48 MATEMATIČKA BIBLIOTEKA 48

ŽARKO MIJAJLOVIĆ, ZORAN MARKOVIĆ, KOSTA DOŠEN

HILBERTOVI PROBLEMI I LOGIKA

ZAVOD ZA UDŽBENIKE I NASTAVNA SREDSTVA — BEOGRAD
1986.

SADRŽAJ

PREDGOVOR

Prošle godine navršilo se 120 godina od Hilbertovog rođenja i 40 godina od Hilbertove smrti. Seminar za matematičku logiku koji se održava na Matematičkom institutu odlučio je da obeleži ove godišnjice serijom predavanja namenjenih široj matematičkoj publici. Ta predavanja održali smo aprila 1983. godine, i ona su se odnosila na prvi, drugi, deseti i sedamnaesti Hilbertov problem, tj. na one Hilbertove probleme koji se tiču matematičke logike.

Posle tih predavanja odlučili smo da napišemo ovu knjigu. U njoj se prikazuju gore navedeni Hilbertovi problemi, koji su svi veoma značajni za matematičku logiku. Preko njih čitalac se može upoznati sa teorijama koje se nalaze u osnovama ove nauke i sa nekim od njenih najlepših rezultata. Ali, ne samo to. Ovi problemi se odnose i na druge grane matematike: teoriju skupova, aritmetiku, algebru, teoriju brojeva, ... Tako čitalac može kroz ove probleme da sazna nešto i o primenama logike u drugim oblastima matematike. Osim toga, kroz ove probleme mogu se upoznati i neka veoma važna pitanja iz filozofije matematike. Najzad, ova knjiga bi trebalo da omogući čitaocu đa sazna nešto i o Davidu Hilbertu, jednom od najvećih matematičara svih vremena, o kome se kod nas relativno malo pisalo.

Posle uvodnog poglavlja o značaju Hilbertovih problema i o Hilbertovom životu i radu, i jednog dodatka u kojem ćemo dati spisak Hilbertovih problema, slede poglavlja o prvom, drugom, desetom i sedamnaestom Hilbertovom problemu. Svako poglavlje podeljeno je na dva dela. U prvom delu se daje analiza problema sa tačke gledišta istorije logike i matematike, i neformalno se govori o njegovom rešavanju. Taj deo treba da omogući čitaocu da shvati značaj problema o kojem je reč i da stekne neku predstavu o njemu. Drugi deo svakog poglavlja se sastoji od jednog ili dva dodatka koji su više tehničke prirode. U njima se daje ili skica rešenja, ili potpuno rešenje,

ili su prikazani oni rezultati matematičke logike koji se tiču datog problema. Najzad, na kraju svakog poglavlja nalaze se bibliografske beleške, u kojima su data uputstva za dalje čitanje.

Poglavlje o prvom Hilbertovom problemu napisao je Zoran Marković, poglavlje o drugom Hilbertovom problemu Kosta Došen, a poglavlja o desetom i sedamnaestom Hilbertovom problemu Žarko Mijajlović. Uvodno poglavlje napisali su Kosta Došen i Žarko Mijajlović. Pošto ova četiri poglavlja obrađuju četiri relativno nezavisne teme, nismo pokušavali da ujednačimo stil izlaganja više nego što je to učinjeno. Osim toga, sa nekim gledištima koja se tiču filozofske interpretacije svi autori se ne bi nužno svuda složili. Zato napominjemo da svaki autor odgovara samo za poglavlje koje je pisao.

Ova knjiga ne pretpostavlja neko veliko poznavanje matematičke logike, ali ipak nešto pretpostavlja. U principu, dovoljno je znati onoliko matematike i logike koliko se može naučiti u srednjoj školi (tamo gde se ti predmeti još predaju). Ovu knjigu bi onda, pogotovu, trebalo da razumeju oni koji su učili matematičku logiku na univerzitetu, i nisu je sasvim zaboravili. Tako bi, osim matematičara koji žele da saznaju nešto više o matematičkoj logici, ovu knjigu mogli da čitaju i filozofi koje zanima filozofija matematike.

Želimo da se zahvalimo svim kolegama koji su slušali naša predavanja o Hilbertovim problemima i čije nas je interesovanje navelo da se odlučimo na pisanje ove knjige. Zahvaljujemo se prof. dr Slaviši Prešiću na korisnim primedbama koje je dao čitajući rukopis ove knjige. Zahvaljujemo se i mr Draganu Blagojeviću, mr Miodragu Kapetanoviću, prof. dr Aleksandru Kronu i dr Slobodanu Vujoševiću što su pročitali delove rukopisa i pomogli nam svojim savetima. Prof. dr Draganu Trifunoviću se zahvaljujemo što se zauzeo oko izdavanja ove knjige.

Ova knjiga se verovatno ne bi pojavila da ne postoji Seminar za matematičku logiku na Matematičkom institutu. Naše kolege logičari sa seminara znaju koliko dugujemo njihovoj saradnji, i njima se od sveg srca zahvaljujemo.

u Beogradu, oktobra 1984.

UVOD

Neki matematički problemi su samo postavljeni. Matematičari su pokušavali da ih reše, nisu umeli, i dalje ne umeju, i to je sve. Takav je, na primer, problem da li ima neparnih savršenih brojeva, koji, izgleda, stoji otvoren još od Euklidovog doba.

Neki drugi matematički problemi su rešeni, ali bez posledica. Znači, pojavi se matematičar koji reši neki takav problem, veoma oštroumno i dosetljivo, i tu se stane. Ne ide se dalje od toga. Evo jednog takvog problema: „Koliko se tačaka može postaviti u krugu poluprečnika 2, pod uslovom da je jedna tačka u centru i da je rastojanje između svake dve tačke veće od 1?“ Ovaj problem je, kao i mnoge druge takve probleme, rešio Erdös. Odgovor je: 20.

Zatim, postoji mogućnost da se rešavanjem nekog matematičkog problema otkrije neki metod. Jedan matematičar reši problem, i vidi se da sredstva koja je upotrebio mogu da posluže za rešavanje čitave klase drugih problema. Metod se može rafinirati, razgranavati, poboljšavati, ... ali sve to još ne znači da tačno znamo šta se dešava. Imamo metod, ali još nemamo opštu teoriju u koju bi se taj metod uklopio. Probleme koji se rešavaju takvim metodima često nalazimo u elementarnoj teoriji brojeva i konačnoj kombinatorici.

Najzad, dolazimo do problema iz kojih su potekle ideje koje se uopšte više ne mogu meriti sa početnim problemom. Ne radi se više samo o dosetkama i metodima, nego o tome da se zahvaljujući tim novim idejama najzad razume šta se dešava. Polazeći od ovih ideja, dugim i napornim radom, koji često obuhvata više generacija, matematičari postaju svesni novih struktura, novih matematičkih objekata, i tako nastaju velike matematičke teorije. Tako je, na primer, nastala teorija grupa. Grupe je uveo Galois, da bi rešio dugo otvoreni problem rešavanja u radikalima algebarskih

jednačina stepena većeg od 4. Vremenom pojam grupe je postao jedan od ključnih pojmova matematike.[1]

Ako Hilbertovi problemi nisu svi ove poslednje vrste, onda su joj izgleda gotovo svi veoma blizu, a neki sasvim sigurno daju najbolje primere problema iz kojih se rađaju velike teorije. Četiri Hilbertova problema koja će biti obrađena u ovoj knjizi tiču se matematičke logike. U vezi sa tim problemima iznikle su teorije koje se nalaze u osnovama ne samo logike nego i drugih grana matematike.

Prvi problem odnosi se na teoriju skupova. Njegovo rešavanje, u okviru formalne teorije skupova, omogućilo je da se razvije ne samo teorija skupova nego i opšta (skupovna) topologija. Ovaj problem je veoma zanimljiv i za filozofiju matematike. Pošto je on rešen u okviru jedne formalne teorije, tj. Zermelo-Fraenkelove teorije skupova, status njegovog rešenja nije za sve matematičare isti. Za nekog ko ima formalističko gledište, kao što ga je donekle imao Hilbert, problem znači da li aksiome teorije skupova povlače hipotezu kontinuuma ili njenu negaciju. Pošto su Gödel i Cohen utvrdili da ni jedno ni drugo nije slučaj, za formalističkog matematičara problem je rešen. S druge strane, za matematičara koji kao Gödel veruje da aksiome samo u većoj ili manjoj meri opisuju neku matematičku stvarnost, problem hipoteze kontinuuma ostaje otvoren i posle Gödelovog i Cohenovog rešenja.

Drugi problem se tiče neprotivrečnosti matematičkih teorija. Jedna od osnovnih disciplina matematičke logike, teorija dokaza, razvila se direktno iz pokušaja da se reši ovaj problem. Ovaj problem je isto tako važan za filozofiju matematike. On se vezuje za pitanje da li se beskonačnost može eliminisati iz matematike, tj. da li se dokazi koji se pozivaju na beskonačnost mogu zameniti dokazima koji se pozivaju samo na konačne matematičke objekte. Kad bi odgovor na ovo pitanje bio potvrdan, onda bi se ispostavilo da beskonačnost ne mora biti kao kod Cantora deo matematičkog sveta, nego se može smatrati kao nešto prisutno samo u jeziku.

Deseti i sedamnaesti Hilbertov problem su nešto drukčijeg karaktera od prva dva problema. Hilbert ih je formulisao u okviru već postojećih, razvijenih teorija, tako da su oni delovali mnogo

---

[1] Ova mala tipologija matematičkih problema inspirisana je člankom [Dieudonné 1976].

konkretnije. Međutim, da bi deseti problem bio rešen bilo je potrebno da se u logici razvije jedna veoma značajna nova disciplina: teorija efektivne izračunljivosti, tj. teorija rekurzivnih funkcija. Rešenje desetog Hilbertovog problema, na koje se čekalo 70 godina, omogućilo je da se reše mnogi drugi značajni problemi u logici, teoriji brojeva, algebri i analizi. Rešenje ovog problema bilo je naročito značajno za teoriju modela formalne aritmetike. Preko te teorije ovaj problem je u vezi sa drugim Hilbertovim problemom.

Prvo rešenje sedamnaestog Hilbertovog problema, koje je dao Artin, bilo je sasvim algebarskog karaktera: u njemu nije bilo ni tragova logičkih metoda. Kada je Robinson dao svoje rešenje metodima matematičke logike, problem je bio već odavno rešen. Ovo logičko rešenje je, zato, značajno zbog metoda: ono predstavlja jednu od prvih ozbiljnih primena teorije modela u algebri. Danas je modelsko-teoretska algebra jedna zasebna disciplina, koja zajedno sa nestandardnom analizom, predstavlja najvažniju konkretnu primenu logike u drugim oblastima matematike.

* * *

Kada je Hilbert formulisao svoje probleme na svetskom matematičkom kongresu 1900. godine on je hteo da ti problemi pokažu put matematičarima u dvadesetom veku. Njegova reputacija, koja je već u doba kongresa bila velika, učinila je da ti problemi odigraju tu ulogu. Pokušaćemo da skiciramo kako je Hilbert stekao tu reputaciju.[2]

David Hilbert je rođen 1862. godine u Kenigsbergu u istočnoj Pruskoj. U tom gradu je i studirao, osim što je proveo jedan semestar u Hajdelbergu. Njegova disertacija, koju je odbranio 1884, posvećena je jednom problemu iz teorije algebarskih invarijanti, i do 1892. godine Hilbert je uglavnom radio na toj teoriji. Tokom tih istraživanja došao je do mnogih značajnih rezultata, od kojih neki nose njegovo ime (Hilbertov *Nullstellensatz*, Hilbertova teorema o nesvodljivosti polinoma). Sa metodima koje je koristio u tim istraživanjima počinje apstraktno tretiranje algebre, koje odonda dominira tom oblašću matematike.

Godine 1886. Hilbert postaje *Privatdozent*, a 1892. vanredni profesor na Univerzitetu u Kenigsbergu. Sledeće godine on nasle-

---

[2] Sledeći biografski podaci preuzeti su iz članaka [Bernays 1967] i [Weyl 1944].

đuje svog učitelja Felixa Lindemanna kao redovni profesor u Kenigsbergu. Godine 1895. Hilbert prihvata poziv Felixa Kleina da pređe na Univerzitet u Getingenu, gde će ostati do kraja života, iako su ga pozivali još na mnoge druge univerzitete. Hilbert je uspeo da njegov drug iz studentskih dana u Kenigsbergu, Hermann Minkowski, pređe u Getingen, i mogućnost da zajedno rade je bila obojici od velikog značaja.

Od 1892. do 1898. godine Hilbert će se uglavnom baviti teorijom polja algebarskih brojeva. Njegova istraživanja iz te oblasti presudno će uticati na dalji razvoj ove discipline. Od 1898. godine on počinje da radi na osnovama matematike, a naročito na osnovama geometrije. Ali ove oblasti ne iscrpljuju ni izdaleka sve ono što ga je tada interesovalo u matematici. Hilbertovi problemi najbolje pokazuju u koliko je matematičkih oblasti Hilbert radio.

U leto 1900. godine održaće se u Parizu Drugi međunarodni kongres matematičara. Hilbert je bio pozvan da održi jedno od glavnih predavanja na kongresu. U jednom pismu Minkowskom s početka 1900. godine on piše kako ne zna tačno o čemu bi govorio. Razmišlja da li da, pošto je na prethodnom kongresu Poincaré održao jedno predavanje o odnosu analize i fizike, on sada ustane u odbranu čiste matematike. Ili da možda govori o pravcu kojim matematika treba da krene u dvadesetom veku, da kaže kojim problemima matematičari treba da se bave u budućnosti. Minkowski mu je odgovorio da mu se ova druga ideja čini privlačnijom, i napisao mu je: „Sa takvom temom može se desiti da ljudi decenijama govore o tom predavanju.“[3]

Predavanje s naslovom *Matematički problemi* [Hilbert 1900] Hilbert je koncipirao ovako. U prvom delu govori se o važnosti problemâ za određivanje pravca razvoja u nauci. Onda se razmatraju neki veliki plodni problemi u matematici, i govori se o zahtevima koje rešenja moraju da zadovolje. Tu Hilbert insistira na rigoroznosti. Zatim slede 23 problema sa komentarima.[4] Prvih nekoliko problema tiču se osnova matematike i sugerisani su onim što je Hilbert smatrao velikim dostignućima veka koji se završio; ta dostignuća su razjašnjavanje osnovnih pojmova vezanih za realne brojeve i otkriće neeuklidskih geometrija. Ovi problemi pokazuju uticaj njegovog rada na osnovama matematike i njegov entuzijazam

---

[3] v. Hilbertovu biografiju od Constance Reid [1970], str. 69.
[4] Spisak ovih problema dat je u dodatku ovog poglavlja.

za aksiomatski metod. Drugi problemi su više specijalizovani — neki su stari, neki novi, ali svi su iz oblasti kojima se Hilbert ili već bavio, ili će se baviti.

Svoje predavanje Hilbert je na kongresu održao na nemačkom, u skraćenoj verziji. Utisak možda nije odmah bio kao da se dešava nešto epohalno (sudeći po jednom, inače prilično duhovitom izveštaju sa kongresa, koji je objavljen iste godine [Angus Scott 1900]). Kao što to često biva na kongresima, pogotovu velikim, diskusija posle Hilbertovog predavanja nije bila ni naročito sređena, ni naročito precizna. Osim toga, postojali su izgleda u to doba i problemi u komuniciranju, i taj isti kongres u Parizu ozbiljno se bavio pitanjem na kom jeziku matematičari treba da komuniciraju (kongresu je prisustvovalo oko 230 matematičara, i to 90 iz Francuske, 25 iz Nemačke, 17 iz Sjedinjenih Država, 15 iz Italije, 13 iz Belgije, 9 iz Rusije, 8 iz Austrije, 8 iz Švajcarske, 7 iz Engleske, 7 iz Švedske, 4 iz Danske. 3 iz Holandije, 3 iz Španije, 3 iz Rumunije, 2 iz Srbije, 2 iz Portugala, 4 iz Južne Amerike, i po jedan iz Grčke, Norveške, Turske, Kanade, Japana i Meksika).

Posle 1900. godine Hilbert će se još oko dve godine baviti osnovama geometrije, a zatim će uglavnom raditi na teoriji integralnih jednačina. Između 1892. i 1909. Hilbert je dao svoje verovatno najveće doprinose matematici. Tu spadaju njegovi rezultati iz osnova geometrije, koji su zahvaljujući knjizi *Osnove geometrije* [Hilbert 1899] postali veoma poznati. Osim toga, u to doba on je pojednostavio postojeće dokaze za transcendentnost brojeva e i π. Zatim je pokazao kako se može opravdati Dirichletov princip da postojanje jednog konformnog preslikavanja sledi iz postojanja minimuma Dirichletovog integrala. Metod koji je tom prilikom upotrebio Hilbert pokazao se izvanredno uspešnim kada su ga razradili Courant i Weyl. Hilbertov doprinos računu varijacija, a naročito njegov „aksiom nezavisnosti“, predstavljali su veliko razjašnjavanje pojmova u ovoj oblasti. Baveći se integralnim jednačinama, Hilbert je uveo analizu sa beskonačno mnogo promenljivih, iz koje će se razviti ono što se danas naziva teorijom Hilbertovih prostora. Te Hilbertove ideje su se pokazale veoma plodne u topologiji i fizici — naročito kvantnoj mehanici. Najzad, 1909. godine Hilbert je rešio Waringov problem o predstavljanju prirodnih brojeva pomoću suma n-tih stepena. Te godine umro je Minkowski, i to je bio veliki udarac za Hilberta.

Posle smrti Minkowskog Hilbert se uglavnom bavio problemima teorijske fizike, sve do 1922. godine. Primenio je teoriju

integralnih jednačina na kinetičku teoriju gasova i na teoriju zračenja. Neposredno posle pojave Einsteinove opšte teorije relativnosti, objavio je prvi pokušaj da se ujedine gravitaciona teorija i elektrodinamika.

Posle 1916, a naročito od 1922. do 1930. Hilbert će se opet baviti osnovama matematike. Ta istraživanja, iz kojih je proistekla knjiga *Principi teorijske logike* [Hilbert, Ackermann 1928] i enciklopedijska rasprava *Osnove matematike* [Hilbert, Bernays 1934], dovešće do stvaranja teorije dokaza, o kojoj će biti reči u poglavlju o drugom Hilbertovom problemu. U starosti Hilbert je držao predavanja koja bi davala detaljan pregled matematike, kao što su ona skupljena u knjizi *Intuitivna geometrija* [Hilbert, Cohn—Vossen 1932]. Isto tako, držao bi popularna predavanja iz filozofije matematike. Hilbert je umro 1943. godine u Getingenu.

Ako se pogleda ko su bili Hilbertovi đaci, vidi se da su to sve sami velikani matematike dvadesetog veka. Pomenućemo neke od njih, one koji su poznati u logici i osnovama matematike. Hilbertov mlađi kolega u Getingenu je bio Ernst Zermelo, a Hilbertovi đaci su Wilhelm Ackermann, Paul Bernays, Gerhard Gentzen i Hermann Weyl. Sa Hilbertom je isto tako tesno sarađivao John von Neumann. Hilbertovi đaci i saradnici Emmy Noether i Emil Artin, iako nisu dali doprinosa logici i osnovama matematike, radili su u oblastima koje se tiču logike, kao što će se videti u poslednjem poglavlju ove knjige.

