzivna budući da se može izraziti na sledeći način: $\mathrm{nula}(c, n) = \mathrm{qt}(c, p_n^{(c)_n + 1})$.

(b) Kod konfiguracije $\mathrm{nasl}(c, n)$ koja se dobija primenom instrukcije naslednika $S(n)$ na konfiguraciju čiji je kod prirodan broj c je primitivno rekurzivna funkcija.

Kako je $\mathrm{nasl}(c, n) = c \cdot p_n$, funkcija $\mathrm{nasl}(c, n)$ je očigledno primitivno rekurzivna.

(c) Kod konfiguracije $\mathrm{pren}(c, m, n)$ koja se dobija primenom instrukcije prenosa $T(m, n)$ na konfiguraciju čiji je kod prirodan broj c je primitivno rekurzivna funkcija.

Kako je $\mathrm{pren}(c, m, n) = \mathrm{qt}(c \cdot p_n^{(c)_m + 1}, p_n^{(c)_n + 1})$, funkcija $\mathrm{pren}(c, m, n)$ je primitivno rekurzivna.

Primer 5. Funkcija $\mathrm{cn}(c, z)$ koja određuje kod konfiguracije dobijene primenom instrukcije čiji je kod z na konfiguraciju čiji je kod prirodan broj

c je primitivno rekurzivna.

To sledi iz činjenice da se funkcija $\mathrm{cn}(c, z)$, na osnovu prethodnih primera, može izraziti na sledeći način:

$$\mathrm{cn}(c, z) = \begin{cases} \mathrm{nula}(c, u(z)) & \text{ako } \mathrm{rm}(z, 4) = 0, \\ \mathrm{nasl}(c, u(z)) & \text{ako } \mathrm{rm}(z, 4) = 1, \\ \mathrm{pren}(c, u_1(z), u_2(z)) & \text{ako } \mathrm{rm}(z, 4) = 2, \\ c & \text{ako } \mathrm{rm}(z, 4) = 3. \end{cases}$$

Primer 6. Funkcija $\nu(c, j, z)$ koja određuje redni broj sledeće instrukcije posle primene instrukcije I_j, čiji je kod z, na konfiguraciju čiji je kod prirodan broj c ako je $j > 0$, a ako je $j = 0$, $\nu(c, j, z) = 0$ je primitivno rekurzivna.

Funkcija $\nu(c, j, z)$ je primitivno rekurzivna budući da se, na osnovu prethodnih primera, može dobiti na sledeći način:

$$\nu(c, , j, z) = \begin{cases} 0 & \text{ako } j = 0, \\ j+1 & \text{ako } \mathrm{rm}(z, 4) \neq 3 \text{ i } j \neq 0, \\ j+1 & \text{ako } (c)_{v_1(z)} \neq (c)_{v_2(z)},\ \mathrm{rm}(z, 4) = 3 \text{ i } j \neq 0, \\ v_3(z) & \text{ako } (c)_{v_1(z)} = (c)_{v_2(z)},\ \mathrm{rm}(z, 4) = 3 \text{ i } j \neq 0. \end{cases}$$

Neka je P_e program i $(x_1, \ldots, x_n)$ početna konfiguracija. Izračunavanje $P_e(\vec{x})$ izvršava se sukcesivnom primenom sledeće instrukcije na konfiguraciju koja je nastala primenom prethodnih instrukcija programa. Izvršavanje jedne instrukcije nazivamo *korakom izračunavanja*.

Za svako $t \geq 0$, *trenutna konfiguracija* c je kod konfiguracije posle izvršenih t koraka izračunavanja $P_e(\vec{x})$.

U svakom trenutku $t \geq 1$, *sledeća instrukcija* j je redni broj instrukcije u programu P_e koja se izvršava u narednom koraku izračunavanja $P_e(\vec{x})$.

Za svako $t \geq 0$, posle t koraka izvršavanja programa P_e, *stanje izračunavanja* $\sigma = \langle c, j \rangle$ je određeno kodom trenutne konfiguracije c i rednim brojem j sledeće instrukcije u koraku izračunavanja t.

Stanje izračunavanja σ, trenutna konfiguracija c i sledeća instrukcija j zavise od indeksa e, početne konfiguracije $\vec{x}$ i broja izvršenih koraka t.

Trenutnu konfiguraciju i sledeću instrukciju posle t koraka izračunavanja definišemo sledećim funkcijama:

$c_n(e, \vec{x}, t) =$ kod konfiguracije posle t koraka izračunavanja $P_e(\vec{x})$ i

$$j_n(e, \vec{x}, t) = \begin{cases} \begin{array}{l} \text{sledeća instrukcija} \\ \text{posle } t \text{ koraka} \\ \text{izračunavanja } P_e(\vec{x}) \end{array} & \text{ako } \neg P_e(\vec{x}) \downarrow \text{ za } t \text{ koraka}, \\ & \\ 0 & \text{ako } P_e(\vec{x}) \downarrow \text{ za } \leq t \text{ koraka}. \end{cases}$$

Za tako definisanu trenutnu konfiguraciju i sledeću instrukciju, posle t koraka izračunavanja $P_e(\vec{x})$, odgovarajuće stanje izračunavanja definišemo funkcijom $\sigma_n(e,\vec{x},t) = \langle c_n(e,\vec{x},t), j_n(e,\vec{x},t)\rangle$.

Primer 7. Pretpostavimo da je u toku izračunavanja po programu P_e trenutno stanje izračunavanja $\sigma = \langle c, j\rangle$. Sledeće funkcije su primitivno rekurzivne:

$$\mathrm{conf}(e,\sigma) = \begin{cases} \text{kod konfiguracije posle} & \\ \text{primene } j\text{-te instrukcije} & \text{ako } 1 \le j \le \ln(e), \\ \text{izračunavanja } P_e(\vec{x}) & \\ & \\ c & \text{inače.} \end{cases}$$

$$\mathrm{sled}(e,\sigma) = \begin{cases} \text{oznaka sledeće instrukcije} & \text{ako } 1 \le j \le \ln(e) \\ \text{posle primene } j\text{-te instruk-} & \text{i ako sledeća ins-} \\ \text{cije na konfiguraciju } c & \text{trukcija postoji,} \\ & \\ 0 & \text{inače.} \end{cases}$$

Primitivna rekurzivnost funkcija $\mathrm{conf}(e,\sigma)$ i $\mathrm{sled}(e,\sigma)$ sledi iz činjenice da se one dobijaju supstitucijom primitivno rekurzivnih funkcija $\mathrm{cn}(c,z)$, $\mathrm{in}(e,j)$ i $\nu(c,j,z)$:

$$\mathrm{conf}(e,\sigma) = \begin{cases} \mathrm{cn}(\pi_1(\sigma), \mathrm{in}(e,\pi_2(\sigma))) & \text{ako } 1 \le \pi_2(\sigma) \le \ln(e), \\ & \\ \pi_1(\sigma) & \text{inače.} \end{cases}$$

$$\mathrm{sled}(e,\sigma) = \begin{cases} \nu(\pi_1(\sigma), \pi_2(\sigma), \mathrm{in}(e,\pi_2(\sigma))) & \text{ako je taj broj} \le \ln(e), \\ & \\ 0 & \text{inače.} \end{cases}$$

Trenutna konfiguracija $\mathrm{conf}(e,\sigma)$ i sledeća instrukcija $\mathrm{sled}(e,\sigma)$ definisane su rekurzivno kao funkcije stanja izračunavanja. S druge strane, stanje izračunavanja, definisali smo kao funkciju trenutne konfiguracije i sledeće instrukcije pa izgleda da je ova definicija cirkularna. Ipak, ona je korektna budući da je stanje u koraku t definisano rekurzijom na osnovu vrednosti funkcija $\mathrm{conf}(e,\sigma)$ i $\mathrm{sled}(e,\sigma)$ u prethodnom koraku.

Primer 8. Stanje $\sigma_n(e,\vec{x},t)$, posle $t \ge 0$ koraka izračunavanja $P_e(\vec{x})$, definišemo rekurzijom pomoću Kantorove kodirajuće funkcije i primitivno rekurzivnih funkcija $\mathrm{conf}(e,\sigma)$ i $\mathrm{sled}(e,\sigma)$:

$$\begin{aligned} &\sigma_n(e,\vec{x},0) = \langle p_1^{x_1+1} \cdots p_n^{x_n+1}, 1\rangle, \\ &\sigma_n(e,\vec{x},t+1) = \langle \mathrm{conf}(e,\sigma_n(e,\vec{x},t)), \mathrm{sled}(e,\sigma_n(e,\vec{x},t))\rangle. \end{aligned}$$

Na osnovu do sada izloženih primera, za svaku početnu konfiguraciju $\vec{x}$ i svako $e \in \omega$, tok izračunavanja $P_e(\vec{x})$ može se kompletno opisati primitivno rekurzivnim funkcijama.

Teorema 2. Svaka izračunljiva funkcija je rekurzivna.

Dokaz : Neka je $f(\vec{x})$ izračunljiva funkcija i P_e program za njeno izračunavanje.

Ako je vrednost $f(\vec{x})$ definisana, izračunavanje $P_e(\vec{x})$ se završava u tačno $t_0 = \mu t\,(\pi_2(\sigma_n(e,\vec{x},t)) = 0)$ koraka i tada je $f(\vec{x}) = (\pi_1(\sigma_n(e,\vec{x},t_0)))_1$

Ako vrednost $f(\vec{x})$ nije definisana, izračunavanje $P_e(x)$ se ne završava, pa funkcija $\pi_2(\sigma_n(e,\vec{x},t))$ nikada nema vrednost nula. To zapravo znači da $\mu t\,(\pi_2(\sigma_n(e,\vec{x},t)) = 0)$ ne postoji. Otuda sledi da je

$$f(\vec{x}) = \pi_1(\sigma_n(e,\vec{x},\mu t\,(\pi_2(\sigma_n(e,\vec{x},t)) = 0)))_1,$$

tj. funkcija $f(\vec{x})$ je rekurzivna. □

Jednakost klasa izračunljivih i rekurzivnih funkcija približava nas ideji Čerčove teze. Dve nezavisne koncepcije intuitivne izračunljivosti daju isti rezultat. Istorijski posmatrano, sredinom ovog veka razvijeno je desetak takvih pristupa, međutim, svi oni vodili su klasi rekurzivnih funkcija tako da će u osnovi naših daljih razmatranja biti rekurzivne funkcije. Na sve druge formulacije ideje izračunljivosti, pozivaćemo se kao na intuitivne.

Intuitivno izračunljiva funkcija jeste funkcija za koju postoji bilo kakav dokaz efektivnosti. Shodno Čerčovoj tezi, takav dokaz smatraćemo dokazom njene rekurzivnosti, odnosno, svaka izračunljivost i rekurzivnost su sinonimi. To zapravo znači da će svi naši budući opisi algoritama rekurzivnih funkcija biti izraženi uobičajenim matematičkim terminima, bez direktnog i potpunog prevođenja u odgovarajući formalizam. Takav dokaz rekurzivnosti nazivamo *dokazom po Čerčovoj tezi.* Kada govorimo o rekurzivnosti procedura koje se izvode nad objektima koji nisu prirodni brojevi, poput formula ili njihovih dokaza, podrazumevamo rekurzivnost odgovarajućih operacija nad njihovim kodovima.

Rekurzivni skupovi

Osnovu teorije izračunljivosti čini efektivno kodiranje programa. Takvo kodiranje garantuje egzistenciju normalne forme izračunljive funkcije i njenu uniformnu parametrizaciju.

Za svaki prirodan broj $n \geq 1$, sa $\varphi_e^{(n)}$ označavamo n-arnu funkciju koja se izračunava po programu P_e. Zapravo, u ranijoj notaciji $\varphi_e^{(n)} = f_{P_e}^{(n)}$.

Klasu n-arnih izračunljivih funkcija označavamo sa $\mathcal{R}_n$. Pritom, niz

$$(\varphi_e^{(n)} : e \in \omega)$$

nabraja sve n-arne rekurzivne funkcije. Ako $f \in \mathcal{R}_n$, prirodan broj $e \in \omega$ takav da $f = \varphi_e$ je *indeks* izračunljive funkcije f.

Kako smo ranije naglasili, izračunljiva funkcija ima beskonačno mnogo programa, pa dakle beskonačno mnogo indeksa. Naravno, svaka rekurzivna funkcija ima prebrojivo mnogo indeksa.

Za svako $n \geq 1$, numeracijom $(\varphi_e^{(n)} : e \in \omega)$ rekurzivnih funkcija određena je i numeracija njihovih domena i kodomena.

Za svako $e \in \omega$, $W_e^{(n)} = \operatorname{dom} \varphi_e^{(n)}$ i $E_e^{(n)} = \operatorname{codom} \varphi_e^{(n)}$. U slučaju unarnih funkcija koristimo oznake φ_e, W_e i E_e.

Centralnu ulogu u teoriji rekurzivnih funkcija ima Klinijeva teorema o normalnoj formi. Za svaki prirodan broj $n \in \omega$, postoji odlučiv predikat čijom minimizacijom se dobija svaka n-arna izračunljiva funkcija. Smisao *Klinijevog predikata* je

$$T_n(e, \vec{x}, y) \quad \Leftrightarrow \quad P_e(\vec{x}) \downarrow (y)_1 \text{ posle } (y)_2 \text{ koraka izračunavanja.}$$

Na osnovu dokaza ekvivalencije rekurzivnih i izračunljivih funkcija, Klinijev predikat je zapravo primitivno rekurzivan.

Teorema 3. Teorema o normalnoj formi: Za svaki prirodan broj $n \geq 1$, postoji primitivno rekurzivan predikat $T_n(e, \vec{x}, y)$ takav da

$$\varphi_e^{(n)}(\vec{x}) = (\mu z\, T_n(e, \vec{x}, z))_1.$$

Dokaz: Za svako $n \geq 1$, $\vec{x} \in \omega$, označimo sa $S_n(e, \vec{x}, y, t)$ relaciju "$P_e(\vec{x}) \downarrow y$ za $\leq t$ koraka". Saglasno ranije uvedenoj notaciji,

$$S_n(e, \vec{x}, y, t) \quad \Leftrightarrow \quad j_n(e, \vec{x}, t) = 0 \text{ i } (c_n(e, \vec{x}, t))_1 = y.$$

Pritom, $j_n(e, \vec{x}, t)$ je redni broj sledeće instrukcije, a $c_n(e, \vec{x}, t)$ je kod konfiguracije posle $t \in \omega$ koraka izračunavanja $P_e(\vec{x})$.

Ako se izračunavanje $P_e(\vec{x})$ završava za $\leq t$ koraka, sledeća instrukcija je 0, pa je $j_n(e, \vec{x}, t) = 0$, a konfiguracija $c_n(e, \vec{x}, t)$ je završna konfiguracija. Rezultat izračunavanja $P_e(\vec{x})$ je sadržaj prvog registra $(c_n(e, \vec{x}, t))_1$. Obe funkcije su primitivno rekurzivne pa je predikat $S_n(e, \vec{x}, y, t)$ je takođe primitivno rekurzivan. Neka je

$$T_n(e, \vec{x}, z) \quad \Leftrightarrow \quad S_n(e, \vec{x}, (z)_1, (z)_2).$$

Kako se predikat $T_n(e, \vec{x}, z)$ dobija supstitucijom primitivno rekurzivnih funkcija $(z)_1$ i $(z)_2$ u primitivno rekurzivnom predikatu $S_n(e, \vec{x}, (z)_1, (z)_2)$, on sam mora biti primitivno rekurzivan. Tvrdimo da za svako $e \in \omega$ i svako $\vec{x} \in \omega^n$,

$$\varphi_e^{(n)}(\vec{x}) \text{ postoji ako i samo ako } \exists z \, T_n(e, \vec{x}, z).$$

Ako je $\varphi_e^{(n)}(\vec{x})$ definisano, postoje $y, t \in \omega$ takvi da $P_e(\vec{x}) \downarrow y$ za $\leq t$ koraka, tj. za $z = 2^y 3^t$ važi $T_n(e, \vec{x}, z)$.

Obratno, ako postoji prirodan broj $z \in \omega$ za koji važi $T_n(e, \vec{x}, z)$, onda po definiciji, $P_e(\vec{x}) \downarrow$, pa dakle $\varphi_e^{(n)}(\vec{x})$ postoji.

Dakle, vrednost $\varphi_e^{(n)}(\vec{x})$ postoji ako i samo ako postoji $z \in \omega$ takvo da važi $T_n(e, \vec{x}, z)$ ako i samo ako $\varphi_e^{(n)}(\vec{x}) = (\mu z \, T_n(e, \vec{x}, z))_1$. $\square$

Teorema o normalnoj formi pokazuje da se svaka rekurzivna funkcija može dobiti samo jednom primenom μ-operatora na primitivno rekurzivnu funkciju. To dokazuje da je klasa μ-rekurzivnih funkcija $\mathcal{R}_0$, koju smo ranije definisali, jednaka klasi totalnih izračunljivih funkcija.

Na osnovu teoreme o normalnoj formi neposredno sledi teorema o efektivnosti numeracije $(\varphi_e^{(n)} : e \in \omega)$ iračunljivih n-arnih funkcija. Rekurzivna funkcija koja vrši takvo nabrajanje naziva se *univerzalna funkcuja*, a njen program *univerzalni program* za klasu $\mathcal{R}_n$.

Teorema 4. Teorema o efektivnoj numeraciji: Za svako $n \geq 1$, postoji prirodan broj $u \in \omega$ takav da

$$\varphi_u^{(n+1)}(e, \vec{x}) = \varphi_e^{(n)}(\vec{x}).$$

Dokaz: Funkcija $f(e, \vec{x}) = (\mu y \, T_n(e, \vec{x}, z))_1$ dobija se minimizacijom odlučivog predikata $T_n(e, \vec{x}, z)$ pa mora biti rekurzivna. Dakle, postoji $u \in \omega$ takvo da $\varphi_u^{(n+1)}(e, \vec{x}) = (\mu z \, T_n(e, \vec{x}, z))_1$. Na osnovu teoreme o normalnoj formi, $\varphi_u^{(n+1)}(e, \vec{x}) = \varphi_e^{(n)}(\vec{x})$. $\square$

Intuitivno, za zadate e i $\vec{x}$, univerzalni program P_u dekodira e i izvršava izračunavanje $P_e(\vec{x})$. Pritom, izračunavanje $P_u(e, \vec{x})$ se završava ako i samo ako $P_e(\vec{x})$ se završava. To znači da je $\varphi_u^{(n+1)}(e, \vec{x}) = \varphi_e^{(n)}(\vec{x})$.

Problem: Prema teoremi o efektivnoj numeraciji, za svako $n \geq 1$, postoji $u(n) \in \omega$ za koji je funkcija $\varphi_{u(n)}^{(n+1)}(e, \vec{x})$ univerzalna za klasu n-arnih izračunljivih funkcija. Da li je $u(n)$ izračunljiva funkcija?

Za proizvoljnu izračunljivu funkciju sa bar dve promenljive, ako se određene promenljive shvate kao parametri, rezultujuća funkcija je takođe izračunljiva, a indeks tako dobijene funkcije može se rekurzivno odrediti iz indeksa polazne funkcije i vrednosti parametara.

Preciznije, za svako $n \geq 1$ i svako $e \in \omega$, ako se u funkciji $\varphi_e^{(n)}(\vec{x})$ fiksira $m \geq 1$ promenljivih $x_{i_1}, \ldots, x_{i_m}$, tj. ako se one shvate kao parametri, dobija se izračunljiva funkcija $\varphi_k^{(n-m)}$, $k \in \omega$, od $(n-m)$ promenljivih. Prirodno, kada je $m \geq n$, parametrizacijom se dobija konstanta.

Prirodno, indeks funkcije $\varphi_k^{(n-m)}$ zavisi od indeksa e funkcije $\varphi_e^{(n)}$ i vrednosti parametara $x_{i_1}, \ldots, x_{i_m}$. Za svako $n \geq 1$, takva parametrizacija transformiše numeraciju n-arnih rekurzivnih funkcija $(\varphi_e^{(n)} : e \in \omega)$ u numeraciju $(n-m)$-arnih rekurzivnih funkcija

$$(\varphi^{(n-m)}_{f(e, x_{i_1}, \ldots, x_{i_m})} : e \in \omega).$$

Teorema o parametrizaciji pokazuje da je ovaj prelaz efektivan, odnosno, da je funkcija $f(e, x_{i_1}, \ldots, x_{i_m})$ rekurzivna. Pre nego što formulišemo opštu varijantu, razmotrićemo najprostiji slučaj ove teoreme.

Primer 1. Ako je $f(x, y)$ rekurzivna funkcija, postoji totalna rekurzivna funkcija $k(x)$ takva da $f(x, y) = \varphi_{k(x)}(y)$.

Za fiksirano $x \in \omega$, funkcija $f(x, y)$ je unarna i izračunljiva, pa postoji prirodan $k(x) \in \omega$ za koji je $f(x, y) = \varphi_{k(x)}(y)$. Indeks $k(x)$ može se rekurzivno odrediti na osnovu vrednosti parametra $x \in \omega$:

Neka je P_e program za izračunavanje funkcije $f(x, y)$. Početnu konfiguraciju $(y, 0, \ldots)$ program $P_{k(x)}$ transformiše u konfiguraciju $(x, y, 0, \ldots)$, a potom izvršava izračunavanje $P_e(x, y)$. Dakle, $k(x)$ je kod programa

$$T(1,2), Z(1), \underbrace{S(1), \cdots, S(1)}_{x \text{ puta}}, P_e.$$

Kod ovog programa zavisi od $x, e \in \omega$ i označava se sa $s(e, x)$. Kako je kodirajuća funkcija totalna i obostrano jednoznačna, $s(e, x)$ je totalna obostrano jednoznačna rekurzivna funkcija. Jasno, kako je indeks e zadat, $k(x) = s(e, x)$ je totalna izračunljiva funkcija $k(x) = s(e, x)$ je određena samim kodiranjem programa.

Teorema 5. Teorema o parametrizaciji: Za sve $m \geq 1$, postoji $(m+1)$-arna totalna izračunljiva funkcija $s_m(e, \vec{x})$ takva da za svako $n \geq 1$,

$$\varphi_e^{m+n}(\vec{x}, \vec{y}) = \varphi^{(n)}_{s_m(e, \vec{x})}(\vec{y}).$$

Dokaz: Za svako $e \in \omega$, neka je $n_e \geq 1$ dubina programa P_e i neka je Q_e program $(T(1, n_e+1), \dots, T(n_e, 2n_e))$. Sadržaje registara $R_1, \dots, R_{n_e}$ koji mogu biti operativni u izvršavanju programa P_e, program Q_e prenosi redom u registre $R_{n_e+1}, \dots, R_{2n_e}$.

Za svaki prirodan broj $i \geq 1$ i svako $x \in \omega$, neka je $I_x(i)$ program koji sadržaj registra R_i zamenjuje brojem x.

Za zadato $m \geq 1$, neka je $s_m(e, \vec{x})$ kod programa koji početnu konfiguraciju $(y_1, \dots, y_n, 0, \dots)$ prevodi u konfiguraciju

$$(x_1, \dots, x_m, y_1, \dots, y_n, 0, \dots),$$

a potom, na takvoj konfiguraciji nastavlja izvršavanje programa P_e. Program $P_{s_m(e,\vec{x})}$ je zapravo sledeći:

$$Q_e, T(n_e+1, m+1), \dots, T(2n_e, m+n_e), I_{x_1}(1), \dots, I_{x_m}(m), P_e.$$

Kod navedenog programa definisan je za sve $e, x_1, \dots, x_m \in \omega$, pa prema Čerčovoj tezi, funkcija $s_m(e, \vec{x})$ je totalna i rekurzivna. $\square$

Često se u literaturi koristi jedna varijanta teoreme parametrizacije koja se uobičajeno naziva s-m-n teoremom. Ova teorema, za proizvoljne prirodne brojeve $m, n \geq 1$, izražava efektivnost parametrizacije $(m+n)$-arne funkcije u kojoj se fiksira m parametara.

Primer 2. s-m-n teorema: Za proizvoljne prirodne brojeve $m, n \geq 1$, postoji $(m+1)$-arna totalna izračunljiva funkcija $s_n^m(e, \vec{x})$ takva da za svaki prirodan broj $e \in \omega$ i sve $\vec{x} \in \omega^m$, $\vec{y} \in \omega^n$,

$$\varphi_e(\vec{x}, \vec{y}) = \varphi_{s_n^m(e,\vec{x})}(\vec{y}).$$

Teorema efektivne numeracije i teorema o parametrizaciji su u izvesnom smislu jedna drugoj inverzne. Teorema efektivne numeracije podiže indeks rekurzivne funkcije u argument, a teorema o parametrizaciji spušta argumente u indeks. Da bi to ilustrovali, u sledećim primerima pokazaćemo efektivnost jednog broja operacija nad rekurzivnim funkcijama.

Primer 3. Postoji totalna izračunljiva funkcija $k(x)$ takva da, za svaki prirodan broj $x \in \omega$, $\varphi_{k(x)} = 2 \cdot \varphi_x$.

Neka je $f(x, y) = 2 \cdot \varphi_x(y)$. Na osnovu teoreme o efektivnoj numeraciji, postoji $u \in \omega$ takvo da $f(x, y) = 2 \cdot \varphi_u^{(2)}(x, y)$, tj. $f(x, y)$ je izračunljiva funkcija.

Ako je $e \in \omega$ indeks funkcije $f(x, y)$, prema teoremi parametrizacije, postoji totalna izračunljiva funkcija $s(x, y)$ takva da

$$f(x,y) = \varphi_e^{(2)}(x,y) = \varphi_{s(e,x)}(y).$$

Funkcija $k(x) = s(e,x)$ je totalna izračunljiva funkcija i $\varphi_{k(x)} = 2 \cdot \varphi_x$.

Primer 4. Za sve $x, y \in \omega$, proizvod $\varphi_x(z) \cdot \varphi_y(z)$ je izračunljiva funkcija i njen indeks se efektivno može odrediti iz indeksa x i y.

Neka je $f(x,y,z) = \varphi_x(z) \cdot \varphi_y(z)$. Na osnovu teoreme o efektivnoj numeraciji, $f(x,y,z) = \varphi_u(x,z) \cdot \varphi_u(y,z)$, pa je $f(x,y,z)$ izračunljiva funkcija. Neka je $e \in \omega$ indeks funkcije f, tj. $f(x,y,z) = \varphi_e^{(3)}(x,y,z)$. Prema teoremi parametrizacije, $f(x,y,z) = \varphi_{s_2(e,x,y)}(z)$. Pritom, $s_2(e,x,y)$ je totalna izračunljiva funkcija.

Slično, postoji totalna izračunljiva funkcija $k(x)$ takva da za svaki prirodan broj $x \in \omega$, $(\varphi_x)^2 = \varphi_{k(x)}$. U ovom slučaju, ako je $e \in \omega$ takvo da $(\varphi_x)^2 = \varphi_{s_2(e,x,x)} = \varphi_{\varphi_{s_1(e,x)}(x)}$, onda $k(x) = \varphi_{s_1(e,x)}(x)$. To zapravo znači da se i indeks totalne izračunljive funkcije $k(x)$ može efektivno odrediti.

Primer 5. (a) Postoje totalne izračunljive funkcije $k(x,y)$ i $h(x,y)$ takve da za proizvoljne $x, y \in \omega$,

$$W_{k(x,y)} = W_x \cup W_y \ \text{ i } \ E_{h(x,y)} = W_x \cup W_y.$$

(b) Isto tvrđenje važi i za uniju skupova oblika W_x i E_x, $x \in \omega$.

Primer 6. (a) Postoji totalna izračunljiva funkcija $g(x)$ takva da za svako $x \in \omega$, ako je φ_x karakteristična funkcija rekurzivnog skupa A, onda je $\varphi_{g(x)}$ karakteristična funkcija skupa A^c.

(b) Postoji $e \in \omega$ takvo da za svako $x \in \omega$, $E_{s(e,x)} = W_x$.

Primer 7. Postoji odlučiv predikat $Q(x,y,z)$ koji zadovoljava sledeće uslove: za sve $x, y \in \omega$,

(a) $y \in E_x$ ako i samo ako $\exists z\, Q(x,y,z)$,
(b) ako $y \in E_x$ i $Q(x,y,z)$, onda $\varphi_x((z)_1) = y$.

Neka je $Q(x,y,z)$ ako i samo ako "$P_x((z)_1) \downarrow y$" za $\leq (z)_2$ koraka. Prema Čerčovoj tezi, $Q(x,y,z)$ je odlučiv predikat i pritom, $y \in E_x$ ako i samo ako $\exists z\, Q(x,y,z)$. Jasno, ako važi $y \in E_x$, onda $\varphi_x((z)_1) = y$.

Primer 8. Postoji izračunljiva funkcija $g(x,y)$ koja zadovoljava sledeće uslove: za sve $x, y \in \omega$,

(a) vrednost $g(x,y)$ postoji ako i samo ako $y \in E_x$.
(b) ako $y \in E_x$, onda $g(x,y) \in W_x$ i $\varphi_x(g(x,y)) = y$.

Egzistencija funkcije $g(x,y)$ dokazuje se na osnovu rezultata iz prethodnog primera. Neka je $e \in \omega$ indeks funkcije $g(x,y)$. Prema teoremi parametrizacije, $g(x,y) = \varphi_{s(e,x)}(y)$, pa na osnovu uslova (a) i (b), $W_{s(e,x)} = E_x$.

Takođe, $E_{s(e,x)} \subseteq W_x$ i ako je $y \in E_x$, onda $\varphi_x(\varphi_{s(e,x)}(y)) = y$. Otuda, ako je φ_x obostrano jednoznačna funkcija, $\varphi_{s(e,x)} = (\varphi_x)^{-1}$ i $E_{s(e,x)} = W_x$.

Primer 9. Ako je $f(x)$ izračunljiva funkcija, postoji $e \in \omega$ takvo da za svako $x \in \omega$, $W_{s(e,x)} = f^{-1}[W_x]$.

Primer 10. Pravila supstitucije, rekurzije i minimizacije su efektivna.

(a) Za svako $m \geq 1$, postoji $e \in \omega$ takvo da za svako $n \geq 1$,

$$\varphi^{(n)}_{s_{m+1}(e,e_0,\ldots,e_m)}(\vec{x}) = \varphi^{(m)}_{e_0}(\varphi^{(n)}_{e_1}(\vec{x}), \ldots, \varphi^{(n)}_{e_m}(\vec{x})),$$

odnosno, indeks funkcije koja se dobija supstitucijom može se efektivno odrediti na osnovu indeksa polaznih funkcija.

(b) Postoji $e \in \omega$ takvo da za svako $n \geq 1$, funkcija $\varphi^{(n+1)}_{s_2(e,x,y)}$ se dobija rekurzijom iz funkcija $\varphi^{(n)}_x$ i $\varphi^{(n+2)}_y$.

(c) Postoji $e \in \omega$ takvo da za sve $n \geq 1$ i $\vec{x} \in \omega^n$,

$$\varphi^{(n)}_{s(e,z)}(\vec{x}) = \mu y\,(\varphi^{(n+1)}_z(\vec{x}, y) = 0),$$

odnosno, indeks funkcije $f(\vec{x})$, koja se dobija minimizacijom funkcije $g(\vec{x}, y)$, može se efektivno odrediti iz indeksa funkcije $g(\vec{x}, y)$.

Neka je $n \geq 1$. Predikat $M \subseteq \omega^n$ je *parcijalno odlučiv* ako postoji prirodan broj $e \in \omega$ takav da $M = W^{(n)}_e$. Ako $M = W_e$, za neko $e \in \omega$, skup M je *parcijalno rekurzivan.* Ako je $n \geq 1$ i $M \subseteq \omega^n$ proizvoljan predikat. *Parcijalna karakteristična funkcija* predikata M je funkcija:

$$p_M(\vec{x}) = \begin{cases} 1 & \text{ako } \vec{x} \in M \\ \text{nedefinisano} & \text{inače} \end{cases}$$

Parcijalno odlučive predikate definisali smo kao domene rekurzivnih funkcija. Svaki odlučiv predikat je parcijalno odlučiv, ali obratno ne važi. Predikat M je parcijalno odlučiv ako i samo ako funkcija p_M je rekurzivna.

Primer 11. Skup $K = \{x : x \in W_x\}$ je parcijalno rekurzivan i nije rekurzivan. Primetimo da se skup K može shvatiti i na jedan od sledećih načina:

$$K = \{x : \varphi_x(x)\downarrow\} = \{x : P_x(x)\downarrow\} = \{x : \varphi^{(2)}_u(x,x)\downarrow\},$$

gde je $u \in \omega$ indeks univerzalne funkcije. Ovaj skup ima vrlo značajnu ulogu u teoriji izračunljivosti.

Da dokažemo tvrđenje, primetimo da parcijalna karakteristična funkcija skupa K ima oblik $p_K(x) = 1(\varphi_x(x))$, gde je $1(x) = 1$, za svako $x \in \omega$.

Na osnovu teoreme o efektivnoj numeraciji, $p_K(x) = 1(\varphi_u^{(2)}(x, x))$. Kao kompozicija rekurzivnih funkcija, p_K(x) je rekurzivna funkcija, tj. skup K je parcijalno rekurzivan.

Ako bi skup K bio rekurzivan, njegova karakteristična funkcija $c_K(x)$ bi bila rekurzivna, pa bi to isto važilo i za funkciju

$$f(x) = \begin{cases} \varphi_x(x) + 1 & \text{ako } x \in K \\ 0 & \text{ako } x \notin K \end{cases}$$

Međutim, za svako $x \in \omega$, $f \neq \varphi_x$, pa skup K nije rekurzivan.

Sledeći primer predstavlja rešenje takozvanog halting problema: "da li program P_x konvergira za ulaz y".

Primer 12. Halting problem: Sledeći predikat nije odlučiv:

$$\begin{aligned} H(x, y) \quad &\Leftrightarrow \quad y \in W_x, \\ &\Leftrightarrow \quad \text{vrednost } \varphi_x(y) \text{ je definisana}, \\ &\Leftrightarrow \quad P_x(y) \downarrow. \end{aligned}$$

Rešenje halting problema sledi neposredno iz činjenice da skup K nije rekurzivan. U suprotnom, bio bi rekurzivan i predikat $H(x, x)$ ako i samo ako $x \in W_x$, što bi značilo da je K rekurzivan skup.

Primer 13. Halting problem je parcijalno odlučiv.

Kako je predikat $H(x, y)$ ekvivalentan predikatu "$\varphi_x(y) \downarrow$", na osnovu teoreme o efektivnoj numeraciji, $p_H(x, y) = 1(\varphi_x(y)) = 1(\varphi_u^{(2)}(x, y))$ je rekurzivna funkcija, pa je predikat $H(x, y)$ parcijalno odlučiv.

Primer 14. Ne postoji izračunljiva funkcija $f(x, y)$ takva da, ako se izračunavanje $P_x(y)$ završava tada se $P_x(y)$ završava za $\leq f(x, y)$ koraka.

Ukoliko bi takva funkcija postojala, Halting problem bi bio odlučiv.

Primer 15. Za svako $m \in \omega$, skup $A_m = \{x : m \in W_x\}$ nije rekurzivan.

Ideja dokaza ovog tvrđenja je sasvim opšta. Kao i u slučaju Halting problema, problem "$x \in K$" svodimo na problem problem "$x \in A_m$".

Ključni argumenti u takvom svođenju su teorema o efiktivnoj numeraciji i teorema parametrizacije. Sa takvom idejom, definišimo funkciju

$$f(x, y) = \begin{cases} y & \text{ako } x \in K \\ \text{nedefinisano} & \text{ako } x \notin K \end{cases}$$

Kako je $f(x,y) = y\cdot 1(\varphi_x(x))$, na osnovu teoreme o efektivnoj numeraciji, $f(x,y) = y \cdot 1(\varphi_u^{(2)}(x,x))$, odnosno, funkcija $f(x,y)$ je rekurzivna. To znači da postoji $e \in \omega$ takvo da $f(x,y) = \varphi_e(x,y)$. Prema teoremi parametrizacije, postoji totalna obostrano jednoznačna izračunljiva funkcija $s(e,x)$ takva da $f(x,y) = \varphi_{s(e,x)}(y)$. Otuda, za svako $x \in \omega$,

$$\begin{array}{l} x \in K \;\Rightarrow\; W_{s(e,x)} = \omega \;\Rightarrow\; m \in W_{s(e,x)} \;\Rightarrow\; s(e,x) \in A_m, \\ x \notin K \;\Rightarrow\; W_{s(e,x)} = \emptyset \;\Rightarrow\; m \notin W_{s(e,x)} \;\Rightarrow\; s(e,x) \notin A_m. \end{array}$$

Dakle, za svako $x \in \omega$, $x \in K$ ako i samo ako $s(e,x) \in A_m$. Neka je $c_m(x)$ karakteristična funkcija skupa A_m. Ako bi $c_m(x)$ bila rekurzivna, onda bi sledeća funkcija takođe bila rekurzivna:

$$c_m(s(e,x)) = \begin{cases} 1 & \text{ako } x \in K, \\ 0 & \text{inače.} \end{cases}$$

To bi zapravo značilo da je skup K rekurzivan, što nije moguće. Dakle, skup A_m nije rekurzivan.

Ovaj primer je veoma karakterističan. Pomoću totalne obostrano jednoznačne rekurzivne funkcije $s(e,x)$, problem $x \in K$ sveli smo na problem $x \in A_m$. To znači da je problem $x \in A_m$ težak bar koliko i problem $x \in K$. Ova ideja može se sistematski izraziti i tako definisati poredak koji karakteriše nerešivost problema, tj. složenost skupova prirodnih brojeva.

Neka su $A, B \subseteq \omega$. Skup A je *svodljiv* na B, u oznaci $A \leq B$, ako postoji totalna rekurzivna funkcija $f(x)$ takva da za svako $x \in \omega$,

$$x \in A \;\Leftrightarrow\; f(x) \in B.$$

Ako je funkcija $f(x)$ obostrano jednoznačna, skup A je 1-*svodljiv* na B. U ovom slučaju koristimo oznaku $A \leq_1 B$.

Intuitivno, ako je $A \leq B$, problem "$x \in B$" nije lakši od problema "$x \in A$". Na primer, za svako $m \in \omega$, $K \leq_1 A_m$, a odgovarajuća funkcija koja vrši svođenje problema K na A_m je $f(x) = s(e,x)$.

Primetimo da, ako $A \leq B$, onda $A^c \leq B^c$, s obzirom na istu funkciju $f(x)$ koja svodi skup A na skup B. Suprotno intuiciji, u opštem slučaju, problemi, odnosno, skupovi A i A^c nisu jednako "teški".

Relacija $\leq$ je refleksivna i tranzitivna. Na skupu svih podskupova skupa prirodnih brojeva, relacija $\leq$ određuje relaciju ekvivalencije:

$$A \equiv B \;\Leftrightarrow\; A \leq B \text{ i } B \leq A.$$

Za svako $A \subseteq \omega$, klasa ekvivalencije $d(A) = \{B : A \equiv B\}$ je *stepen nerešivosti* problema ili skupa A.

Slično, relacija $\leq_1$ određuje relaciju ekvivalencije $\equiv_1$. Odgovarajuća klasa ekvivalencije $d_1(A) = \{B : A \equiv_1 B\}$ je 1-*stepen nerešivosti* problema A.

Primer 16. (a) Ako je A rekurzivan skup i $B \leq A$, skup B je takođe rekurzivan.

(b) Ako je A rekurzivan skup i $B \neq \emptyset, \omega$, onda je $A \leq B$.

(c) Ako je A parcijalno rekurzivan skup i $B \leq A$, skup B je parcijalno rekurzivan.

(d) Ako je A parcijalno rekurzivan skup, onda $A \leq K$.

(e) Za svaki skup A, $A \leq \omega$ ako i samo ako $A = \omega$. Takođe, za svaki skup A, $A \leq \emptyset$ ako i samo ako $A = \emptyset$.

(f) Za svaki skup A, $\omega \leq A$ ako i samo ako $A \neq \emptyset$. Takođe, za svaki skup A, $\emptyset \leq A$ ako i samo ako $A \neq \omega$.

Na osnovu tvrđenja (a) i (b), možemo zaključiti da su svi rekurzivni skupovi jednako složeni, odnosno, da su svi takvi problemi jednako teški.

Stepen nerešivosti rekurzivnih skupova označavamo sa **0**.

Iz tvrđenja (e) i (f) sledi da prazan skup i skup prirodnih brojeva čine minimalne stepene nerešivosti koje označavamo redom sa **o** i **n**.

Minimalni stepeni **o** i **n** nisu uporedivi, a stepen nerešivosti **n** je njihov supremum.

Stepen nerešivosti skupa K označavamo sa **0'**.

Na osnovu tvrđenja (c), svaki skup A takav da $A \leq K$ je parcijalno rekurzivan. Obratno, prema tvrđenju (d), ako je A parcijalno rekurzivan skup, A može se svesti na K. Otuda sledi da je stepen nerešivosti svakog parcijalno rekurzivnog skupa manji ili jednak **0'**.

Kako K nije rekurzivan skup, $\mathbf{0} < \mathbf{0'}$. O problemu karakterizacije skupova koji pripadaju stepenu **0'**, kao i o skupovima stepena nerešivosti između **0** i **0'**, govorićemo u kasnijim izlaganjima. Veći deo teorije izračunljivosti posvećen je istraživanjima svojstava strukture poretka stepena nerešivosti u ovom intervalu.

Dokazaćemo samo tvrđenje (d). Sva ostala tvrđenja dokazuju se jednostavnije. Definišimo funkciju $f(x, y)$ tako da

$$f(x,y) = \begin{cases} 1 & \text{ako } x \in A \\ \text{nedefinisano} & \text{ako } x \notin A \end{cases}$$

Funkcija f je rekurzivna, pa postoji $e \in \omega$ takvo da $f(x,y) = \varphi_e(x,y)$. Prema teoremi parametrizacije, $f(x,y) = \varphi_{s(e,x)}(y)$.

Za svaki prirodan broj $x \in \omega$, $x \in A$ ako i samo ako vrednost $\varphi_{s(e,x)}(s(e,x))$ postoji ako i samo ako $s(e,x) \in K$. Kako je $s(e,x)$ totalna, obostrano jednoznačna izračunljiva funkcija, $A \leq_1 K$.

Primer 17. Ako je $\mathrm{Tot} = \{x : W_x = \omega\}$, onda $K \leq_1 \mathrm{Tot}$.

Zapravo, Tot je skup svih indeksa totalnih izračunljivih funkcija, a skup K je 1-svodljiv na Tot. Definišimo funkciju $f(x,y)$ tako da

$$f(x,y) = \begin{cases} 1 & \text{ako } x \in K \\ \text{nedefinisano} & \text{ako } x \notin K \end{cases}$$

Kako je $f(x,y) = 1(\varphi_u^{(2)}(x,x))$, gde je $\varphi_u^{(2)}$ univerzalna funkcija, $f(x,y)$ je rekurzivna funkcija, pa postoji $e \in \omega$ takvo da $f(x,y) = \varphi_e(x,y)$.

Na osnovu teoreme o parametrizaciji, postoji totalna obostrano jednoznačna izračunljiva funkcija $s(e,x)$ takva da $f(x,y) = \varphi_{s(e,x)}(y)$.

Dakle, za svako $x \in \omega$,

$$\begin{aligned} x \in K \ &\Rightarrow\ \varphi_{s(e,x)} = 1 \ \Rightarrow\ s(e,x) \in \mathrm{Tot}, \\ x \notin K \ &\Rightarrow\ W_{s(e,x)} = \emptyset \ \Rightarrow\ s(e,x) \notin \mathrm{Tot}. \end{aligned}$$

To znači da funkcija $s(e,x)$ skup K svodi na skup Tot.

Ubuduće, kada su instrukcije za izračunavanje funkcije $f(x,y)$ efektivne, nećemo se pozivati na teoremu o parametrizaciji. Jednostavno, umesto o $f(x,y)$ govorićemo o funkciji $\varphi_{h(x)}(y)$, gde je $h(x)$ totalna obostrano jednoznačna izračunljiva funkcija.

Primer 18. (a) Skup K može se 1-svesti na skup $A = \{x : \varphi_x(x) = 0\}$. Isto važi i u slučaju skupa $B = \{x : W_x = \emptyset\}$.

(b) Za svako $y \in \omega$, K je 1-svodljiv na skup $A_y = \{x : \varphi_x = \varphi_y\}$.

U principu, ukoliko je skup A definisan nekim svojstvom izračunljivih funkcija, pomoću teoreme o parametizaciji, skup K može se svesti na A. Međutim, takvo svođenje nije moguće ako je skup A definisan nekim svojstvom samih indeksa izračunljivih funkcija.

Skup $A \subseteq \omega$ je *indeksni skup* ako za sve $x, y \in \omega$, $x \in A$ i $\varphi_x = \varphi_y$ implicira $y \in A$. Indeksni skup $A \subseteq \omega$ je *netrivijalan* ako $A \neq \emptyset$ i $A \neq \omega$.

Teorema 6. Ako je A netrivijalan indeksni skup, $K \leq_1 A$ ili $K \leq_1 A^c$.

Dokaz: Neka je $A \subseteq \omega$ netrivijalan indeksni skup i neka je $e_0 \in \omega$ indeks nigde definisane funkcije. Tvrdimo da, ako $e_0 \in A^c$, onda je $K \leq_1 A$. U suprotnom, važilo bi $K \leq_1 A^c$.

Kako je A netrivijalan indeksni skup, postoji $e_1 \in A$ takvo da $\varphi_{e_0} \neq \varphi_{e_1}$. Prema teoremi parametrizacije, neka je $f(x)$ totalna obostrano jednoznačna rekurzivna funkcija takva da

$$\varphi_{f(x)}(y) = \begin{cases} \varphi_{e_1}(y) & \text{ako } x \in K \\ \text{nedefinisano} & \text{ako } x \notin K \end{cases}$$

Ako $x \in K$, onda $\varphi_{f(x)} = \varphi_{e_1}$. Po pretpostavci, $e_1 \in A$, pa kako je A indeksni skup, $f(x) \in A$.

Obratno, ako $x \notin K$, onda je $\varphi_{f(x)} = \varphi_{e_0}$, pa kako $e_0 \notin A$ i kako je A indeksni skup, $f(x) \notin A$, što znači da je $K \leq_1 A$. $\square$.

Primer 19. Rajsova teorema: Indeksni skup $A \subseteq \omega$ je rekurzivan ako i samo ako A je trivijalan indeksni skup.

Primer 20. (a) Disjunkcija u prethodnoj teoremi nije isključiva. Na primer, $K \leq_1$ Tot i istovremeno $K \leq_1 (\mathrm{Tot})^c$.

(b) Neka je $K_1 = \{x : W_x \neq \emptyset\}$. Skup K_1 je netrivijalan indeksni skup i $K \equiv_1 K_1$.

(c) Neka je $\mathrm{Fin} = \{x : |W_x| < \omega\}$ i $\mathrm{Inf} = (\mathrm{Fin})^c$. Skupovi Fin i Inf su netrivijalni indeksni skupovi i Tot $\equiv_1$ Inf.

Primer 21. (a) Postoji parcijalna rekurzivna funkcija koja se ne može proširiti do totalne rekurzivne funkcije.

(b) Skup indeksa svih rekurzivnih funkcija koje se mogu proširiti do totalne rekurzivne funkcije je netrivijalan indeksni skup. Taj skup označavamo sa Ext.

(b) Skupovi $\mathrm{Cof} = \{x : |W_x^c| < \omega\}$ i $\mathrm{Rec} = \{x : W_x \text{ je rekurzivan}\}$, su netrivijalni indeksni skupovi i Rec $\equiv_1$ Cof $\equiv_1$ Ext.

Disjunktni skupovi A i B su *nerastavljivi* ako ne postoji rekurzivan skup C takav da $A \subseteq C$ i $C \cap B = \emptyset$.

Primer 22. Neka je $A_0 = \{x : \varphi_x(x) = 0\}$ i $A_1 = \{x : \varphi_x(x) = 1\}$.

Skupovi A_0 i A_1 su nerastavljivi parcijalno rekurzivni i zadovoljavaju relacije: $K \equiv_1 A_0 \equiv_1 A_1$.

Rekurzivno nabrojivi skupovi

Parcijalno rekurzivne skupove definisali smo kao domene rekurzivnih funkcija. Ipak, ta klasa skupova u suštini izražava jednu drugu ideju. Parcijalno rekurzivni su oni skupovi koji se mogu efektino nabrojati, odnosno, skupovi čije elemente generiše totalna rekurzivna funkcija.

Neprazan skup $A \subseteq \omega$ je *rekurzivno nabrojiv* ako postoji totalna izračunljiva funkcija $f(x)$ takva da $A = \mathrm{codom}(f)$.

To zapravo znači da je neprazan skup A rekurzivno nabrojiv ako postoji totalna rekurzivna funkcija $f(x)$ za koju je

$$A = \{f(0), f(1), f(2), \dots\}.$$

Parcijalno rekurzivni skupovi mogu se shvatiti i kao projekcije rekurzivnih skupova, odnosno, to su skupovi koji se mogu dobiti egzistencijalnom kvantifikacijom rekurzivnih predikata.

Skup prirodnih brojeva $A \subseteq \omega$ je tipa Σ_1 ili $A \in \Sigma_1$, ako postoji rekurzivna relacija $R \subseteq \omega^2$ za koju je $A = \{x \in \omega : \exists y\, R(x, y)\}$.

Teorema 7. Za svaki skup $A \subseteq \omega$, sledeći uslovi su ekvivalentni:

(a) skup A je parcijalno rekurzivan,
(b) $A = \emptyset$ ili A je rekurzivno nabrojiv skup,
(c) skup A je tipa Σ_1.

Dokaz: Pretpostavimo da je A parcijalno rekurzivan, neprazan skup. Tada postoji $e \in \omega$ takvo da $A = W_e$. Izaberimo $a \in A$ i definišimo funkciju $f(x, t)$ tako da

$$f(x,t) = \begin{cases} x & \text{ako } P_e(x) \downarrow \text{ za } t \text{ koraka}, \\ a & \text{inače}. \end{cases}$$

Funkcija $f(x, t)$ je totalna i izračunljiva, pa totalna unarna izračunljiva funkcija $h(y) = f((y)_1, (y)_2)$ zadovoljava uslov $\mathrm{codom}(f) = \mathrm{codom}(h) = A$.

Neka je $A \neq \emptyset$ rekurzivno nabrojiv skup takav da $A = \mathrm{codom}(\varphi_e)$ i neka je $R(e, x, y)$ predikat "$P_e((y)_1) \downarrow x$ za $\leq (y)_2$ koraka". Prema Čerčovoj tezi, predikat $R(e, x, y,)$ je rekurzivan i pritom, za svako $x \in \omega$, $x \in A$ ako i samo ako $\exists y\, R(e, x, y)$, tj. $A \in \Sigma_1$.

Konačno, pretpostavimo da $A \in \Sigma_1$. Po definiciji Σ_1 skupova, postoji rekurzivna relacija $R \subseteq \omega^2$ za koju je $A = \{x : \exists y\, R(x, y)\}$. Ako je $f(x) = \mu y\, R(x, y)$, to znači da je $A = \mathrm{dom}(f)$. $\square$

Primer 1. Ako je $R(x, y)$ parcijalno rekurzivan predikat, predikat $\exists y\, R(x, y)$ je takođe parcijalno rekurzivan.