Hilbertov uticaj na matematiku je i danas veoma veliki. Deo tog uticaja se prenosi preko njegovih problema. U ovoj knjizi pokušaćemo da pokažemo kako taj deo Hilbertovog uticaja osećaju logičari.

SPISAK HILBERTOVIH PROBLEMA

1. *Cantorov problem kardinalnog broja kontinuuma;*
2. *Neprotivrečnost aritmetičkih aksioma;*
3. *Jednakost zapremina dva tetraedra jednakih baza i jednakih visina* (naći dva tetraedra jednakih baza i jednakih visina koja se ni na koji način ne mogu rastaviti na kongruentne tetraedre, i koja se ne mogu kombinovati sa kongruentnim poliedrima da bi načinili dva poliedra koja se mogu rastaviti na kongruentne tetraedre);
4. *Problem prave linije kao najkraćeg rastojanja između dve tačke* (ispitati status teoreme o pravoj liniji kao najkraćem rastojanju između dve tačke u neeuklidskim geometrijama);
5. *Liev pojam neprekidne grupe transformacija bez pretpostavke diferencijabilnosti funkcija koje čine grupu;*
6. *Matematičko ispitivanje aksioma fizike* (ispitati aksiomatski one grane fizike u kojima matematika igra važnu ulogu — pre svega, teoriju verovatnoće i mehaniku);
7. *Iracionalnost i transcendentnost određenih brojeva* (dokazati da ako je u jednakokrakom trouglu odnos ugla na osnovici i ugla pri vrhu algebarski ali ne racionalan, onda je odnos osnovice i kraka uvek transcendentan; dokazati da je α^{β}, za algebarski broj α i iracionalan algebarski broj β, npr. broj $2^{\sqrt{2}}$ ili $e^{\pi}=i^{-2i}$, uvek transcendentan, ili bar iracionalan broj);
8. *Problemi koji se tiču prostih brojeva* (dokazati da, izuzevši poznate negativne celobrojne realne nule, sve nule funkcije $\zeta(s)$ definisane redom

$$\zeta(s)=1+\frac{1}{2^s}+\frac{1}{3^s}+\cdots$$

imaju realni deo 1/2 ; utvrditi da razlika između broja prostih

brojeva manjih od nekog broja x i celobrojnog logaritma od x postaje beskonačna reda ne većeg od 1/2 u x; utvrditi da li povremeno zgušnjavanje prostih brojeva, koje je uočeno njihovim prebrojavanjem, zaista nastaje zbog onih članova Riemannove formule koji zavise od prve kompleksne nule funkcije $\zeta(s)$; rešiti Goldbachov problem, tj. da li se svaki celi broj može izraziti kao suma dva pozitivna prosta broja; rešiti problem da li postoji beskonačno mnogo parova prostih brojeva sa razlikom 2; rešiti problem da li linearna diofantovska jednačina

$$ax + by + c = 0$$

sa celobrojnim međusobno prostim koeficijentima, uvek ima rešenja u prostim brojevima x i y; primeniti rezultate koji se tiču distribucije racionalnih prostih brojeva na teoriju distribucije idealnih prostih brojeva u datom polju brojeva k);

9. *Dokaz najopštijeg zakona reciprociteta u proizvoljnom polju brojeva* (za proizvoljno polje brojeva, dokazati zakon reciprociteta za reziduale l-tog stepena, gde l označava neki neparan prost broj, ili stepen od 2, ili stepen nekog neparnog prostog broja);
10. *Određivanje rešivosti neke diofantovske jednačine*;
11. *Kvadratne forme sa proizvoljnim algebarskim numeričkim koeficijentima* (naći rešenja neke date kvadratne jednačine sa algebarskim numeričkim koeficijentima i proizvoljnim brojem promenljivih u celim brojevima ili razlomcima koji pripadaju algebarskoj oblasti racionalnosti koja je određena tim koeficijentima);
12. *Proširenje Kroneckerove teoreme o abelovskim poljima na proizvoljnu algebarsku oblast racionalnosti*;
13. *Nemogućnost rešenja opšte jednačine sedmog stepena pomoću funkcija sa samo dva argumenta* (dokazati da jednačina sedmog stepena

$$f^7 + xf^3 + yf^2 + zf + 1 = 0$$

ne može da se reši pomoću neprekidnih funkcija sa samo dva argumenta);
14. *Dokaz konačnosti određenih sistema funkcija* (naći konačan sistem relativno celobrojnih funkcija pomoću kojih se može racionalno i celobrojno predstaviti svaka relativno celobrojna funkcija);

15. *Rigorozno zasnivanje Schubertovog enumerativnog računa*;
16. *Problem topologije algebarskih krivih i algebarskih površi* (ispitati odnose grana algebarskih krivih kada je njihov broj maksimalan, i analogno tome ispitati broj, oblik i položaj slojeva algebarskih površi u prostoru);
17. *Predstavljanje definitnih formi pomoću kvadrata*;
18. *Građenje prostora od kongruentnih poliedara* (da li u n-dimenzionalnom euklidskom prostoru ima samo konačno mnogo esencijalno različitih grupa kretanja sa fundamentalnom oblašću; da li postoje poliedri koji nisu fundamentalne oblasti neke grupe kretanja, a pomoću čijih se kongruentnih kopija ipak može ispuniti prostor?);
19. *Da li su rešenja regularnih problema u računu varijacija nužno analitička*? (da li svaka Lagrangeova parcijalna diferencijalna jednačina regularnog variacionog problema ima isključivo analitičke integrale?);
20. *Opšti problem graničnih vrednosti* (da li svaki regularni variacioni problem ima rešenje, pod uslovom da su zadovoljene neke pretpostavke koje se tiču datih graničnih uslova, npr. funkcije sa datim graničnim uslovima su neprekidne i imaju jedan ili više izvoda u nekim delovima, i pod uslovom da se, ako je to potrebno, pojam rešenja može na određeni način proširiti?);
21. *Dokaz postojanja linearnih diferencijalnih jednačina sa zadatom monodromskom grupom*;
22. *Uniformizacija analitičkih relacija pomoću automorfnih funkcija* (rešiti probleme koji se javljaju u vezi sa Poincaréovim dokazom mogućnosti uniformizacije proizvoljnih analitičkih relacija sa dve promenljive; rešiti problem uniformizacije algebarskih i drugih analitičkih relacija sa tri ili više kompleksnih promenljivih);
23. *Razvijanje metodâ računa varijacija.*

I PRVI HILBERTOV PROBLEM

Cantorov problem kardinalnog broja kontinuuma

„ . . . Cantorova istraživanja takvih skupova tačaka sugerišu jednu vrlo verovatnu teoremu, koju međutim, uprkos najupornijim naporima, niko nije uspeo da dokaže. Ovo je teorema:

Svaki sistem od beskonačno mnogo realnih brojeva, to jest, svaki skup brojeva (ili tačaka), je ekvivalentan ili skupu prirodnih brojeva, 1, 2, 3, . . . ili skupu svih realnih brojeva i prema tome kontinuumu, to jest, skupu svih tačaka na pravoj; što se tiče ekvivalencije postoje, dakle, samo dva skupa brojeva, prebrojivi skup i kontinuum.[1]

Uvod

Šta je to problem kontinuuma? Navedimo prvo dve jednostavne formulacije. Koliko ima različitih podskupova skupa prirodnih brojeva? Ili, najjednostavnije: koliko ima realnih brojeva, odnosno tačaka na pravoj u euklidskom prostoru?

Ove formulacije podrazumevaju da umemo da prebrojavamo beskonačne skupove, to jest, da pojam „brojanja“ (odnosno „broja“ ili „prebrojavanja“) možemo proširiti na sasvim određen, jednoznačan, način sa konačnih na beskonačne skupove. Upravo to je, međutim, pokazao Cantor krajem XIX veka. On je smatrao da pojam broja, odnosno kardinalnog broja nekog skupa, dobijamo dvostrukom apstrakcijom: zanemarujući, prvo, prirodu elemenata tog skupa, a zatim i njihove međusobne odnose (poredak, na primer). Na osnovu toga, prirodna je sledeća definicija jednakosti kardi-

---

[1] [Hilbert 1900]

nalnih brojeva: dva skupa imaju isti kardinalni broj ako se njihovi elementi mogu dovesti u jednoznačnu korespondenciju, odnosno, koristeći savremenu terminologiju, ako postoji 1—1 funkcija koja slika jedan *na* drugi. Slično se definiše i kada je kardinalni broj $|A|$ skupa A manji ili jednak od kardinalnog broja $|B|$ skupa B, naime $|A| \leqslant |B|$ ako i samo ako postoji funkcija $f: A \to B$ koja je 1—1 (ali ne mora biti *na*)[2]. Odatle prirodno proizilazi i definicija za „strogo manje": $|A| < |B|$ akko $|A| \leqslant |B|$ i $|A| \neq |B|$. Jedan od prvih rezultata koje je Cantor dobio u ovoj novoj teoriji jeste da je broj podskupova nekog skupa uvek veći od broja njegovih elemenata, to jest, $|X| < |P(X)|$. Odatle odmah sledi, da osim prirodnih brojeva, koji su kardinalni brojevi konačnih skupova, postoji i beskonačno mnogo različitih beskonačnih kardinalnih brojeva. Takođe, pokazalo se da se aritmetičke operacije (uključujući i beskonačne sume i proizvode) mogu na potpuno prirodan način proširiti na beskonačne brojeve, očuvavajući pri tom uobičajena pravila računanja (uglavnom).

Uz pomoć aksiome izbora dobija se jedna sistematska (kanonska) reprezentacija svih beskonačnih kardinalnih brojeva (nalik na dekadnu reprezentaciju celih brojeva):

$$\aleph_0, \aleph_1, \aleph_2, \cdots, \aleph_\omega, \aleph_{\omega+1}, \ldots$$

gde je $\aleph_0$ kardinalni broj prebrojivog skupa, $\aleph_1$ najmanji neprebrojiv kardinal (prvi kardinal koji je veći od $\aleph_0$), $\aleph_2$ je najmanji kardinalni broj veći od $\aleph_1$, i slično dalje.

Sada se naš problem može preciznije izreći: kome od alefa je jednak kardinalni broj kontinuuma? Odnosno, kom alefu je jednako $2^{\aleph_0}$ ($2^{\aleph_0} = |P(N)| = |R|$). (Tako se ovaj problem pojavljuje i kao elementaran problem kardinalne aritmetike.) Cantorova hipoteza kontinuuma jeste da je:

$$(CH) \qquad 2^{\aleph_0} = \aleph_1 .$$

Prirodno uopštenje se zove Generalisana hipoteza kontinuuma:

$$(GCH) \qquad 2^{\aleph_\alpha} = \aleph_{\alpha+1} \qquad \text{(za svaki redni broj } \alpha).$$

---

[2] Cantorova notacija za kardinalni broj skupa A bila je $\overline{\overline{A}}$, gde dvostruka crta treba da asocira na dvostruku apstrakciju.

Hilbertov prvi problem onda glasi: dokazati Cantorovu hipotezu kontinuuma.

Treba naglasiti da je Hilbert očekivao pozitivno rešenje ovog problema, što se vidi već iz njegove formulacije. On je i sam kasnije pokušavao da ga reši. Čak je jednom prilikom (1925. godine, na kongresu Vestfalskog matematičkog društva) izjavio da poseduje dokaz hipoteze kontinuuma i dao jednu skicu dokaza koja, međutim, nikad nije realizovana. Prvi korak trebalo je da bude dokaz da je svaki matematički problem (u principu) rešiv, a to je trebalo da proizađe iz Hilbertovog tadašnjeg velikog projekta — teorije dokaza (vidi sledeće poglavlje, o drugom problemu). Izvodljivost tog prvog koraka postala je sasvim sumnjiva nekoliko godina kasnije, posle Gödelovih rezultata o esencijalnoj nepotpunosti formalne aritmetike (i svih jačih formalnih sistema).

Osim Hilberta veći broj vrsnih matematičara je radio na rešavanju ovog problema, ali su rezultati bili slabi. Praktično jedini konkretan doprinos, iako sasvim ograničenog dometa, bio je Königov rezultat još iz 1904: kontinuum ne može biti granična vrednost prebrojivog niza manjih kardinalnih brojeva. (To, na primer, isključuje $\aleph_\omega$ kao moguću kardinalnost kontinuuma.)

Interesantan, i u početku dosta obećavajući, bio je razvoj stvari u takozvanoj deskriptivnoj teoriji skupova, koja izučava „lepo opisane" podskupove skupa realnih brojeva shvaćenog kao topološki prostor. Još je Cantor primetio da hipoteza kontinuuma važi za zatvorene skupove: oni su ili prebrojivi ili moći kontinuuma. Hausdorff i Aleksandrov su pokazali da isto važi i za Borelove skupove[3], a Suslin je to proširio dalje i na analitičke skupove[4]. Ovakva progresija rezultata mogla je da deluje kao „empirijska" potpora hipoteze kontinuuma. Međutim, analitičkih skupova ima jako malo u odnosu na ukupan broj podskupova kontinuuma — to su sasvim specijalni i još uvek relativno pravilni podskupovi. Već kod komplemenata analitičkih skupova stvar je stala — uprkos velikim naporima, za njih kao ni za druge projektivne skupove (koji se dobijaju od analitičkih primenom operacija komplement i

---

[3] Familija Borelovih skupova se dobija zatvaranjem familije zatvorenih skupova za operacije komplement i prebrojiva unija.

[4] Analitički skupovi se dobijaju od Borelovih kada dozvolimo izvesne neprebrojive unije (operacija „fuzije"), ili ekvivalentno, analitički skupovi na pravoj su ortogonalne projekcije dvodimenzionalnih Borelovih skupova.

ortogonalna projekcija) nije bilo moguće dokazati važenje hipoteze kontinuuma. Kao što će se pokazati kasnije to je bio krajnji domet opšte prihvaćenih principa teorije skupova. Ova škola proizvela je i veliki broj hipoteza koje su ekvivalentne hipotezi kontinuuma, slede iz nje ili je povlače. Tu treba spomenuti još i Sierpińskog kao i našeg matematičara Đuru Kurepu.

U međuvremenu, od kako je prvi Hilbertov problem postavljen pa do 30-tih godina, došlo je do velikog rada na osnovama matematike. U vreme kada ga je Hilbert postavio, ovo je bio problem intuitivne, kako se danas kaže „naivne", teorije skupova. Isti smisao problem zadržava jedino ako se prihvati pristup osnovama matematike koji se naziva realizam, odnosno, u ekstremnom obliku, platonizam. Prema takvom gledištu, beskonačni skupovi objektivno postoje pa i hipoteza kontinuuma ima sasvim jasan smisao: ili je kardinalnost kontinuuma jednaka $\aleph_1$ ili nije, hipoteza je ili istinita ili lažna. Iako ovakvo shvatanje sasvim odgovara načinu na koji većina matematičara doživljava svoj predmet, realizam je već početkom veka bio dosta diskreditovan, jer takva filozofska pozicija ima ozbiljne epistemološke probleme.

U okviru koncepcije o osnovama matematike koju je razvio Brouwer, koja se zove intuicionizam, problem kontinuuma u velikoj meri gubi smisao. Prema intuicionističkom shvatanju, matematički objekti postoje samo kao konstrukcije ljudskog uma, pa prema tome teorija alefa većih od $\aleph_1$ nema nikakvo značenje, a različite, klasično ekvivalentne, formulacije hipoteze kontinuuma postaju sasvim različite tvrdnje od kojih je na neke odgovoreno pozitivno a na neke negativno.

Prema Hilbertovoj koncepciji, razvijenoj dvadesetih godina, koja se, ne sasvim adekvatno, naziva formalizam[5], beskonačni skupovi su idealni objekti, pa se onda, strogo posmatrano, ne bi moglo govoriti o istinitosti (ili lažnosti) hipoteze kontinuuma. Problem kontinuuma razume se ostaje, ali kao pitanje da li je hipoteza kontinuuma izvodljiva u okviru formalne teorije skupova. Činjenica

[5] Taj naziv zanemaruje drugi, filozofski možda važniji, aspekt Hilbertove koncepcije — finitizam. Prema toj koncepciji, ukratko, samo konačni objekti (kao prirodni brojevi) su realni i tvrdnje o njima su realni iskazi koji mogu biti istiniti ili lažni. Beskonačni objekti su idealni i služe samo za lakše ispitivanje realnih objekata (kao što se, na primer, u teoriji brojeva služimo kompleksnom analizom). Za detalje videti poglavlje o drugom problemu.

je, ipak, da je u to vreme Hilbert i dalje pridavao izuzetan značaj problemu kontinuuma. Moglo bi se možda čak tvrditi da, za razliku od Brouwera, Hilbert u ovom slučaju nije bio sasvim dosledan svojoj koncepciji i da je hipotezu kontinuuma ipak shvatao u izvesnom smislu kao realan (a ne idealan) iskaz. Naime, u već pomenutom govoru na kongresu Vestfalskog matematičkog društva on problem kontinuuma formuliše kao problem prebrojavanja tačaka nekog intervala. Treba znati, pri tom, da na drugom mestu on insistira da je pojam geometrijskog kontinuuma pojam za sebe, nezavisan od pojma broja, što znači da on može biti shvaćen kao realan objekt za razliku od beskonačnog skupa realnih brojeva, koji je prema njegovoj koncepciji nužno jedan idealan objekat. Proizilazi da je Hilbert problem prebrojavanja elemenata tog realnog objekta možda ipak smatrao realnim problemom. Posebno je ovde indikativno s kakvom se on oštrinom u Vestfalskom predavanju obara na „ . . . matematičare koji su mislili da mogu da se otarase ovog problema poričući njegovo postojanje . . . “.

U toku dvadesetih i tridesetih godina došlo je do još jednog razvoja, vrlo relevantnog za problem kontinuuma a posebno za ovakve dileme o njegovom smislu — razvijene su aksiomatske teorije skupova: Zermelo—Fraenkel (*ZF*) i Gödel—Bernays (*GB*). Ove teorije su rezultat logičke analize pojma skupa izvedenog iz predstave o kumulativnoj hijerarhiji (za razliku od teorija Fregea i Russella i Whiteheada koje polaze od ideje o podeli univerzuma u dve kategorije). Aksiome *ZF*-a i *GB*-a su sasvim precizne i dopuštaju potpunu formalizaciju. Tako je problem kontinuuma dobio i formalni — kombinatorni aspekt. Naime, postavlja se pitanje da li se formula, kojom je zapisana hipoteza kontinuuma, može izvesti u okviru formalnog sistema *ZF* (ili *GB*), a to je jedan čisto kombinatorni problem, koji se tiče manipulacije simbolima. Ovaj aspekt problema zadržava svoje značenje nezavisno od filozofske pozicije. Čak i za intuicioniste ovo je sasvim punopravan problem (iako, možda, ne mnogo interesantan).

Neprotivrečnost

To je istorijska situacija u kojoj se pojavio prvi deo odgovora na Hilbertov prvi problem. Godine 1938. K. Gödel je dokazao neprotivrečnost generalisane hipoteze kontinuuma sa aksiomama

teorije *GB*, odnosno pokazao je da ako je teorija *GB* neprotivrečna, onda se iz njenih aksioma ne može izvesti negacija *GCH*. S obzirom da su sistemi *GB* i *ZF* ekvivalentni[6], isti rezultat automatski važi i za *ZF*. Gödelov dokaz ima dva ravnopravna i nezavisna aspekta: semantički i sintaktički. Cela stvar se može ispričati kao da se radi o konstrukciji modela i dokazivanju njegovih svojstava ili kao da se radi o manipulaciji sa formulama i o određenim transformacijama formalnih dokaza. Radi boljeg razumevanja suštine dokaza, prikazaćemo ukratko oba aspekta. Nešto više tehničkih detalja može se naći u Dodatku.