Primer 2. Za svako $e \in \omega$, $\mathrm{graf}(\varphi_e) = \{(x, y) : \varphi_e(x) = y\}$ je parcijalno rekurzivan skup.

Primer 3. Ako je $R \subseteq \omega^2$ parcijalno rekurzivna relacija, postoji rekurzivna funkcija $f(x)$ takva da za sve $x \in \omega$,

(a) vrednost $f(x)$ postoji ako i samo ako $\exists y\, R(x,y)$,

(b) ako $f(x)$ postoji, onda $R(x, f(x))$.

Relacija $R(x,y)$ je parcijalno rekurzivna, pa postoji rekurzivna relacija $Q(x,y,z)$ takva da $R(x,y) = \exists z\, Q(x,y,z)$. Kako je $g(x) = \mu t\, Q(x,(t)_1,(t)_2)$ rekurzivna funkcija, jednostavno se proverava da funkcija $f(x) = (g(x))_1$ zadovoljava uslove tvrđenja.

Primer 4. Ako su $A, B \subseteq \omega$ parcijalno rekurzivni skupovi, postoje parcijalno rekurzivnu skupovi $A_1 \subseteq A$ i $B_1 \subseteq B$ takvi da $A_1 \cap B_1 = \emptyset$ i $A \cup B = A_1 \cup B_1$.

Relacija $R = A \times \{0\} \cup B \times \{1\}$ je parcijalno rekurzivna, pa postoji rekurzivna funkcija $f(x)$ koja zadovoljava uslove prethodnog primera. Neka je $A_1 = \{x : f(x) = 0\}$ i $B_1 = \{x : f(x) = 1\}$.

Primer 5. (a) Funkcija $f(x)$ je rekurzivna ako i samo ako $\mathrm{graf}(f)$ je parcijalno rekurzivan skup.

(b) Ako je $f(x)$ totalna rekurzivna funkcija, $\mathrm{graf}(f)$ je rekurzivan skup.

Primer 6. Skup A je rekurzivan ako i samo ako A i A^c su parcijalno rekurzivni.

Neka su R i S odlučivi predikati takvi da za sve $x \in \omega$,

$$
\begin{aligned}
x \in A &\ \Leftrightarrow\ \exists y\, R(x,y),\\
x \in A^c &\ \Leftrightarrow\ \exists y\, S(x,y).
\end{aligned}
$$

Funkcija $f(x) = \mu y\, (R(x,y) \text{ ili } S(x,y))$ je totalna, izračunljiva i za svako $x \in \omega$, $x \in A$ ako i samo ako $R(x, f(x))$.

Primer 7. (a) Skup K^c nije parcijalno rekurzivan.

(b) Za svaki skup $A \subseteq \omega$, ako $K^c \leq A$, skup A nije rekurzivno nabrojiv.

(c) Skupovi Tot, Fin i Rec nisu rekurzivno nabrojivi.

Primer 8. Postoje totalne rekurzivne funkcije $k(x)$ i $h(x)$ takve da za svako $x \in \omega$, $W_x = E_{k(x)}$ i $E_x = W_{h(x)}$.

Primer 9. Ako je $f(x)$ rekurzivna funkcija i $A \subseteq \mathrm{dom}(f)$, funkcija $f \restriction A$ je rekurzivna ako i samo ako A je rekurzivno nabrojiv skup.

Primer 10. Ne postoji rekurzivna funkcija $f(x)$ takva da za svako $x \in \omega$, ako je W_x rekurzivan skup, vrednost $f(x)$ je definisana i $W_{f(x)} = W_x^c$.

Na osnovu teoreme o parametrizaciji, neka je $g(x)$ totalna izračunljiva funkcija takva da

$$
\varphi_{g(x)}(y) = \begin{cases} 1 & \text{ako } x \in K,\\ \text{nedefinisano} & \text{inače.} \end{cases}
$$

Pretpostavimo da postoji rekurzivna funkcija $f(x)$ koja zadovoljava uslove tvrđenja. U tom slučaju, za sve $x \in \omega$,

$$\begin{aligned} x \in K &\Rightarrow W_{g(x)} = \omega \Rightarrow W_{f(g(x))} = \emptyset, \\ x \notin K &\Rightarrow W_{g(x)} = \emptyset \Rightarrow W_{f(g(x))} = \omega. \end{aligned}$$

Otuda, za svako $x \in \omega$, $x \in K^c$ ako i samo ako $W_{f(g(x))} \neq \emptyset$. Međutim, za svako $x \in \omega$, $W_{f(g(x))} \neq \emptyset$ ako i samo ako $\exists y \exists z\, T_1(f(g(x)), y, z)$, pa kako je Klinijev predikat T_1 rekurzivan i $f \circ g$ rekurzivna funkcija, to bi značilo da je skup K^c parcijalno rekurzivan.

Primer 11. Neka je $A \subseteq \omega$ neprazan skup. Dokazati da je skup A rekurzivan ako i samo ako A je kodomen totalne, neopadajuće izračunljive funkcije.

Neka je A neprazan rekurzivan skup. Definišimo funkciju $f(x)$ tako da:

$$\begin{aligned} &f(0) = \mu x\,(x \in A) \\ &f(n+1) = \mu y\,(y \in A \text{ i } f(n) < y), \text{ za sve } n \in \omega. \end{aligned}$$

Očigledno, funkcija $f(x)$ je totalna neopadajuća izračunljiva funkcija i pritom je $A = \mathrm{codom}(f)$.

Obratno, ako je $A = \mathrm{codom}(f)$ i f neopadajuća, totalna izračunljiva funkcija, skup A je rekurzivan jer, za svako $x \in \omega$,

$$x \in A \Leftrightarrow \exists n \leq x\,(f(n) = x).$$

Primer 12. (a) Svaki beskonačan rekurzivno nabrojiv skup sadrži beskonačan rekurzivan podskup.

(b) Svaki beskonačan rekurzivno nabrojiv skup može se numerisati bez ponavljanja.

Primer 13. (a) Skup $A \subseteq \omega^n$ je parcijalno rekurzivan ako i samo ako skup $\{2^{x_1} \cdots p_n^{x_n} : (x_1, \ldots, x_n) \in A\}$ je parcijalno rekurzivan.

(b) Funkcija $f(x)$ je izračunljiva ako i samo ako $\{2^x \cdot 3^{f(x)} : x \in \mathrm{dom}(f)\}$ je rekurzivno nabrojiv skup.

Na osnovu Rajsove teoreme, znamo da netrivijalni indeksni skupovi nisu rekurzivni. Sledeća teorema je dobar kriterijum rekurzivne nabrojivosti indeksnih skupova.

Šapiro-Rajsova teorema: Ako je $\mathcal{A} \subseteq \mathcal{R}_1$ skup rekurzivnih funkcija takav da je $A = \{x : \varphi_x \in \mathcal{A}\}$ parcijalno rekurzivan skup, onda za svako $f \in \mathcal{R}_1$,

$$f \in \mathcal{A} \Leftrightarrow \text{ postoji konačno } \theta \subseteq f, \theta \in \mathcal{A}.$$

Dokaz: Neka je $f \in \mathcal{A}$ i za svaku konačnu funkciju $\theta \subseteq f$, $f \notin \mathcal{A}$. Neka je $e \in \omega$ takvo da $W_e = K$. Na osnovu teoreme o parametrizaciji postoji totalna, rekurzivna, obostrano jednoznačna funkcija $g(x)$ takva da

$$\varphi_{g(x)}(t) = \begin{cases} f(t) & \text{ako } \neg P_e(x) \downarrow \text{ za } \leq t \text{ koraka,} \\ \text{nedefinisano} & \text{inače.} \end{cases}$$

Ako $x \in K$, postoji $t_0 \in \omega$ takvo da $P_e(x) \downarrow$ za t_0 koraka. Kako za svako $t \geq t_0$, vrednost $\varphi_{g(x)}(t)$ ne postoji, $\varphi_{g(x)} \subseteq f$ je konačna funkcija, pa dakle mora biti $g(x) \notin A$.

S druge strane, ako $x \notin K$, za svako $t \in \omega$, $\varphi_{g(x)}(t) = f(t)$, pa dakle $g(x) \in A$. Otuda sledi da za svako $x \in \omega$, $x \in K^c$ ako i samo ako $g(x) \in A$, odnosno, $K^c \leq_1 A$ što nije moguće.

Obratno, pretpostavimo da $f \notin \mathcal{A}$ i neka je $\theta \subseteq f$ konačna funkcija takva da $\theta \in \mathcal{A}$. Neka je $g(x)$ totalna izračunljiva obostrano jednoznačna funkcija takva da

$$\varphi_{g(x)}(t) = \begin{cases} f(t) & \text{ako } x \in \mathrm{dom}(\theta) \text{ ili } x \in K, \\ \text{nedefinisano} & \text{inače.} \end{cases}$$

Ako $x \in K$, onda $\varphi_{g(x)} = f$, pa $g(x) \notin A$. Sa druge strane, ako $x \notin K$, onda $\varphi_{g(x)} = \theta$ pa $g(x) \in A$. To znači da za svako $x \in \omega$, $x \in K^c$ ako i samo ako $g(x) \in A$, što nije moguće budući da je A rekurzivno nabrojiv skup. □

Primer 14. Na osnovu prethodne teoreme neposredno sledi da indeksni skupovi Tot, $(\mathrm{Tot})^c$, $\{x : W_x \neq \emptyset\}$, Fin i Inf nisu rekurzivno nabrojivi.

Za svako $t \in \omega$, ako je $x, y, e < t$, neka je $\varphi_{e,t}(x) = y$ ako i samo ako $P_e(x) \downarrow y$ za $< t$ koraka i neka je $W_{e,t} = \mathrm{dom}(\varphi_{e,t})$.

Po definiciji, $\varphi_e(x) = y$ ako i samo ako $\exists t\, (\varphi_{e,t}(x) = y)$. Primetimo da za svaki prirodan broj $t \in \omega$, ako $x \in W_{e,t}$, onda $x, e < t$. Pritom, $x \in W_e$ ako i samo ako $\exists t\, (x \in W_{e,t})$.

Primer 15. Postoji rekurzivna funkcija $f(x, y)$ takva da za svako $e \in \omega$, ako $W_e \neq \emptyset$, $f(e, y)$ je totalna izračunljiva funkcija i $W_e = \{f(e, y) : y \in \omega\}$.

Zapravo, tvrdi se da postoji funkcija $f(x, y)$ koja je univerzalna za neprazane parcijalno rekurzivane skupove. Definišimo funkciju $g(x)$ tako da za svako $x \in \omega$, $g(x) = \mu z\, (\pi_1(z) \in W_{x,\pi_2(z)})$

Budući da se dobija minimizacijom po rekurzivnom predikatu, funkcija $g(x)$ je rekurzivna. Definišimo funkciju $f(x, y)$ tako da

$$f(x, y) = \begin{cases} \pi_2(y) & \text{ako } \pi_2(y) \in W_{x,\pi_1(y)+1} - W_{x,\pi_1(y)}, \\ g(x) & \text{inače.} \end{cases}$$

Jasno, funkcija $f(x, y)$ je rekurzivna. Ako je $W_e \neq \emptyset$, za svako $y \in \omega$, vrednost $f(e, y)$ je definisana i pritom, ako $z \in W_e$, onda postoji najmanji $t \in \omega$ takav da $z \in W_{e,t+1}$. Ako je $y = \langle t, z \rangle$, onda $f(e, y) = z$, tj. skup W_e je kodomen funkcije $h(y) = f(e, y)$. Pritom, svaki $z \in W_e$, različit od $g(e)$, javlja se tačno jednom u numeraciji skupa W_e funkcijom $h(y)$,

Primer 16. Pretpostavimo da je A rekurzivno nabrojiv skup. Skupovi $\bigcup_{x \in A} W_x$ i $\bigcup_{x \in A} E_x$ su rekurzivno nabrojivi. Međutim, skup $\bigcap_{x \in A} W_x$ nije nužno rekurzivno nabrojiv.

Teorema rekurzije

Ključni rezultat ovog odeljka predstavlja jedno uopštenje pravila rekurzije. Ono omogućava dokaz izračunljivosti određenih implicitno definisanih funkcija. Iz tih razloga, ovaj Klinijev rezultat uobičajeno se naziva *teoremom rekurzije*. Dokaz teoreme rekurzije je sasvim jednostavan i zasniva se na teoremi parametrizacije.

Teorema 8. Za svaku totalnu rekurzivnu funkciju f, postoji prirodan broj $n \in \omega$ za koji je $\varphi_n = \varphi_{f(n)}$.

Dokaz: Na osnovu teoreme o parametrizaciji, postoji obostrano jednoznačna , totalna izračunljiva funkcija $d(x)$ takva da

$$\varphi_{d(x)}(y) = \begin{cases} \varphi_{\varphi_x(x)}(y) & \text{ako } \varphi_x(x) \text{ postoji,} \\ \text{nedefinisano} & \text{inače.} \end{cases}$$

Dijagonalnu funkciju $d(x)$ definisali smo nezavisno od funkcije f. Slično funkcijama s_m, $m \geq 1$, ona je zadata samim kodiranjem programa. Neka je $e \in \omega$ indeks funkcije $f \circ d$. Tvrdimo da za $n = d(e)$ važi $\varphi_n = \varphi_{f(n)}$.

Kako je f totalna, funkcija $f \circ d = \varphi_e$ je takođe totalna, pa je $\varphi_e(e)$ definisano i na osnovu definicije $\varphi_{d(e)} = \varphi_{\varphi_e(e)}$. Otuda, za $n = d(e)$, redom imamo: $\varphi_n = \varphi_{d(e)} = \varphi_{\varphi_e(e)} = \varphi_{(f \circ d)(e)} = \varphi_{f(n)}$. $\Box$

Ako funkciju f shvatimo kao funkcional $f : \mathcal{R}_1 \to \mathcal{R}_1$ takav da, za svako $x \in \omega$, $f(\varphi_x) = \varphi_{f(x)}$, funkcija $\varphi_n \in \mathcal{R}_1$ je fiksna tačka funkcionala f, odnosno, $f(\varphi_n) = \varphi_n$. Iz tih razloga, teorema rekurzije naziva se i teoremom o fiksnoj tački.

Primer 1. (a) Ako je $n \in \omega$ fiksna tačka totalne izračunljive funkcije f, prirodan broj n može se efektivno odrediti iz indeksa funkcije f, odnosno, postoji totalna, obostrano jednoznačna izračunljiva funkcija g takva da, ako $f = \varphi_x$, onda $n = g(x)$.

(b) Za svaku totalnu izračunljivu funkciju postoji beskonačan rekurzivno nabrojiv skup njenih fiksnih tačaka.

Ako je $v(x)$ totalna rekurzivna funkcija takva da $\varphi_{v(x)} = \varphi_x \circ d$, neka je $g(x) = d(v(x))$. Prema teoremi parametrizacije, d i v su obostrano jednoznačne totalne funkcije.

Ako je F beskonačan rekurzivno nabrojiv podskup skupa svih indeksa funkcije f, kako je d obostrano jednoznačna funkcija, skup $\{d(x) : x \in F\}$ je beskonačan rekurzivno nabrojiv skup fiksnih tačaka funkcije f.

Primer 2. Za svaku izračunljivu funkciju $f(x, \vec{y})$, $\vec{y} \in \omega^n$, $n \geq 1$, postoji prirodan broj $e \in \omega$ takav da je $\varphi_e(\vec{y}) = f(e, \vec{y})$.

Prema teoremi parametrizacije, postoji totalna izračunljiva funkcija $g(x)$ takva da $\varphi_{g(x)} = f(x, \vec{y})$. Broj e je fiksna tačka funkcije g.

Teorema rekurzije omogućava da funkciju φ_e definišemo pomoću zadate totalne izračunljive funkcije f tako da $\varphi_e = \varphi_{f(e)}$. Ili, na osnovu prethodnog primera, φ_e može se definisati "rekurzijom" oblika $\varphi_e(x) = f(e, x)$, za neku zadatu rekurzivnu funkciju f. Iako je funkcija φ_e definisana preko sopstvenog koda e, zahvaljujući teoremi rekurzije, ova definicija nije cirkularna.

Primer 3. Na osnovu prethodnog primera, može se dokazati rekurzivnost Akermanove funkcije.

Definišimo rekurzivnu funkciju $g(x, y, z)$ tako da

$$g(x, y, z) = \begin{cases} y + 1 & \text{ako } x = 0, \\ \varphi_z^{(2)}(x - 1, 1) & \text{ako } x > 0 \text{ i } y = 0, \\ \varphi_z^{(2)}(x - 1, \varphi_z^{(2)}(x, y - 1)) & \text{inače.} \end{cases}$$

Prema prethodnom primeru, postoji prirodan broj $e \in \omega$ takav da $g(x, y, e) = \varphi_e^{(2)}(x, y)$. Indukcijom po $x \in \omega$, sa indukcijom po $y \in \omega$ u induktivnom koraku, dokazuje se da je $\varphi_e^{(2)}$ Akermanova funkcija.

Primer 4. Postoji program P_e, $e \in \omega$, takav da za svaki prirodan broj $x \in \omega$, važi $P_e(x) \downarrow e$.

Za svaki ulaz $x \in \omega$, program idealnog računara P_e sa navedenim svojstvom reprodukuje sopstveni kod $e \in \omega$. Zanimljivo je da na realnom računaru postoji program, u svim jezicima u kojima se može simulirati rekurzija, takav da rezultat njegove primene na svaki ulaz jeste on sam.

Primer 5. (a) Postoji prirodan broj $n \in \omega$ takav da važi $W_n = \{n\}$.
(b) Ako je $A \subseteq \omega$ indeksni skup, onda nije $A \leq A^c$.

Primer 6. Rajsova teorema neposredno sledi iz teoreme rekurzije.

Ako je A netrivijalan indeksni skup, izaberimo $a \in A$ i $b \notin A$ i definišimo funkciju $f(x)$ tako da $f(x) = a$ ako $x \notin A$, a $f(x) = b$ ako $x \in A$. Jasno, za svako $x \in \omega$, $f(x) \in A$ ako i samo ako $x \notin A$.

Ako bi A bio rekurzivan skup, funkcija f bila bi totalna rekurzivna funkcija, pa bi postojao prirodan broj n takav da $\varphi_n = \varphi_{f(n)}$, tj. takav da $f(n) \in A$ ako i samo ako $n \in A$, što nije moguće.

Primer 7. Iz teoreme rekurzije sledi da K nije indeksni skup.

Primer 8. Ne postoji rekurzivna funkcija $f(x)$ takva da, ako je W_x rekurzivan skup, vrednost $f(x)$ postoji i $\varphi_{f(x)}$ je karakteristična funkcija skupa W_x.

Za svaku rekurzivnu funkciju $f(x)$, na osnovu teoreme rekurzije, definišimo funkciju

$$\varphi_e(x) = \begin{cases} 0 & \text{ako } x = 0,\ f(e) \text{ postoji i } \varphi_{f(e)}(0) = 0, \\ \text{nedefinisano} & \text{inače.} \end{cases}$$

Kako je $W_e = \{0\}$, funkcija $\varphi_{f(e)}$ nije karakteristična funkcija skupa W_x. Naime, $0 \in W_e$ i pritom $\varphi_{f(e)}(0) = 0$.

Primer 9. Numeracija $(\varphi_x : x \in \omega)$ je numeracija sa ponavljanjem. Izborom najmanjeg indeksa svake funkcije, dobija se numeracija bez ponavljanja: neka je $f(0) = 0$ i za svako $n \geq 0$ neka je

$$f(n+1) = \mu z\,(\varphi_z \neq \varphi_{f(0)}, \ldots, \varphi_{f(n)}).$$

Funkcija f je obostrano jednoznačna, ali "rekurzija" koja se javlja u definiciji funkcije f uopšte nije legitimna, odnosno, funkcija f nije rekurzivna. Da se to dokaže prvo treba primetiti da f nije identitet, tj. da postoji $k \in \omega$ takvo da za sve $n \geq k$, $f(n) > n$. Po definiciji funkcije f, to znači da je $\varphi_{f(n)} \neq \varphi_n$. Ako je f rekurzivna, f ima beskonačno mnogo fiksnih tačaka, pa postoji $n \geq k$ takvo da $\varphi_{f(n)} = \varphi_n$, što nije moguće.

Skup $A = \{x : \forall y < x\,(\varphi_x \neq \varphi_y)\}$, minimalnih indeksa izračunljivih funkcija, ipak jeste rekurzivno nabrojiv. I to sledi iz teoreme rekurzije.

Jedno od mogućih uopštenja teoreme rekurzije je njena varijanta sa parametrima. Dokaz je vrlo sličan osnovnoj teoremi rekurzije.

Primer 10. *Teorema rekurzije sa parametrima*: Za svaku totalnu izračunljivu funkciju $f(x, y)$, postoji totalna izračunljiva funkcija $n(y)$ takva da $\varphi_{n(y)} = \varphi_{f(n(y),y)}$.

Slično dokazu teoreme rekurzije, postoji totalna rekurzivna funkcija $d(x, y)$ takva da

$$\varphi_{d(x,y)}(z)\begin{cases}\varphi_{\varphi_x(x,y)}(z) & \text{ako vrednost } \varphi_x(x,y) \text{ postoji,}\\ \text{nedefinisano} & \text{inače.}\end{cases}$$

Izaberimo $e \in \omega$ tako da $\varphi_e(x,y) = f(d(x,y),y)$, onda je $n(y) = d(e,y)$.

Primer 11. Na osnovu teoreme rekurzije sa parametrima, dobija se i teorema dvojne rekurzije. Ako su $f(x,y)$ i $g(x,y)$ totalne rekurzivne funkcije, onda postoje $a, b \in \omega$ takvi da $\varphi_a = \varphi_{f(a,b)}$ i $\varphi_b = \varphi_{g(a,b)}$.

Kompletni skupovi

U prethodnom poglavlju napomenuli smo da poredak stepena nerešivosti sadrži stepene praznog skupa $\mathbf{o}$, skupa prirodnih brojeva $\mathbf{n}$, zatim stepen nerešivosti rekurzivnih skupova $\mathbf{0}$ i stepen nerešivosti skupa K, koji smo označili sa $\mathbf{0}'$. Kako sno ranije videli, postoje skupovi koji nisu svodljivi na K. Na primer, takvi su skupovi Tot, Ext ili Cof. U istraživanjima stepena nerešivosti pokazalo se da njihov poredak ima veoma složenu strukturu. To važi i za njen inicijalni deo određen stepenima $\mathbf{0}$ i $\mathbf{0}'$. U narednim razmatranjima okarakterisaćemo skupove stepena $\mathbf{0}'$ i pokazati da postoje stepeni rekurzivno nabrojivih skupova između $\mathbf{0}$ i $\mathbf{0}'$.

Primer 1. Neka je $A \oplus B = \{2x : x \in A\} \cup \{2x+1 : x \in B\}$, za proizvoljne $A, B \subseteq \omega$. Stepen $d(A \oplus B)$ je supremum stepena $d(A)$ i $d(B)$.

Ovaj rezultat zapravo pokazuje da uređenje stepena nerešivosti ima strukturu polumreže. Ta polumreža nije mreža. U njoj postoje stepeni rekurzivno nabrojivih skupova koji nemaju infimum.

S druge strane, uređenje 1-stepena nije polumreža. Postoje rekurzivno nabrojivi 1-stepeni koji nemaju supremum u uređenju 1-stepena.

Rekurzivno nabrojiv skup $A \subseteq \omega$ je *kompletan* ako za svaki rekurzivno nabrojiv skup $B \subseteq \omega$, $B \leq A$.

Zapravo, klasa kompletnih skupova je supremum svih stepena nerešivosti rekurzivno nabrojivih skupova.

Rekurzivno nabrojiv skup $A \subseteq \omega$ je 1-*kompletan* ako za svaki rekurzivno nabrojiv skup $B \subseteq \omega$, važi $B \leq_1 A$.

Primer 2. Kako smo ranije pokazali, skup K je 1-kompletan.

Skup A je 1-kompletan ako i samo ako $A \equiv_1 K$, odnosno skup A je 1-kompletan ako i samo ako A je rekurzivno nabrojiv i $K \leq_1 A$.

Otuda možemo zaključiti da stepen nerešivosti $\mathbf{0}'$ sadrži sve 1-kompletne rekurzivno nabrojive skupove.

Skup prirodnih brojeva $A \subseteq \omega$ je *produktivan* ako postoji totalna obostrano jednoznačna izračunljiva funkcija $\pi_A(x)$ – koju nazivamo *produktivnom funkcijom* skupa A – takva da za svako $x \in \omega$,

$$W_x \subseteq A \ \Rightarrow \ \pi_A(x) \in A - W_x.$$

Rekurzivno nabrojiv skup je *kreativan* ako je njegov komplement produktivan skup.

Intuitivno, kreativan skup A je "efektivno nerekurzivan" jer, ako je $W_x \subseteq A^c$, onda postoji efektivan kontraprimer $\pi_A(x) \in A^c \backslash W_x$ koji svedoči da W_x nije komplement skupa A. Nekompletnost rekurzivno aksiomatskih sistema je zapravo posledica egzistencije kreativnih skupova. Takve skupove Emil Post je smatrao potvrdom "esencijalne kreativnosti matematičkog mišljenja".

Primer 3. Skup K je kreativan.

Skup $K^c = \{x : x \notin W_x\}$ je produktivan. Njegova produktivna funkcija je identitet jer, ako $W_x \subseteq K^c$, onda $x \in K^c \backslash W_x$.

Primer 4. Ako je $A \subseteq \omega$ produktivan skup i $A \leq B$, onda je skup B produktivan.

Neka je $\pi_A(x)$ produktivna funkcija skupa A i $f(x)$ totalna izračunljiva funkcija takva da za svako $x \in \omega$, $x \in A$ ako i samo ako $f(x) \in B$.

Na osnovu teoreme o parametrizaciji, postoji totalna obostrano jednoznačna funkcija $s(x)$ takva da za svako $x \in \omega$, $W_{s(x)} = f^{-1}[W_x]$.

Za svako $x \in \omega$, ako $W_x \subseteq B$, onda $W_{s(x)} \subseteq A$, pa kako je π_A produktivna funkcija skupa A, $\pi_A(s(x)) \in A - W_{s(x)}$. Otuda sledi da za svako $x \in \omega$, ako $W_x \subseteq B$, onda $f \circ \pi_A \circ s(x) \in B - W_x$.

Funkcija $\pi = f \circ \pi_A \circ s$ ima sve osobine produktivne funkcije skupa B sa izuzetkom obostrane jednoznačnosti. Stoga, neka je $h(x)$ funkcija takva da $W_{h(x)} = W_x \cup \{\pi(x)\}$. Za svako $x \in \omega$, ako $W_x \subseteq B$, onda $W_{h(x)} \subseteq B$.

Neka je $\pi_B(0) = \pi(0)$. Za svako $x \in \omega$, vrednost $\pi_B(x+1)$ određujemo na sledeći način:

Izračunavamo redom vrednosti $\pi(x+1)$, $\pi h(x+1)$, $\pi h^2(x+1)$, itd. sve dok se ne pojavi vrednost $y \in \omega$ takva $y \notin \{\pi_B(0), \ldots, \pi_B(x)\}$ ili sve dok se izračunata vrednost ne ponovi. U prvom slučaju, $\pi_B(x+1) = y$. Ako se izračunata vrednost ponovi, to znači da $W_{x+1} \nsubseteq B$, pa možemo uzeti da je $\pi_B(x+1) = \mu y \, (y \notin \{\pi_B(0), \ldots, \pi_B(x)\})$.

Primer 5. Svaki netrivijalan indeksni skup koji sadrži indeks nigde definisane funkcije je produktivan.

Neka je $A \subseteq \omega$ netrivijalan indeksni skup, $e_0 \in A$ indeks nigde definisane funkcije i $e_1 \in \omega$ takav da $e_1 \notin A$.

Na osnovu teoreme o parametrizaciji, neka je $s(x)$ totalna obostrano jednoznačna funkcija takva da

$$\varphi_{s(x}(y) = \begin{cases} \varphi_{e_1}(y) & \text{ako } x \in K, \\ \text{nedefinisano} & \text{inače.} \end{cases}$$

Na osnovu ovog rezultata sledi da je svaki rekurzivno nabrojiv netrivijalan indeksni skup kreativan.

Primer 6. Skup Mono $= \{x : \varphi_x$ je "1-1"$\}$ je produktivan. Njegov komplement je kreativan skup.

S druge strane, skup Epi $= \{x : \varphi_x$ je "na" $\}$ je produktivan, ali njegov komplement nije kreativan.

Primer 7. (a) Ako je B rekurzivno nabrojiv skup i $A \cap B$ produktivan, skup A je produktivan.

(b) Postoji $2^{\aleph_0}$ produktivnih skupova.

Primer 8. (a) Ako je A kreativan i B rekurzivno nabrojiv skup, skup $A \oplus B$ je kreativan.

(b) Ako je B rekurzivan skup, važi i obrnuta implikacija.

Primer 9. Neka je $\mathcal{A} \subseteq \mathcal{R}_1$. Ako postoji $f \in \mathcal{A}$ takvo da za svako konačno $\theta \subseteq f$, $\theta \notin \mathcal{A}$, skup $A = \{x : \varphi_x \in \mathcal{A}\}$ je produktivan.

Otuda sledi da je Pol $= \{x : \varphi_x$ je polinom $\}$ produktivan skup. Primetimo da je i komplement ovog skupa produktivan.

Disjunktni skupovi A i B su *rekurzivno nerastavljivi* ako postoji totalna, obostrano jednoznačna izračunljiva funkcija $f(x, y)$ takva da, ako $A \subseteq W_x$, $B \subseteq W_y$ i $W_x \cap W_y = \emptyset$, onda $f(x, y) \notin W_x \cup W_y$.

Primer 10. Skupovi $A = \{x : \varphi_x(x) = 0\}$ i $B = \{x : \varphi_x(x) = 1\}$ su rekurzivno nerastavljivi.

Na osnovu teoreme o parametrizaciji, postoji totalna izračunljiva funkcija $f(x, y)$ takva da, ako $W_x \cap W_y = \emptyset$, onda

$$\varphi_{f(x,y)}(z) = \begin{cases} 1 & \text{ako } z \in W_x, \\ 0 & \text{ako } z \in W_y, \\ \text{nedefinisano} & \text{inače.} \end{cases}$$

Pretpostavimo da prirodni brojevi $x, y \in \omega$ zadovoljavaju uslove $A \subseteq W_x$, $B \subseteq W_y$ i $W_x \cap W_y = \emptyset$, onda $f(x,y) \notin W_x \cup W_y$.

Primer 11. Neka su A i B rekurzivno nerastavljivi skupovi.
(a) Ako je A rekurzivno nabrojiv, B^c je produktivan skup.
(b) Ako su A i B rekurzivno nabrojivi, A i B su kreativni skupovi.

Primer 12. Neka je $A_x = \{y : \varphi_y = \varphi_x\}$, $x \in \omega$.
(a) Za svako $x \in \omega$, A_x je produktivan skup.
(b) Ako je $\varphi_y \neq \varphi_x$, skupovi A_x i A_y su nerastavljivi.

Teorema 9. Svaki kreativan skup je kompletan.

Dokaz: Neka je A kreativan skup. Dokazaćemo da za svaki rekurzivno nabrojiv skup B, $B \leq_1 A$.

Neka je $\pi(x)$ produktivna funkcija za A^c. Na osnovu teoreme o parametrizaciji, neka je $s(x,y)$ totalna izračunljiva obostrano jednoznačna funkcija takva da za sve $x, y, x \in \omega$,

$$\varphi_{s(x,y)}(z) = \begin{cases} 0 & \text{ako } z = \pi(x) \text{ i } y \in B, \\ \text{nedefinisano} & \text{inače.} \end{cases}$$

Na osnovu teoreme rekurzije sa parametrom, postoji totalna obostrano jednoznačna izračunljiva funkcija $n(y)$ takva da $\varphi_{s(n(y),y)} = \varphi_{n(y)}$. Tvrdimo da za svako $y \in \omega$,

$$y \in B \quad \Leftrightarrow \quad \pi(n(y)) \in A.$$

Kako je $\pi(n(y))$ totalna obostrano jednoznačna izračunljiva funkcija, to će značiti da je $B \leq A$.

Neka $y \in B$. Tada $W_{s(n(y),y)} = \{\pi(n(y))\}$, pa prema definiciji funkcije $n(y)$, $W_{n(y)} = \{\pi(n(y))\}$. Ako $\pi(n(y)) \notin A$, $W_{n(y)} \subseteq A^c$, pa zbog produktivnosti funkcije π, $\pi(n(y)) \notin W_{n(y)}$, što nije moguće.

Obratno, ako $y \notin B$, onda $W_{n(y)} = \emptyset \subseteq A^c$, pa kako je π produktivna funkcija skupa A, $\pi(n(y)) \in A^c$. $\square$

Ako je $A \subseteq \omega$ kreativan skup, funkcije $\pi(x)$ i $n(x)$ su totalne, obostrano jednoznačne izračunljive funkcije. Dakle, skup A je kreativan ako i samo ako A je kompletan skup, odnosno, ako i samo ako A je 1-kompletan skup. To znači da stepen nerešivosti $\mathbf{0}'$ sadrži tačno kreativne skupove.

Primer 13. Skup $A \subseteq \omega$ je produktivan ako i samo ako $K^c \leq A$, odnosno, ako i samo ako $K^c \leq_1 A$.

Primer 14. Svaki produktivan skup sadrži beskonačan rekurzivno nabrojiv skup.

Neka je $\pi(x)$ produktivna funkcija skupa A. Na osnovu teoreme o parametrizaciji, definišimo totalnu obostrano jednoznačnu izračunljivu funkciju $s(x)$ takvu da za svako $x \in \omega$, $W_{s(x)} = W_x \cup \{\pi(x)\}$.

Izaberimo $n_0 \in \omega$ takvo da $W_{n_0} = \emptyset$ i definišimo funkciju $g(x)$ tako da $g(0) = n_0$ i za sve $x \in \omega$, $g(x+1) = s(g(x))$.

Za svako $x \in \omega$, $W_{g(x)} \subseteq A$ i $|W_{g(x)}| = x + 1$. Kako je $\pi(x)$ produktivna funkcija skupa A, $B = \{\pi(g(x)) : x \in \omega\} \subseteq A$, a po konstrukciji B je beskonačan rekurzivno nabrojiv skup.

Ukoliko postoji, skup čiji je stepen nerešivosti između $\mathbf{0}$ i $\mathbf{0}'$ je rekurzivno nabrojiv, nije rekurzivan i nije kreativan. Na osnovu prethodnog primera, ovo poslednje znači da njegov komplement ne sadrži beskonačan rekurzivno nabrojiv skup. Nerekurzivnost, podrazumeva da komplement takvog skupa mora biti beskonačan.

Skup $A \subseteq \omega$ je *prost* ako je A rekurzivno nabrojiv, A^c beskonačan i A^c ne sadrži beskonačan rekurzivno nabrojiv skup.

Teorema 10. Postoji prost skup.

Dokaz: Neka je $f(x) = \varphi_x(\mu y\,(\varphi_x(y) > 2x))$. Jasno, funkcija $f(x)$ je rekurzivna i neka je $A = \mathrm{codom}(f)$. Tvrdimo da je A prost skup.

Kako je A kodomen rekurzivne funkcije, dovoljno je dokazati da je A^c beskonačan i da ne sadrži beskonačan rekurzivno nabrojiv skup.

Skup A^c je beskonačan jer, za svako $x \in \omega$, $f(x) > 2x$, pa najviše x elemenata skupa $\{0, 1, \ldots, 2x\}$ pripada A, tj. za svako $x \in \omega$, A^c sadrži bar x elemenata.

Ako je W_x beskonačan skup, postoji $y \in \omega$ takvo da $y \in W_x$ i $y > 2x$. To znači da je vrednost $f(x)$ definisana i da $f(x) \in W_x$. Dakle, skup W_x nije sadržan u A^c. $\Box$

Primer 15. Neka je $f(x)$ totalna, obostrano jednoznačna rekurzivna funkcija takva da skup $\mathrm{codom}(f)$ nije rekurzivan. Ako je

$$A = \{x : \exists y\,(x < y \text{ i } f(x) > f(y))\},$$

skup A je prost.

Ako bi skup A^c bio konačan, postojao bi beskonačan strogo opadajući niz vrednosti funkcije $f(x)$, što nije moguće.

Ako bi postojalo $e \in \omega$ za koje je $W_e \subseteq A^c$ beskonačan skup, onda bi skup A bio rekurzivan što nije moguće.

Da to dokažemo, pretpostavimo da je $W_e \subseteq A^c$ beskonačan skup. To znači da za svako $z \in \omega$, postoji $s(z) \in W_e$ takvo da je $f(s(z)) > z$.

Kako $s(z) \notin A$, za svako $y \in \omega$, ako $f(y) < f(s(z))$, onda $y \leq s(z)$. Dakle, $z \in A$ ako i samo ako $\exists y \leq s(z)\,(f(y) = z)$. Kako je $s(z)$ rekurzivna funkcija, A je rekurzivan skup.

Aritmetički skupovi

Osim strukture stepena nerešivosti, u teoriji izračunljivosti postoje i druge hijerarhije složenosti podskupova prirodnih brojeva. Jedna takva hijerarhija dobija se analizom složenosti formalne definicije skupova prirodnih brojeva. Kasnije ćemo videti da su to zapravo skupovi koji se mogu definisati formulom u jeziku Peanove aritmetike. U ovom kontekstu, oni će biti definisani kao relacije koje se dobijaju kvantifikacijama rekurzivnih relacija.

Indukcijom po $n \in \omega$, definišemo skupove ili klase relacija Σ_n, Π_n i Δ_n prirodnih brojeva:

(a) skup Σ_0 je skup svih rekurzivnih relacija,
(b) za svako $n \geq 0$, skup Π_n se sastoji od negacija elemenata skupa Σ_n,
(c) za svako $n \geq 0$, $\Delta_n = \Pi_n \cap \Sigma_n$ i
(d) za svako $n \geq 0$, skup Σ_{n+1} se sastoji od svih relacija koje se mogu dobiti egzistencijalnom kvantifikacijom elemenata skupa Π_n.

Koristeći kodiranje konačnih nizova, umesto o relacijama, možemo govoriti o skupovima prirodnih brojeva. Svaku relaciju $R \subseteq \omega^n$ možemo shvatiti kao skup $R = \{\langle x_1, \ldots, x_n \rangle : R(x_1, \ldots, x_n)\} \subseteq \omega$. U daljem izlaganju takva identifikacija se podrazumeva.

Za svako $n \in \omega$, skupovi Σ_n, Π_n i Δ_n su *aritmetički skupovi*.

Primer 1. Relacija R je rekurzivna ako i samo ako R^c je rekurzivna relacija. Otuda sledi da je $\Sigma_0 = \Pi_0 = \Delta_0$.

Za svako $n \in \omega$, sve Π_{n+1} relacije se dobijaju univerzalnom kvantifikacijom Σ_n relacija.

Indukcijom po $n \in \omega$ dokazuje se da za svaku Σ_n relaciju $P \subseteq \omega^m$, postoji rekurzivna relacija $R \subseteq \omega^{m+n}$, takva da za sve $\vec{x} \in \omega^m$, $\vec{y} \in \omega^n$,

$$P(\vec{x}) = \exists y_1 \forall y_2 \exists y_3 \cdots Q y_n \, R(\vec{x}, y_1, \ldots, y_n)$$

Primer 2. Svi aritmetički skupovi zatvoreni su za supstituciju totalnih rekurzivnih funkcija: ako su $f_1(\vec{x}), \ldots, f_k(\vec{x})$ totalne rekurzivne funkcije i

$P(\vec{y})$, $\vec{y} \in \omega^k$, relacija koja pripada nekom od aritmetičkih skupova, istoj klasi pripada i relacija

$$R(\vec{x}) = P(f_1(\vec{x}), \ldots, f_k(\vec{x})).$$

Primer 3. Za svaki prirodan broj $n \geq 1$, skup Σ_n je zatvoren za egzistencijalnu, a skup Π_n za univerzalnu kvantifikaciju.

Primer 4. Svaki aritmetički skup je zatvoren za konjunkciju, disjunkciju i ograničenu kvantifikaciju. Za svaki prirodan broj $n \in \omega$, skup Δ_n je zatvoren i za negaciju.

Primer 5. Za svaki prirodan broj $n \in \omega$, važi $\Sigma_n \cup \Pi_n \subseteq \Delta_{n+1}$.

Tvrđenje dokazujemo indukcijom po $n \in \omega$. Za $n = 0$, svaka rekurzivna relacija $R(\vec{x})$ može se trivijalno predstaviti kao relacija:

$$\begin{aligned} R(\vec{x}) &= \exists y\,(R(\vec{x}) \wedge y = y) \\ &= \forall y\,(R(\vec{x}) \wedge y = y). \end{aligned}$$

To znači da relacija R pripada skupovima Σ_1 i Π_1, odnosno, relacija R pripada klasi Δ_1.

Neka je $n > 0$ i $R \in \Sigma_n$. Tada postoji relacija $Q \in \Pi_{n-1}$ za koju je $R(\vec{x}) = \exists y\, Q(\vec{x}, y)$. Po induktivnoj pretpostavci, $Q \in \Delta_n \subseteq \Pi_n$, pa dakle važi $R \in \Sigma_{n+1}$.

Kako je $R(\vec{x}) = \forall y\,(R(\vec{x}) \wedge y = y)$, $R \in \Pi_{n+1}$. Otuda sledi da $R \in \Delta_{n+1}$, odnosno, da je $\Sigma_n \subseteq \Delta_{n+1}$. Na sličan način dobija se da je $\Pi_n \subseteq \Delta_{n+1}$.

Na osnovu prethodnog primera, možemo zaključiti da između aritmetičkih skupova oblika Δ_n, Σ_n i Π_n, $n \in \omega$, postoje sledeći odnosi:

$$\Delta_0 = \Sigma_0 = \Delta_1 \subseteq \Sigma_1 \subseteq \Delta_2 \subseteq \Sigma_2 \subseteq \Delta_3 \subseteq \Sigma_3 \subseteq \cdots,$$

$$\Delta_0 = \Pi_0 = \Delta_1 \subseteq \Pi_1 \subseteq \Delta_2 \subseteq \Pi_2 \subseteq \Delta_3 \subseteq \Pi_3 \subseteq \cdots.$$

Relacije skupa $\Sigma = \bigcup_{n\in\omega} \Sigma_n = \bigcup_{n\in\omega} \Pi_n = \bigcup_{n\in\omega} \Delta_n$ nazivamo *aritmetičkim relacijama*, odnosno, aritmetičkim skupovima kada relacije shvatimo kao skupove njihovih kodova. Navedene nizove, uzete u ukupnosti nazivaćemo *aritmetičkom hijerarhijom.*

Na osnovu Klinijeve teoreme o efektivnoj numeraciji, za svaki prirodan broj $n \geq 1$, određena je kanonska forma aritmetičkih relacija tipa Σ_n.

Teorema 11. Teorema o kanonskoj formi: Relacija $R \subseteq \omega^m$ pripada klasi Σ_{n+1} ako i samo ako postoji $e \in \omega$ takvo da za sve $\vec{x} \in \omega^m$,

(a) ako je $n \in \omega$ paran broj,

$$R(\vec{x}) = \exists y_1 \forall y_2 \cdots \forall y_n \exists y_{n+1}\, T_{m+n}(\vec{x}, y_1, \ldots, y_{n+1}) \text{ ili}$$

(b) ako je $n \in \omega$ neparan broj,

$$R(\vec{x}) = \exists y_1 \forall y_2 \cdots \exists y_n \forall y_{n+1}\, \neg T_{m+n}(\vec{x}, y_1, \ldots, y_{n+1}).$$

Dokaz: Dovoljno je dokazati tvrđenje za slučaj skupa Σ_1. Svi ostali slučajevi slede neposredno iz definicije aritmetičkih skupova tipa Σ_n.

Ako je $R(\vec{x}) = \exists y\, T_m(e, \vec{x}, y)$, budući da je Klinijev predikat primitivno rekurzivan, mora biti $R \in \Sigma_1$.

Obratno, ako $R \in \Sigma_1$, onda postoji rekurzivan predikat $Q(\vec{x}, y)$ takav da za sve $\vec{x} \in \omega^n$, $R(\vec{x}) = \exists y\, Q(\vec{x}, y)$. Neka je $f(\vec{x}) = \mu y\, Q(\vec{x}, y)$ i $e \in \omega$ indeks izračunljive funkcije $f(\vec{x})$. Prema Klinijevoj teoremi o normalnoj formi, $f(\vec{x}) = (\mu y\, T_n(e, \vec{x}, y))_1$ što znači da je $R(\vec{x}) = \exists y\, T_n(e, \vec{x}, y)$. $\square$

Slično kao u teoremi o efektivnoj numeraciji rekurzivnih funkcija, kanonska forma aritmetičkog predikata omogućava nam da za svako $m \geq 1$ definišemo *univerzalnu aritmetičku relaciju* $Q(e, \vec{x})$, $e \in \omega$, koja efektivno numeriše sve n-arne Σ_1 relacije.

Primer 6. Za svako $m \geq 1$ i svako $n \in \omega$, postoji $(m+1)$-arna relacija $Q \in \Sigma_{n+1}$ koja efektivno numeriše sve m-arne Σ_{n+1} relacije.

Za svako $\vec{x} \in \omega^m$, neka je $Q(e, \vec{x}) = \exists y\, T_m(e, \vec{x}, y)$. Očigledno, Q je $(m+1)$-arna Σ_1 relacija, a na osnovu teoreme o kanonskoj formi, svaka m-arna Σ_1 relacija je oblika $Q(e, \vec{x})$, za neko $e \in \omega$.

Na osnovu teoreme o kanonskoj formi, za svako $m \in \omega$, postoji $(m+1)$-arna Σ_{n+1} koja je univerzalna za klasu m-arnih Σ_{n+1} relacija.

Primer 7. (a) Za svaki prirodan broj $n \in \omega$, svaka aritmetička relacija tipa Π_{n+1} ima kanonsku formu.

U formulaciji teoreme o kanonskoj formi za slučaj Π_{n+1} relacija, u odnosu na odgovarajuću teoremu za Σ_{n+1} relacije, uzajamno su zamenjene uloge egzistencijalnog i univerzalnog kvantifikatora, kao i uloge predikata T_{m+n} i $\neg T_{m+n}$.

(b) Za svaki prirodan broj $m \geq 1$, postoji $(m+1)$-arna univerzalna relacija za klasu m-arnih aritmetičkih relacija tipa Π_{n+1}.

Primer 8. (a) Tvrđenja o kanonskoj formi i univerzalnoj relaciji ne važe u slučaju Δ_{n+1} relacija.

(b) Teorema o kanonskoj formi ne važi za Σ_0 i Π_0 relacije.

Aritmetičku hijerarhiju Σ definisali smo kao uniju rastućih nizova aritmetičkih skupova. Međutim, uopšte nije jasno do kog stepena ovako definisana familija može da raste i da li uopšte raste. Pre nego što dokažemo da Σ jeste hijerarhija u pravom smislu te reči navodimo ocenu nivoa u aritmetičkoj hijerarhiji kojem pripadaju neki od skupova koje smo do sada definisali.

Primer 9. (a) Skup Fin pripada klasi Σ_2.
(b) Skup $\{\langle x, y\rangle : W_x \subseteq W_y\}$ pripada klasi Π_2.
(c) Skupovi $\{\langle x, y\rangle : W_x = W_y\}$ i Tot pripadaju klasi Π_2.

Primer 10. (a) Skupovi Rec i Ext pripadaju klasi Σ_3.
(b) Skup $\{x : W_x \text{ je kreativan}\}$ je Σ_3 skup.
(c) Isto važi i za skup $\{\langle x, y\rangle : W_x \text{ i } W_y \text{ su rastavljivi}\}$.
Prirodni primeri složenijih skupova u ovoj hijerarhiji su veoma retki.

Skup $A \in \Sigma_n$ je Σ_n*-kompletan* ako za svako $B \in \Sigma_n$, $B \leq A$. Na isti način definišemo i pojam Π_n-kompletnosti, $n \geq 1$.

Ako su (A_1, A_2) i (B_1, B_2) parovi skupova prirodnih brojeva takvi da $A_1 \cap A_2 = B_1 \cap B_2 = \emptyset$, onda $(A_1, A_2) \leq (B_1, B_2)$ ako postoji totalna rekurzivna funkcija $f(x)$ takva da

$$f[B_1] \subseteq A_1,\ f[B_1] \subseteq A_1 \text{ i } f[(B_1 \cup B_2)^c] \subseteq (A_1 \cup A_2)^c.$$

Primer 11. Za svako $A \in \Sigma_2$, $(A, A^c) \leq$ (Fin,Tot). Dakle, Fin je Σ_2-kompletan, a Tot Π_2-kompletan skup.

Neka je $A \in \Sigma_2$. To znači da je $A^c \in \Pi_2$ pa postoji rekurzivna relacija $R(x, y, z)$ takva da za svako $x \in \omega$, $x \in A^c$ ako i samo ako $\forall y \exists z\, R(x, y, z)$. Na osnovu teoreme o parametrizaciji, neka je $f(x)$ totalna, obostrano jednoznačna funkcija takva da

$$\varphi_{f(x)}(u) = \begin{cases} 0 & \text{ako } \forall y \leq u\, \exists z\, R(x, y, z), \\ \text{nedefinisano} & \text{inače.} \end{cases}$$

Ako $x \in A^c$, onda $W_{f(x)} = \omega$, pa $f(x) \in$ Tot. S druge strane, ako $x \in A$, onda $|W_{f(x)}| < \omega$ pa mora biti $f(x) \in$ Fin.

Primer 12. Prethodnom metodom, sa nešto više tehničkih detalja, može se dokazati da su Cof i Ext Σ_3-kompletni skupovi.

U prethodnim razmatranjima dokazali smo da skupovi Fin i Tot ne pripadaju klasi Σ_1, pa dakle $\Sigma_1 \neq \Sigma_2$. Za skupove Cof i Ext čak znamo da su Σ_3-kompletni, ali nismo dokazali da oni zaista nisu Σ_2 skupovi. Možda je $\Sigma_2 = \Sigma_3$? Da to nije slučaj pokazuje sledeća teorema.

Teorema 12. Teorema o aritmetičkoj hijerarhiji: Za svako $n \in \omega$, postoji relacija $R \subseteq \omega$ takva da $R \in \Sigma_{n+1}$ i $R \notin \Pi_{n+1}$.

Dokaz: Neka je $Q(x,y)$ binarna Σ_{n+1} relacija koja efektivno numeriše sve unarne relacije klase Σ_{n+1}.