Semantički posmatrano, dokaz je izveden metodom unutrašnjih modela. Ta metoda je već u XIX veku korišćena u geometriji — za dokazivanje neprotivrečnosti neeuklidskih geometrija, a takođe i u samoj teoriji skupova — prilikom izgradnje sistema *ZF* i *GB*. Osnovna ideja te metode, kojom se dokazuje *relativna* neprotivrečnost, je sledeća: pretpostavi se da je neki skup aksioma neprotivrečan, odnosno da ima model; onda se u tom modelu (ili u svakom takvom modelu) definiše neka struktura koja će biti model kako za polazni skup aksioma tako i za neku dodatnu aksiomu čija se neprotivrečnost sa polaznim skupom ispituje. Osnovna novost koju je uveo Gödel je pojam konstruktibilnog skupa — kolekcija svih konstruktibilnih skupova u datom modelu čini, sa relacijom pripadanja ($\in$), unutrašnji model u kome važi *GCH*, a takođe i aksioma izbora (*AC*). Ideja konstruktibilnih skupova je, inače, u vezi sa idejom predikativnih definicija, koja je dosta korišćena početkom veka u pokušajima da se eliminišu paradoksi iz teorije skupova. Predikativna definicija nekog objekta je takva definicija u kojoj se pominju samo objekti koji su već prethodno definisani. Impredikativna bi, na primer, bila definicija nekog podskupa prirodnih brojeva u kojoj se između ostalog pominju *svi* podskupovi prirodnih brojeva. Dosta rašireno mišljenje bilo je da je upravo slobodna upotreba impredikativnih definicija izvor paradoksa u teoriji skupova. Ideja je onda bila da se teorija skupova (i matematika uopšte) može dobro zasnovati tako što bi se odbacila pretpos-

---

[6] Teorija *ZF* ima promenljive samo za skupove, dok *GB* ima promenljive i za skupove i za klase. Precizna formulacija ove ekvivalencije glasi: *GB* je konzervativno proširenje *ZF*, tj. teoreme *GB* u kojima se pominju samo skupovi su iste kao teoreme *ZF*. Takođe, pokazano je da je pretpostavka o neprotivrečnosti teorije *ZF* ekvivalentna sa pretpostavkom o neprotivrečnosti teorije *GB*.

tavka da totalitet svih skupova postoji sam po sebi[7] već bi se tvrdila egzistencija samo onih skupova koji se mogu predikativno definisati. Pokušaji takvog zasnivanja matematike (na primer H. Weyl) dali su, međutim, samo delimično zadovoljavajuće rezultate. Ideja Gödela, koji nije prihvatao takvo ontološko stanovište, bila je drukčija. On je pokazao da se u svakom modelu teorije *GB* (ili u univerzumu svih skupova) transfinitnim ponavljanjem (preko svih ordinala) predikativnih definicija može konstruisati podmodel L u kome osim aksioma *GB* važi i vrlo jaka *aksioma konstruktibilnosti* ($V=L$), koja tvrdi da su svi skupovi konstruktibilni. Pokazuje se onda da u teoriji *GB* iz $V=L$ sledi ne samo (*GCH*) i (*AC*), već i neki jaki stavovi deskriptivne teorije skupova[8]. U radu iz 1938. Gödel je definisao ramifikovanu hijerarhiju konstruktibilnih skupova na sledeći način. Ako je skup M zadat, skup M' čine podskupovi y od M koji se mogu definisati kao

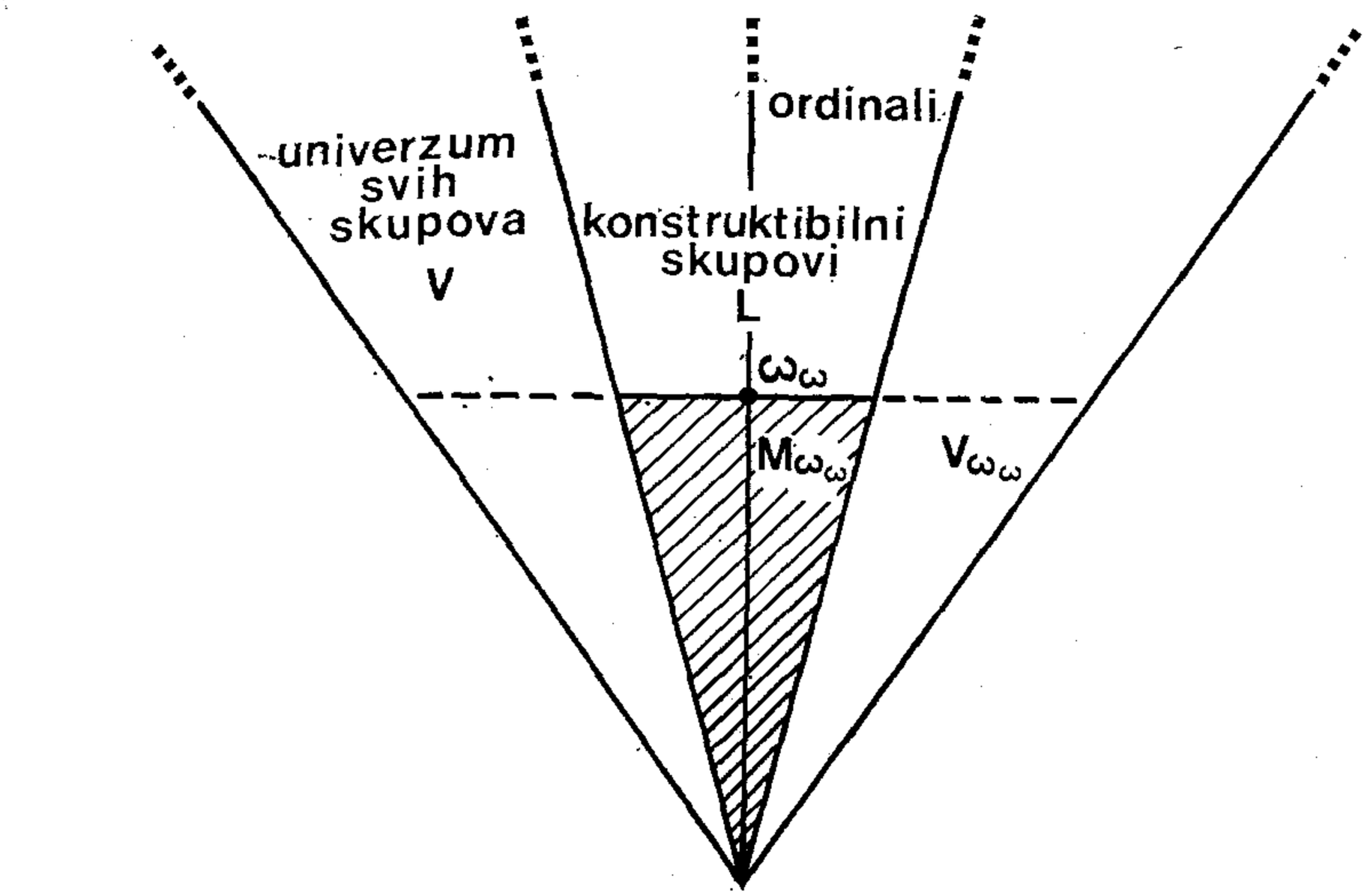
$$y=\{x\in M:\varphi(x)\}$$

za neku formulu φ koja od nelogičkih simbola sadrži relacijski znak $\in$ i konačno mnogo imena (konstanti) za elemente iz M, a svi kvantifikatori su ograničeni na M. Hijerarhija je onda definisana sa $M_o=\{\varnothing\}$, $M_{\alpha+1}=M_\alpha'$ za proizvoljan ordinal α, i za granične ordinale α, $M_\alpha=\bigcup_{\beta<\alpha} M_\beta$. Za skup x se onda kaže da je konstruktibilan ako postoji ordinal α takav da je $x\in M_\alpha$. Zatim se pokazuje da klasa svih konstruktibilnih skupova L zadovoljava aksiome teorije skupova, kao i aksiomu $V=L$, a takođe i *GCH* i *AC*. Gödel u stvari u radu iz 1938. pokazuje da je za Zermelove aksiome (uobičajene aksiome ali bez aksiome zamene, odnosno aksiome supstitucije) dovoljno posmatrati već M_{ω_ω}. Sledeća shema (str. 23) je dosta ilustrativna. Može se reći, da su konstruktibilni oni skupovi koji su sadržani u svakom modelu koji sadrži sve ordinale, odnosno, ako neki model sadrži ordinal α onda on mora sadržati i ceo M_α. Očigledno je da konstruktibilni skupovi nisu predikativni u pravom smislu reči, jer je egzistencija ordinala pretpostavljena unapred.

---

[7] Takva pretpostavka omogućava slobodnu upotrebu impredikativnih definicija.

[8] Na primer: postoji dobro uređenje kontinuuma koje je relativno jednostavno — naime, odgovarajući skup uređenih parova je projekcija komplementa analitičkog skupa $\left(\sum\nolimits_2^1\right)$.



Sintaktički posmatrano, Gödelov rezultat se može opisati ovako: pokazano je da ako postoji (formalan) dokaz kontradikcije iz $GB+V=L$ onda se taj dokaz može preraditi u dokaz kontradikcije koji koristi samo aksiome iz GB. Drugačije rečeno, ako GB nije protivrečna, ne može ni $GB+V=L$ biti protivrečna, pa onda ni $GB+GCH$ (s obzirom da $GB+V=L\vdash GCH$). Takav pristup preovlađuje u Gödelovoj monografiji [1940], koja je nastala na osnovu njegovih predavanja u Princetonu, u jesen 1938. „Važenje u modelu" ovde postaje samo govorna figura kojom se opisuju relativizirane formule. Naime, prvo se opisuje formula sa jednom promenljivom $L(x)$, čija interpretacija treba da bude „x je konstruktibilan", a zatim se definiše relativizacija formula na L koja se sastoji u ograničavanju kvantifikatora: $\exists x\psi$ se zamenjuje sa $\exists x(L(x)\wedge\psi)$, a $\forall x\psi$ se zamenjuje sa $\forall x(L(x)\rightarrow\psi)$. Pokazuje se da su relativizacije aksioma GB kao i rečenica $V=L$, teoreme u GB, tj., umesto o važenju neke aksiome u konstruktibilnom univerzumu, ovde govorimo o dokazivosti njene relativizacije u formalnoj teoriji GB. Sada se vidi kako se formalni dokaz kontradikcije (kao konačan niz formula) iz $GB+V=L$ može preraditi. Prvo se sve formule zamene njihovim relativizacijama. Aksiome koje se javljaju u dokazu postaju sada teoreme, pa je potrebno dodati njihovo iz-

vođenje iz *GB*. Isto važi i za $V=L$. Kontradikcija, međutim, ostaje i dalje kontradikcija, pa je na ovakav način dobijen dokaz kontradikcije koji koristi samo aksiome *GB*. S obzirom da $GB+V=L\vdash GCH$, sledi da ni hipoteza kontinuuma ne donosi protivrečnost ako ona nije već prisutna u *GB*. Sve isto važi, razume se, i za *ZF*.

Dok semantički pristup uvodi važan nov pojam konstruktibilnog skupa, sintaktički pristup uvodi podjednako značajne pojmove relativizacije i apsolutnosti[9] formula. Takođe, u sintaktičkom pristupu vidljiva je dalja razrada metoda kodiranja metateorije i semantike u objekt teoriji, metoda koji je uveden u dokazu nepotpunosti aritmetike.

Iako je Gödelov dokaz uveo značajne nove pojmove i moćne tehnike, sasvim u skladu sa Hilbertovim očekivanjem da je tako nešto neophodno za rešavanje problema kontinuuma, on nije doveo do življeg rada na teoriji skupova — pre bi se moglo reći suprotno. Razlozi za to su verovatno, bar delimično, psihološki. Veliki rad obavljen u deskriptivnoj teoriji skupova proizveo je izvestan broj vrlo neugodnih, kontraintuitivnih posledica hipoteze kontinuuma, tako da je počelo da preovlađuje mišljenje da je hipoteza kontinuuma možda, ipak, lažna. Moglo bi se reći, da je rad na analitičkim i projektivnim skupovima bio usmeren, bar delimično, na konstruisanje kontraprimera za *CH*. Gödel je međutim pokazao da je tako nešto nemoguće, da se negacija *CH* ne može dokazati. Tako je postala sasvim realna mogućnost da je hipoteza kontinuuma neodlučiva na osnovu postojećih aksioma teorije skupova — što uopšte nije bilo očekivano (bez obzira na Gödelove rezultate o postojanju neodlučivih stavova u aritmetici). Gödel je već 1947. izneo neke indikacije za koje je smatrao da ukazuju da je problem kontinuuma nerešiv na osnovu prihvaćenih aksioma. Takođe, pojavila se sumnja da bi i neki od otvorenih problema deskriptivne teorije skupova, koji su već godinama odolevali svim naporima, mogli da budu u istom smislu nerešivi.

S druge strane, nije se ni naslućivalo kako bi mogao da izgleda dokaz nezavisnosti. Postoje tvrdnje da je Gödel već krajem četrdesetih godina imao dokaz nezavisnosti aksiome izbora ali taj dokaz nikad nije objavljen. 1953. Shepherdson je dokazao da se po-

---

[9] Apsolutne su, grubo rečeno, one formule čije se važenje ne menja relativizacijom. Neapsolutna je, npr. formula $\exists x(\neg L(x))$.

moću uobičajene metode unutrašnjih modela ne može dokazati nezavisnost hipoteze kontinuuma (kao ni bilo koje druge hipoteze čija je neprotivrečnost dokaziva pomoću unutrašnjih modela). Znači, smanjujući neki model za *ZF* nemoguće je dobiti model za *ZF* u kome bi važilo $\neg CH$. Prema tome, jedini način koji je preostao je da se proširuju modeli.

Nezavisnost

Godine 1963, P. Cohen je uspeo da dokaže nezavisnost *CH* proširujući prebrojiv model za $ZF+V=L$ do takozvanog generičkog modela za *ZFC* u kome važi $2^{\aleph_0} \geqslant \aleph_2$. To proširenje je izvedeno na vrlo ekonomičan način, potpuno novom metodom „iznuđivanja" (*forcing*) — dodaju se samo oni novi skupovi čija je egzistencija „iznuđena aksiomama i takozvanim „uslovima" (više detalja o ovoj metodi, kao i o dokazu nezavisnosti, dato je u dodatku). Ukratko, pođe se od skupa koji u polaznom modelu *M* predstavlja kardinal $\aleph_2$ (spolja gledano, taj skup je razume se prebrojiv, kao i ceo model *M*). Za svaki element tog skupa u model se doda po jedan nov podskup prirodnih brojeva — znači, iz modela *M* gledano — $\aleph_2$ novih podskupova. Osim njih u novi model se dodaju još samo oni skupovi čija je egzistencija „iznuđena". Zahvaljujući tako štedljivom i kontrolisanom dodavanju kardinali ostaju isti, pa u novom modelu skup prirodnih brojeva ima bar $\aleph_2$ podskupova. Potpuno ista konstrukcija prolazi i za proizvoljan $\aleph_\alpha$ ($\alpha \geqslant 2$), osim, razume se, za one isključene Königovim rezultatom (vidi stranu 18). Razume se i ovi rezultati su, kao i dokaz neprotivrečnosti *CH*, relativni, tj. polazi se od pretpostavke da teorija *ZF* ima model, odnosno da je neprotivrečna.

Koliko je metoda iznuđivanja bila revolucionarna vidi se, pre svega, po tome što je vrlo mali broj specijalista koji su uspeli odmah da ovladaju metodom, za nekoliko godina dobio izvanredno mnogo rezultata — došlo je do prave eksplozije znanja. S druge strane bile su potrebne godine da nešto širi krug logičara i matematičara shvati tehničke detalje i suštinu nove metode, da razume jedan potpuno nov način mišljenja, donekle nalik na situaciju sa Gödelovim dokazom nepotpunosti aritmetike, koji je za celu generaciju, uz retke izuzetke, do kraja ostao misteriozan i sumnjiv.

Ovo će svakako biti interesantan slučaj za neku buduću istoriju ideja. Uprkos svoj neobičnosti i neočekivanosti metode iz-

nuđivanja, glavne ideje su ipak već praktično visile u vazduhu. Razni ljudi, radeći u različitim oblastima, došli su do ideja koje su u suštini vrlo slične, ali su ih primenjivali u strogo ograničenim kontekstima. Još krajem pedesetih godina Beth i Kripke razvili su semantike za intuicionističku i modalnu logiku koje su bazirane na relacijama sasvim nalik na Cohenovu relaciju iznuđivanja. Kripke je pišući svoj rad 1963., u kome prilagođava svoju semantiku sa modalne logike (za koju je ona prvobitno bila definisana) na intuicionističku logiku, već znao za Cohenove rezultate i dodao je deo u kome pokazuje kako se Cohenova relacija iznuđivanja može dobiti kao specijalan slučaj njegove. Neke ideje sasvim nalik na iznuđivanje skicirao je i Kreisel još 1959, ali one nisu nikada razvijene. Znači metoda je postojala bar nekoliko godina pre Cohena ali nikome nije na pamet padalo da bi se modeli teorije skupova mogli proširivati koristeći intuicionističku logiku (tj. njen fragment — bez implikacije i univerzalnog kvantifikatora). Ipak, treba istaći, da su i Kripkeovi rezultati bili sa svoje strane, u svojoj oblasti, revolucionarni (bar u modalnoj logici, gde je problem potpune semantike za neke modalne sisteme već dugo bio otvoren), tako da je rad na njihovom punom iskorišćavanju tek počinjao.

Osim toga, interesantan je razvoj bulovsko-vrednosnih modela[10]. Već 1965. R. Solovay je pokazao da se u bulovskom modelu može jednostavno opisati relacija iznuđivanja. Solovay i D. Scott (koji je prvi primetio vezu između Cohenove relacije i intuicionističke logike) razvili su zatim teoriju bulovskih modela teorije skupova i pokazali da su bulovski modeli i Cohenov metod dva alternativna (ekvivalentna) pristupa koji dovode do istih rezultata, iako metodički gledano, svaki ima svoje prednosti i mane[11]. Međutim, bu-

---

[10] Za razliku od uobičajenih dvovrednosnih modela, u kojima neka rečenica važi ili ne važi (ima jednu od dve istinosne vrednosti), u bulovsko-vrednosnom modelu rečenica kao istinosnu vrednost može da ima bilo koji element zadate Booleove algebre.