Za svako $x \in \omega$, neka je $R(x) = Q(x,x)$. Relacija R pripada klasi Σ_{n+1}. Pritom, ako $R \in \Pi_{n+1}$, onda $\neg R \in \Sigma_{n+1}$, pa postoji $e \in \omega$ takvo da $\neg R(x) = Q(e,x)$. To zapravo znači da za svako $x \in \omega$, $\neq Q(x,x) = Q(e,x)$ što za $x = e$ nije moguće. $\Box$

Relativna izračunljivost

Ideju svođenja problema, koju smo do sada razvili u okviru stepena nerešivosti, uopštićemo tako da ona odgovara intuitivnoj ideji relativne izračunljivosti skupova prirodnih brojeva. Skup $A \subset \omega$ je relativno izračunljiv u odnosu na skup $B \subseteq \omega$ ako se karakteristična funkcija skupa A može rekurzivno izraziti pomoću karakteristične funkcije skupa B. Tako se dobija sasvim prirodna hijerarhija stepena nerešivosti.

Pretpostavimo da je f totalna funkcija. Najmanja klasa funkcija prirodnih brojeva, koja sadrži funkciju f, bazne funkcije i zatvorena je za supstituciju, rekurziju i minimizaciju, u oznaci $\mathcal{R}^f$, je klasa *f-rekurzivnih funkcija*. Ako $g \in R^f$, funkcija g je *relativno rekurzivna* s obzirom funkciju f ili f-rekurzivna.

Slično idealnom računaru, kao paradigmi rekurzivnih funkcija, može se definisati i f-idelani računar koji odgovara f-rekurzivnim funkcijama. Takvo uopštenje omogućava da teoriju relativno rekurzivnih funkcija razvijemo na isti način na koji je ranije razvijena teorija rekurzivnih funkcija.

Pretpostavljamo da za svako $n \geq 1$, f-idealni računar sadrži instrukciju $F(n)$ koja sadržaj r_n registra R_n zamenjuje sa $f(r_n)$. Program P^f ovako proširenog računara je konačan niz instrukcija koji, eventualno, sadrži i određen broj instrukcija $F(n)$. Kao i u slučaju običnog idealnog računara, definišemo pojam izračunavanja $P^f(\vec{x})$ i klasu *f-izračunljivih* funkcija $\mathcal{I}^f$.

Primer 1. Pojmovi f-izračunljivosti i f-rekurzivnosti su ekvivalentni. Za svaku totalnu funkciju f, važi jednakost $\mathcal{I}^f = \mathcal{R}^f$.

Primer 2. Neznatnim modifikacijama kodiranja programa idealnog računara dobija se kodiranje programa f-idealnog računara i za svako $n \in \omega$, numeracija f-rekurzivnih n-arnih funkcija $(\varphi_x^{(n),f} : x \in \omega)$.

Primer 3. Za svako $n \geq 1$, numeracija f-rekurzivnih n-arnih funkcija je efektivna i postoji funkcija $\varphi_u^{(n+1),f}(e,\vec{x}) = \varphi_e^{(n),f}(\vec{x})$ koja je univerzalna za klasu n-arnih f-rekurzivnih funkcija. Univerzalni program P_u je nezavisan od funkcije f.

Primer 4. Za relativnu rekurzivnost takođe važi teorema o parametrizaciji. Pritom, funkcije oblika $s_m(e, \vec{x})$ su totalne izračunljive funkcije u apsolutnom smislu, odnosno, ne zavise od funkcije f.

Skup je *f-rekurzivan* ako je njegova karakteristična funkcija f-rekurzivna, a *f-parcijalno rekurzivan* ako je njegova parcijalna karakteristična funkcija f-rekurzivna. index$f$-rekurzivan skup

Primer 5. Skup A je f-rekurzivan ako i samo ako skupovi A i A^c su f-parcijalno rekurzivni.

Primer 6. Skup A je f-parcijalno rekurzivan ako i samo ako postoji $e \in \omega$ takvo da $A = W_x^f$, ako i samo ako $A = \emptyset$ ili A je kodomen totalne f-izračunljive funkcije, ako i samo ako postoji f-odlučiv predikat $R(x, y)$ takav da, za svako $x \in \omega$, $x \in A$ ako i samo ako $\exists y\, R(x, y)$.

Primer 7. Ako je $K^f = \{x : x \in W_x^f\}$, skup K^f je f-parcijalno rekurzivan i nije f-rekurzivan.

Ako je c_A karakteristična funkcija skupa $A \subseteq \omega$, umesto o c_A-izračunljivosti govorimo o A-izračunljivosti. Slično, oznake φ_x^A, W_x^A ili K^A, podrazumevaju odgovarajuće oznake relativne izračunljivosti s obzirom na funkciju c_A.

Primer 8. Neka je A proizvoljan skup. Za svaki rekurzivno nabrojiv skup B postoji prirodan broj $e \in \omega$ takav da važi $B = W_e^A$.

Ako je A rekurzivan skup, za svaki prirodan broj $e \in \omega$, skup W_e^A je rekurzivno nabrojiv. U tom slučaju skup K^A je rekurzivno nabrojiv i nije rekurzivan.

Primer 9. (a) Ako je skup A relativno rekurzivan u odnosu na B i skup B relativno rekurzivan u odnosu na C, skup A je relativno rekurzivan u odnosu na C.

(b) Ako je skup A relativno rekurzivno nabrojiv u odnosu na B i skup B relativno rekurzivan u odnosu na C, skup A je relativno rekurzivno nabrojiv u odnosu na C.

(c) Ako je skup A relativno rekurzivan u odnosu na B i skup B relativno rekurzivno nabrojiv u odnosu na C, skup A nije nužno C-rekurzivno nabrojiv.

Primer 10. Skup B je A-rekurzivan ako i samo ako $B \leq K^A$.

Skup $A \subseteq \omega$ je *T-svodljiv* na skup $B \subseteq \omega$, odnosno, svodljiv u Tjuringovom smislu, u oznaci $A \leq_T B$, ako je A B-rekurzivan skup.

Skupovi $A, B \subseteq \omega$ su T-ekvivalentni, u oznaci $A \equiv_T B$, ako $A \leq_T B$ i $B \leq_T A$. Klasa ekvivaklencije $d_T(A) = \{B : A \equiv_T B\}$ je *T-stepen nerešivosti*.

Svaki T-stepen koji sadrži rekurzivan skup je *rekurzivan T-stepen*, a svaki T-stepen koji sadrži rekurzivno nabrojiv skup je *rekurzivno nabrojiv T-stepen*.

Ako su $\mathbf{a}$ i $\mathbf{b}$ proizvoljni T-stepeni, njihov poredak definišemo tako da: $\mathbf{a} \leq \mathbf{b}$ ako postoje $A \in \mathbf{a}$ i $B \in \mathbf{b}$ takvi da $A \leq_T B$.

Primer 11. (a) Ako $A \leq B$, onda $A \leq_T B$.

(b) Za svaki skup A, važi $A \equiv_T A^c$.

(c) Ako je A rekurzivan skup i $B \leq_T A$, B je rekurzivan skup. Ako je A rekurzivno nabrojiv skup, onda $A \leq_T K$.

Primer 12. Postoji jedinstven T-stepen, u oznaci $\mathbf{0}$, koji sadrži sve rekurzivne skupove. Ako je $\mathbf{0}'$ stepen skupa K, onda $\mathbf{0} < \mathbf{0}'$ i $\mathbf{0}'$ je maksimalan rekurzivno nabrojiv T-stepen.

Primer 13. (a) Za proizvoljne $A, B \subseteq \omega$, važi $d(A) \subseteq d_T(A)$.

(b) Ako $d(A) \leq d(B)$, onda $d_T(A) \leq d_T(B)$.

Primer 14. Neka su $A, B \subseteq \omega$ proizvoljni skupovi prirodnih brojeva.

(a) Skup K^A je A-rekurzivno nabrojiv.

(b) Ako je B A-rekurzivno nabrojiv skup, onda onda važi $B \leq_T K^A$.

(c) Ako je A rekurzivan skup, onda $K^A \equiv_T K$.

(d) Za svaki skup $A \subseteq \omega$, važi $A <_T K^A$.

(e) Ako $A \leq_T B$, onda $K^A \leq_T K^B$ i ako $A \equiv_T B$, onda $K^A \equiv_T K^B$.

Za proizvoljan skup $A \subseteq \omega$, skup K^A je *skok* skupa A. Pritom, $K^\emptyset = K$. Skok skupa A označavamo sa A'.

Za svaki skup $A \subseteq \omega$, n-ti skok skupa A, u oznaci $A^{(n)}$, definišemo induktivno; $A^{(0)} = A$ i za svako $n \geq 0$, $A^{(n+1)} = (A^{(n)})'$.

Ako je $\mathbf{a}$ T-stepen i $A \in \mathbf{a}$, stepen $d(K^A) = \mathbf{a}'$ je *skok* stepena $\mathbf{a}$.

Primer 15. Na osnovu prethodnog primera, tvrđenje (e), definicija skoka je korektna. Takođe, ona je saglasna sa definicijom stepena $\mathbf{0}'$.

Primer 16. (a) Za svako $\mathbf{a}$, $\mathbf{a} < \mathbf{a}'$.

(b) Za proizvoljne $\mathbf{a}, \mathbf{b}$, ako $\mathbf{a} \leq \mathbf{b}$, onda $\mathbf{a}' \leq \mathbf{b}'$.

(c) Ako $A \in \mathbf{a}$, $B \in \mathbf{b}$ i B A-rekurzivno nabrojiv, onda $\mathbf{b} \leq \mathbf{a}'$.

Primer 17. Kako smo već napomenuli, $\mathbf{0}' = d_T(K)$. Osim toga, $\mathbf{0}'' = d_T(\mathrm{Tot}) = d_T(\mathrm{Fin})$ i $\mathbf{0}''' = d_T(\mathrm{Rec}) = d_T(\mathrm{Ext})$.

Primer 18. Na osnovu aksiome izbora može se dokazati da T-stepena nerešivosti ima tačno $2^{\aleph_0}$.

Primer 19. (a) Za svaki prirodan broj $n \in \omega$, $A \in \Sigma_{n+1}$ za neko $B \in \Pi_n$, A je B-parcijalno rekurzivan skup, ako i samo ako za neko $B \in \Sigma_n$, A je B-parcijalno rekurzivan skup.

(b) Za svako $n > 0$, skup $\emptyset^{(n)}$ je Σ_n-kompletan.

(c) Za svako $A \subseteq \omega$, $A \in \Sigma_{n+1}$ ako i samo ako A je $\emptyset^{(n)}$-parcijalno rekurzivan skup.

(d) Za svako $A \subseteq \omega$, $A \in \Delta_{n+1}$ ako i samo ako $A \leq_T \emptyset^{(n)}$.

Primer 20. Za svaki prirodan broj $n \geq 1$, $\Delta_n \neq \Sigma_n$ i $\Delta_n \neq \Pi_n$.

Ovaj rezultat predstavlja još jedan dokaz teoreme o aritmetičkoj hijerarhiji. Prema prethodnom primeru, za svako $n \geq 1$, $\emptyset^{(n)} \in (\Sigma_n - \Pi_n)$ i slično, $\emptyset^{(n)} \in (\Pi_n - \Sigma_n)$.

Slično stepenima nerešivosti, T-stepeni čine polumrežu, odnosno, za proizvoljne T-stepene $\mathbf{a}$ i $\mathbf{b}$ određen je njihov supremum i on se dobija isto kao i supremum stepena nerešivosti.

Međutim, strukture ovih stepena bitno se razlikuju. Kako smo ranije napomenuli, za proizvoljne skupove $A, B \subseteq \omega$, $d(A) \subseteq d_T(A)$ i ako $d(A) \leq d(B)$, onda $d_T(A) \leq d_T(B)$, ali više od toga se teško može reći.

Primer 21. Svaki T-stepen nerekurzivnih parcijalno rekurzivnih skupova sadrži prost skup.

Ako je B nerekurzivan rekurzivno nabrojiv skup i $B = \text{codom}(f)$, gde je f totalna izračunljiva funkcija, onda je $A = \{x : \exists y\, (f(y) < f(x) \text{ i } y > x)\}$ prost skup i pritom, $A \equiv_T B$.

Ovaj rezultat pokazuje da T-stepen $\mathbf{0}'$ sadrži prost skup. Za razliku od stepena nerešivosti, u slučaju T-stepena, prosti skupovi ne rešavaju problem egzistencije stepena $\mathbf{a}$ takvog da $\mathbf{0} < \mathbf{a} < \mathbf{0}'$. Završavajući ovaj pregled, napominjemo da takav stepen zaista postoji.

Proširenja logike prvog reda

Svaka formalizacija matematičkih rezultata ima određena ograničenja. Uverili smo se da ona postoje i u teorijama koje izražavaju svojstva relativno jednostavnih matematičkih struktura. Načelno posmatrano, granicu do koje je moguća formalizacija matematičkog mišljenja određuje upravo aritmetika prirodnih brojeva.

Sa jednim takvim ograničenjem susreli smo se na samom početku našeg izlaganja. U jeziku aritmetike $\mathcal{L}_{\mathrm{PA}}$ definisali smo Peanovu aritmetiku, odnosno teoriju PA, čije aksiome obuhvataju rekurzivne definicije sabiranja, množenja i shemu matematičke indukcije. Takođe, definisali smo i kompletnu aritmetiku $\mathrm{Th}(\mathcal{N})$, kao teoriju koja sadrži sve istine prirodnih brojeva izražene u jeziku aritmetike. U oba slučaja, dokazali smo da ove teorije imaju nestandardne modele, odnosno, da u njima nije moguća potpuna karakterizacija prirodnih brojeva.

Međutim, potpuni opis strukture prirodnih brojeva jeste moguć metamatematičkim sredstvima. Ako se aksioma indukcije formuliše na podskupovima skupa ω, takva aritmetika do na izomorfizam karakteriše strukturu prirodnih brojeva. Na prvi pogled, moglo bi se prosto reći da jezik $\mathcal{L}_{\mathrm{PA}}$ nije dovoljan da izrazi ovu činjenicu i da se u nekom njegovom proširenju takav rezultat može dobiti. Međutim, na osnovu Skolemove teoreme, ekstenzije ovih teorija u bilo kom jeziku prvog reda imale bi nestandardne modele. Potpuna formalizacija aritmetike nije moguća u logici prvog reda.

Logika drugog reda

Jezik drugog reda dobija se proširenjem jezika $\mathcal{L}$ prebrojivim skupom relacijskuh promenljivih. Preciznije, za svako $n \in \omega$, jezilk $\mathcal{L}_2 \supseteq \mathcal{L}$ sadrži skup simbola relacijskih promenljivih $\{X_i^n : i \in \omega\}$.

Skup pravila koji generiše formule jezika $\mathcal{L}_2$ određen je skupom pravila jezika $\mathcal{L}$ koji je proširen sledećim pravilima:

(a) ako je X n-arna relacijska promenljiva i $t_1, \ldots, t_n$ termi jezika $\mathcal{L}$, onda je $X(t_1, \ldots, t_n)$ elementarna formula jezika $\mathcal{L}_2$,

(b) ako je φ formula jezika $\mathcal{L}_2$ i X relacijska promenljiva, onda je $\exists X\, \varphi$ formula jezika $\mathcal{L}_2$.

Neka je $\mathcal{A}$ model jezika $\mathcal{L}$. Valuacija a promenljivih jezika $\mathcal{L}_2$ je funkcija takva da, za svaku n-arnu relacijsku promenljivu X, $a(X)$ je n-arna relacija skupa A. U slučaju individualnih promenljivih, $a(v_n)$ je element skupa A, odnosno, na promenljivim prvog reda, definicija valuacije se poklapa sa valuacijom promenljivih jezika $\mathcal{L}$.

Definiciju relacije zadovoljenja, u odnosu na jezik prvog reda, neophodno je dopuniti sledećim uslovima:

(a) $\mathcal{A} \models_a X(t_1, \ldots, t_n)$ ako i samo ako $([t_1]_a^A, \ldots, [t_n]_a^A) \in a(X)$,

(b) $\mathcal{A} \models_a \exists X\, \varphi$ ako i samo ako postoji $C \subseteq A^n$, $\mathcal{A} \models_{a(X/C)} \varphi$.

Pritom, valuacija $a(X/C)$ za promenljivu X ima vrednost C, a u svim drugim slučajevima poklapa se sa valuacijom a. Rečenica φ drugog reda je valjana, u oznaci $\models \varphi$, ako za svaki model $\mathcal{A}$ jezika $\mathcal{L}$, $\mathcal{A} \models \varphi$.

Primer 1. Rečenica $\forall x \forall y\, (x = y \leftrightarrow \forall\, X(X(x) \leftrightarrow X(y)))$ je valjana u logici drugog reda. Ona izražava princip intenzionalnosti koji je Lajbnic nazivao *identitas indiscernibilium*. Objekti su jednaki ako i samo ako imaju ista svojstva.

Primer 2. Postoji rečenica φ_{fin} jezika $\mathcal{L}_2$ takva da, za svaki model $\mathcal{A}$ drugog reda, $\mathcal{A} \models \varphi$ ako i samo ako A je konačan skup.

Skup A je konačan ako i samo ako svaka obostrano jednoznačna funkcija $f : A \to A$ je "na". Rečenica φ_{fin} dobija se formalizacijom ove definicije konačnog skupa u logici drugog reda.

Primer 3. U logici drugog reda ne važi stav kompaktnosti.

Naime, skup rečenica $\{\varphi_{\text{fin}}\} \cup \{\varphi_{\geq n} : n \geq 2\}$ je protivrečan, a svaki njegov konačan podskup ima model.

Kako su formule logike drugog reda konačni nizovi simbola jezika $\mathcal{L}_2$, odsustvo stava kompaktnosti pokazuje da se u ovoj logici ne može definisati sintaksa, u kojoj bi dokazi bili konačni nizovi, koja bi bila saglasna i potpuna u odnosu na semantiku logike drugog reda.

Primer 4. Pretpostavimo da jezik drugog reda $\mathcal{L}_2$ sadrži relacijsku konstantu $\leq$. Za svaki model $\mathcal{A}$ jezika $\mathcal{L}_2$, rečenica

$$\varphi_{\text{du}} = \forall X\, (\exists x\, X(x) \to \exists x\, (X(x) \wedge \forall y\, (X(y) \to x \leq y)))$$

važi u modelu $\mathcal{A}$ ako i samo ako $(A, \leq)$ je dobro uređenje.

Primer 5. Parcijalno uređenje $\mathcal{P}$ je *drvo* ako za svako $x \in P$, inicijalni segment $P_x = \{y : y < x\}$ je dobro uređen. Kao u prethodnom primeru, pretpostavljamo da jezik drugog reda $\mathcal{L}_2$ sadrži relacijsku konstantu $\leq$.

Postoji rečenica jezika $\mathcal{L}_2$ oblika $\exists X\, \varphi$, gde je φ formula bez relacijskih kvantifikatora, takva da za svaki model $\mathcal{A}$ jezika $\mathcal{L}_2$, $\mathcal{A} \models \exists X\, \varphi$ ako i samo ako uređenje $(A, \leq)$ je drvo.

Primer 6. Aritmetika drugog reda je teorija u jeziku $\mathcal{L}_2 = \{s, 0\}$, čije su aksiome sledeće rečenice:

$$\begin{aligned}
&\varphi_1 = \forall x\, (s(x) \neq 0),\\
&\varphi_2 = \forall x \forall y\, (s(x) = s(y) \to x = y),\\
&\varphi_3 = \forall X\, (X(0) \wedge \forall x\, (X(x) \to X(s(x))) \to \forall x\, X(x).
\end{aligned}$$

Jasno je da su φ_1, φ_2 rečenice prvog reda i da rečenica φ_3 izražava princip matematičke indukcije u logici drugog reda.

Ako je $\varphi_{\text{PA}} = \varphi_1 \wedge \varphi_2 \wedge \varphi_3$, za svaki model $\mathcal{M}$ jezika $\mathcal{L}_{\text{PA}}$,

$$\mathcal{M} \models \varphi_{\text{PA}} \quad \Leftrightarrow \quad \mathcal{N} \cong \mathcal{M}.$$

Ovo tvrđenje dokazali smo u uvodnim razmatranjima. Ono pokazuje da je aritmetika drugog reda konačno aksiomatska kategorična teorija.

Primer 7. Postoji rečenica φ_ω jezika $\mathcal{L}_2$ čiji je logički deo prazan takva da, za svaki model $\mathcal{A}$ jezika $\mathcal{L}_2$,

$$\mathcal{A} \models \varphi_\omega \quad \Leftrightarrow \quad |A| = \omega.$$

Ako se u rečenici φ_{PA} funkcija s zameni unarnom relacijskom promenljivom Y, a konstanta 0 promenljivom z, dobija se formula $\psi(Y, z)$ jezika drugog reda $\mathcal{L}_2$ koji ne sadrži nelogičke simbole. Ako je φ_ω rečenica čiji je smisao "postoji funkcija Y i postoji jedinstven element z takvi da važi $\psi(Y, z)$", na osnovu prethodnog primera, za svaki model $\mathcal{A}$ logike drugog reda, $\mathcal{A} \models \varphi_\omega$ ako i samo ako $|A| = \omega$.

Primer 8. U logici drugog reda ne važi donja Skolemova teorema.

Neka je $\varphi_{\leq\omega} = \varphi_\omega \vee \varphi_{\text{fin}}$. Za svaki model $\mathcal{A}$, $\mathcal{A} \models \varphi_{\leq\omega}$ ako i samo ako A je prebrojiv skup. Rečenica $\neg\varphi_{\leq\omega}$ važi u modelu $\mathcal{A}$ ako i samo ako A je neprebrojiv skup, pa dakle u logici drugog reda ne važi Skolemova teorema.

Primer 9. Postoji rečenica φ_R jezika $\mathcal{L}_2$, koji sadrži jezik teorije polja, takva da za svaki model $\mathcal{A}$ jezika $\mathcal{L}_2$, $\mathcal{A} \models \varphi_R$ ako i samo ako $\mathcal{A} \cong \mathcal{R}$.

Rečenica φ je konjunkcija aksioma uređenih polja i principa maksimalnosti koji se može formulisati u logici drugog reda. Dakle, slično aritmetici prirodnih brojeva, u logici drugog reda, aritmetika realnih brojeva je konačno aksiomatska i kategorična.

Primer 10. Postoji rečenica φ_{2^ω} jezika $\mathcal{L}_2$ koji ne sadrži logičke simbole takva da za svaki model $\mathcal{A}$ logike drugog reda, $\mathcal{A} \models \varphi_{2^\omega}$ ako i samo ako $|A| = 2^\omega$.

Ako se u rečenici φ_R jezika teorije polja funkcijske i relacijske konstante zamene relacijskim promenljivim drugog reda, a individualne konstante promenljivim prvog reda, slično kao u slučaju rečenice φ_ω, dobija se rečenica φ_{2^ω} jezika $\mathcal{L}_2$ bez nelogičkih simbola takva da, za svaki model $\mathcal{A}$ jezika $\mathcal{L}_2$, $\mathcal{A} \models \varphi_{2^\omega}$ ako i samo ako $|A| = 2^\omega$.

Primer 11. Postoji formula $\psi(X)$ jezika $\mathcal{L}_2$ koji ne sadrži logičke simbole takva da u svakom modelu $\mathcal{A}$ logike drugog reda, za svaku valuaciju a, $\mathcal{A} \models_a \varphi(X)$ ako i samo ako $a(X)$ je prebrojiv skup ili postoji bijekcija g skupa $a(X)$ na A.

U jeziku $\mathcal{L}_2$ može se definisati formula $\text{Fun}(f)$ čiji je smisao "f je funkcija", pa je $\psi(X)$ sledeća formula:

$$\varphi_{\leq\omega}(X) \;\vee\; \exists f \; \mathrm{Fun}(f) \wedge \; (\forall x \, X(f(x)) \wedge \\ \forall x \forall y \, (f(x) = f(y) \to x = y) \wedge \forall y \, (X(y) \to \exists x \, f(x) = y))).$$

Kontinuum hipoteza tvrdi da za svako $X \subseteq 2^\omega$, skup X je ili prebrojiv ili postoji bijekcija skupa 2^ω na X. U logici drugog reda ona se može izraziti rečenicom

$$\varphi_{\mathrm{CH}} = \varphi_{2^\omega} \to \forall \, X \psi(X).$$

Rečenica φ_{CH} formulisana je u jeziku $\mathcal{L}_2$ bez nelogičkih simbola. Na osnovu prethodnih primera, u logici drugog reda

$$\models \varphi_{\mathrm{CH}} \quad \Leftrightarrow \quad \mathrm{CH}.$$

Dakle, u logici drugog reda, kontinuum hipoteza je ili istinita ili lažna, tj. teorija ZFC nije dovoljno jaka da okarakteriše njenu semantiku.

Ako se u logici $\mathcal{L}_2$ kvantifikatori relacijskih promenljivih ograniče na konačne skupove, odnosno, ako se zadovoljenje egzistencijalnih formula drugog reda zameni uslovom

$$\mathcal{A} \models_a \exists X \, \varphi \quad \Leftrightarrow \quad \text{postoji konačan } C \subseteq A^n, \, \mathcal{A} \models_{a(X/C)} \varphi,$$

dobija se *slaba logika* drugog reda. Činjenicu da rečenica slabe logike φ važi u modelu $\mathcal{A}$ označavamo sa $\mathcal{A} \models^s \varphi$.

Primer 12. Postoji rečenica φ i postoji model $\mathcal{A}$ jezika $\mathcal{L}_2$ takvi da $\mathcal{A} \models^s \varphi$ i pritom, nije da $\mathcal{A} \models \varphi$.

Primer 13. Za svaku rečenicu φ jezika $\mathcal{L}_2$, postoji rečenica φ^* takva da za svaki model $\mathcal{A}$, važi relacija $\mathcal{A} \models^s \varphi \;\; \Leftrightarrow \;\; \mathcal{A} \models \varphi^*$.

Za datu rečenicu φ, rečenica φ^* dobija se relativizacijom relacijskih promenljivih na predikat $\varphi_{\mathrm{fin}}(X)$.

Primer 14. U slaboj logici drugog reda ne važi stav kompaktnosti.