[11] Standardno, model teorije skupova — kumulativna hijerarhija — izgrađuje se, polazeći od praznog skupa, sukcesivnom primenom operacija partitivni skup i unija — u graničnim koracima ($V_0=\varnothing$; $V_{\alpha+1}=V_\alpha \cup P(V_\alpha)$; a za granične ordinale α, $V_\alpha = \bigcup_{\beta<\alpha} V_\beta$). Ako posmatramo podskupove nekog skupa x, svakom $y\subseteq x$ odgovara njegova karakteristična funkcija $\chi_y: x \to \{0, 1\}$ (za $z\in x$ $\chi_y(z)=1$ ako je $z\in y$, i $\chi_y(z)=0$ ako $z\notin y$), i obrnuto svakoj funkciji $f: x \to \{0, 1\}$ odgovara neki podskup od x. Jasno je da se konstrukcija modela može izvesti i koristeći karakteristične funkcije umesto podskupova. Bulovsko-vrednosni model

lovski modeli potiču još iz ranih pedesetih godina. A. Church je predložio konstrukciju bulovskih modela za teoriju tipova ali je taj predlog ostao potpuno zanemaren. Mostowski je uveo bulovske, odnosno hajtingovske modele (sa istinosnim vrednostima u Heytingovoj algebri), kao semantiku za intuicionistički predikatski račun — dosta prirodno uopštenje algebarskih semantika za iskazne račune. Taj pristup je dosta razvijala tokom pedesetih godina poljska logička škola, a naročito (pored Mostowskog) Rasiowa i Sikorski. Oni su sistematski izučavali modele sa vrednostima u Booleovoj ili Heytingovoj algebri kao i u raznim mrežama. Bulovskim modelima bavila se i škola algebarske logike (Tarski, Henkin i drugi). Međutim, svi oni su izučavali uglavnom valjanost rečenica prvog reda, to jest zadovoljenost u svim modelima, a ne zadovoljenost u jednom konkretnom modelu, pogotovo ne u modelu teorije skupova. Treba pomenuti i razvoj univerzalne algebre (Birkhoff i drugi), jer konstrukcija generičkih modela metodom iznuđivanja dosta podseća na konstrukciju slobodne algebre terma po modulu neke klase zakona.

Koliko je poznato Cohen se nije koristio tim raznorodnim rezultatima, i svoj metod je razvio potpuno nezavisno. To još više potvrđuje da je ovde u pitanju tipičan primer situacije kad, posle jednog perioda stagnacije u nekoj oblasti nauke, potpuno nov način mišljenja istovremeno sazreva u glavama najkreativnijih istraživača.

Pored nezavisnosti *CH*, Cohen je dokazao, istim metodom, i nezavisnost aksiome izbora i aksiome konstruktibilnosti ($V=L$). On je, takođe, pokazao i da kardinalnost kontinuuma može biti ne samo proizvoljno velika (što se tiče aksioma *ZF*), već i da se može sasvim proizvoljno izabrati. Naime, za svaki zadati kardinal[12] k može se konstruisati model u kome je kardinalnost kontinuuma baš k.

se dobija ako se kao karakteristične funkcije koriste funkcije koje slikaju u datu Booleovu algebru B (umesto u Booleovu algebru $\{0, 1\}$). U takvom modelu rečenice imaju kao istinosne vrednosti — elemente algebre B. Od bulovskog modela može se dobiti uobičajen model uvođenjem nekog ultrafiltera u algebru B. U novom modelu neka rečenica važi (je zadovoljena) ako, i samo ako, joj je bulovska vrednost u ultrafilteru. Sada se vidi da izborom pogodne Booleove algebre i ultrafiltera u njoj, možemo kontrolisati koje će rečenice važiti u krajnjem modelu.

[12] Jedina ograničenja su već klasična — Cantorovo: da je $k>\aleph_0$ i Königovo: da k nije prebrojiva unija manjih kardinala.

Vrlo brzo, primenom iznuđivanja i bulovskih modela, razrešen je status velikog broja starih otvorenih problema, između ostalog i Suslinove i Kurepine hipoteze, i pokazani njihovi međusobni odnosi. Što se tiče problema kontinuuma, najinteresantniji su rezultati Eastona, koji je uopštio Cohenove rezultate sa *CH* na *GCH*, i u potpunosti razrešio status regularnih kardinala[13]. On je pokazao da kada je $\aleph_\alpha$ regularan $2^{\aleph_\alpha}$ može biti praktično proizvoljno[14]. Šta više, neprotivrečno je istovremeno pretpostaviti razne takve tvrdnje (na primer, postoji model u kome je: $2^{\aleph_0}=\aleph_5$, $2^{\aleph_1}=\aleph_{17}$, ...). Drugim rečima, stepena funkcija $\aleph_\alpha \to 2^{\aleph_\alpha}$ može se ponašati sasvim haotično na regularnim kardinalima. Iako se očekivalo da slično mora važiti i za singularne kardinale, taj problem je ostao još duže vremena otvoren. Tek 1973, na opšte iznenađenje, Silver je dokazao suprotno, da vrednost stepene funkcije na singularnom kardinalu zavisi od vrednosti na manjim kardinalima, i da to sledi već iz *ZFC* (*ZF*+*AC*). Na primer, ako je $\aleph_\alpha$ singularan kardinal, kofinalnosti[15] veće od $\aleph_0$ i ako *CH* važi za većinu manjih kardinala[16], onda *CH* važi i za $\aleph_\alpha$ (tj. $2^{\aleph_\alpha}=\aleph_{\alpha+1}$) .

Zaključak i perspektive

Na kraju, možemo se pitati kakav je sada status Hilbertovog prvog problema? Interesantno je da posle svega još uvek ostaju dva pitanja:

(i) da li je problem rešen?

(ii) da li je to uopšte matematički problem?

---

[13] Kardinal k je regularan ako se ne može predstaviti kao unija (supremum) familije od manje od k kardinala, od kojih je svaki $<k$. Obrnuto, k je singularan ako se može predstaviti kao jedna takva unija, tj. postoji $\lambda<k$ i familija kardinala $\{\mu_\alpha:\alpha<\lambda\}$ takva da je za svako $\alpha<\lambda$, $\mu_\alpha<k$ a ipak $\cup\{\mu_\alpha:\alpha<\lambda\}=k$. Na primer: $\aleph_\omega=\cup\{\aleph_n:n<\omega\}$ je singularan.

[14] Königova teorema u opštem slučaju tvrdi da $2^{\aleph_\alpha}$ ne može biti unija od $\leqslant\aleph_\alpha$ kardinala koji su $<2^{\aleph_\alpha}$.

[15] Kofinalnost kardinalnog broja k, $cf\,(k)$, je najmanji λ takav da je k suma od λ kardinala manjih od k.

[16] Preciznije $\{\aleph_\beta:\beta<\alpha \text{ i } 2^{\aleph_\beta}=\aleph_{\beta+1}\}$ je stacionaran skup.

Što se tiče prvog pitanja, jasno je da ako Hilbertov prvi problem shvatimo u najužem smislu (kao na str. 20), kao formalno-kombinatorni problem izvodljivosti *CH* iz aksioma *ZF* (ili *GB*), onda je odgovor nedvosmisleno potvrdan. Šta više, ne samo da je dokazana neodlučivost *CH* na osnovu aksioma *ZF*, već je i status *GCH* detaljno ispitan i sve mogućnosti su određene, izuzimajući jedino problem singularnih kardinala prebrojive kofinalnosti.

Međutim, Gödel je, anticipirajući Cohenov rezultat, smatrao da je ipak odgovor na oba ova pitanja — ne. Kao možda jedini veliki matematičar dvadesetog veka koji je otvoreno zastupao koncepciju realizma u filozofiji matematike, on je smatrao da problem kontinuuma ima smisla i nezavisno od trenutno prihvaćenih aksioma. To što je hipoteza kontinuuma neodlučiva na osnovu aksioma samo pokazuje da su one preslabe.

Razume se, odmah se postavlja pitanje u kom smislu su aksiome preslabe, i za šta? Platonistički odgovor, da one treba da opišu jednu objektivno postojeću realnost, je filozofski neprikladan zbog epistemoloških problema. Na prirodno sledeće pitanje, kako mi dolazimo do saznanja o toj realnosti, platonizam nije u stanju da pruži zadovoljavajući odgovor. Gödel svoju poziciju gradi na jednoj umerenijoj realističkoj koncepciji. Po njemu, mi imamo sasvim jasnu intuiciju o skupovima, ali to ne mora da znači ni da baš skupovi objektivno postoje (to bi vodilo u platonizam), ni da je intuicija sposobnost neposrednog saznavanja činjenica o matematičkim objektima. Pre je u pitanju nešto sasvim posredno — kao što u našim empirijskim idejama postoje i neki apstraktni elementi.

Bez obzira koliko nam njegovi filozofski argumenti izgledali ubedljivi, činjenica da je Gödel smatrao da je aksiomama teorije skupova neophodna dopuna ne može se olako zanemariti. Pogotovu, s obzirom da je on kao i mnogi drugi dao i neke mnogo konkretnije argumente.

Pre svega, ne može se smatrati zadovoljavajućom teorija koja ostavlja neodlučenim neke relativno elementarne probleme, kao što to svakako jeste problem kardinalnosti kontinuuma, pogotovu ako je neodređenost tako drastična kao što proizilazi iz Eastonovih rezultata. I sam pojam kardinalnog broja postaje onda dosta relativan. Činjenica je i da je *CH* odlučiva u teoriji skupova drugog reda (teoriji koja osim o skupovima govori i o svojstvima skupova), iako ne znamo kako, da li je dokaziva ona ili njena negacija.

Kako bi mogla izgledati eventualna proširenja sistema *ZF*? Prvi izvor eventualnih novih aksioma su takozvani veliki kardinali. Najmanji od njih se zovu nedostižni kardinali[17]. Oni su nedostižni u smislu da se ne mogu dostići ni sumama ni proizvodima, kao ni stepenima manjih kardinala. Prvi nedostižan kardinal je $\aleph_0$. Ako na *ZF* dodamo aksiomu koja tvrdi da postoji neprebrojiv nedostižan kardinal (*NK*), dobijamo značajno proširenje polazne teorije. Kao što je poznato iz Gödelovih teorema o nepotpunosti, nijedna teorija koja sadrži aritmetiku (što podrazumeva i *ZF*) ne može dokazati svoju neprotivrečnost. Međutim, ako je k najmanji nedostižni kardinal, onda $(V_k, \in)$ (V_k je k-ti nivo kumulativne hijerarhije) čini model za *ZF*. Znači, iz $ZF + NK$ sledi neprotivrečnost *ZF*, pa prema tome *NK* ne može biti teorema *ZF*. Posebno je interesantna asimetrija između *NK* i $\neg NK$. Već pomenuti V_k je model ne samo za *ZF* već i za $\neg NK$ (jer očigledno u V_k nema nedostižnih kardinala), i to je dokazivo već u *ZF*. Ako pretpostavimo, međutim, da ne postoje nedostižni kardinali, ne dobijamo nikakve interesantne posledice, iako je i to jedno proširenje *ZF*. Šta više, za razliku od $\neg NK$, *NK* ima posledice i u aritmetici. Zahvaljujući Gödelovom kodiranju (vidi Dodatak A sledećeg poglavlja) tvrdnja konzistencije *ZF*, Con_{ZF}, je jedan aritmetički iskaz vrlo jednostavnog oblika: $\forall x A(x)$, gde je $A(n)$ odlučivo svojstvo prirodnih brojeva čije se važenje za dati broj n može proveriti računanjem.

Iznad nedostižnih kardinala definisana je, i izučavana, čitava progresija sve većih i većih velikih kardinala. Svi oni proizvode efekte nalik na efekte nedostižnih kardinala: dodavanjem aksiome o egzistenciji nekog od njih, dobija se dokaz neprotivrečnosti teorije *ZF* proširene pretpostavkama o egzistenciji velikih kardinala manjih od tog koji je u pitanju, kao i odgovarajuće nove aritmetičke teoreme. Takođe, zadržava se i asimetrija između aksiome koja tvrdi egzistenciju velikog kardinala i njene negacije. Među najviše izučavane velike kardinale spadaju merljivi kardinali. Kardinal k je merljiv ako se na $P(k)$ može definisati dvovrednosna $(0-1)$ mera μ, koja osim uobičajenih svojstava mere ima i sledeće: ako je $\mu(A_i)=0$ za svako $i\in I$ i $|I|<k$, onda i $\mu\left(\bigcup_{i\in I} A_i\right)=0$. I ovde je prvi primer $\aleph_0$, a pravo pitanje je da li postoji neprebrojiv merljiv kardinal. Aksioma

---

[17] Kardinal k je nedostižan ako je regularan i ako za svako $\lambda<k$ važi $2^\lambda<k$.

koja to tvrdi označava se sa *MK*. Iako ne spadaju u najveće velike kardinale, merljivi kardinali su toliko veliki da je bilo vrlo ozbiljnih pokušaja da se dokaže da oni ne postoje. Pre nekoliko godina je čak Jensen, jedan od najvećih autoriteta u teoriji skupova, najavio da ima dokaz da merljivi kardinali ne postoje. Srećom po izvestan broj matematičara koji su sagradili karijere na pretpostavci da merljivi kardinali postoje, ubrzo se pokazalo da je dokaz pogrešan.

Kardinali još veći od merljivih, uglavnom gube bilo kakav intuitivni smisao i aksiome o njihovom postojanju mogu se pravdati jedino uticajem koji imaju na otvorene probleme (kao i time što dodaju nove aritmetičke teoreme). Što se tiče *GCH*, međutim, efekat takvih aksioma je vrlo mali jer one, kao što se pokazalo, ne mogu da odluče *GCH* i imaju samo izvesnog posrednog uticaja. *MK* je recimo, protivrečna sa $V=L$, a u deskriptivnoj teoriji skupova ima za posledicu da se važenje hipoteze kontinuuma proširuje za još jednu stepenicu — na $\sum_2^1$ skupove (projekcije komplemenata analitičkih skupova; vidi fusnote [3] i [4]). Magidor je nedavno dokazao, koristeći aksiome o egzistenciji velikih kardinala, da Silverova teorema ne važi za singularne kardinale prebrojive kofinalnosti.

Drugi važan izvor novih aksioma su istraživanja u deskriptivnoj teoriji skupova, koja je u poslednjih dvadesetak godina doživela pravu renesansu. Do te renesanse došlo je zahvaljujući, u velikoj meri, prožimanju sa dve znatno mlađe oblasti logike, teorijom rekurzije i teorijom igara — takozvanih beskonačnih igara savršene informacije. Upravo u terminima teorije igara formulisana je tvrdnja koja je danas verovatno najozbiljniji kandidat za novu aksiomu teorije skupova — aksioma projektivne determinisanosti (*PD*). Za proizvoljan $A \subseteq {}^{\omega}\omega$[18], definiše se igra G_A na sledeći način: igrači I i II redom biraju po jedan prirodan broj. Rezultat igre je jedan beskonačan niz brojeva, element iz ${}^{\omega}\omega$. Igrač I pobeđuje ako je taj niz u A, a II pobeđuje ako niz nije u A. Kaže se da je igra determinisana ako jedan od igrača ima strategiju kojom uvek može da pobedi, pri čemu strategija ima sasvim intuitivno značenje. Pokazano je da ako je A otvoren, zatvoren, pa čak i Borelov skup, G_A je determinisano, i to je krajnji domet *ZF*. Iz

---

[18] U novije vreme, u deskriptivnoj teoriji skupova umesto realnog kontinuuma R, posmatra se Baireov prostor $\omega\omega$ koji je pogodniji za rad.

$V=L$ sledi da postoji analitička igra koja nije determinisana, dok iz *MK* sledi da su sve analitičke igre determinisane. Aksioma *PD* tvrdi da su i sve projektivne igre (kada je skup *A* projektivan) determinisane. *PD* ima vrlo ugodne posledice u deskriptivnoj teoriji skupova i to je osnovni razlog zašto je mnogi smatraju prihvatljivom. Dok je s jedne strane *PD* protivrečna sa $V=L$, s druge strane, sve pravilnosti koje se za projektivne skupove mogu dokazati uz pomoć *MK* slede i iz *PD*, kao i neke druge (recimo: svaki projektivan skup je Lebesgue—merljiv i ima Baireovo svojstvo). Te pravilnosti, međutim, ne idu u prilog hipotezi kontinuuma i oni koji smatraju *PD* prihvatljivom aksiomom, uglavnom, takođe, smatraju i da je *CH* lažna.

Ova dva pravca su najvažnija i na njima se najviše radi, ali postoje razmišljanja o proširavanju spiska aksioma teorije skupova u drugim pravcima. U svakom slučaju, posle prvog šoka, izazvanog Cohenovim i Eastonovim rezultatima, kada su se pojavila i neka, verovatno prenagljena, mišljenja o teoriji skupova kao sholastici XX veka, postepeno je preovladalo uverenje, zahvaljujući verovatno i pojavi novih ideja i pristupa, da u teoriji skupova ipak može, i treba, i dalje da se radi, između ostalog i na pronalaženju novih aksioma.

Što se tiče Hilbertovog prvog problema, iako on nije rešen na način i u smislu koji je Hilbert očekivao, iako možda, po nekim gledištima, uopšte nije ni rešen, ipak on je vrlo uspešno odigrao ulogu koju mu je Hilbert namenio. U toku više od šezdeset godina ovog veka, on je usmeravao (bar delimično) razvoj teorije skupova i neki od najvažnijih pojmova i metoda teorije skupova razvijeni su upravo za njegovo rešavanje. Čak i danas, iako možda više nije u prvom planu, problem kontinuuma ostaje jedan od najvažnijih kriterijuma za testiranje eventualnih novih aksioma teorije skupova.

DODATAK: GÖDELOV I COHENOV DOKAZ

§ 1. **Zermelo-Fraenkelova teorija skupova.** Nasuprot dosta raširenom shvatanju, teorija *ZF* nije rezultat *ad hoc* pokušaja da se iz teorije skupova eliminišu paradoksi. Ona je nastala kao rezultat logičke analize jedne intuitivno jasne koncepcije o kumulativnoj hijerarhiji skupova (iterativna koncepcija skupa). U ovom delu izložićemo prvo tu koncepciju i istorijske okolnosti njenog nastanka, a zatim opisati ukratko samu teoriju *ZF*, odnosno razvoj osnovnih pojmova teorije skupova u njoj.

Krajem devetnaestog veka (uglavnom između 1874. i 1897. godine) Georg Cantor je razvio osnovne pojmove nove matematičke discipline — teorije skupova. Pojam skupa, odnosno klase, kao i osnovne operacije: unija, presek i komplement bili su poznati i pre Cantora — na primer, Boole je uveo račun klasa još 1847. Glavna novina Cantorove teorije je omogućavanje preciznog rada sa beskonačnim skupovima — prvenstveno razlikovanje po veličini različitih beskonačnih skupova, odnosno uvođenje jedne rastuće hijerarhije različitih beskonačnosti.

Prvi pokušaj aksiomatskog zasnivanja teorije skupova potiče od Gottloba Fregea. Frege je želeo da pokaže da se aritmetika, kao i analiza, može izvesti iz logike, to jest da su teoreme aritmetike analitičke *a priori* istine. U svom životnom delu *Osnovni zakoni aritmetike* [1893], Frege definiše prirodne brojeve kao, u suštini, kardinalne brojeve izvesnih konačnih skupova, i pokazuje kako se teoreme aritmetike mogu izvesti iz nekih osnovnih osobina skupova. S druge strane, skup definiše kao obim (ekstenziju) pojma, tako da sve potrebne osobine skupova slede iz osnovnih principa logike formulisanih u pet postulata („osnovnih zakona"). Može se reći da je ta koncepcija skupa zasnovana na intuiciji o podeli univerzuma na dve klase: skup svih mogućih objekata koji spadaju u obim datog pojma (tj. koji imaju neko zadato svojstvo) i skup svih onih objekata koji ne spadaju u obim tog pojma.

Međutim, 1902. godine, neposredno pred izlazak iz štampe drugog toma Fregeovih *Osnovnih zakona aritmetike*, Bertrand Russell je pokazao da je Fregeov sistem protivrečan (čuveni Russellov paradoks). U međuvremenu, već 1895. Cantor je uočio da se u njegovoj intuitivno formulisanoj teoriji pojavljuje paradoks (takozvani Burali-Forti paradoks). Tokom sledećih desetak godina otkriven je veliki broj različitih paradoksa.

S obzirom na značaj u zasnivanju matematike, koji je teorija skupova već bila stekla, pojava paradoksa je izazvala velike rasprave. Javile su se različite teze o poreklu paradoksa i načinima za njihovu eliminaciju. Kao problematični su označeni: nepredikativne definicije, suviše veliki skupovi (kao skup svih skupova, skup svih ordinala i sl.), aktualna beskonačnost, pa čak, i cela teorija skupova.

U takvoj situaciji javio se Ernst Zermelo 1908. godine jednim novim pristupom. Suština njegove ideje je da skupovi koji se javljaju u matematici nisu zasnovani na intuiciji o podeli univerzuma svih mogućih objekata na dva dela (skup svih objekata koji imaju zadato svojstvo i skup svih onih koji ga nemaju), već na predstavi o postepenoj, kumulativnoj izgradnji skupova polazeći od nekih unapred zadatih objekata — urelemenata (praelemenata), pri čemu neki skup može kao elemente sadržati samo skupove koji su izgrađeni pre njega. Znači na prvom stupnju skupovi se grade kao sve moguće kolekcije urelemenata (na nultom, polaznom, stupnju imamo samo urelemente). Na drugom stupnju se grade skupovi koji su kolekcije urelemenata i skupova prvog stupnja itd. Zermelove aksiome predstavljaju, u stvari, opis svojstava ovako izgrađenih skupova (doprinos Fraenkela je prvenstveno u dodavanju aksiome zamene). Russellova teorija tipova, koja se prvi put pojavila iste 1908. godine, zasnovana je na vrlo sličnoj koncepciji, s tim što kod Russella hijerarhija igra važnu ulogu u teoriji, dok se u Zermelovoj jednostavnoj teoriji hijerarhija gubi a ostaju samo skupovi dobijeni pomoću hijerarhije.

Ubrzo se pokazalo da urelementi nisu neophodni i da se svi skupovi koji se javljaju u matematici mogu izgraditi polazeći od praznog skupa. Prema tome, predstava o kumulativnoj hijerarhiji skupova koja odgovara teoriji *ZF* može se opisati ovako.

Skupovi se izgrađuju u stupnjevima. Među stupnjevima postoji poredak i za svaki stupanj postoji stupanj koji je neposredno posle njega. Na polaznom, nultom, stupnju imamo samo prazan

skup. Na stupnju S, od svake kolekcije skupova koji su napravljeni pre S pravimo skup. Ovo je dovoljno za izgradnju konačnih skupova, ali postavlja se pitanje: ako je x neka kolekcija skupova, a S kolekcija odgovarajućih stupnjeva, tj. svaki skup y iz kolekcije x napravljen je na nekom stupnju Sy iz kolekcije S, da li postoji stupanj koji je posle svih stupnjeva iz S? Shoenfield, kao i mnogi drugi, smatra da je odgovor *da*, ukoliko možemo zamisliti situaciju u kojoj su svi stupnjevi iz S već završeni. Jedan takav slučaj je kada je kolekcija S neki beskonačan niz $S_0, S_1, \ldots$. Onda, na stupnju koji dolazi posle svih tih stupnjeva, od kolekcije x možemo napraviti skup. Ovo je dovoljno za Zermelove aksiome. Međutim, za opravdanje aksiome zamene neophodno je prihvatiti i slučaj kada je S kolekcija stupnjeva indeksirana nekim skupom, tj. postoji neki *skup* z i za svaki $y \in z$ stupanj Sy, tako da je S baš kolekcija svih stupnjeva Sy za $y \in z$. Mora se priznati da se ovde već pomalo gubi neposredna intuitivna jasnost, ali dosta čvrsta motivacija ipak postoji. Ako je z skup, znači da je formiran na nekom stupnju i taj stupanj dolazi posle svih stupnjeva na kojima su pravljeni elementi od z, tj. svi ti stupnjevi su završeni. Analogno tome, možemo, onda, zamisliti situaciju u kojoj su svi stupnjevi Sy (za y iz z) već završeni i onda je prirodno očekivati jedan stupaj koji dolazi posle svih njih — analogno stupnju na kome je z napravljen.

§ 2. Aksiome *ZF*. Teorija *ZF* (Zermelo-Fraenkel) je formulisana u predikatskom računu prvog reda sa jednakošću. Od nelogičkih simbola ova teorija ima samo binarni relacijski simbol $\in$. Aksiome su univerzalna zatvorenja sledećih formula:

A1. *aksioma ekstenzionalnosti*

$$x = y \leftrightarrow \forall z\,(z \in x \leftrightarrow z \in y);$$

intuitivno, dva skupa su jednaka akko su im jednaki elementi;

A2. *aksioma praznog skupa* ($\varnothing$)

$$\exists x \forall y\,(\neg y \in x);$$

A3. *aksioma neuređenog para* ($\{x, y\}$)

$$\exists z \forall u\,(u \in z \leftrightarrow u = x \vee u = y);$$

A4. *aksioma unije* $(\bigcup x)$

$$\exists z \forall u (u \in z \leftrightarrow \exists v (u \in v \wedge v \in x));$$

A5. *aksioma partitivnog skupa* $(P(x))$

$$\exists z \forall u (u \in z \leftrightarrow \forall v (v \in u \rightarrow v \in x));$$

A6. *aksioma beskonačnosti* (ω)

$$\exists x (\varnothing \in x \wedge \forall y (y \in x \rightarrow y \cup \{y\} \in x);$$

A7. *aksioma regularnosti*

$$\forall x (x = \varnothing \vee \exists y (y \in x \wedge \neg \exists z (z \in x \wedge z \in y)));$$

$A8_{(\varphi)}$ *shema aksioma zamene*

$$\forall x \exists! y \varphi(x, y) \rightarrow \forall u \exists v \forall y (y \in v \leftrightarrow \exists x (x \in u \wedge \varphi(x, y)))$$

(ako je $f(x) = y$ funkcija definisana formulom φ, onda za svaki skup u, $\{f(x) : x \in u\}$ je skup);

A9. *aksioma izbora*

$$\forall x \exists y (\text{„}y : x \rightarrow \bigcup x\text{“} \wedge \forall z \in x (z \neq \varnothing \rightarrow y(z) \in z)).$$

Sa *ZF* označavamo teoriju koja uključuje aksiome A1—A8, a sa *ZFC* teoriju koja uključuje i aksiomu izbora.

Aksioma izbora je jedina aksioma teorije skupova koju su i nelogičari od početka zvali aksiomom (ostale aksiome su valjda smatrane „istinama o skupovima“). Ona je bila sumnjiva zbog svog izrazito nekonstruktivnog karaktera. Dok ostale aksiome (osim A7 koja je tehničkog karaktera — obezbeđuje da uređenje ordinala bude dobro zasnovano) tvrde egzistenciju skupova za koje je očigledno kako se mogu konstruisati, polazeći od nekih već zadatih skupova, aksioma izbora tvrdi egzistenciju izbornih funkcija za koje u mnogim konkretnim slučajevima uopšte nije jasno kako (i da li) se mogu konstruisati. Klasičan primer je dobro uređenje skupa realnih brojeva. Međutim, veliki delovi savremene matematike izgledali bi sasvim drugačije bez aksiome izbora, naročito u topologiji, algebri, funkcionalnoj analizi i teoriji mere. Čak i tako elementarna stvar kao što je ekvivalencija, u realnoj analizi, dveju definicija granične tačke (preko nizova i preko okolina) neposredno zavisi od

aksiome izbora. Konstruisan je i model teorije skupova u kome aksioma izbora ne važi i u kome te dve definicije granične tačke nisu ekvivalentne.

Aksioma izbora se najčešće koristi u nekom od sledećih ekvivalentnih oblika:

Multiplikativna aksioma

Direktan proizvod nepraznih skupova je neprazan.

Zermelova teorema o dobrom uređenju

Svaki skup se može dobro urediti.
(Dobro uređenje skupa X je linearno uređenje u kojem svaki neprazan podskup od X ima najmanji element.)

Zornova lema

Ako u parcijalno uređenom skupu $(P, \leqslant)$ svaki lanac (linearno uređen podskup) ima gornju među, onda skup P ima maksimalan element (neki $x \in P$ takav da za svako $p \in P$ $(\neg x < p)$).

Neki primeri poznatijih teorema koje se dokazuju uz pomoć aksiome izbora su:

u topologiji: Tihonovljeva (Tychonoff) teorema, Stone-Čech kompaktifikacija, Radoova lema selekcije;

u funkcionalnoj analizi: Hahn-Banachova teorema o produženju linearnih funkcionala;

u algebri: teoreme o egzistenciji maksimalnih ideala (ultrafiltera) u bulovima algebrama, teorema o egzistenciji baze vektorskog prostora;

u logici: teorema kompaktnosti;

u teoriji mere: osnovna svojstva Borelovih skupova i Lebesgueove mere.

U samoj teoriji skupova, teorija kardinalnih brojeva bi, na primer, bila sasvim haotična bez aksiome izbora. Između ostalog, ne bi se moglo dokazati čak ni da kontinuum nije prebrojiva unija prebrojivih skupova. Za našu temu, prvi Hilbertov problem, posebno je interesantno da su i Cantor i Hilbert smatrali da bi važan

korak u dokazu hipoteze kontinuuma mogla da bude konstrukcija nekog dobrog uređenja realnih brojeva.

Uobičajene operacije, svojstva i relacije skupova mogu se definisati formulama u *ZFC*. Na primer, ordinali su tranzitivni skupovi (x je tranzitivan ako $y\in x$ povlači $y\subseteq x$) koji su potpuno uređeni relacijom $\in$. Odgovarajuća formula $On(x)$ je:

$$\forall y\,(y\in x\to y\subseteq x)\wedge\forall y,\,z\,(y\in x\wedge z\in x\to y\in z\vee y=z\vee z\in y),$$

pri čemu je $y\subseteq x$ zamena za formulu $\forall z\,(z\in y\to z\in x)$. Možemo definicijama uvesti i konstante:

$$0=\varnothing,\ 1=\{\varnothing\},\ 2=\{0,\,1\},\ 3=\{0,\,1,\,2\},\ \ldots,\ \omega=\{0,\,1,\,2,\,\ldots\},$$

$$\omega+1=\omega\cup\{\omega\},\ \ldots,\ \alpha,\ \alpha+1,\ \ldots$$

U stvari, ω se uvodi definicijom:

$$x=\omega\Leftrightarrow_{df}[\varnothing\in x\wedge\forall y\,(y\in x\to y\cup\{y\}\in x)]\wedge\forall z\,[(\varnothing\in z\wedge$$

$$\wedge\forall y\,(y\in z\to y\cup\{y\}\in z))\to z=x\vee x\subseteq z],$$

a da je baš $\omega=\{0,\,1,\,2,\,\ldots\}$ se dokazuje.

Poredak ordinala je definisan sa $\alpha<\beta\leftrightarrow\alpha\in\beta$. Zahvaljujući aksiomi regularnosti (A7) to je jedno dobro uređenje.

Ordinal α je nasledni ako zadovoljava $\exists\beta\in\alpha\,(\alpha=\beta\cup\{\beta\})$, a α je granični ordinal ako zadovoljava:

$$Lim(\alpha)\Leftrightarrow_{df}On(\alpha)\wedge\alpha\neq0\wedge\forall x\in\alpha\,(x\cup\{x\}\in\alpha).$$

Biti funkcija, $F_n(f)$, je opisano sledećom formulom:

$$\forall x\,(x\in f\to\exists u,\,v\,(x=\langle u,\,v\rangle))\wedge\forall u,\,v,\,w\,(\langle u,\,v\rangle\in f\wedge\langle u,\,w\rangle\in f\to$$

$$\to v=w)\qquad(\langle u,\,v\rangle=_{df}\{\{u\},\,\{u,\,v\}\}).$$

Slično se definišu i pojmovi „biti 1—1 funkcija“, „biti funkcija iz A u (*na*) B“ itd. Na primer:

$$„f\colon A\to B“\Leftrightarrow_{df}Fn(f)\wedge\forall w\in f\,\exists x\in A\,\exists y\in B\,(w=\langle x,\,y\rangle)\wedge$$

$$\wedge\forall x\in A\,\exists y\in B\,(\langle x,\,y\rangle\in f).$$

Ordinal α je kardinal ako se ne može preslikati 1—1 funkcijom u manji ordinal:

$$Kard(\alpha) \Leftrightarrow_{df} On(\alpha) \wedge \neg \exists f \exists \beta (On(\beta) \wedge \beta \subseteq \alpha \wedge Fn(f) \wedge$$

$$\wedge \text{„}f \text{ je } 1-1\text{“} \wedge \text{„}f: \alpha \to \beta\text{“}).$$

Za dalju izgradnju pojmova teorije skupova u okviru *ZFC* veoma je značajna sledeća matateorema koja se naziva teorema rekurzije ili teorema transfinitne indukcije. Intuitivna ideja, zasnovana na kumulativnoj hijerarhiji, je da analogno definiciji pomoću rekurzije u aritmetici, definišemo funkciju F na ordinalima tako što $F(\alpha)$ određujemo uz pomoć vrednosti $F(\beta)$ za $\beta < \alpha$ i neke već poznate funkcije G.

Teorema rekurzije

Ako je G neka funkcija, postoji jedinstvena funkcija F definisana na ordinalima, takva da je

$$F(\alpha) = G(F \restriction \alpha),$$

gde je $F \restriction \alpha = \{\langle \beta, F(\beta)\rangle : \beta \in \alpha\}$.

Ovo je najjednostavnija formulacija teoreme. U najopštijem obliku, i formalizovana u okviru *ZFC*, teorema glasi:

Za svaku formulu $\psi(x, x_1, \ldots, x_n, y)$ postoji formula $\varphi(x_1, \ldots, x_n, y)$ takva da je sledeće dokazivo u *ZFC*

$$\forall x \forall x_1 \ldots \forall x_n \exists! y \psi(x, x_1, \ldots, x_n, y) \to$$

$$[\forall x_1 \ldots \forall x_n \exists! y \varphi(x_1, \ldots, x_n, y) \wedge$$

$$\forall x_1 \ldots \forall x_n \forall y (\varphi(x_1, \ldots, x_n, y) \leftrightarrow \psi(\{\langle x_1', \ldots, x_n', y'\rangle : x_1' \in x_1, \ldots, x_n' \in x_n, y' \in y, \varphi_1(x_1', \ldots, x_n', y')\}, x_1, \ldots, x_n, y))].$$

Pomoću ove teoreme, možemo sada rekonstruisati kumulativnu hijerarhijú u okviru *ZFC*. Naime, definišemo funkciju

$$V_\alpha = \bigcup \{P(V_\beta) : \beta \in \alpha\}.$$

Sada ordinale možemo posmatrati kao stupnjeve, a za skup x kažemo da je formiran na stupnju α ako je $x \subseteq V_\alpha$.

Koristeći teoremu rekurzije mogu se definisati i alefi — kao funkcije koje slikaju ordinale u kardinale. Prvo se dokaže da za svaki kardinal k postoji najmanji kardinal k^+ veći od njega, odnosno da je funkcija k^+ dobro definisana. Onda se definiše:

$$\aleph(0) = \omega$$

$$\aleph(\alpha + 1) = (\aleph(\alpha))^+$$

$\aleph(\beta) = \cup\{(\aleph\alpha) : \alpha < \beta\}$ ako je β granični ordinal, s tim što obično pišemo $\aleph_\alpha$ umesto $\aleph(\alpha)$.

Model teorije *ZFC* je par (M, E), gde je M neki skup ili klasa a $E \subseteq M^2$ (interpretacija simbola $\in$), takav da su u njemu zadovoljene sve aksiome *ZFC*. Pri tom se relacija zadovoljenja ($\models$) definiše na uobičajeni način. Recimo, za $a, b \in M$:

$$(M, E) \models a \in b \quad \text{akko} \quad (a, b) \in E$$

$$(M, E) \models a = b \quad \text{akko} \quad a \cap M = b \cap M$$

itd.

Model (M, E) se zove standardni model ako je E baš relacija pripadanja ograničena na M ($(a, b) \in E$ akko $a, b \in M$ i $a \in b$). Uglavnom se izučavaju samo standardni modeli i onda umesto (M, E) pišemo M. Ukoliko je M tranzitivan skup ili klasa, onda se model zove tranzitivnim.

Primetimo da ako je klasa M definabilna, tj. ako za neku formulu $\varphi(x)$ teorija skupova važi: $x \in M$ akko $\varphi(x)$, onda se relacija $M \models \psi$ može predstaviti formulom teorije skupova. Na primer:

$$M \models \forall x \exists y (x \in y) \quad \leftrightarrow_{df} \quad \forall x (\varphi(x) \rightarrow \exists y (\varphi(y) \wedge x \in y)).$$

Uopšte, „$M \models \psi$“ se dobija od ψ ograničavanjem svih kvantifikatora na M (tj. na definicionu formulu $\varphi(x)$). Prema tome, ako je ψ ograničena formula (svi kvantifikatori su već ograničeni) i ako je M tranzitivna klasa, onda za svako $x_1, \ldots, x_n \in M$ važi

$$*) \qquad (M \models \psi(x_1, \ldots x_n)) \leftrightarrow \psi(x_1, \ldots x_n)$$

(to jest, to je teorema *ZFC*)

Za proizvoljnu formulu ψ, ako (*) važi, kaže se da je ψ apsolutna za M. Pokazuje se da su Δ_1 formule apsolutne za tranzitivne modele *ZFC*. ψ je Δ_1 ako postoje formule $\exists x \varphi(x)$ i $\forall x \chi(x)$, gde su φ i χ ograničene formule, takve da $ZFC \vdash \psi \leftrightarrow \exists x \varphi(x)$ i $ZFC \vdash \psi \leftrightarrow \forall x \chi(x)$. Na primer, formule $On(x)$, $Tran(x)$ (x je tranzitivan), $Fn(x)$, $Lim(x)$ su Δ_1 formule. Formule $Kard(x)$, $y = P(x)$, „x je prebrojiv“ (to jest formula $\exists f(Fn(f) \wedge$ „$f: \omega \to x$“ $\wedge$ „f je 1—1“)) nisu Δ_1. $Kard(x)$ je Π_1 formula (tj. ekvivalentna je, u *ZFC*, nekoj formuli oblika $\forall y \chi(y)$, gde je χ ograničena formula), a za te formule važi: $\varphi \to (M \vDash \varphi)$.

„x je prebrojiv“ je Σ_1 formula (tj. ekvivalentna je nekoj formuli $\exists y \psi(y)$, gde je ψ ograničena), a za njih važi:

$$(M \vDash \varphi) \to \varphi.$$

§ 3. **Neprotivrečnost.** Za svaki skup M definišemo skup svih podskupova od M koji se mogu „predikativno“ definisati polazeći od M:

$$M' = \{y: \text{ za neku formulu } \varphi \text{ i neko } x_1, \ldots x_n \in M,$$

$$y = \{x \in M : M \vDash \varphi(x, x_1, \ldots, x_n)\}\}.$$

Brzo se vidi da ako je M tranzitivan, onda je $M \subseteq M'$ (jer $x \in M$ povlači $x = \{z \in M : M \vDash z \in x\} \in M'$).