Kasnije ćemo dokazati da u slaboj logici drugog reda važi jedna varijanta Skolemove teoreme.

Primer 15. Neka su $\mathcal{A}$ i $\mathcal{B}$ linearna uređenja i $\mathcal{C}$ njihov leksikografski proizvod. Postoji rečenica φ jezika $\mathcal{L}_2$, koja sadrži samo unarne relacijske promenljive, takva da $\mathcal{C} \models \varphi$ ako i samo ako $\mathcal{A} \cong \mathcal{B}$.

Otuda sledi da rečenice drugog reda koje važe u strukturi $\mathcal{C}$ nisu determinisane rečenicama koje važe u strukturama $\mathcal{A}$ i $\mathcal{B}$. Opštije, kako praktično ni jedna algebarska konstrukcija ne čuva sve formule jezika $\mathcal{L}_2$, teorija modela logike drugog reda je veoma ograničena. Delimično, ona je moguća samo na nekim fragmentima logike drugog reda, na primer, na fragmentima poput slabe logike.

Infinitarne logike

Osim logike drugog reda, koja se dobija uvođenjem relacijskih promenljivih, proširenja predikatskog računa prvog reda mogu se dobiti uopštavanjem njegovih logičkih veznika. Na primer, ako se u jeziku $\mathcal{L}$ dopuste disjunkcije i konjunkcije beskonačne dužine, dobijaju se *infinitarne logike*. Najjednostavniji slučaj infinitarne logike jeste jezik $\mathcal{L}_{\omega_1\omega}$ koji sadrži prebrojive konjunkcije i disjunkcije.

Jezik $\mathcal{L}_{\omega_1\omega}$ dobija se proširivanjem jezika $\mathcal{L}$ infinitarnim logičkim veznikom $\bigvee$, pravilima koja generišu skup formula dodaje se sledeće pravilo:

(a) Ako je Φ prebrojiv skup formula, $\bigvee \Phi$ je formula jezika $\mathcal{L}_{\omega_1\omega}$.

Nije uopšte jasno u kojoj meri se račun sa ovak definisanim formulama može smatrati logičkim sistemom. Sa skupovno-teorijskog stanovišta, definicija njegovih formula i indukcija po njihovoj složenosti pretpostavlja transfinitnu indukciju.

Definiciju zadovoljenja formula infinitarne logike, u odnosu na jezik $\mathcal{L}$, proširujemo sledećim uslovom:

(b) Ako je Φ prebrojiv skup formula jezika $\mathcal{L}_{\omega_1\omega}$, $\mathcal{A}$ model i $a \in A^\omega$ valuacija promenljivih jezika $\mathcal{L}$ u modelu $\mathcal{A}$, onda:

$$\mathcal{A} \models_a \bigvee \Phi \quad \Leftrightarrow \quad \mathcal{A} \models_a \phi, \text{ za neko } \varphi \in \Phi.$$

Skup $S(\varphi)$ potformula formule φ jezika $\mathcal{L}_{\omega_1\omega}$ definišemo indukcijom po složenosti formule φ. U odnosu na formule prvog reda, ova definicija obuhvata i uslov

$$S(\bigvee \Phi) = \{\Phi\} \cup \bigcup_{\psi\in\Phi} S(\psi).$$

Za proizvoljnu formulu φ jezika $\mathcal{L}_{\omega_1\omega}$, neka je $V(\varphi)$ skup svih slobodnih promenljivih formule φ. Ako je φ formula oblika $\bigvee \Phi$, $V(\varphi) = \bigcup_{\psi\in\Phi} V(\psi)$.

Primer 1. (a) Za svaku formulu φ jezika $\mathcal{L}_{\omega_1\omega}$, skup njenih potformula $S(\varphi)$ je najviše prebrojiv.

(b) Postoje formule jezika $\mathcal{L}_{\omega_1\omega}$ sa beskonačno mnogo slobodnih promenljivih. Ako formula ima konačno mnogo slobodnih promenljivih, svaka njena potformula takođe sadrži konačan broj slobodnih promenljivih. Ako je φ rečenica jezika $\mathcal{L}_{\omega_1\omega}$, svaka potformula formule φ ima konačan broj slobodnih promenljivih.

Primer 2. U logici $\mathcal{L}_{\omega_1\omega}$ ne važi stav kompaktnosti.

Neka je $\varphi = \bigvee\{\neg\varphi_{\geq n} : n \geq 2\}$. Rečenica φ važi u modelu $\mathcal{A}$ ako i samo ako skup A je konačan. Otuda sledi da skup rečenica

$$\{\varphi\} \cup \{\varphi_{\geq n} : n \geq 2\}$$

nema model i pritom, svaki njegov konačan podskup ima model, tj. u logici $\mathcal{L}_{\omega_1\omega}$ ne važi stav kompaktnosti.

Ako se dozvole dokazi beskonačne dužine, logika $\mathcal{L}_{\omega_1\omega}$ ima sintaksu koja je potpuna u odnosu na prethodno definisanu semantiku. Preciznije, u logici $\mathcal{L}_{\omega_1\omega}$ može se definisati pojam dokaza tako da, za svaki skup rečenica Σ i svaku rečenicu φ jezika $\mathcal{L}_{\omega_1\omega}$,

$$\Sigma \vdash \varphi \quad\Leftrightarrow\quad \Sigma \models \varphi.$$

Na prvi pogled, ova napomena protivreči prethodnom primeru, odnosno činjenici da u logici $\mathcal{L}_{\omega_1\omega}$ ne važi stav kompaktnosti. Međutim, budući da se radi o sintaksi koja dopušta dokaze beskonačne dužine, ovi rezultati nisu protivrečni. U meri u kojoj smo uopštili pojam konačnog dokaza, modelsko-teorijski rezultati logike prvog reda se mogu preneti na logiku $\mathcal{L}_{\omega_1\omega}$ tako da ona ima značajno razvijenu teoriju modela. U tom smislu, u njoj važi i jedna varijanta stava kompaktnosti o kojoj ovde nećemo govoriti.

Primer 3. Neka je φ rečenica jezika $\mathcal{L}_{\omega_1\omega}$ koji sadrži najviše prebrojiv skup nelogičkih simbola. Ako je $\mathcal{A}$ model jezika $\mathcal{L}_{\omega_1\omega}$ u kojem važi rečenica φ, onda postoji prebrojiv model $\mathcal{B} \subseteq \mathcal{A}$ takav da $\mathcal{B} \models \varphi$.

Konstrukcija modela $\mathcal{B}$ se u principu ne razlikuje od odgovarajuće konstrukcije u slučaju jezika $\mathcal{L}$. Definiše se rastući niz prebrijivih skupova $(B_n : n \in \omega)$ koji zadovoljava sledeće uslove.

(a) Skup B_0 je prebrojiv i sadrži interpretacije svih individualnih konstanti jezika $\mathcal{L}_{\omega_1\omega}$.

(b) Ako je $m \in \omega$ i F operacijski simbol jezika $\mathcal{L}_{\omega_1\omega}$ dužine $n \geq 1$, onda za sve $a_1, \ldots, a_n \in B_m$, $F^A(a_1, \ldots, a_n) \in B_{m+1}$.

(c) Za svako $m \in \omega$ i svaku formulu $\psi(x_1, \ldots, x_n, x) \in S(\varphi)$, ako su $a_1, \ldots, a_n \in B_m$ takvi da $\mathcal{A} \models \exists x\, \psi[a_1, \ldots, a_n]$, onda za neko $a \in B_{m+1}$, $\mathcal{A} \models \psi[a_1, \ldots, a_n, a]$.

Kako su skupovi $S(\varphi)$ i B_m prebrojivi, skup B_{m+1} je prebrojiv. Neka je $B = \bigcup B_n$ i $\mathcal{B}$ model jezika $\mathcal{L}_{\omega_1\omega}$ sa domenom B. Model $\mathcal{B}$ je prebrojiv, a indukcijom po složenosti potformula formule φ dokazuje se da, za svaku formulu $\psi(x_1, \ldots, x_n) \in S(\varphi)$ i proizvoljne $a_1, \cdots, a_n \in B$,

$$\mathcal{B} \models \psi[a_1, \ldots, a_n] \quad\Leftrightarrow\quad \mathcal{A} \models \psi[a_1, \ldots, a_n].$$

Na osnovu prethodnog primera sledi da u logici $\mathcal{L}_{\omega_1\omega}$ važi sledeća varijanta Skolemove teoreme:

Primer 4. Ako rečenica φ jezika $\mathcal{L}_{\omega_1\omega}$ ima model, onda φ ima i prebrojiv model.

Ovo tvrđenje je neposredna posledica činjenice da skup potformula svake formule jezika $\mathcal{L}_{\omega_1\omega}$ može biti najviše prebrojiv. Primetimo da se iz ove varijante Skolemove teoreme, neposredno dobija Skolemove teorema za predikatski račun prvog reda.

Primer 5. Bez obzira na broj nelogičkih simbola, skup svih formula jezika $\mathcal{L}_{\omega_1\omega}$ je neprebrojiv.

Primer 6. U logici $\mathcal{L}_{\omega_1\omega}$ klasa konačno generisanih grupa je aksiomatska.

Primer 7. Aritmetika u logici $\mathcal{L}_{\omega_1\omega}$ sadrži rečenice φ_1 i φ_2, koje se smo definisali u aritmetici drugog reda i aksiomu indukcije

$$\varphi = \forall x \bigvee \{x = s^n(0) : n \in \omega\}.$$

Ovako definisana aritmetika je konačno aksiomatska i kategorična. Iz ove činjenice sledi da u logici $\mathcal{L}_{\omega_1\omega}$ ne važi gornja Skolemova teorema.

Jedno od ključnih pitanja teorije modela beskonačnih logika jeste karakterizacija odnosa elementarne ekvivalencije i izomorfizma. U izvesnom smislu, logika $\mathcal{L}_{\omega_1\omega}$ je daleko od toga da se u njoj ovi pojmovi mogu identifikovati. Isto važi i za njena najprirodnija uopštenja, odnosno, za logike $\mathcal{L}_{\kappa^+\omega}$, u kojima su dozvoljene disjunkcije skupa formula kardinalnosti κ. Tek u infinitarnoj logici tipa $\mathcal{L}_{\infty\omega}$, u kojoj su dozvoljene disjunkcije proizvoljne dužine, elementarno ekvivalentni modeli su izomorfni.

Primer 8. Grupa je prosta ako ne sadrži normalnu podgrupu. U logici $\mathcal{L}_{\omega_1\omega}$, klasa prostih grupa je konačno aksiomatska.

Normalna podgrupa grupe $\mathcal{G}$ generisana elementom $a \in G$, $a \neq 1$, sastoji se od elemenata $x \in G$ oblika $x = x_0 a^{k_0} x_0^{-1} \cdots x_n a^{k_n} x_n^{-1}$, gde je $n \in \omega$, $k_0, \ldots, k_n$ celi brojevi, a $x_0, \ldots, x_n$ elementi grupe $\mathcal{G}$. U prostoj grupi, svaki element različit od neutralnog normalno generiše celu grupu, pa ako je φ_G konjunkcija aksioma grupe i

$$\varphi(x, y, v_0, \ldots, v_n) = \bigvee_{k_0,\ldots,k_n \in Z} y = v_0 x^{k_0} v_0^{-1} \cdots v_n x^{k_n} v_n^{-1})),$$

aksioma klase prostih grupa u jeziku $\mathcal{L}_{\omega_1\omega}$ je sledeća rečenica:

$$\varphi_G \;\wedge\; \forall x\, (x \neq 1 \to \forall y \bigvee_{n\in\omega} (\exists v_0, \ldots, \exists v_n\, \varphi(x, y, v_0, \ldots, v_n)))$$

Na osnovu Skolemove teoreme za logiku $\mathcal{L}_{\omega_1\omega}$, ako je $\mathcal{G}$ prosta grupa i i $M \subseteq G$ prebrojiv skup, onda postoji prebrojiva prosta podgrupa grupe $\mathcal{G}$ generisana sa skupom M.

Primer 9. Ako je $\mathcal{P}$ drvo, za svako $x \in P$, tip uređenja skupa $P_x = \{y : y < x\}$ je *visina elementa* x u drvetu $\mathcal{P}$. Najmanji ordinal veći od visine svakog elementa je *visina drveta* $\mathcal{P}$. U logici $\mathcal{L}_{\omega_1\omega}$, klasa drveta visine ω je konačno aksiomatska.

Primer 10. Za svaku rečenicu φ slabe logike, postoji rečenica ψ logike $\mathcal{L}_{\omega_1\omega}$ takva da za svaki model $\mathcal{A}$, $\mathcal{A} \models^s \varphi$ ako i samo ako $\mathcal{A} \models \psi$.

Iz ovog rezultata sledi da u slaboj logici važi Skolemova teorema. Imajući u vidu ono što smo već naglasili o logici $\mathcal{L}_{\omega_1\omega}$, u slaboj logici drugog reda se do određenog stepena može razviti teorija modela.

Primer 11. (a) Ako je $\mathcal{A}$ model jezika $\mathcal{L}$, svaka relacija, koja se u modelu $\mathcal{A}$ može definisati formulom slabe logike drugog reda, definabilna je i u logici $\mathcal{L}_{\omega_1\omega}$.

(b) Svaki skup prirodnih brojeva je definabilan u logici $\mathcal{L}_{\omega_1\omega}$.

Osim konjunkcije i disjunkcije, u logici prvog reda mogu se uopštavati i kvantifikatori. Za svaki ordinal α, jezik prvog reda $\mathcal{L}$ može se proširiti kvantifikatorom Q_α. Tako se dobija jezik $\mathcal{L}_{Q_\alpha}$, čiji se račun uobičajeno naziva *logikom uopštenih kvantifikatora*.

Skup formula jezika $\mathcal{L}_{Q_\alpha}$ generisan je pravilima koja, pored standardnih, sadrže sledeće pravilo: ako je φ formula i x promenljiva u $\mathcal{L}_{Q_\alpha}$,

(a) Izraz oblika $Q_\alpha x\, \varphi$ je formula jezika $\mathcal{L}_{Q_\alpha}$.

Interpretacija formule oblika $Q_\alpha x\, \varphi$ u modelu $\mathcal{A}$ za valuaciju $a \in A$ definisana je tako da:

$$\mathcal{A} \models_a Q_\alpha x \varphi \quad \Leftrightarrow \quad |\{b \in A : \mathcal{A} \models_{a(x/b)} \varphi\}| \geq \omega_\alpha.$$

Primer 12. Neka je $\varphi = \neg Q_0(x = x)$. Za svaki model $\mathcal{A}$ jezika $\mathcal{L}_{Q_0}$, $\mathcal{A} \models \varphi$ ako i samo ako $|A| < \omega$.

Primer 13. U logici $\mathcal{L}_{Q_0}$ ne važi stav kompaktnosti. S druge strane, u $\mathcal{L}_{Q_0}$ važi Skolemova teorema.

Primer 14. Za svaku formulu $\varphi(x_1, \ldots, x_n)$ jezika $\mathcal{L}_{Q_0}$, postoji formula $\varphi^*(x_1, \ldots, x_n)$ slabe logike takva da, za svaki model $\mathcal{A}$ i sve $a_1, \ldots, a_n \in A$,

$$\mathcal{A} \models \varphi[a_1, \ldots, a_n] \quad \Leftrightarrow \quad \mathcal{A} \models^s \varphi^*[a_1, \ldots, a_n].$$

Kvantifikator Q_1, u semantici logike $\mathcal{L}_{Q_1}$, ima značenje "postoji neprebrojivo mnogo". Zanimljivo je da ova logika ima sintaksu koja je kompletna u odnosu na njenu semantiku u sledećem smislu: za svaki prebrojiv skup formula Σ, $\Sigma \vdash \phi$ ako i samo ako $\Sigma \models \phi$.

Primer 15. Neka je $\varphi = \neg Q_1(x = x)$. Za svaki model $\mathcal{A}$ jezika $\mathcal{L}_{Q_1}$, $\mathcal{A} \models \varphi$ ako i samo ako $|A| \leq \omega$.

Primer 16. Postoji rečenica φ jezika $\mathcal{L}_{Q_1} = \{\leq\}$ takva da za svaki model $\mathcal{A}$, $\mathcal{A} \models \varphi$ ako i samo ako $\mathcal{A}$ je linearno uređenje u kojem svaki element ima najviše prebrojivo mnogo prethodnika.

U svim uopštenjima predikatskog računa prvog reda, o kojima je do sada bilo reči, narušavan je stav kompaktnosti. Pored ostalog, logika $\mathcal{L}_{Q_1}$ zanimljiva je zbog toga što u njoj, bar u prebrojivom slučaju, važi stav kompaktnosti.

Primer 17. Ako je Σ prebrojiv skup rečenica jezika logika $\mathcal{L}_{Q_1}$, onda Σ ima model ako i samo ako svaki konačan $\Sigma_0 \subseteq \Sigma$ ima model.

Ova varijanta stava kompaktnosti posledica je činjenice da logika $\mathcal{L}_{Q_1}$ ima sintaksu koja je saglasna i potpuna u odnosu na njenu semantiku. Međutim, u ovoj logici ne važi Skolemova teorema, budući da formula $Q_1 x\,(x = x)$ nema prebrojiv model.

Pregled uopštenja logike prvog reda, koji je ovde relativno površno izložen, ukazuje da u svakom takvom uopštenju ne važi ili stav kompaktnosti ili Skolemova teorema. Zanimlivo je da ovi stavovi, kao čisto modelsko-teorijska svojstva, u potpunosti karakterišu logiku prvog reda. Naime, svaki formalni sistem u kojem važi stav kompaktnosti i Skolemova teorema ekvivalentan je predikatskom računu prvog reda [1].

Neodlučivost predikatskog računa

U platonističkom shvatanju matematike, njena tvrđenja imaju objektivan sadržaj, nezavisan od uslova pod kojim taj sadržaj saznajemo. Implicitno, ovo je stanovište prisutno u uverenju da matematika podrazumeva potpun ili nepotpun opis unapred zadate strukture prirodnih brojeva. Međutim, prethodna razmatranja pokazuju da, u tom smislu, potpuna formalizacija matematike nije moguća. Preciznije, saznajna sredstva pod kojima ona jeste moguća su problematična. Ta sredstva podrazumevaju nesrazmerno jaku teoriju skupova, logiku drugog reda za koju nemamo odgovarajuću sintaksu ili infinitarne logike u kojima su dokazi sasvim problematični.

Da bismo izbegli epistemološke probleme, mogli bismo reći da pravi zadatak matematike nije da okarakteriše strukture kao takve, već da odgovori na pitanje šta se, u odgovarajućem jeziku, o njima može reći. U slučaju prirodnih brojeva, na primer, predmet naših istraživanja više neće biti odnos teorija poput PA ili Th($\mathcal{N}$) i njihovih modela, već one same po sebi.

Ideju izračunljivosti formulisali smo u prirodnim brojevima, ali nema principijelnih razloga zbog kojih o njoj ne bismo mogli govoriti u bilo kom kontekstu koji se na efektivan način može prevesti u prirodne brojeve. Na osnovu Čerčove teze, bilo koji dokaz efektivnosti određene procedure na konačnim objektima možemo smatrati dokazom njene rekurzivnosti.

U daljim razmatranjima, skup određenih objekata je rekurzivan, parcijalno nabrojiv, kreativan ili produktivan ako se može efektivno kodirati i ako skup njegovih kodova ima odgovarajuće svojstvo. Na primer, ako je zadato efektivno kodiranje $(\theta_0, \theta_1, \dots)$ svih rečenica jezika $\mathcal{L}$, skup formula Σ je prost ako i samo ako to isto važi sa skup prirodnih brojeva $\{n : \theta_n \in \Sigma\}$.

Neka je Σ teorija jezika $\mathcal{L}$. Sa $\mathrm{Cn}(\Sigma)$ označavamo skup svih njenih posledica, odnosno, deduktivno zatvorenje teorije Σ. Teorija Σ je *rekurzivno aksiomatska* ako postoji rekurzivan skup rečenica Γ takav da $\mathrm{Cn}(\Gamma) = \mathrm{Cn}(\Sigma)$.

Primer 1. Rekurzivno aksiomatska teorija je rekurzivno nabrojiva.

Neka je Γ rekurzivan skup aksioma teorije Σ. Pretpostavimo da je zadat efektivan niz svih konačnih nizova formula. Redom, za svaki konačan niz formula proveravamo da li on jeste dokaz iz pretpostavki Γ.

Kako je Γ rekurzivan skup, to se može proveriti u konačnom broju koraka. Ako to jeste slučaj, dobili smo rečenicu teorije Σ. Ako je φ rečenica teorije Σ, njen dokaz je konačan niz koji se javlja u nizu svih konačnih nizova formula. To znači da ova procedura generiše sve rečenice teorije Σ, tj. Σ je rekurzivno nabrojiv skup.

Kako je skup aksioma predikatskog računa rekurzivan, teorija $\mathrm{Cn}(\emptyset)$ je rekurzivno nabrojiva. Dakle, skup teorema jezika $\mathcal{L}$ je rekurzivno nabrojiv, a zbog stava potpunosti, takav je i skup istina predikatskog računa.

Primer 2. (a) Rekurzivno nabrojiva kompletna teorija je rekurzivna.

(b) Svaka rekurzivno aksiomatska kompletna teorija je rekurzivna.

Neka je Σ rekurzivno nabrojiva kompletna teorija i neka je efektivno zadat niz svih njenih rečenica. Kako je Σ kompletna teorija, za svaku rečenicu φ, u tom nizu se javlja ili φ ili $\neg\varphi$. Ako se javlja φ, onda $\varphi \in \Sigma$, a ako se javlja $\neg\varphi$, onda $\varphi \notin \Sigma$, pa je predikat "$\varphi \in \Sigma$" rekurzivan.

Primer 3. Ako je Γ rekurzivno nabrojiv skup rečenica i $\Sigma = \mathrm{Cn}(\Gamma)$, tada je Σ rekurzivno aksiomatska teorija.

Ako je $\Gamma = \{\varphi_0, \varphi_1, \varphi_2, \dots\}$ rekurzivno nabrojiv skup rečenica jezika $\mathcal{L}$ i $\Gamma' = \{\varphi_0, \varphi_0 \wedge \varphi_1, \varphi_0 \wedge \varphi_1 \wedge \varphi_2, \dots\}$, onda je $\Sigma = \mathrm{Cn}(\Gamma')$, a kodovi formula skupa Γ' su strogo rastući, tj. Γ' je rekurzivan skup.

Problem odlučivosti logičkih istina je veoma star. Iako nije jasno šta je to u njegovom vremenu moglo da znači, još je i Lajbnic postavio pitanje procedure za utvrđivanje "logički istinitih tvrđenja".

Teorema 13. Skup logičkih istina predikatskog računa prvog reda nije rekurzivan.

Dokaz: Za svaki program P idealnog računara definisaćemo formulu $\psi_p(x)$ jezika $\mathcal{L}$ takvu da za svako $a \in \omega$,

$$P(a)\downarrow \ \Leftrightarrow \ \models \psi_p(\mathbf{a}).$$

Pritom, za svako $a \in \omega$, $\mathbf{a}$ je term jezika $\mathcal{L}$ bez slobodnih promenljivih.

To znači da se halting problem svodi na problem odlučivosti predikatskog računa, pa dakle skup valjanih formula jezika $\mathcal{L}$ nije rekurzivan.

Neka je $P = (I_1, \dots, I_s)$ program dubine $n_p = d$ i $a \in \omega$. Da bismo u predikatskom računu opisali izračunavanje $P(a)$, nepohodan je jezik $\mathcal{L}$ koji sadrži sledeće simbole:

(a) individualnu konstantu $\mathbf{0}$, koju interpretiramo sa $0 \in \omega$,

(b) operacijsku konstantu s, koju interpretiramo kao funkciju $x + 1$,

(c) predikat $Q(x_1, \dots, x_d, x)$ dužine $d + 1$ čija interpretacija, u svakom koraku, izražava stanje izračunavanja $P(a)$.

Za svako $n \in \omega$, sa $\mathbf{n}$ označavamo numeral $s^n(\mathbf{0})$. U modelu $\mathcal{A}$ jezika $\mathcal{L}$, interpretacija predikatske konstante Q definisana je tako da za proizvoljne $r_1, \dots, r_d \in A$, i svako $k \geq 1$,

$([\mathbf{r}_1]^A, \dots, [\mathbf{r}_d]^A, [\mathbf{k}]^A) \in Q^A$ ako i samo ako "tokom izračunavanja $P(a)$ pojavljuje se stanje sa konfiguracijom $(r_1, \dots, r_d, 0, \dots)$ u kojem je sledeća instrukcija I_k".

Za svaku instrukciju I_i postoji rečenica φ_i koja izražava efekat delovanja instrukcije I_i. Na primer, u slučaju instrukcije prelaza $I_i = J(m, n, q)$, odgovarajuća rečenica je

$$\begin{aligned}\varphi_i = \forall x_1 \cdots \forall x_d \, [Q(x_1, \dots, x_d, \mathbf{i}) \to (x_m = x_n \to \\ Q(x_1, \dots, x_d, \mathbf{q})) \wedge (x_m \neq x_n \to Q(x_1, \dots, x_d, \mathbf{i} + \mathbf{1}))].\end{aligned}$$

Na sličan način, rečenicama jezika $\mathcal{L}$ opisuju se i ostale instrukcije idealnog računara. Kako u svakom modelu $\mathcal{A}$, za sve $a, b \in A$, $s^A(a) = s^A(b)$ implicira $a = b$, opis izračunavanja $P(a)$ mora da sadrži i rečenicu

$$\varphi_0 = \forall x \forall y\, ((s(x) = s(y) \to x = y) \land s(x) \neq 0).$$

Konačno, formulu $\psi_p(x)$ definišemo na sledeći način:

$$\psi_p(x) = \varphi_0 \land \cdots \land \varphi_s \land Q(x, \mathbf{0}, \ldots, \mathbf{0}, 1) \to \\ \exists x_1 \cdots \exists x_n\, Q(x_1, \ldots, x_d, \mathbf{s+1}).$$

Pritom, rečenica $Q(\mathbf{a}, \mathbf{0}, \ldots, \mathbf{0}, 1))$ odgovara početnom stanju u kojem se, za konfiguraciju $(a, 0, \ldots)$, izvršava instrukcija I_1, a završno stanje izračunavanja $P(a)$ izražava rečenica $\exists x_1 \cdots \exists x_n\, Q(x_1, \ldots, x_d, \mathbf{s+1})$ Tvrdimo da

$$P(a)\downarrow \;\Leftrightarrow\; \models \psi_p(\mathbf{a}).$$

Pretpostavimo da se izračunavanje $P(a)$ završava i neka je $\mathcal{A}$ model jezika $\mathcal{L}$ u kojem važe sve rečenice $Q(\mathbf{a}, \mathbf{0}, \ldots, \mathbf{0}, 1)$ i $\varphi_0, \ldots, \varphi_s$.