Konstruktibilna hijerarhija:

$$L_0 = \varnothing$$

$$L_{\alpha+1} = (L_\alpha)'$$

$$L_\alpha = \bigcup_{\beta \in \alpha} L_\beta \quad \text{ako je ordinal } \alpha \text{ granični}$$

$$L = \bigcup \{L_\alpha : \mathrm{On}(\alpha)\}.$$

Aksioma konstruktibilnosti ($V = L$):

$$\forall x \exists \alpha (x \in L_\alpha).$$

Osobine hijerarhije L_α:

1) $\alpha<\beta \to L_\alpha \subset L_\beta$:

2) svaki L_α je tranzitivan skup;

3) $L_\alpha \in L_{\alpha+1}$;

4) $\alpha \subseteq L_\alpha$;

5) α je najmanji ordinal koji nije u L_α;

6) $|L_{\alpha+1}| = |L_\alpha|$ za $\alpha \geqslant \omega$;

7) ako je α granični ordinal, $|L_\alpha| = |\alpha|$.

Da je L_α jedna funkcija definisana na ordinalima i da se može predstaviti formulom u *ZFC*, dokazuje se uz pomoć teoreme rekurzije. Znači da je za svaku formulu φ, „$L \vDash \varphi$“ jedna formula koja se dobija relativizovanjem svih kvantifikatora u φ na formulu $\exists \alpha (x \in L_\alpha)$ (to ćemo kraće pisati $L(x)$). Šta više, koristeći kodiranje formula konačnim skupovima, sasvim nalik na Gödelovo kodiranje u aritmetici (vidi Dodatak A poglavlja o drugom Hilbertovom problemu), može se pokazati da je formula $(x \in L_\alpha)$ jedna Δ_1 formula, pa je znači apsolutna za tranzitivne modele *ZFC*.

Teorema.

(i) $L \vDash ZF$

(ii) $L \vDash AC$

(iii) $L \vDash V = L$

(iv) $L \vDash GCH$.

Dokaz. (i) se dokazuje neposrednom proverom. Za primer pokazujemo $L \vDash$ A3. Treba pokazati:

$$\forall x \forall y (x \in L \wedge y \in L \to \exists z \in L \forall u \in L (u \in z \leftrightarrow u = x \vee u = y)).$$

Neka su $x, y \in L$. Sledi da postoje ordinali α i β takvi da $x \in L_\alpha$ i $y \in L_\beta$. Neka je $\alpha \leqslant \beta$. Onda $x, y \in L_\beta$. Onda je

$$\{x, y\} = \{z \in L_\beta : L_\beta \vDash (z = x \vee z = y)\} \in L_{\beta+1}.$$

(ii) se dokazuje tako što se dobro uredi cela klasa L. S obzirom na dobro uređenje ordinala, prvo se svaki element iz L_α proglasi manjim od svakog elementa iz $L_\beta - L_\alpha$ za $\beta > \alpha$. Zatim se, induktivno, dobro uređuju elementi iz $L_{\alpha+1}$ koristeći pretpostavku da su elementi iz L_α već dobro uređeni. Po definiciji je $L_{\alpha+1} = (L_\alpha)'$, pa je znači svaki $y \in L_{\alpha+1} - L_\alpha$ oblika $y = \{x \in L_\alpha : L_\alpha \models \varphi(x, x_1, \ldots, x_n)\}$ za neku formulu φ i neke $x_1, \ldots, x_n \in L_\alpha$. S obzirom da se sve formule mogu dobro urediti kao i n-torke elemenata iz L_α, neposredno dobijamo dobro uređenje elemenata iz $L_{\alpha+1} - L_\alpha$. Za stare elemente, iz L_α, zadržavamo staro uređenje.

(iii) Treba pokazati $L \models \forall x \exists \alpha (x \in L_\alpha)$, to jest

$$\forall x \in L \ \exists \alpha \in L (L \models On(\alpha) \wedge x \in L_\alpha).$$

Već smo istakli da je formula $x \in L_\alpha$ apsolutna za tranzitivne modele *ZFC*, što L jeste na osnovu (i) i (ii). I formula $On(\alpha)$ je apsolutna za L jer je, kao što smo videli, ograničena. Takođe, L sadrži sve ordinale pa onda očigledno za $x \in L$ postoji ordinal $\alpha \in L$, tako da $L \models x \in L_\alpha$.

(iv) Treba pokazati da za svaki ordinal α, $L \models 2^{\aleph_\alpha} = \aleph_{\alpha+1}$. Koristi se sledeća lema: ako $L \models Kard(k)$ i ako za neki $\alpha < k$ $x \subseteq L_\alpha$, onda $x \in L_k$.

Pretpostavimo sad $L \models x \subseteq \omega_\alpha$. Pošto je $\omega_\alpha \subseteq L_{\omega_\alpha}$, sledi $x \subseteq L_{\omega_\alpha}$. Lako je proveriti da $Kard(k) \to (L \models Kard(k))$, pa prema tome $L \models Kard(\omega_{\alpha+1})$. Na osnovu leme, sledi onda $x \in L_{\omega_{\alpha+1}}$.

Znači $L \models P(L\omega_\alpha) \subseteq L_{\omega_{\alpha+1}}$. Međutim, $|L_{\omega_{\alpha+1}}| = |\omega_{\alpha+1}| = \aleph_{\alpha+1}$, pa prema tome $L \models 2^{\aleph_\alpha} = \aleph_{\alpha+1}$.

§ 4. Nezavisnost. Suština Cohenovog metoda je da se polazeći od jednog prebrojivog tranzitivnog modela $M \models ZFC$ konstruiše njegovo proširenje N, takođe model za *ZFC*, koji uz to ima još neke poželjne osobine (recimo, u njemu ne važi *GCH*). Ta konstrukcija, u opštem slučaju, ima dva ključna momenta:

(1) Konstrukcija je izvodljiva u okviru polaznog modela M. Svi novi elementi su kodirani nekim imenima. Prvo uvedemo imena

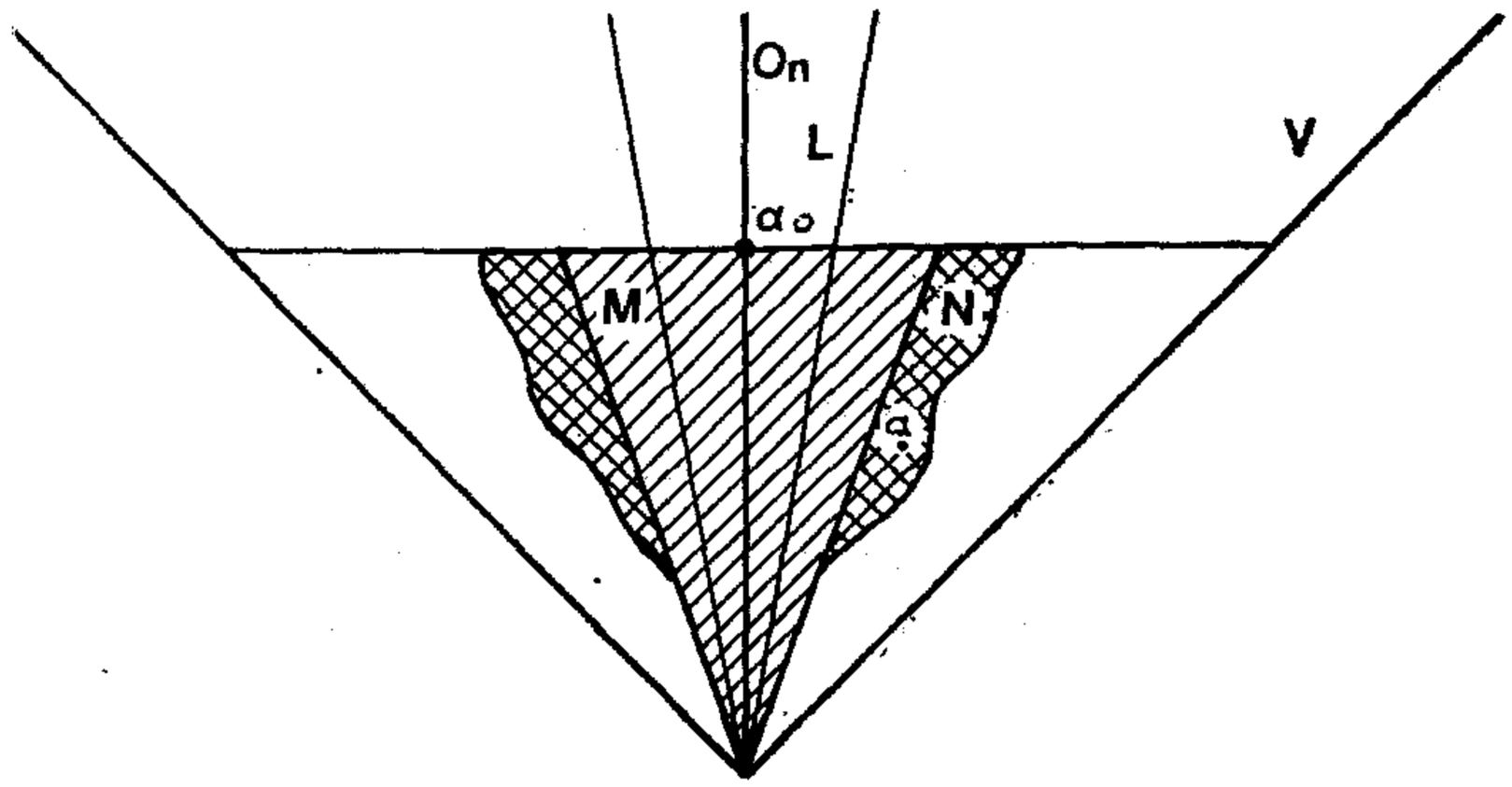
(simbole konstanti) za neke nove skupove koji su nam potrebni da bi obezbedili da novi model ima poželjne osobine. Međutim, ako smo dodali neki novi skup a, novi model N mora sadržati i sve skupove koji se, na osnovu aksioma, mogu konstruisati od a — recimo $\{a\}$, $\bigcup a$, $P(a)$ itd. Takođe, ako je $x \in M$, u N moraju biti i $a \cup x$, $a \cap x$, $\{a, x\}$, $\langle a, x\rangle$, $a \times x$ i slično. Kao imena tih skupova koristiće se kôdovi definicionih formula. Opšti pristup je da, osim tih skupova koje je neophodno dodati (da bi N bio model za *ZFC*), ne dodajemo ništa drugo.

(2) Osobine novog modela se u napred određuju pomoću *uslova* (konačnih skupova atomskih i negiranih atomskih rečenica) i *relacije iznuđivanja* $\Vdash$ *(forcing)*, koja je relacija između uslova i rečenica.

Relacija iznuđivanja je nalik na relacije $\vdash$ („sintaktička posledica“) i $\models$ („semantička posledica“), relacije između nekog skupa hipoteza i njihovih logičkih posledica. Međutim, za relaciju iznuđivanja ne važi klasična logika već jedna vrsta intuicionističke logike. To je u vezi sa štedljivošću u dodavanju novih skupova — na primer, egzistencijalna rečenica $\exists x \varphi(x)$ je iznuđena samo ako je $\varphi(c)$ iznuđeno za neko c, gde je c jedno od imena pomenutih pod (1). Uslove posmatramo kao fragmentarne konačne informacije o novim objektima (koji stari objekti, elementi polaznog modela M, jesu elementi novog skupa a, i koji nisu).Relaciju $p \Vdash \varphi$ (p je uslov, φ rečenica) možemo intuitivno shvatiti kao: „informacije sadržane u p iznuđuju da u novom, generičkom, modelu važi φ“. Ova relacija se, takođe, definiše u polaznom modelu M — zahvaljujući kodiranju.

Sam novi model N dobija se konstrukcijom koja je sasvim nalik na neke konstrukcije u algebri, kao što je konstrukcija slobodne algebre terma nad nekim skupom generatora po modulu neke klase zakona, ili specijalnije, konstrukcija prstena polinoma nad datim poljem. Umesto skupa terma, napravljenih od generatora i operacijskih simbola, ovde imamo skup definicionih formula napravljenih od imena za elemente polaznog modela i novih konstanti. Umesto relacije ekvivalencije među termima koja proističe iz zakona, ovde je relacija ekvivalencije određena relacijom iznuđivanja: dva „terma“ (konstante ili definicione formule) određuju isti skup u novom modelu ako je to iznuđeno uslovima i aksiomama *ZF*.

Odnos između polaznog modela M, novog modela N, klase ordinala On i univerzuma skupova V ilustrovan je sledećim crtežom:



Imena

Skup imena S sadrži imena za nove elemente koje dodajemo, imena za stare elemente (iz M), kao i imena za nove elemente koji na osnovu aksioma mogu od njih da se konstruišu. Kao imena ovih poslednjih možemo uzeti, na primer, kôdove (u Gödelovom smislu) formula kojima su oni definisani. Ako je α_0 najmanji ordinal koji nije u M ($\alpha_0 = M \cap On$), S možemo definisati induktivno u α_0 koraka, imitirajući definiciju konstruktibilne hijerarhije, s tim što polazimo od skupa imena za nove elemente i imena za elemente iz M.

Uslovi

Uslovi su, kao što smo rekli, konačni skupovi rečenica. U primerima koje ćemo ovde razmatrati, to su rečenice oblika $(n \in a)$ i $(n \notin a)$, gde je a ime za novi podskup od ω, a $n \in \omega$. Odmah vidimo da se uslovi mogu kodirati konačnim funkcijama $p : \omega \to \{0, 1\}$, tj. p je konačan podskup od $\omega \times \{0, 1\}$. Na taj način je $p \in M$. Šta više, i skup svih uslova P je element modela M, pa i relacija poretka $\subseteq$ na P (za $p, q \in P$, $p \subseteq q$ se shvata bukvalno kao skupovna inkluzija a p i q kao skupovi uređenih parova). Znači $(P, \subseteq) \in M$. U opštem slučaju, kao skup uslova može se uzeti proizvoljan neprazan parcijalno uređen skup $(P, \leqslant) \in M$.

Za skup $D \subseteq P$ kaže se da je *gust* u P ako za svaki $p \in P$ postoji $q \in D$ tako da je $p \leqslant q$ (u odgovarajućoj uređajnoj topologiji (bazni otvoreni skupovi su $0_p = \{q : p \leqslant q\}$) — D je stvarno gust).

Neprazan skup $I \subseteq P$ je *ideal* u P ako:

(i) $p \in I$, $q \leqslant p$ povlači $q \in I$,

(ii) $p, q \in I$ povlači da postoji $r \in I$ tako da je $p \leqslant r$ i $q \leqslant r$.

Ideal $G \subseteq P$ se zove *generički skup uslova nad* M ako za svaki $D \in M$ koji je gust podskup od P važi $G \cap D \neq \varnothing$.

Kao što će se videti, generički skup uslova u potpunosti određuje nove elemente modela N, tako da se N obeležava i sa $M[G]$.

Relacija iznuđivanja $\Vdash$

Ako je p uslov, a φ rečenica koja može da sadrži konstante iz S, relaciju $p \Vdash \varphi$ definišemo indukcijom po složenosti rečenice φ.

1) a) Ako je $\varphi = (n \in a)$ gde je a ime novog (generičkog) elementa, a n ime nekog elementa iz M (u našem slučaju prirodnog broja), onda
$p \Vdash n \in a$ *akko* $(n \in a) \in p$ (preciznije, $p(n) = 1$).

b) Ako je $\varphi = c \in d$ gde su c i d imena elemenata iz M, onda $p \Vdash c \in d$ *akko* $M \models c \in d$.

c) Ako je $\varphi = c \in d$ gde je c ime nekog elementa iz M a d kôd definicione formule $\psi(x)$ (za neki skup konstruktibilan od novih elemenata), onda
$p \Vdash c \in d$ *akko* $p \Vdash \psi(c)$.

2) $p \Vdash \exists x \psi(x)$ *akko* za neko $c \in S$ $p \Vdash \psi(c)$.

3) $p \Vdash \psi \vee \chi$ *akko* $p \Vdash \psi$ ili $p \Vdash \chi$.

4) $p \Vdash \neg \psi$ *akko* za svako $q \in P$ za koje je $p \leqslant q$, *nije* $q \Vdash \psi$.

S obzirom da su ostali logički veznici ($\wedge$, $\forall$, $\rightarrow$, $\leftrightarrow$) definisani pomoću $\exists$, $\wedge$, $\neg$, ove klauzule su dovoljne. Definicija za $p \Vdash c = d$ sledi iz aksiome ekstenzionalnosti.

Razmotrićemo prvo jedan jednostavniji primer — dodavanje jednog novog skupa prirodnih brojeva u polazni model. Znači, neka je $M \models ZFC$ jedan prebrojiv tranzitivan model. Dodaćemo mu neki skup $a \subseteq \omega$ takav da $a \notin M$. Uslovi će biti sve konačne funkcije iz M koje slikaju prirodne brojeve u skup $\{0, 1\}$, to jest $p \in P$ ako je $p \subseteq \omega \times \{0, 1\}$ konačan i $p \in M$ i $M \models Fn(p)$. Uslove možemo shvatiti kao konačne parčiće karakterističnih funkcija. Odmah se vidi da je $(P, \subseteq) \in M$. S obzirom da je M prebrojiv, postoji generički skup uslova $G \subseteq P$. (U opštem slučaju potrebno je dokazati da za dati skup uslova $(P, \leqslant)$ postoji generički skup. Takođe, u opštem slučaju, ne mora biti $G \in M$, ali je uvek $G \in M[G] = N$.)

Lako se pokazuje da svaki generički skup G određuje jedan novi podskup od ω, onaj čija je karakteristična funkcija $f = \bigcup G$:

(i) $f: \omega \to \{0, 1\}$.

Za svaki $n \in \omega$, $D_n = \{p \in P : n \in dom(p)\}$ je jedan gust podskup od P (i $D_n \in M$), jer za proizvoljan $p \in P$, ako $n \notin dom(p)$, onda $p \subseteq \subseteq p \cup \{\langle n, 0\rangle\} \in D_n$ ($dom(p) = \{n \in \omega : \langle n, 0\rangle \in p$ ili $\langle n, 1\rangle \in p\}$). Sledi $G \cap D_n \neq \varnothing$, pa prema tome $dom(f) = \omega$. Da je skup uređenih parova f jedna funkcija, sledi iz definicije ideala.

Neka je $a = \{n: \langle n, 1\rangle \in f\}$. Očigledno $a \subseteq \omega$ ali

(ii) $a \notin M$.

Jer, ako je $b \in M$ proizvoljan podskup od ω u M, postoji u M gust skup $D_b = \{p \in P : p \not\subset \chi_b\}$ (χ_b je karakteristična funkcija za b). D_b je gust jer za proizvoljan $p \in P$, ako $p \subseteq \chi_b$, s obzirom da je p konačan, postoji $n \in \omega$ tako da $n \notin dom(p)$. Ako je $\chi_b(n) = 0$, onda $p \subseteq p \cup \{\langle n, 1\rangle\} \in D_b$. Sledi $G \cap D_b \neq \varnothing$, to jest, postoji $n \in \omega$ tako da je $f(n) \neq \chi_b(n)$. Znači $a \neq b$.

Sada je jasno kako bi mogao da ide dokaz nezavisnosti *GCH*. Treba samo istovremeno dodati bar $\aleph_2$ ovakvih novih podskupova od ω. Ovde je, razume se, $\aleph_2$ ono što model M „misli“ da je $\aleph_2$; spolja gledano, to je jedan prebrojiv ordinal, kao što je i sam M prebrojiv.

Neka je sada k jedan kardinal u M veći od $\aleph_1$, to jest, za neki

$$\alpha \geqslant 2,\ M \models Kard(k) \wedge k = \aleph_\alpha^!.$$

Konstruišemo model $M[G]$ takav da

$$M \subseteq M[G],$$
$$M[G] \models ZFC,$$
$$M[G] \models 2^{\aleph_0} \geqslant k.$$

Neka je P skup svih konačnih funkcija p takvih da je

(i) $dom(p)\subseteq k\times\omega$

(ii) $p(\alpha, n)\in\{0, 1\}$ za svako $\alpha\in k$, $n\in\omega$.

$(P, \subseteq)$ će nam biti skup uslova. Jasno je da $(P, \subseteq)\in M$. Neka je G jedan generički skup uslova. Pokazujemo da G potpuno određuje k različitih podskupova od ω. Neka je $f=\bigcup G$. Slično kao ranije, pokazuje se da je f funkcija i da je $dom(f)=k\times\omega$ (jedino sada posmatramo guste podskupove $D_{(\alpha, n)}=\{p\in P: (\alpha, n)\in dom(p)\}$, za $\alpha\in k$, $n\in\omega$). Za svako $\alpha\in k$ definišemo funkciju $f_\alpha:\omega\to\{0, 1\}$ sa

$$f_\alpha(n)=f(\alpha, n).$$

Očigledno je f_α karakteristična funkcija nekog skupa

$$a_\alpha=\{n\in\omega: f_\alpha(n)=1\}.$$

Potpuno isto kao u prethodnom slučaju, pokazuje se da $a_\alpha\notin M$. Šta više, ako su $\alpha, \beta\in k$ i $\alpha\neq\beta$, onda $a_\alpha\neq a_\beta$. To važi jer u M postoji gust podskup od P: $D_{(\alpha, \beta)}=\{p\in P:$ za neko $n\in\omega$ je $p(\alpha, n)\neq p(\beta, n)\}$. Znači $G\cap D_{(\alpha, \beta)}\neq\varnothing$, pa prema tome, za neko $n\in\omega$, $f_\alpha(n)\neq f_\beta(n)$, to jest $a_\alpha\neq a_\beta$.

Sada je jasno kako treba definisati skup imena S. Neka je $\{c_x: x\in M\}$ skup imena za elemente iz M, i neka je α_0 najmanji ordinal koji nije u M. Neka je za formule definisano neko kodiranje u M: $\varphi\to\ulcorner\varphi\urcorner$, gde je $\ulcorner\varphi\urcorner\in M$.

$$S_0=\{a_\alpha: \alpha\in k\}\cup\{c_x: x\in M\},$$

$$S_{\alpha+1}=\{\ulcorner\varphi(x)\urcorner: \varphi(x) \text{ je formula sa jednom slobodnom promenljivom na jeziku } S_\alpha\},$$

$$S_\alpha=\bigcup_{\beta<\alpha} S_\beta, \quad \text{ako je } \alpha \text{ granični ordinal},$$

$$S=\bigcup_{\alpha<\alpha_0} S_\alpha.$$

Elemente novog modela $M[G]$ dobijamo induktivno od elemenata iz S. Ako je $a_\alpha\in S_0$ onda $\bar{a}_\alpha=\{n\in\omega:$ za neko $p\in G$, $p(\alpha, n)=1\}$. Za $x\in M$ je $\bar{c}_x=x$.

Ako je $\ulcorner\varphi(x)\urcorner\in S_\alpha$, onda $\ulcorner\overline{\varphi(x)}\urcorner=\{\bar{c}: c\in S_\beta$ za neko $\beta<\alpha$ i postoji $p\in G$ tako da $p\Vdash\varphi(c)\}$. Definiše se na kraju: $M[G]=\{\bar{s}: s\in S\}$.

Odmah vidimo da je $M \subseteq M[G]$ i

$$\bar{a}_\alpha \in M[G] \quad \text{za svako} \quad \alpha \in k.$$

Pošto model $M[G]$ treba da bude standardan, definiše se

$$M[G] \models c_1 \in c_2 \text{ akko } \bar{c}_1 \in \bar{c}_2.$$

Međutim, pokazuje se da to važi ako, i samo ako, postoji neki $p \in G$ tako da $p \Vdash c_1 \in c_2$. Šta više, za svaku rečenicu φ (sa konstantama iz S) pokazuje se indukcijom po složenosti φ da važi:

$$M[G] \models \varphi \quad \text{akko} \quad \text{za neko } p \in G, \quad p \Vdash \varphi.$$

Vidimo da je na taj način, s obzirom da su uslovi p u M, važenje u novom modelu $M[G]$ kontrolisano iz starog modela M.

Onaj ko poznaje teoriju modela primetiće da je teorija $T = \{\varphi : \varphi$ je rečenica na jeziku S i za neko $p \in G$, $p \Vdash \varphi\}$, u stvari jedna henkinovska teorija (potpuna, sa skupom svedoka S). Model $M[G]$ je baš njen kanonski model, napravljen od konstanti iz S.

Jednostavno se proverava da $M[G] \models ZFC$. Dokaz je sasvim nalik na dokaz da $L \models ZFC$.

Očigledno je da $M[G] \models a_\alpha \subseteq \omega$ i

$$M[G] \models \forall\, \alpha;\ \beta \in k\, (\alpha \neq \beta \to a_\alpha \neq a_\beta).$$

(Pretpostavimo $M[G] \models \alpha, \beta \in k \wedge \alpha \neq \beta$. Neka je $p \in G \cap D_{(\alpha, \beta)}$. Onda $p \Vdash \neg\, a_\alpha = a_\beta$.)

Prema tome, ostaje još da pokažemo da je k i dalje isti kardinal koji je bio u M, to jest,

$$M[G] \models Kard(k) \wedge k = \aleph_\alpha.$$

To sledi iz dve leme koje navodimo bez dokaza.

Definicija. Dva elementa p i q parcijalno uređenog skupa $(P, \leqslant)$ su *inkompatibilna* ako ne postoji $r \in P$ takav da je $p \leqslant r$ i $q \leqslant r$.

Skup $W \subseteq P$ je *inkompatibilan* ako su mu svaka dva elementa inkompatibilna.

Lema 1. Ako je P definisan kao gore (skup svih konačnih funkcija koje slikaju $k \times \omega$ u $\{0, 1\}$), onda je svaki inkompatibilan podskup od $(P, \subseteq)$ najviše prebrojiv.

Lema 2. Ako skup uslova P ne sadrži neprebrojiv inkompatibilan podskup, onda modeli M i $M[G]$ imaju iste kardinale.

Znači da naš model $M[G]$ ima bar $\aleph_\alpha$ različitih skupova prirodnih brojeva ($\alpha \geqslant 2$), pa prema tome u njemu ne važi hipoteza kontinuuma. Jedino ograničenje za k je ono koje proističe iz Königovog rezultata, k nije prebrojive kofinalnosti. Tako onda, istim metodom, možemo konstruisati modele u kojima je kontinuum proizvoljno veliki.

BIBLIOGRAFSKE BELEŠKE

Detaljniji prikaz konstruktibilnih skupova može se naći u svakoj savremenoj knjizi (udžbeniku) iz teorije skupova. Na srpskohrvatskom postoji prevod jedne takve knjige [Krivine 1972].

Cohenov metod iznuđivanja (*forcing*) i dokazi nezavisnosti prikazuju se u udžbenicima nešto višeg nivoa, kao što je [Kunen 1980]. Knjiga [Jech 1978] predstavlja enciklopediju rezultata i tehnika, uključujući i najnovije.

Na ruskom jeziku postoji prevod knjige [Shoenfield 1967] koji uključuje i prevod Shoenfieldovog rada [1971] koji je izvor savremenih (slegnutih) prikaza metode iznuđivanja.

Knjiga [Bell 1977] predstavlja najpristupačniji uvod u bulovske modele, uključujući i dokaze nezavisnosti *GCH* i *AC*.

Sažeti i jasni prikazi novijih rezultata mogu se naći u knjizi [Barwise 1977]. Posebno skrećemo pažnju na članke J. Shoenfielda (*Axioms of Set Theory*), J. P. Burgessa (*Forcing*) i D. Martina (*Descriptive Set Theory*).

Prikaz intuitivnih predstava na kojima je zasnovana teorija *ZFC* dat je u [Boolos 1971]. Što se tiče filozofskih problema, preporučujemo zbornik [Benacerraf, Putnam 1964], gde je preštampan veći broj „klasičnih" tekstova, uključujući i Gödelov *What is Cantor's Continuum Problem*, kao i Hilbertovo saopštenje na kongresu Vestfalskog matematičkog društva, pod naslovom *On the Infinite* (ovo predavanje je preštampano u engleskom prevodu i u [van Heijenoort 1967]).

II DRUGI HILBERTOV PROBLEM

Neprotivrečnost aritmetike

Uvod

Drugi problem koji je postavio na svetskom matematičkom kongresu 1900. godine Hilbert je formulisao ovako:

> „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.“[1]

Aksiome koje je Hilbert imao u vidu na kongresu odnose se na aritmetiku realnih brojeva: to su aksiome polja, aksiome uređenja, Arhimedova aksioma, i jedna dosta neobična aksioma koja garantuje da se sistem ne može dalje širiti (v. [Hilbert 1899], § 13). Kasnije, a naročito počevši od dvadesetih godina ovog veka, problem je shvaćen kao da se odnosi, pre svega, na aritmetiku u pravom smislu te reči, tj. na teoriju prirodnih brojeva i Peanove aksiome. Tek pošto bi problem bio rešen za tu aritmetiku, prešlo bi se na teorije realnih brojeva i analizu.

Kada je formulisao ovaj problem Hilbert je izgleda imao sledeću motivaciju. U devetnaestom veku izvršena je aritmetizacija matematike, tj. analiza je svedena na aritmetiku sa nešto teorije skupova. Tako se pitanje konzistentnosti (neprotivrečnosti) čitave matematike svodi na pitanje konzistentnosti aritmetike. A pitanje konzistentnosti matematike je za Hilberta važno zato što je on, početkom veka, verovao da je u matematici tvrditi da je neka teorija istinita isto što i tvrditi da je neprotivrečna. Odatle dobijamo da je dovoljno da utvrdimo neprotivrečnost neke matematičke teorije da bismo mogli da tvrdimo da objekti o kojima govori ta teorija postoje. Gledište slično ovom imao je i Poincaré.

---

[1] [Hilbert 1900]

Problem konzistentnosti aritmetike bio je posebno težak, i zato ga je Hilbert izdvojio na kongresu, jer nije bilo jasno kako prići tom problemu. Hilbert ne očekuje za aritmetiku dokaz konzistentnosti dobijen pomoću interpretacije u nekoj drugoj teoriji, za koju verujemo da je neprotivrečna, onako kao što se konzistentnost geometrije može utvrditi interpretacijom u teoriji realnih brojeva. Za aritmetiku, koja je osnovna matematička teorija, traži se *direktan* dokaz. Četiri godine posle kongresa, Hilbert je u jednom radu dao indikacije kako bi se taj direktan dokaz mogao sprovesti. Da bismo dokazali da sve formule u klasi aritmetičkih teorema imaju neko svojstvo, treba da utvrdimo da aksiome imaju to svojstvo i da pravila zaključivanja čuvaju to svojstvo. Kada se radi o dokazu konzistentnosti, svojstvo koje ispitujemo je, na primer, da formula nema oblik $1=0$. Uz klasičnu logiku, ako je neka protivrečnost dokaziva, dokaziva je i bilo koja formula, pa prema tome i $1=0$ (u klasičnom iskaznom računu važi *ako p i ne p, onda q*); i obrnuto, ako je $1=0$ dokazivo, dobijamo protivrečnost, jer je dokazivo i $1\neq 0$.

Ovaj način dokazivanja konzistentnosti aritmetike je prototip budućih pokušaja da se reši drugi Hilbertov problem. On pretpostavlja da je izvršena izvesna formalizacija aritmetike, tj. da je aritmetika data kao *formalni sistem.* To znači da se jezik aritmetike svodi na efektivno dat skup formula, a teoreme aritmetike se dobijaju tako što je efektivno dat skup aksioma i pravila zaključivanja. Ovaj pojam efektivnosti je sasvim precizno određen u teoriji rekurzivnih funkcija (v. Dodatak B poglavlja o desetom Hilbertovom problemu). Da je neki skup efektivno dat znači intuitivno da postoji procedura, algoritam, kojim se u konačno mnogo koraka može odlučiti da li nešto pripada tom skupu ili ne pripada. Skup formula obično nije konačan, a ni skup aksioma i pravila zaključivanja ne mora biti konačan, ali mora biti *odlučivo* (u konačno mnogo koraka) da li je nešto element tih skupova. Teoreme formalnog sistema su sve formule do kojih se može doći, polazeći od aksioma, konačnim brojem primena pravila zaključivanja, tj. sve formule za koje postoji dokaz u tom formalnom sistemu.

Najvažniji sistem koji formalizuje aritmetiku naziva se *Peanova aritmetika prvog reda,* ili *formalna Peanova aritmetika,* ili jednostavno *formalna aritmetika.* On je dobijen proširivanjem klasičnog računa predikata prvog reda Peanovim aksiomama (detaljniji opis ovog sistema dat je u § 1 Dodatka A ovog poglavlja). Tu formalizaciju

aritmetike, koja se zasniva na formalizaciji logike koju je započeo Frege, Hilbert će detaljno izvesti tek dvadesetih godina ovog veka. Ali tada se Hilbertovo gledište o osnovama matematike nešto promenilo (delimično zbog kritike Brouwera i intuicionista), i mada se on ništa manje ne interesuje za konzistentnost aritmetike, ovaj problem dobija posebno mesto u jednoj složenijoj teoriji koja se naziva *Hilbertovim programom*, ili *Hilbertovom teorijom dokaza*, ili još *metamatematikom*.

Hilbertov program

Mada u radovima u kojima formuliše svoj program Hilbert, tu i tamo, i dalje izjavljuje da je istinitost u matematici isto što i neprotivrečnost, izgleda da ova teza nema više smisla sama za sebe. Sada je treba shvatiti u kontekstu drugih, složenijih gledišta, a ta gledišta se mogu izreći i bez te teze.

Da bismo bolje razumeli mesto Hilbertovog programa među filozofijama matematike, daćemo prvo jednu klasifikaciju tih filozofija. Ova klasifikacija, koja se zasniva na kriterijima teorije značenja, možda nije jedina moguća klasifikacija filozofija matematike, ali je pogodna da se odredi mesto Hilbertovog programa.

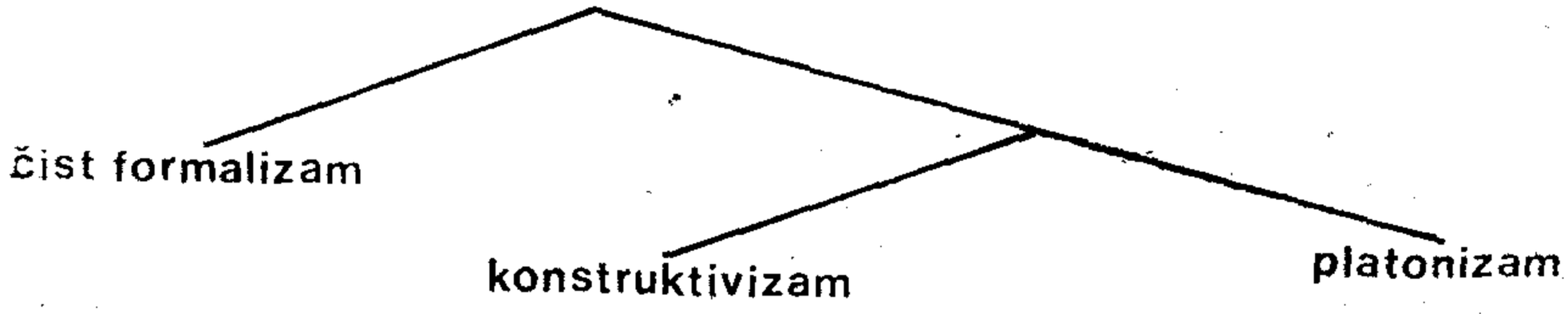
Ako na pitanje da li se matematički iskazi odnose na nešto, da li im kao jezičkim objektima odgovara nešto što oni opisuju, odgovorimo sa *ne*, dobijamo gledište koje se može nazvati *čistim formalizmom*. Ovo gledište je dosledno zastupao Curry, jedan od tvoraca kombinatorne logike. Inače je izgleda češća situacija u kojoj se neko gledište samo donekle približava čistom formalizmu. Tako mu je po nekim svojim idejama blizak Hilbert, a osim njega, na primer, Poincaré, ili Bourbaki. Čisti formalist će prirodno biti sklon tvrđenju da se za matematičke iskaze ne postavlja toliko pitanje njihove istinitosti koliko pitanje njihove korisnosti.

Ako na pitanje da li se matematički iskazi odnose na nešto odgovorimo sa *da*, moguće je dalje tvrditi da je ono što ti iskazi opisuju nešto čije postojanje zavisi od ljudskog uma, nešto što taj um konstruiše. Ovde se pretpostavlja da ljudski um može konstruisati samo nešto konačno. Prema tome, beskonačnost u matematici je samo potencijalna, a ne aktualna, kao što to pretpostavlja klasična matematika. Ovo gledište se naziva *konstruktivizmom*, i pod njega potpadaju ne samo intuicionisti, nego i druge škole koje su

htele da manje ili više ograniče sredstva klasične matematike. Konstruktivisti će prirodno zameniti interesovanje za istinitost matematičkih iskaza interesovanjem za njihovu dokazivost.

Ako, međutim, tvrdimo da postojanje onog što opisuju matematički iskazi ne zavisi od ljudskog uma, da je to nešto što ljudski um ne konstruiše, nego samo saznaje, manje ili više dobro, i ako uz to tvrdimo da je beskonačnost u matematici aktualna, onda dobijamo gledište koje se naziva *platonizmom*. Takvo je gledište, na primer, zastupao Gödel. To nije gledište oko kojeg postoji neka organizovana škola, kao oko intuicionizma — to je gledište na koje je upućena velika većina matematičara, budući da prihvata klasičnu logiku i izvesna nekonstruktivna sredstva klasične matematike, a u isto vreme smatra da se za matematičke iskaze postavlja pitanje njihove istinitosti ili neistinitosti. Osim toga, većina logičara je upućena na platonizam zato što je teorija modela dominantna logička disciplina, a ta disciplina je po mnogo čemu u duhu platonizma. Samo se platonista u pravom smislu reči interesuje za istinitost matematičkih iskaza, a ne za neko drugo svojstvo tih iskaza.

Slika koju dobijamo je znači sledeća:



Logicizam, gledište koje tvrdi da se matematika svodi na logiku, nije obuhvaćen ovom klasifikacijom. Istorijski gledano, logicisti Frege i Russell su bili platonisti. Međutim, moguće je zamisliti i formalistički logicizam, koji bi tvrdio da je logika čista sintaksa. Na prvi pogled, čist formalizam pre odgovara logici nego matematici.

Formalizam koji Hilbert zastupa u svom programu je negde između čistog formalizma i konstruktivizma, a s druge strane on se slaže s platonizmom u prihvatanju sredstava klasične matematike. (Možda ga je između ostalog i ovakva solomonska pozicija činila primamljivim.)

Cilj Hilbertovog programa je da eliminiše beskonačnost iz matematike. Kao što je Weierstrass eliminisao beskonačno male i

beskonačno velike iz analize, Hilbert će eliminisati ono što ostaje od beskonačnosti kad npr. govorimo o beskonačnim nizovima ili kvantifikujemo preko svih prirodnih brojeva. Eliminisati beskonačnost ne znači zabraniti pozivanje na nju, nego samo pokazati da je ona *korisna fikcija*. Eliminisanje beskonačnosti nije odbacivanje metodâ klasične matematke, nego njihovo opravdavanje.