Koristeći navedene rečenice, korak po korak, rekonstruišemo sve rečenice koje opisuju izračunavanje $P(a)$. Završno stanje opisano je rečenicom $Q(\mathbf{r}_1, \ldots, \mathbf{r}_d, \mathbf{s+1})$ koja važi u strukturi $\mathcal{A}$, pa dakle u strukturi $\mathcal{A}$ važi rečenica $\exists x_1 \cdots \exists x_n\, Q(x_1, \ldots, x_d, \mathbf{s+1})$, odnosno, $\mathcal{A} \models \psi_p(\mathbf{a})$.

Obrnuto, ako $\models \psi_p(\mathbf{a})$, onda $\psi_p(\mathbf{a})$ važi u strukturi $\mathcal{N}$ u kojoj je predikat Q interpretiran relacijom: za sve $k, r_1, \ldots, r_d \in \omega$,

$R(r_1, \ldots, r_d, k)$ ako i samo ako u nekom stanju izračunavanja $P(a)$, za konfiguraciju $(r_1, \ldots, r_d)$, sledeća instrukcija je I_k.

Kako rečenice $\varphi_0, \ldots, \varphi_s$ i $Q(\mathbf{a}, \mathbf{0}, \ldots, \mathbf{0}, 1)$ važe u strukturi $\mathcal{N}$, rečenica $\exists x_1 \cdots \exists x_n\, Q(x_1, \ldots, x_d, \mathbf{s+1})$ takođe važi u $\mathcal{N}$, a to znači da se izračunavanje $P(a)$ završava. $\Box$

Za neodlučivost predikatskog računa dovoljna je pretpostavka da jezik $\mathcal{L}$ sadrži simbole koje smo koristili u prethodnom dokazu. Međutim, isti rezultat može se dobiti ako se pretpostavi da jezik $\mathcal{L}$ sadrži bar jedan binarni relacijski simbol. Kako smo ranije dokazali, predikatski račun unarnih predikatskih simbola, kao i račun jednakosti su odlučivi računi. Ako eksplicitno ne navedemo jezik o kojem se radi, uvek pretpostavljamo jezik $\mathcal{L}$ u kojem skup valjanih rečenica nije rekurzivan.

Značajno je primetiti da, za svaki program P i svako $a \in \omega$, ako $P(a)\downarrow$, rečenica $\psi_p(\mathbf{a})$ ima konačan model $\mathcal{A}_p$. To sledi iz činjenice da se tokom izračunavanja $P(a)$, u bilo kom vidu, javlja samo konačno mnogo prirodnih brojeva.

Rečenica φ jezika $\mathcal{L}$ je *zadovoljiva* ako postoji model u kojem važi φ, a *konačno zadovoljiva* ako ima konačan model. Neka je Σ_{sat} skup svih zadovoljivih rečenica, Σ_{fin} skup svih konačno zadovoljivih rečenica i Σ_{val} skup svih konačno valjanih rečenica, tj. skup svih rečenica koje važe u svim konačnim modelima jezika $\mathcal{L}$.

Primer 4. Skup Σ_{sat} nije rekurzivno nabrojiv.

Primer 5. Ako jezik $\mathcal{L}$ sadrži operacijski simbol f i

$$\varphi = \forall x \forall y\,(f(x) = f(y) \to x = y) \to \forall x \exists y\,(f(y) = x),$$

onda $\varphi \in \Sigma_{\text{val}}$, $\neg\varphi \notin \Sigma_{\text{fin}}$ i rečenica φ nije valjana.

Skup logičkih istina jezika $\mathcal{L}_2$ drugog reda nije parcijalno rekurzivan, odnosno, logika drugog reda nema rekurzivnu aksiomatizaciju. Da bismo to dokazali, neophodna je jedna sasvim jednostavna redefinicija idealnog računara. Ona će obezbediti informaciju o broju izvršenih koraka u toku svakog izračunavanja.

Primer 6. Skup Σ_{fin} je rekurzivno nabrojiv i nije rekurzivan.

Neka je φ rečenica jezika $\mathcal{L}$. Kako je jezik rečenice φ konačan i broj neizomorfnih struktura kardinalnosti $n \geq 1$ je konačan, pa se u konačno mnogo koraka proverava da li rečenica φ važi u svim takvim strukturama.

Neka je $(\varphi_0, \varphi_1, \dots)$ efektivno kodiranje rečenica jezika $\mathcal{L}$. Za svaki prirodan broj $n \in \omega$, u svim strukturama sa domenom kardinalnosti $\leq n$, proverimo sve rečenice φ_k, $k \leq n$. Tako se proverava konačna zadovoljivost svih rečenica, što znači da je Σ_{fin} rekurzivno nabrojiv skup.

Da bismo dokazali da skup Σ_{fin} nije rekurzivan, redefinisaćemo idealni računar. Pretpostavićemo da novi idealni računar sadrži nulti registar i instrukcije I_k^* koje izvršavaju isto što i instrukcije I_k i istovremeno uvećavaju sadržaj nultog registra za jedan. Na taj način, svakom programu P idealnog računara odgovara program P^* novog idealnog računara. Očigledno, za svako $\vec{x} \in \omega^n$, $P(\vec{x})\downarrow$ ako i samo ako $P^*(\vec{x})\downarrow$.

Kao u dokazu neodlučivosti predikatskog računa, za svaki program P^* postoji formula $\varphi_p(x)$ jezika $\mathcal{L}$ takva da za svako $a \in \omega$,

$$P^*(a)\downarrow \;\Leftrightarrow\; \models \varphi_p(\mathbf{a}).$$

Za svaki program P^* i svako $a \in \omega$, ako $P^*(a)\downarrow$, onda $\varphi_p(\mathbf{a})$ ima konačan model. Obrnuto, ako $P^*(a)\uparrow$, onda svaki model $\mathcal{A}$, u kojem važi rečenica φ_p^a, sadrži beskonačan niz $(0^A, 1^A, \dots)$ koji generiše brojač izmenjenog idealnog računara.

Dakle, $P^*(a)\downarrow$ ako i samo ako $\varphi_p(\mathbf{a}) \in \Sigma_{\text{fin}}$, pa se halting problem svodi na problem $\varphi \in \Sigma_{\text{fin}}$, tj. skup Σ_{fin} nije rekurzivan.

Primer 7. Skup Σ_{val} nije rekurzivno nabrojiv.

Ovo tvrđenje je posledica prethodnog primera i činjenice da za svaku rečenicu φ jezika $\mathcal{L}$, $\varphi \notin \Sigma_{\text{fin}}$ ako i samo ako $\neg\varphi \in \Sigma_{\text{val}}$.

Teorema 14. Skup svih logičkih istina logike drugog reda nije rekurzivno nabrojiv.

Dokaz: Ako je φ_{fin} rečenica jezika $\mathcal{L}_2$ koja karakteriše konačne modele, onda za svaku rečenicu φ jezika $\mathcal{L} \subseteq \mathcal{L}_2$,

$$\varphi \in \Sigma_{\text{val}} \quad \Leftrightarrow \quad \models \varphi_{\text{fin}} \rightarrow \varphi.$$

Ako bi skup valjanih formula jezika $\mathcal{L}_2$ bio rekurzivno nabrojiv, to bi važilo i za skup Σ_{val} što, na osnovu prethodnog primera, nije moguće. $\Box$

U ranijim razmatranjima, na osnovu činjenice da u logici drugog reda ne važi stav kompaktnosti, zaključili smo da u njoj nije moguće definisati pojam dokaza iz hipoteza, odnosno sintaksu koja bi zadovoljavala uslov: $\Sigma \vdash \varphi$ ako i samo ako $\Sigma \models \varphi$, za svaki skup rečenica Σ i svaku rečenicu φ jezika $\mathcal{L}_2$. Prethodna teorema pokazuje da logika drugog reda nije potpuna ni u slabom smislu, odnosno, da u njoj ne postoji pojam dokaza koji zadovoljava uslov: za svaku rečenicu φ jezika $\mathcal{L}_2$, $\vdash \varphi$ ako i samo ako $\models \varphi$.

Primer 8. Skup valjanih rečenica logike drugog reda nije rekurzivno nabrojiv ni u slučaju jezika $\mathcal{L}_2$ koji uopšte ne sadrži nelogičke simbole.

Naime, nelogički simboli jezika $\mathcal{L} \subseteq \mathcal{L}_2$, koji obezbeđuju njegovu neodlučivost, mogu se definisati formulama jezika $\mathcal{L}_2 = \emptyset$.

Nepotpunost aritmetike

Kompletna aritmetika $\text{Th}(\mathcal{N})$ nije odlučiva, odnosno, skup svih rečenica jezika $\mathcal{L}_{\text{PA}}$ koje važe u modelu $\mathcal{N}$, nije rekurzivan. Ovu činjenicu dokazaćemo slično kao i neodlučivost predikatskog računa, tj. proceduru izračunavanja na idealnom računaru izrazićemo formulom jezika $\mathcal{L}_{\text{PA}}$.

Teorema 15. Kompletna aritmetika nije rekurzivna.

Dokaz: Za svaki program P definisaćemo formulu $\varphi_p(x)$ u jeziku $\mathcal{L}_{\text{PA}}$ tako da, za svako $a \in \omega$,

$$P(a)\downarrow \quad \Leftrightarrow \quad \mathcal{N} \models \varphi_p(\mathbf{a}).$$

Na taj način, halting problem sada svodimo na problem odlučivosti kompletne aritmetike.

Neka je $P = (I_1, \ldots, I_s)$ program dubine d. Intuitivno, treba odrediti formulu $\psi_p(\vec{x}, y, \vec{z})$ jezika $\mathcal{L}_{\mathrm{PA}}$, sa $2d+1$ slobodnih promenljivih, takvu da za svako $k \in \omega$ i sve $a_1, \ldots, a_d; b_1, \ldots, n_d \in \omega$,

$\mathcal{N} \models \psi_p[a_1, \ldots, a_d, k, b_1, \ldots, n_d]$ ako i samo ako

"posle konačno mnogo koraka izračunavanja $P(a_1, \ldots, a_d)$ pojavljuje se konfiguracija $(b_1, \ldots, b_d)$ i sledeća instrukcija je I_k", odnosno,

"postoji $m \in \omega$ i postoji niz $(k_1, \vec{x}_0, k_2, \vec{x}_2, \ldots, k_m, \vec{x}_m)$ takav da $k_1 = 1$, $\vec{x}_0 = (a_1, \ldots a_d)$ i za sve $i < m$, instrukcija I_{k_i} prevodi $\vec{x}_i$ u $\vec{x}_{i+1}$, a sledeća instrukcija je $I_{k_{i+1}}$, $k_m = k$, $\vec{x}_m = (b_1, \ldots b_d)$ i sledeća instrukcija je I_k".

Ako konstruišemo formulu ψ_p sa navedenim svojstvom, onda je

$$\varphi_p(x) = \exists y_1 \cdots \exists y_d \, \psi_p(x, \mathbf{0}, \ldots, \mathbf{0}, \mathbf{s+1}, y_1, \ldots, y_d).$$

Jedina principijelna teškoća u definisanju formule ψ_p sastoji se u tome što se u njoj javlja kvantifikacija preko konačnog niza. Za takvu kvantifikaciju neophodna je definicija primitivno rekurzivne funkcije $(y)_x$ u jeziku $\mathcal{L}_{\mathrm{PA}}$. Rešenje ovog problema zasniva se na takozvanoj *kineskoj teoremi o ostacima*:

Lema : Neka su $b_0, \ldots, b_n$ pozitivni prirodni brojevi, čiji su parovi uzajamno prosti i $a_0, \ldots, a_n \in \omega$ takvi da za svako $i \leq n$, $a_i < b_i$. Tada postoji $x < b_0 \cdots b_n$ takvo da za sve $i \leq n$, $\mathrm{rm}(x, b_i) = a_i$.

Dokaz : Pretpostavimo da su $b_0, \ldots, b_n$ pozitivni prirodni brojevi i neka je $b = b_0 \cdots b_n$. Različitih nizova oblika $(a_0, \ldots, a_n)$ takvih da za sve $i \leq n$, $a_i < b_i$ ima tačno b. Isto toliko ima i brojeva $x < b$ i svaki takav x određuje niz $(\mathrm{rm}(x, b_0), \ldots, \mathrm{rm}(x, b_n))$. Takođe, različiti brojevi x i x' određuju različite nizove. U suprotnom, ako $0 \leq x < x' < b$ i ako za sve $i \leq n$, $\mathrm{rm}(x, b_i) = \mathrm{rm}(x', b_i)$, kako su parovi brojeva $b_0, \ldots, b_n$ uzajamno prosti, $x' - x$ mora biti deljivo sa b, što nije moguće. $\square$

Vratimo se dokazu teoreme. U definiciji kvantifikacije po konačnim nizovima koristimo funkciju u

$$\beta(x, y, z) = \mathrm{rm}(x, y \cdot (z+1) + 1).$$

Tvrdimo da za svaki niz $(a_0, \ldots, a_n)$, postoje prirodni brojevi $x, y \in \omega$ takvi da za sve $z \leq n$, $\beta(x, y, z) = a_z$.

Za svaki niz $(a_0, \ldots, a_n)$, neka je $y = n! \cdot \max\{a_0 + 1, \ldots, a_n + 1\}$. Za svako $z \leq n$, brojevi $b_z = y \cdot (z+1) + 1$ su uzajamno prosti, pa prema kineskoj teoremi o ostacima, postoji x takvo da je $\mathrm{rm}(x, y \cdot (z+1) + 1) = a_z$.

Ako je $\varphi_{\mathrm{rm}}(x, y, z) = (z < y) \wedge \exists u \, (x = u \cdot y + z) \vee (y = 0 \wedge z = x)$, onda za proizvoljne prirodne brojeve $k, m, n \in \omega$,

$$\mathrm{rm}(k,m) = n \quad \Leftrightarrow \quad \mathcal{N} \models \varphi_{\mathrm{rm}}[k,m,n].$$

Otuda neposredno sledi da postoji formula $\varphi_\beta(x,y,z,u)$ jezika $\mathcal{L}_{\mathrm{PA}}$ takva da za proizvoljne $m,n,p,q \in \omega$,

$$\beta(m,n,p) = q \quad \Leftrightarrow \quad \mathcal{N} \models \varphi_\beta[m,n,p,q].$$

Kako se kodirajuće funkcije $\langle x,y\rangle$, π_1 i π_2 mogu jednostavno formulisati u jeziku $\mathcal{L}_{\mathrm{PA}}$, za proizvoljne $k,m,n \in \omega$,

$$(k)_m = n \quad \Leftrightarrow \quad \mathcal{N} \models \varphi_\beta[\pi_1(k), \pi_2(k), m, n].$$

Otuda sledi da za sve $x, x_0, \ldots, x_n \in \omega$, "prirodan broj x je kod niza $(x_1,\ldots,x_n)$" ako i samo ako za sve $i \leq n$,

$$\mathcal{N} \models \varphi_\beta[\pi_1(x), \pi_2(x), i, x_i].$$

Dakle, kvantifikacija po konačnim nizovima može se izraziti u jeziku $\mathcal{L}_{\mathrm{PA}}$. Kako se prelaz stanja izračunavanja $(k_i, \vec{x}_i)$ u stanje $(k_{i+1}, \vec{x}_{i+1})$, $i \leq m$, jednostavno opisuje u $\mathcal{L}_{\mathrm{PA}}$, po definiciji formule ψ_p, ona zaista jeste formula jezika $\mathcal{L}_{\mathrm{PA}}$. Tehnički detalji u ovom opisu uopšte nisu teški, a izostavljeni su samo zbog njihove preterane dužine. □

Primer 1. (a) Za svaku rekurzivnu relaciju $R(\vec{x})$, $\vec{x} \in \omega^n$, postoji formula $\varphi_r(x_1,\ldots,x_n)$ jezika $\mathcal{L}_{\mathrm{PA}}$ takva da za sve $a_1,\ldots,a_n \in \omega$,

$$R(a_1,\ldots,a_n) \quad \Leftrightarrow \quad \varphi_r(\mathbf{a}_1,\ldots,\mathbf{a}_n) \in \mathrm{Th}(\mathcal{N}).$$

(b) Za proizvoljnu rekurzivnu funkciju $f(\vec{x})$, $\vec{x} \in \omega^n$, postoji formula $\varphi_f(x,x_1,\ldots,x_n)$ jezika $\mathcal{L}_{\mathrm{PA}}$ takva da za sve $a,a_1,\ldots,a_n \in \omega$,

$$f(a_1,\ldots,a_n) = a \quad \Leftrightarrow \quad \varphi_f(\mathbf{a},\mathbf{a}_1,\ldots,\mathbf{a}_n) \in \mathrm{Th}(\mathcal{N})$$

i pritom, $\exists^* x\, \varphi_f(x,\mathbf{a}_1,\ldots,\mathbf{a}_n) \in \mathrm{Th}(\mathcal{N})$.

Ovo tvrđenje neposredno sledi iz dokaza prethodne teoreme. Ono zapravo pokazuje da su sve rekurzivne relacije i sve rekurzivne funkcije predstavljive u teoriji $\mathrm{Th}(\mathcal{N})$.

Primer 2. Teorija $\mathrm{Th}(\mathcal{N})$ je produktivna.

Zapravo, tvrdi se da je skup kodova teorije $\mathrm{Th}(\mathcal{N})$ produktivan. Da to dokažemo, koristićemo predstavljivost rekurzivnih relacija u teoriji $\mathrm{Th}(\mathcal{N})$. Kako je skup K rekurzivno nabrojiv, postoji rekurzivan predikat $R(x,y)$ takav da za svako $x \in \omega$,

$$x \in K \quad \Leftrightarrow \quad \exists y\, R(x,y).$$

Neka je $\varphi_r(x, y)$ formula jezika $\mathcal{L}_{\mathrm{PA}}$ koja predstavlja rekurzivnu relaciju R u teoriji $\mathrm{Th}(\mathcal{N})$. Ako je $\varphi_k(x) = \exists y\, \varphi_r(x, y)$, onda za svako $n \in \omega$,

$$\begin{array}{lcl} n \in K & \Leftrightarrow & \varphi_k(\mathbf{n}) \in \mathrm{Th}(\mathcal{N}) \text{ i} \\ n \notin K & \Leftrightarrow & \neg\varphi_k(\mathbf{n}) \in \mathrm{Th}(\mathcal{N}). \end{array}$$

Za svako $n \in \omega$ neka je $g(n)$ kod formule $\neg\varphi_k(\mathbf{n})$ i neka je T skup svih kodova teorije $\mathrm{Th}(\mathcal{N})$. Funkcija $g(n)$ je totalna, obostrano jednoznačna rekurzivna funkcija i pritom, za sve $n \in \omega$,

$$\begin{array}{lcl} x \in K^c & \Leftrightarrow & \neg\varphi_k(\mathbf{n}) \in \mathrm{Th}(\mathcal{N}) \\ & \Leftrightarrow & g(n) \in T. \end{array}$$

Dakle, skup K^c je 1-svodljiv na skup T, pa kako je K^c produktivan skup, kompletna aritmetika $\mathrm{Th}(\mathcal{N})$ je produktivna.

Elemente aritmetičke hijerarhije $\bigcup_{n\in\omega} \Sigma_n$ nazivali smo aritmetički relacijama, odnosno, aritmetičkim skupovima. Sledeći primer pokazuje da je takva terminologija sasvim opravdana.

Primer 3. Relacija R je aritmetička, ako i samo ako R je predstavljiva u kompletnoj aritmeticiteoriji $\mathrm{Th}(\mathcal{N})$.

Kasnije ćemo videti da sam skup kodova $T \subseteq \omega$ teorije $\mathrm{Th}(\mathcal{N})$ nije aritmetički skup. To znači da je problem "$\varphi \in \mathrm{Th}(\mathcal{N})$" veoma težak.

Predstavljivost relacija i operacija prirodnih brojeva, o kojoj smo do sada govorili samo u smislu teorije $\mathrm{Th}(\mathcal{N})$, može se definisati u odnosu na proizvoljnu teoriju jezika $\mathcal{L}_{\mathrm{PA}}$.

Relacija $R(\vec{x})$, $\vec{x} \in \omega^n$, je *predstavljiva* u teoriji Σ jezika $\mathcal{L}_{\mathrm{PA}}$ ako postoji formula $\varphi_r(x_1, \ldots, x_n)$ takva da za sve $a_1, \ldots, a_n \in \omega$,

$$\begin{array}{rcl} R(a_1, \ldots, a_n) & \Rightarrow & \Sigma \vdash \varphi_r(\mathbf{a}_1, \ldots, \mathbf{a}_n), \\ \neg R(a_1, \ldots, a_n) & \Rightarrow & \Sigma \vdash \neg\varphi_r(\mathbf{a}_1, \ldots, \mathbf{a}_n). \end{array}$$

Funkcija $f(\vec{x})$, $\vec{x} \in \omega^n$, je *predstavljiva* u teoriji Σ jezika $\mathcal{L}_{\mathrm{PA}}$ ako je $\mathrm{graf}(f)$ predstavljiva relacija u teoriji Σ.

Primer 4. (a) Neka su Σ i Σ' teorije u jeziku $\mathcal{L}_{\mathrm{PA}}$. Ako $\Sigma \subseteq \Sigma'$, sve relacije predstavljive u Σ predstavljive su u Σ'. Ako je Σ rekurzivna neprotivrečna teorija, sve relacije predstavljive u Σ su rekurzivne.

(b) Sve rekurzivne relacije su predstavljive u PA. Ako je $R \in \omega^n$ parcijalno rekurzivna relacija, onda postoji formula $\varphi_r(x_1, \ldots, x_n)$ jezika $\mathcal{L}_{\mathrm{PA}}$ takva da za sve $a_1, \ldots, a_n \in \omega$,

$$R(a_1, \ldots, a_n) \;\Rightarrow\; \mathrm{PA} \vdash \varphi_r(\mathbf{a}_1, \ldots, \mathbf{a}_n).$$

Relacija koja zadovoljava ovaj uslov je *slabo predstavljiva* u teoriji PA.

Sve relacije i funkcije, koje se javljaju u opisu procedure izračunavanja na idealnom računaru, su predstavljive u PA. Pažljivijom analizom definicije funkcije $\beta(x, y, z)$, lako je uveriti se da su sva njena svojstva koja smo koristili u opisu procedure izračunavanja dokaziva u teoriji PA. Pritom, u takvom dokazu ne koristi se shema indukcije.

Teoriju PA bez sheme indukcije označavaćemo sa QA. Teorija QA je konačno aksiomatska i u njoj su predstavljive sve rekurzivne relacije. Više od toga, u teoriji QA su slabo predstavljive sve Σ_1 relacije. Kasnije ćemo videti da ne postoji rekurzivno neprotivrečno proširenje teorije QA u kome su slabo predstavljive sve Π_1 relacije.

Primer 5. Pomoću funkcije $\beta(x, y, z)$ može se u jeziku $\mathcal{L}_{\mathrm{PA}}$ izraziti primitivna rekurzija.

Ako je funkcija $f(\vec{x}, y)$ dobijena rekurzijom iz $g(\vec{x})$ i $h(\vec{x}, y, z)$, $\vec{x} \in \omega^n$, onda

$$\begin{aligned} f(\vec{x}, y) = z \quad \Leftrightarrow \quad & \exists u \exists v \, (\beta(u, v, 0) = g(\vec{x}) \wedge \\ & \forall t < y \, \beta(u, v, t+1) = h(\vec{x}, t, \beta(u, v, t)) \\ & \wedge \, \beta(u, v, y) = z). \end{aligned}$$

Relacija $R(\vec{x})$, $\vec{x} \in \omega^n$, je *elementarna* ako postoji polinom $p(\vec{x})$ takav da za sve $x_1, \ldots, x_n \in \omega$, važi $R(x_1, \ldots, x_n) \quad \Leftrightarrow \quad p(x_1, \ldots, x_n) = 0$.

Relacija $R(\vec{x})$ je *diofantovska* ako se može dobiti egzistencijalnom kvantifikacijom elementarne relacije.

Primer 6. Deseti Hilbertov problem: Aritmetička relacija R je diofantovska ako i samo ako R je Σ_1 relacija.

Primetimo da je funkcija $\beta(x, y, z)$ definisana diofantovskim formulama teorije PA. Takođe, u prethodnom primeru dokazali smo da se rekurzija može opisati funkcijom $\beta(x, y, z)$. Na osnovu Klinijeve teoreme o efektivnoj numeraciji, svaki Σ_1 predikat može se dobiti egzistencijalnom kvantifikacijom Klinijevog predikata, odnosno, primitivno rekurzivnog predikata. Dakle, na osnovu definicije rekurzije pomoću funkcije β, za dokaz prethodnog tvrđenja dovoljno je pokazati da je klasa diofantovskih relacija zatvorena za ograničenu univerzalnu kvantifikaciju.

Odgovor na ovo pitanje zapravo predstavlja rešenje desetog Hilbertovog problema. Nije svaka diofantovska jednačina algoritamski rešiva. Korak koji nam u tome nedostaje je samo tehnički komplikovan, pa ga iz tih razloga izostavljamo [5].

Predstavljivost rekurzivnih relacija i funkcija u nekoj teoriji omogućava izučavanje osobina takve teorije njenim sopstvenim sredstvima. Na primer, ako je zadato efektivno kodiranje simbola jezika $\mathcal{L}_{\mathrm{PA}}$, predikati "$x$ je kod terma jezika $\mathcal{L}_{\mathrm{PA}}$" ili "$x$ je kod formule jezika $\mathcal{L}_{\mathrm{PA}}$" su rekurzivni, pa u jeziku $\mathcal{L}_{\mathrm{PA}}$ postoje formule $\mathrm{Term}(x)$, odnosno, $\mathrm{For}(x)$ kojima su ti predikati predstavljeni. Nas će pre svega zanimati do kog stepena Peanova aritmetika, zatim teorija ZF i njima bliske teorije, mogu da govore same o sebi.

Ubuduće, pretpostavljamo da je zadato efektivno kodiranje svih konačnih nizova simbola jezika $\mathcal{L}_{\mathrm{PA}}$. Kod formule φ označavamo sa $\ulcorner\varphi\urcorner$. Kada se kod formule javlja u nekoj formuli, na primer u formuli $\psi(\ulcorner\varphi\urcorner)$ ili $\varphi(\ulcorner\varphi\urcorner)$, podrazumevamo da se radi o numeralu koji odgovara kodu $\ulcorner\varphi\urcorner$.

Ako je zadat kod $\ulcorner\varphi\urcorner$ formule $\varphi(x)$ sa jednom slobodnom promenljivom i $n \in \omega$, na efektivan način može se odrediti kod $\ulcorner\varphi(\mathbf{n})\urcorner$ rečenice koja se dobija supstitucijom numerala $\mathbf{n}$, odnosno terma $s^n(\mathbf{0})$ u formuli $\varphi(x)$. Takva supstitucija izražava se funkcijom

$$\mathrm{sub}(m,n) = \begin{cases} \ulcorner\varphi(\mathbf{n})\urcorner & \text{ako za neku formulu } \varphi,\ m = \ulcorner\varphi(x)\urcorner \\ 0 & \text{inače.} \end{cases}$$

Funkcija $\mathrm{sub}(x,y)$ je rekurzivna, pa postoji formula jezika $\mathcal{L}_{\mathrm{PA}}$, označavamo je sa $\mathrm{sub}(x,y) = z$, koja u teoriji PA reprezentuje funkciju $\mathrm{sub}(x,y)$.

Po definiciji funkcije $\mathrm{sub}(x,y)$, za svaku formulu $\varphi(x)$ jezika $\mathcal{L}_{\mathrm{PA}}$ i svaki prirodan broj $n \in \omega$, $\mathrm{PA} \vdash \mathrm{sub}(\ulcorner\varphi(x)\urcorner, \mathbf{n}) = \ulcorner\varphi(\mathbf{n})\urcorner$.

Funkciju $d(x) = \mathrm{sub}(x,x)$ nazivaćemo *dijagonalnom funkcijom*. Funkcija $d(x)$ je rekurzivna i za svaku formulu φ jezika $\mathcal{L}_{\mathrm{PA}}$, sa jednom slobodnom promenljivom, $d(\ulcorner\varphi\urcorner) = \ulcorner\varphi(\ulcorner\varphi\urcorner)\urcorner$.

Za svaku formulu $\psi(x)$ jezika $\mathcal{L}_{\mathrm{PA}}$, formulu $\psi(d(x))$ nazivačemo *dijagonalizacijom formule* $\psi(x)$. U suštini, dijagonalizacija formule $\psi(x)$ može se definisati u svakoj teoriji Σ jezika $\mathcal{L}_{\mathrm{PA}}$ u kojoj su predstavljive sve rekurzivne relacije.

Primer 7. Skup T kodova teorije $\mathrm{Th}(\mathcal{N})$ nije aritmetički.

Pretpostavimo suprotno, tj. neka je "$x \in T$" aritmetička relacija. Aritmetičke relacije su zatvorene za logičke operacije, pa kako je $d(x)$ rekurzivna funkcija, relacija $d(x) \in T^c$ je aritmetička.

Neka je $\varphi(x)$ formula koja predstavlja relaciju $d(x) \in T^c$ u teoriji $\mathrm{Th}(\mathcal{N})$. To znači da za svako $n \in \omega$, $\varphi(\mathbf{n}) \in \mathrm{Th}(\mathcal{N})$ ako i samo ako $d(x) \in T^c$.

Specijalno, $\varphi(\ulcorner\varphi\urcorner) \in \mathrm{Th}(\mathcal{N})$ ako i samo ako $d(\ulcorner\varphi\urcorner) \in T^c$. Međutim, po definiciji predstavljivosti, $d(\ulcorner\varphi\urcorner) \in T^c$ ako i samo ako $\varphi(\ulcorner\varphi\urcorner) \notin \mathrm{Th}(\mathcal{N})$, što nije moguće.

Za svaku formulu ψ jezika $\mathcal{L}_{\mathrm{PA}}$, relacija $\psi \in \mathrm{Th}(\mathcal{N})$ može se shvatiti kao relacija "ψ je istina prirodnih brojeva". U posebnom slučaju, smisao relacije $\varphi(\ulcorner\varphi\urcorner) \notin \mathrm{Th}(\mathcal{N})$ bio bi "$\varphi(\ulcorner\varphi\urcorner)$ je laž", što bi značilo da rečenica $\varphi(\ulcorner\varphi\urcorner)$

tvrdi nešto poput "ja lažem". Opštije, u svakoj teoriji jezika $\mathcal{L}_{\mathrm{PA}}$ u kojoj su predstavljive rekurzivne relacije, za svaku formulu $\psi(x)$, postoji rečenica φ čiji je smisao "ja imam svojstvo ψ".

Teorema 16. Ako je Σ teorija u jeziku $\mathcal{L}_{\mathrm{PA}}$ u kojoj su predstavljive sve rekurzivne relacije, onda za svaku formulu $\psi(x)$ postoji rečenica φ takva da važi $\Sigma \vdash \varphi \leftrightarrow \psi(\ulcorner\varphi\urcorner)$.

Dokaz: Neka je $\psi(x)$ formula jezika $\mathcal{L}_{\mathrm{PA}}$. Kako su rekurzivne relacije predstavljive u teoriji Σ, formula $\psi(x)$ ima dijagonalizaciju $\theta(x) = \psi(d(x))$. Ako je $\varphi = \theta(\ulcorner\theta(x)\urcorner)$, onda rečenica φ zadovoljava uslov teoreme.

Naime, po definiciji formule $\theta(x)$, $\Sigma \vdash \varphi \leftrightarrow \psi(d(\ulcorner\theta(x)\urcorner))$, pa prema definiciji dijagonalizacije $d(x)$, $\Sigma \vdash \varphi \leftrightarrow \psi(\ulcorner\theta(\ulcorner\theta(x)\urcorner)\urcorner)$, odnosno, prema definiciji rečenice φ, $\Sigma \vdash \varphi \leftrightarrow \psi(\ulcorner\varphi\urcorner)$. $\square$

Primer 8. Neka je Σ neprotivrečna teorija jezika $\mathcal{L}_{\mathrm{PA}}$ u kojoj su predstavljive sve rekurzivne relacije. Ako je skup $\mathrm{Cn}(\Sigma)$ predstavljiv u teoriji Σ, onda Σ nije kompletna teorija.

Neka je $\psi(x)$ formula jezika $\mathcal{L}$ koja reprezentuje $\mathrm{Cn}(\Sigma)$ u teoriji Σ. Prema prethodnoj teoremi, postoji rečenica φ takva da $\Sigma \vdash \varphi \leftrightarrow \neg\psi(\ulcorner\varphi\urcorner)$. Otuda, ako $\Sigma \vdash \varphi$, onda $\varphi \notin \mathrm{Cn}(\Sigma)$, pa dakle nije $\Sigma \vdash \varphi$. Slično, nije da $\Sigma \vdash \neg\varphi$, tj. teorija Σ nije kompletna.

Primer 9. Svaka neprotivrečna rekurzivna teorija u kojoj su predstavljive sve rekurzivne relacije nije kompletna.

Peanova aritmetika je rekurzivna teorija u kojoj su predstavljive sve rekurzivne relacije, pa postoji rečenica φ jezika $\mathcal{L}_{\mathrm{PA}}$ koja važi u strukturi $\mathcal{N}$ i nije dokaziva u PA. Međutim, sa neformalnog stanovišta, Peanova aritmetika ima veliku izražajnu moć. Skoro sva poznata tvrđenja o prirodnim brojevima se mogu formulisati u jeziku $\mathcal{L}_{\mathrm{PA}}$ i dokazati u teoriji PA. Konkretan primer rečenice φ koja važi u strukturi $\mathcal{N}$ i nije dokaziva u Peanovoj aritmetici konstruisan je koristeći argument iz dokaza prethodne teoreme.

Neka je Σ rekurzivna teorija koja sadrži PA i neka je $R(x,y)$ relacija definisana tako da za sve $x, y \in \omega$,

$$R(x,y) \quad \Leftrightarrow \quad \begin{array}{l}\text{"}y \text{ je kod dokaza u teoriji } \Sigma \text{ za}\\ \text{formulu čiji je kod } x\text{".}\end{array}$$

Zbog efektivnosti kodiranja, relacija $R(x,y)$ je rekurzivna pa postoji formula $\mathrm{Prov}_\Sigma(x,y)$ jezika $\mathcal{L}_{\mathrm{PA}}$ koja u teoriji Σ predstavlja relaciju $R(x,y)$. U teoriji Σ sada možemo definisati predikat $\mathrm{Pr}_\Sigma(x) = \exists y\, \mathrm{Prov}_\Sigma(x,y)$. Ako je φ rečenica jezika $\mathcal{L}_{\mathrm{PA}}$, smisao rečenice $\mathrm{Pr}_\Sigma(\ulcorner\varphi\urcorner)$ je "$\Sigma \vdash \varphi$". Kada je iz konteksta jasno o kojoj teoriji se radi, formulu $\mathrm{Pr}_\Sigma(x)$ označavamo sa $\mathrm{Pr}(x)$.

Primer 10. Neka je Σ rekurzivna teorija koja sadrži PA i φ, ψ rečenice jezika $\mathcal{L}_{\mathrm{PA}}$. Predikat $\mathrm{Pr}(x)$ zadovoljava sledeće uslove:

(a) $\Sigma \vdash \varphi$ implicira $\Sigma \vdash \mathrm{Pr}(\ulcorner\varphi\urcorner)$
(b) $\Sigma \vdash \mathrm{Pr}(\ulcorner\varphi\urcorner) \to \mathrm{Pr}(\ulcorner\mathrm{Pr}(\ulcorner\varphi\urcorner)\urcorner)$
(c) $\Sigma \vdash \mathrm{Pr}(\ulcorner\varphi \to \psi\urcorner) \to (\mathrm{Pr}(\ulcorner\varphi\urcorner) \to \mathrm{Pr}(\ulcorner\psi\urcorner))$

Da važi tvrđenje (a) sledi iz činjenice da je skup $Pr = \{\varphi : \Sigma \vdash \varphi\}$ parcijalno rekurzivan. U svakoj teoriji koja sadrži QA, takvi skupovi su slabo predstavljivi, pa ako $\Sigma \vdash \varphi$, onda važi relacija $\mathrm{Pr}(\ulcorner\varphi\urcorner) \in Pr$, pa dakle $\Sigma \vdash \mathrm{Pr}(\ulcorner\varphi\urcorner)$.

Tvrđenje (b) se dokazuje tako što u teoriji Σ formalizujemo dokaz za (a), odnosno, skup $\{\varphi : \ulcorner\varphi\urcorner \in Pr$ implicira $\ulcorner\mathrm{Pr}(\ulcorner\varphi\urcorner)\urcorner \in Pr\}$ koji je parcijalno rekurzivan, reprezentujemo u teoriji Σ. Tvrđenje (c) se neposredno dokazuje.

Primer 11. Ako $\Sigma \subseteq \mathrm{Th}(\mathcal{N})$, onda $\Sigma \vdash \mathrm{Pr}(\ulcorner\varphi\urcorner)$ implicira $\Sigma \vdash \varphi$.

Ako $\Sigma \vdash \mathrm{Pr}(\ulcorner\varphi\urcorner)$ i $\Sigma \subseteq \mathrm{Th}(\mathcal{N})$, onda $\mathcal{N} \models \mathrm{Pr}(\ulcorner\varphi\urcorner)$. Otuda sledi da postoji prirodan broj $n \in \omega$ koji je kod dokaza formule φ u teoriji Σ, tj. $\Sigma \vdash \varphi$.

Dijagonalizacijom formule $\neg\,\mathrm{Pr}(x)$ dobija se rečenica φ jezika $\mathcal{L}_{\mathrm{PA}}$ takva da $\Sigma \vdash \varphi \leftrightarrow \neg\,\mathrm{Pr}(\ulcorner\varphi\urcorner)$. Rečenica φ sama za sebe tvrdi "ja nisam dokaziva". Ako je teorija Σ neprotivrečna, rečenica φ je "u pravu", tj. ona zaista nije dokaziva u teoriji Σ.

Primer 12. Prva teorema nepotpunosti: Ako je Σ neprotivrečna teorija i φ rečenica jezika $\mathcal{L}_{\mathrm{PA}}$ takva da $\Sigma \vdash \varphi \leftrightarrow \neg\,\mathrm{Pr}(\ulcorner\varphi\urcorner)$, onda

(a) nije da $\Sigma \vdash \varphi$
(b) ako $\Sigma \vdash \mathrm{Pr}(\ulcorner\varphi\urcorner)$ implicira $\Sigma \vdash \varphi$, onda nije da $\Sigma \vdash \neg\varphi$

Pritom, u teoriji PA zadovoljen je uslov $\Sigma \vdash \mathrm{Pr}(\ulcorner\varphi\urcorner)$ implicira $\Sigma \vdash \varphi$.

U sledećoj teoremi dokazaćemo da je rečenica φ ekvivalentna rečenici $\neg\,\mathrm{Pr}(\ulcorner 0 = 1\urcorner)$ koju označavamo sa $\mathrm{Con}(\Sigma)$. Ova rečenica ima sasvim konkretan smisao "u teoriji Σ ne može se dokazati $0 = 1$", odnosno, teorija Σ je neprotivrečna.

Teorema 17. Druga teorema nepotpunosti::Ako je Σ neprotivrečna rekurzivna teorija jezika $\mathcal{L}_{\mathrm{PA}}$, koja sadrži teoriju PA, onda nije $\Sigma \vdash \mathrm{Con}(\Sigma)$.

Dokaz: Neka je φ rečenica takva da $\Sigma \vdash \varphi \leftrightarrow \neg\,\mathrm{Pr}(\ulcorner\varphi\urcorner)$. Tvrdimo da je $\Sigma \vdash \varphi \leftrightarrow \mathrm{Con}(\Sigma)$.

Po definiciji rečenice φ i zbog svojstava (a) i (c) predikata $\mathrm{Pr}(x)$ imamo:

$$
\begin{array}{lcl}
\Sigma & \vdash & (0=1) \to \varphi, \\
\Sigma & \vdash & \mathrm{Pr}(\ulcorner 0=1 \urcorner) \to \mathrm{Pr}(\ulcorner \varphi \urcorner), \\
\Sigma & \vdash & \neg \mathrm{Pr}(\ulcorner \varphi \urcorner) \to \neg \mathrm{Pr}(\ulcorner 0=1 \urcorner), \\
\Sigma & \vdash & \varphi \to \mathrm{Con}(\Sigma).
\end{array}
$$

Obratno, primenom već spomenutog svojstva (b) predikata $\mathrm{Pr}(x)$ dobijamo $\Sigma \vdash \mathrm{Pr}(\ulcorner\varphi\urcorner) \to \mathrm{Pr}(\ulcorner \mathrm{Pr}(\ulcorner\varphi\urcorner)\urcorner)$. Kako po definiciji rečenice φ imamo $\Sigma \vdash \neg\varphi \leftrightarrow \mathrm{Pr}(\ulcorner\varphi\urcorner)$, to znači da $\Sigma \vdash \mathrm{Pr}(\ulcorner\varphi\urcorner) \to \mathrm{Pr}(\ulcorner\neg\varphi\urcorner)$, pa dakle mora biti $\Sigma \vdash \mathrm{Pr}(\ulcorner\varphi\urcorner) \to (\mathrm{Pr}(\ulcorner\varphi\urcorner) \wedge \mathrm{Pr}(\ulcorner\neg\varphi\urcorner))$.

Kako $\vdash \varphi \to (\neg\varphi \to (\varphi \wedge \neg\varphi))$, sada primenom svojstava (a) i (c) predikata $\mathrm{Pr}(x)$ dobijamo $\Sigma \vdash \mathrm{Pr}(\ulcorner\varphi\urcorner) \wedge \mathrm{Pr}(\ulcorner\neg\varphi\urcorner) \to \mathrm{Pr}(\ulcorner\varphi \wedge \neg\varphi\urcorner)$, pa otuda sledi da važi $\Sigma \vdash \mathrm{Pr}(\ulcorner\varphi\urcorner) \to \mathrm{Pr}(\ulcorner\varphi \wedge \neg\varphi\urcorner)$.

Otuda, na osnovu $\vdash \varphi \wedge \neg\varphi \to (0=1)$, primenom svojstava (a) i (c) predikata $\mathrm{Pr}(x)$ imamo $\Sigma \vdash \mathrm{Pr}(\ulcorner\varphi\urcorner) \to \mathrm{Pr}(\ulcorner 0=1\urcorner)$, pa se neposredo dobija $\Sigma \vdash \neg\varphi \to \neg\,\mathrm{Con}(\Sigma)$, što konačno znači da važi $\Sigma \vdash \mathrm{Con}(\Sigma) \to \varphi$. Na osnovu prve teoreme nepotpunosti, nije da $\Sigma \vdash \mathrm{Con}(\Sigma)$. $\Box$

Primer 13. Ne postoji rekurzivno neprotivrečno proširenje teorije QA u kome su slabo predstavljive sve Π_1 relacije.

Druga teorema nepotpunosti tvrdi da se neprotivrečnost Peanove aritmetike ne može dokazati sredstvima same aritmetike. Većina matematičara veruje da je dokazom ove teoreme Gedel pokazao da Hilbertov program nije ostvariv, odnosno, da finitistički dokaz neprotivrečnosti matematike nije moguć.

Druga teorema nepotpunosti odnosi se na sve rekurzivne teorije u kojima se može interpretirati aritmetika. Dakle, ako je ZFC neprotivrečna teorija, onda nije $\mathrm{ZFC} \vdash \mathrm{Con}(\mathrm{ZFC})$, što znači da se neprotivrečnost ZFC ne može dokazati sredstvima raspoloživim u ZFC. Kako se matematika može zasnovati u ZFC, ovaj Gedelov rezultat može se izraziti i na sledeći način:

Ako je matematika uopšte neprotivrečna, njena neprotivrečnost ne može se dokazati matematičkim sredstvima.

Nepotpunost teorije ZF sledi iz činjenice da u njoj nisu dokazive ni kontinuum hipoteza ni njena negacija. Dakle postoji konkretno matematičko svojstvo skupova koje se ne može dokazati ni opovrgnuti u ZF. Osim rečenice CH sada znamo da to važi i za rečenicu Con(ZF).

Po definiciji, rečenica Con(ZF) je tipa Π_1, što znači da je njena negacija Σ_1 rečenica. Na osnovu rešenja desetog Hilbertovog problema, postoji polinom $p(\vec{x})$, $\vec{x} \in \omega^n$ takav da

$$\mathrm{Con}(\mathrm{ZF}) \quad \Leftrightarrow \quad \neg\exists\vec{x}\,(p(\vec{x})=0),$$

što znači da Con(ZF) ako i samo ako $\forall \vec{x}\,(p(\vec{x}) \neq 0)$.

Kako u teoriji ZF nije dokazivo ni Con(ZF) ni $\neg$ Con(ZF), ukoliko je to uopšte neprotivrečna teorija, postoji model $\mathcal{A}$ teorije ZF u kojem važi Con(ZF) i model $\mathcal{B}$ teorije ZF u kojem važi $\neg$ Con(ZF).

Neka je P program na idealnom računaru koji lista sve nizove $\vec{x} \in \omega^n$ i proverava da li je $p(\vec{x}) = 0$.

U matematičkom svetu $\mathcal{A}$, važi Con(ZF), pa jednačina $p(\vec{x}) = 0$ nema rešenja, odnosno, izračunavanje $P(\vec{x})$ se ne završava. S druge strane, u matematičkom svetu $\mathcal{B}$, važi $\neg$ Con(ZF), pa jednačina $p(\vec{x}) = 0$ ima rešenja, odnosno, izračunavanje $P(\vec{x})$ se završava [5].

Ista primedba važi i u slučaju teorije ZFC budući da se i njena neprotivrečnost može izraziti rečenicom tipa Π_1. Zbunjujuće je da se ni sredstvima ove teorije ne mogu raspraviti svojstva sasvim jednostavnog objekta kao što je idealni računar.

Istovremeno, kako je hipoteza kontinuuma formulisana Π_1 rečenicom jezika $\mathcal{L}_{\mathrm{ZF}}$, ništa manje ne zbunjuje ni činjenica da se metodom kodiranja i ovaj problem može svesti na problem egzistencije rešenja jedne diofantovske jednačine.

Izgleda nam da platonisti s pravom shvataju hipotezu kontinuuma na bitno drugačiji način. Njihovo stanovište da relativna neprotivrečnost i nezavisnost ove hipoteze govore samo o svojstvima jedne rekurzivno aksiomatske teorije, a nikako ne predstavljaju rešenje problema kontinuuma, deluje mnogo ubedljivije od formalističkog shvatanja matematike kao pozitivne nauke, a pogotovo od konstruktivističkih pokušaja revizije njenih osnova i njene potpune rekonstrukcije.

Napomene

– Klasu rekurzivnih funkcija definisao je Gedel 1934. godine. Za istu klasu funkcija Klini je 1936. godine definisao takozvani drugačiji pristup i dokazao njihovu ekvivalenciju. Iste godine, Tjuring je uspeo da izračunljivost interpretira mehanički, a idealni računar, kao paradigma izračunljivosti, formulisan je kasnih oko 1960. godine u radovima Lambeka, Minskog, Šeferdsona i Stardžesa [3].

– Kao metamatematički princip, Čerčova teza formulisana je 1936. godine [2]. Implicitno, ona je prisutna u Tjuringovim radovima iz 1936. godine. Teoreme o efektivnoj enumeraciji, parametrizaciji i teoremu rekurzije otkrio je i dokazao Klini, između 1936. i 1938. godine [4].

– U formi u kojoj je ovde izložena, aritmetičku hijerarhiju definisao je Klini i dokazao teoremu o hijerahiji 1943. godine [4]

– Kreativne skupove i pojmove svodljivosti definisao je Post 1944. godine a pojam produktivnog skupa Deker 1955. godine. Takođe, Post je formulisao strukturu stepena nerešivosti i postavio većinu pitanja u vezi sa njenom prirodom [6].

– Nepotpunost Peanove aritmetike dokazao je Gedel 1931. godine u jednoj varijanti u kojoj je pretpostavljen uslov ω-neprotivrečnosti: ako je rečenica $\neg\forall x\,\varphi$ dokaziva u teoriji Σ, onda postoji $n \in \omega$, takvo da formula $\varphi(n)$ nema dokaz u teoriji Σ. Nešto kasnije, 1936. godine, Roser je pokazao da je neprotivrečnost bilo koje rekurzivne teorije koja sadrži PA dovoljna pretpostavka za dokaz njene nepotpunosti [7].

– Neodlučivost predikatskog računa dokazao je Čerč 1936. godine. Tarski je 1935. godine dokazao da skup istina prirodnih brojeva nije aritmetički [7]. Da logika drugog reda nije aksiomatska, dokazao je Gedel 1930. godine.

– Od 1900. godine, kada je prvi put eksplicitno formulisan, problem određivanja algoritma za rešavanje diofantovskih jednačina je snažno uticao na razvoj teorije izračunljivosti. Faktički ona je nastala u pokušajima da se ovaj problem reši. Kasnih pedesetih godina, zahvaljujući opsežnim istraživanjima velike grupe matematičara, problem je bio sveden na dokaz zatvorenosti diofantovskih predikata za ograničenu univerzalnu kvantifikaciju. Taj korak, koji nije izložen u ovom pregledu teorije izračunljivosti, napravio je 1970. godine Matijasevič [5].

Literatura

[1] Barvise, J., Feferman, S. *Model Theoretic Logics.* Springer-Verlag, Berlin, 1984.

[2] Church, A. *Introduction to Mathematical Logic,* Princeton Univ. Press, Princeton, 1956.

[3] Cutland, N. *Computability,* Cambr. Univ. Press, Cambridge, 1980.

[4] Klini, S.C. *Introduction to Metamathematic,* North-Holland, Amsterdam, 1952.

[5] Mijajlović, Ž., Marković, Z., Došen, K. *Hilbertovi problemi i logika,* Zavod za izd. udžben., Beograd, 1986.

[6] Soare, R.S. *Recursively Enumerable Sets and Degrees,* Springer-Verlag, Berlin, 1987.

[7] Tarski, A., Mostovski,A., Robinson,R.M. *Undecidable theories,* North-Holland, Amsterdam, 1953.

Index