Matematičke izkaze koji se ne pozivaju na beskonačnost Hilbert naziva *finitarnima*, a matematiku u kojoj se javljaju samo takvi iskazi *finitističkom*. Ti pojmovi su kod Hilberta objašnjeni samo intuitivno. Ako se traži precizna kodifikacija, onda je finitističku matematiku najbolje zamišljati kao *Skolemovu primitivno rekurzivnu aritmetiku*, ili nešto veoma slično tome. (To je implicirano i u Hilbertovim i Bernaysovim *Osnovama matematike*, u I tomu [1934], kada se raspravlja o primitivno rekurzivnoj aritmetici.) U primitivno rekurzivnoj aritmetici nemamo kvantifikatorâ, i teoreme su samo formule formalne aritmetike sa slobodnim promenljivima ili bez promenljivih. Dozvoljeno je korišćenje primitivno rekurzivnih definicija za uvođenje novih funkcija ili predikata (v. § 3 Dodatka B trećeg poglavlja), i korišćenje pravila matematičke indukcije. Ograničeni kvantifikatori se mogu uvesti kao skraćenice za konjunkcije i disjunkcije. Primitivno rekurzivna aritmetika ima znatno slabiju izražajnu moć od Peanove aritmetike prvog reda; ona je ne samo pravi podsistem Peanove aritmetike, nego i pravi podsistem *Heytingove (intuicionističke) aritmetike* (za ovu poslednju aritmetiku v. § 1 Dodatka A ovog poglavlja). Za Hilberta se jedino finitistička matematika odnosi na nešto: njen predmet su konačni *grafički* konstrukti ljudskog uma, kao, na primer, članovi niza

$$|,\ ||,\ |||,\ \ldots$$

U tome se Hilbert slaže sa konstruktivizmom, i tu je on čak striktniji od intuicionista. Finitizam je veoma striktni konstruktivizam, u kojem se matematički objekti zamišljaju kao da postoje u prostoru i vremenu, tako da su njihova svojstva proverljiva direktnim opažanjem. Ono što te objekte čini matematičkim je to što kod njih naš um apstrahuje sve osim činjenice da su ti objekti jednaki ili različiti.

Ali ograničiti matematiku na finitističku bilo bi za Hilberta sakaćenje. Zato, kao što u geometriji, radi jednostavnosti i lakoće, uvodimo tačke u beskonačnosti, tako i finitističku matematiku širimo *idealnim* iskazima koji se pozivaju na beskonačnost. Ti iskazi,

sa kojima unosimo i čitavu klasičnu matematiku, se u stvari ne odnose ni na šta, i zbog toga je Hilbert formalista. Sa Hilbertovim programom se dobija nešto što umnogome podseća na interpretacije naučnih teorija u kojima se razlikuju empirijski (kod Hilberta finitarni) od teorijskih (kod Hilberta idealnih) iskaza, pri čemu teorijski iskazi služe samo kao instrumenti za dedukovanje empirijskih.

Uvođenje idealnih iskaza Hilbert je nameravao da opravda u dva koraka. Pretpostavimo da se radi o idealnim iskazima aritmetike, tj. teorije prirodnih brojeva. U prvom koraku treba formalizovati aritmetiku: svakom intuitivnom aritmetičkom dokazu, bez obzira da li se poziva na beskonačnost ili ne, sada treba da odgovara dokaz u formalnoj Peanovoj aritmetici. Sam taj dokaz je jedan konačan grafički objekt koji se može ispitivati u finitističkoj matematici. Među formulama formalne aritmetike, one koje su formule primitivno rekurzivne aritmetike (ili nečeg veoma sličnog) nazivaće se finitarnima, a ostale idealnima. Primitivno rekurzivna aritmetika predstavlja finitistički deo formalne aritmetike. Taj deo formalne aritmetike kodifikuje celu finitističku matematiku.

Može se dogoditi da u dokazu neke finitarne formule u formalnoj aritmetici koristimo i neke idealne formule. U drugom koraku treba da pokažemo da se takvi dokazi mogu eliminisati i zameniti dokazima istih teorema u primitivno rekurzivnoj aritmetici. Drugim rečima, treba da pokažemo da je formalna aritmetika *konzervativna ekstenzija* svog finitističkog dela. Ako to uspemo, pokazaćemo da svakoj finitarnoj formuli dokazivoj u formalnoj aritmetici odgovara iskaz koji je finitistički tačan. Taj dokaz konzervativnosti odvija se u metajeziku formalne aritmetike, i treba i sam da bude finitistički da bi bio potpuno uverljiv: inače bismo u opravdavanju uvođenja idealnih iskaza već pretpostavljali da je opravdano uvesti te iskaze. Tako treba da pokažemo da je dodavanje idealnih iskaza finitističkoj matematici opravdano jer je bezopasno: ono ne daje nove istine na jeziku finitističke matematike. A nemamo razloga da ne prihvatimo nešto što daje odlične rezultate, a bezopasno je.

Neka φ bude formula finitističkog dela formalne aritmetike, neka $\vdash_F \varphi$ znači da je φ dokazivo u tom delu, a neka $\vdash \varphi$ znači da je φ dokazivo u formalnoj aritmetici. Onda se teorema konzervativnosti koju tražimo u drugom koraku gore može zapisati na sledeći način:

$$\text{(Cnsr)} \quad \vdash \varphi \Rightarrow \vdash_F \varphi.$$

Hilbert, međutim, ne preporučuje da se direktno utvrdi (Cnsr), nego umesto toga traži da se utvrdi konzistentnost formalne aritmetike, tj.

(Cnst) *ne* ($\vdash\varphi$ *i* $\vdash\neg\varphi$).

(Pošto iz $\vdash\psi$ *i* $\vdash\neg\psi$ sledi da je bilo koja formula dokaziva u formalnoj aritmetici, (Cnst) je ekvivalentno sa *ne* ($\vdash\psi$ *i* $\vdash\neg\psi$), gde je ψ proizvoljna formula formalne aritmetike, a ne nužno finitarna.) Tu Hilbert čini izvestan skok i ne razlikuje utvrđivanje (Cnsr) od utvrđivanja (Cnst). Da bi se taj skok opravdao mora se nekako rekonstruisati Hilbertovo rezonovanje. (U prikazima Hilbertovog programa ovaj skok često nije sasvim jasan.) Pokušaćemo da pokažemo da je uz neke pretpostavke, za koje je moguće da ih je Hilbert imao na umu, (Cnsr) ekvivalentno sa (Cnst).

U sledećim pretpostavkama φ' će biti neka formula dobijena iz φ zamenom slobodnih promenljivih konstantama, ili sâmo φ ako φ nema promenljivih:

(1) *ne* ($\vdash_F\varphi$ *i* $\vdash_F\neg\varphi$);

(2) *ne* $\vdash_F\varphi \Rightarrow \vdash_F\neg\varphi'$, *za neko* φ';

(3) $\vdash\varphi \Rightarrow \vdash\varphi'$;

(4) $\vdash_F\varphi \Rightarrow \vdash\varphi$.

Pretpostavka (1) tvrdi da je finitistički deo formalne aritmetike konzistentan, a pretpostavka (2) tvrdi da je taj deo na izvestan način potpun. Pretpostavka (3) je prirodna logička pretpostavka. Pretpostavka (4) tvrdi da formalna aritmetika sadrži svoj finitistički deo.

Pretpostavimo da važi (Cnsr); onda (Cnst) možemo dokazati na sledeći način:

$$\begin{aligned} \vdash\varphi \Rightarrow\ & \vdash_F\varphi && \text{(Cnsr)}\\ \Rightarrow\ & ne \vdash_F\neg\varphi && \text{(1)}\\ \Rightarrow\ & ne \vdash\neg\varphi && \text{(Cnsr).} \end{aligned}$$

Sada pretpostavimo da važi (Cnst); onda (Cnsr) možemo dokazati na sledeći način:

$$\begin{aligned} \vdash\varphi \ \ i \ \ ne \vdash_F\varphi \Rightarrow\ & \vdash\varphi \ \ i \ \ \vdash_F\neg\varphi' && \text{(2)}\\ \Rightarrow\ & \vdash\varphi' \ \ i \ \ \vdash_F\neg\varphi' && \text{(3)}\\ \Rightarrow\ & \vdash\varphi' \ \ i \ \ \vdash\neg\varphi' && \text{(4);} \end{aligned}$$

pošto uz (Cnst) $\vdash\varphi$ *i ne* $\vdash_F\varphi$ implicira protivrečnost, sledi

$$\vdash\varphi \Rightarrow \vdash_F\varphi.$$

(Jedino u poslednjem koraku koristimo jedan princip klasične iskazne logike koji ne važi intuicionistički u opštem slučaju, ali možda važi u ovom finitističkom rezonovanju u metajeziku formalne aritmetike. Primetimo još da u ovom dokazu ekvivalencije (Cnsr) i (Cnst) ne koristimo nikakva specijalna svojstva formalne aritmetike, tako da se ta ekvivalencija može dokazati i za bilo koji sistem koji sadrži jedan konzistentan i potpun podsistem.)

Bez obzira da li je rezonovao ovako ili nekako drukčije, tek, Hilbert je u drugom koraku opravdavanja uvođenja idealnih iskaza zamenio problem konzervativnosti problemom konzistentnosti. Pri tome, dokaz konzistentnosti treba da bude finitistički, kao što je to trebalo da bude dokaz konzervativnosti. Znači, da bi se izveo Hilbertov program, onako kako ga je on zamislio, potrebno je uraditi dve stvari: dati potpunu formalizaciju intuitivne klasične matematike i finitistički dokazati konzistentnost dobijenog formalnog sistema. To pre svega treba uraditi za aritmetiku, a posle i za njena proširenja koja obuhvataju analizu. (Ekvivalentnost konzervativnosti sa konzistentnošću se za ova proširenja pokazuje analogno onome što imamo za formalnu aritmetiku.) Poznati Gödelovi rezultati s početka tridesetih godina pokazali su da se ni za aritmetiku ni za njena proširenja ne može uraditi ni jedno ni drugo.

Prva Gödelova teorema o nepotpunosti pokazuje da nema formalnog sistema koji bi kodifikovao sve dokaze intuitivne aritmetike. Tačnije rečeno, iz te teoreme sledi da u svakom konzistentnom formalnom sistemu čiji je podsistem formalna Peanova aritmetika, postoji finitarna formula φ bez slobodnih promenljivih tako da ni φ ni $\neg\varphi$ nisu dokazivi u tom sistemu, a iskaz koji odgovara formuli φ važi u intuitivnoj finitističkoj aritmetici. (To dovodi u pitanje pretpostavku (2).) Znači, nema formalnog sistema za celu matematiku, nego svaki formalni sistem pokriva samo deo matematike.

Druga Gödelova teorema o nepotpunosti pokazuje da se konzistentnost nekog konzistentnog formalnog sistema čiji je podsistem formalna aritmetika ne može dokazati sredstvima koja su kodifikovana u formalnoj aritmetici; pogotovu se onda ta konzistentnost ne može dokazati finitističkim sredstvima koja su kodifikovana u formalnoj aritmetici. Međutim, nije isključeno da se ta konzistent-

nost može dokazati sredstvima koja su bar u nečem jača od primitivno rekurzivne aritmetike sadržane u formalnoj aritmetici, a ipak se mogu smatrati finitističkim u nekom smislu te reči. (U Dodatku A ovog poglavlja razmotrićemo nešto detaljnije Gödelove teoreme o nepotpunosti.)

Gentzenovi rezultati u teoriji dokaza

Hilbertov program više pogađa prva Gödelova teorema o nepotpunosti nego druga. Pored toga što poriče mogućnost potpune formalizacije matematike, prva teorema dovodi u pitanje i ekvivalentnost konzistentnosti i konzervativnosti. Drugu teoremu je, kao što smo na kraju prošlog odeljka primetili, moguće zaobići. Naime, može se očekivati da je konzistentnost formalne aritmetike, i konzistentnost nekih formalnih sistema za analizu, dokaziva sredstvima koja su bar u nekom smislu te reči finitistička. Tako se i posle Gödelovih teorema o nepotpunosti nastavilo da radi na rešavanju drugog Hilbertovog problema, i dobijeni su dokazi konzistentnosti za formalnu aritmetiku i formalne sisteme koji pokrivaju delove analize. Ti rezultati eventualno omogućuju da se sprovede i neka okrnjena i modifikovana verzija Hilbertovog programa. Od tih rezultata spomenućemo one koji potiču od Gentzena, i koji spadaju među neke od najlepših rezultata matematičke logike.

U prvoj polovini tridesetih godina Gödel i Gentzen su pokazali, nezavisno jedan od drugoga, da se klasična formalna Peanova aritmetika može potopiti u Heytingovu intuicionističku aritmetiku. Ako se pretpostavi konzistentnost ove druge, dobijamo izvesno rešenje drugog Hilbertovog problema.

Međutim, prvi pravi dokaz konzistentnosti formalne aritmetike — dokaz onog tipa koji je Hilbert predložio 1904. godine — dao je Gentzen sredinom tridesetih godina (iz tog dokaza proizilazi i dokaz za izvestan oblik (Cnsr)). Pokušaćemo da ukratko predstavimo taj dokaz (detaljniji prikaz ovog dokaza dat je u Dodatku B ovog poglavlja).

Gentzenov dokaz koristi transfinitnu indukciju preko jednog inicijalnog segmenta ordinala. Iza konačnih ordinala 0, 1, 2, 3, ... sledе prebrojivi transfinitni ordinali iz Cantorove druge klase brojeva:

$$\omega,\ \omega+1,\ \omega+2,\ \ldots,\ \omega\cdot 2,\ \omega\cdot 2+1,\ \ldots,\ \omega\cdot 3,\ \ldots,$$

$\omega^2,\ \omega^2+1,\ \ldots,\ \omega^2+\omega,\ \ldots,\ \omega^2+\omega\cdot 2,\ \ldots,\ \omega^2\cdot 2,\ \ldots,$

$\omega^3,\ \omega^3+1,\ \ldots,$

$\ldots,$

$\omega^\omega,\ \omega^\omega+1,\ \ldots,$

ω^{ω^ω}, itd.

U transfinitnoj indukciji do α, tj. po inicijalnom segmentu ordinala manjih od ordinala α, pokazujemo da za svaki ordinal $\beta<\alpha$, ako svi ordinali $\gamma<\beta$ imaju neko svojstvo, onda i β ima to svojstvo; odatle zaključujemo da svi ordinali manji od α imaju to svojstvo. To se može ovako zapisati:

$$(\forall\,\beta<\alpha)\,((\forall\,\gamma<\beta)\,F(\gamma)\ \Rightarrow\ F(\beta))\ \Rightarrow\ (\forall\,\delta<\alpha)\,F(\delta).$$

(Ovde se koristi sažeti oblik indukcije u kojem su baza i induktivni korak dati zajedno; slučaj $\beta=0$, gde je skup ordinalâ γ prazan, se, ukoliko to želimo, može tretirati posebno kao baza indukcije.)

Transfinitnu indukciju imamo već kad sprovodimo običnu indukciju do ω preko dve promenljive tako što u toku indukcije po prvoj promenljivoj sprovodimo indukciju po drugoj. Takvu dvostruku indukciju možemo predstaviti kao jednostruku indukciju do ordinala ω^2. Ordinali manji od ω^2 se mogu predstaviti kao parovi prirodnih brojeva sa uređenjem

$$(n_1,\ m_1)<(n_2,\ m_2)\ \Leftrightarrow_{df}\ n_1<n_2\quad \textit{ili}\quad (n_1=n_2\ \textit{i}\ m_1<m_2).$$

Kao što dvostruku indukciju zamenjujemo indukcijom po ovim parovima, tako postupamo i sa trostrukom koristeći se trojkama, itd, sve do indukcije koja odgovara ordinalu ω^ω. Gentzenova indukcija je složenija od svih ovih: on koristi transfinitnu indukciju do ε_0. Ordinal ε_0, koji je najmanje rešenje za ξ u jednačini $\omega^\xi=\xi$ (rešenja ove jednačine se zovu *epsiloni*), je limit niza ordinala $\omega,\ \omega^\omega,\ \omega^{\omega^\omega},\ \omega^{\omega^{\omega^\omega}},\ \ldots$ Ordinal ε_0 je prebrojiv i isto pripada drugoj klasi brojeva — on je manji od ω_1, prvog neprebrojivog ordinala.

Ideja iza Gentzenovog dokaza konzistentnosti formalne aritmetike je sledeća. Naš zadatak je da razmotrimo sve moguće dokaze u formalnoj aritmetici i utvrdimo da su svi korektni, tj. da nijedan

od njih nije dokaz za $1=0$. Korektnost nekog dokaza zavisi od korektnosti nekih jednostavnijih dokaza koji su u njemu sadržani kao specijalni slučajevi ili kao njegovi delovi. Sve dokaze ćemo urediti linearno tako da dokazi od čije korektnosti zavisi korektnost nekog drugog dokaza prethode ovom drugom dokazu. To uređenje se dobija tako što svakom dokazu pripišemo jedan ordinal: dokazi koji prethode nekom datom dokazu su oni dokazi čiji ordinali prethode ordinalu datog dokaza.

Ilustrujmo ovo na primeru jednog sasvim jednostavnog podsistema formalne aritmetike. Jedina aksioma je $0=0$, a jedino pravilo zaključivanja je da sa $n=n$ možemo preći na $n'=n'$, gde je n' naslednik od n. Onda dokazu formule $n=n$, gde je n oblika

$$0\overbrace{'\ldots'}^{n}$$

pripisujemo prirodni broj n. Da su svi dokazi korektni utvrđuje se običnom indukcijom do ω.

Međutim, za numerisanje dokaza u formalnoj aritmetici nisu dovoljni prirodni brojevi, nego moramo koristiti i transfinitne ordinale. Zašto? Zato što se može dogoditi da korektnost nekog dokaza zavisi od korektnosti beskonačno mnogo drugih dokaza. Pretpostavimo, na primer, da je u nekom dokazu dokazana pomoću indukcije formula $\forall x \varphi(x)$. Korektnost ovog dokaza zavisi od korektnosti beskonačnog niza dokazâ za svaku formulu $\varphi(n)$. Transfinitni ordinali nam trebaju da bismo dokaze prirodno uredili po složenosti. Iz tog uređenja, na čije pravljenje se prenosi sva težina Gentzenovog dokaza, odmah sledi da ako je za sve dokaze koji prethode nekom dokazu utvrđeno da su korektni, onda je i sam taj dokaz korektan. Odatle transfinitnom indukcijom sledi da su svi dokazi korektni.

Nešto određenije, Gentzenov dokaz se odvija ovako. Svakom dokazu u jednoj posebnoj formalizaciji Peanove aritmetike pripisuje se jedan ordinal manji od ε_0. Grubo rečeno, transfinitni ordinali se javljaju kad god dokazi sadrže pravilo indukcije. Osim toga, Genjtzen daje jednu proceduru *redukcije*: za dokaz formule koja odgovara formuli $1=0$ sa ordinalnim brojem α on nalazi dokaz za istu formulu sa ordinalnim brojem manjim od α. Grubo rečeno, ordinali se smanjuju eliminisanjem pravila indukcije i jednog pravila koje se zove pravilo *sečenja*, i koje može da se shvati kao uopštenje

pravila tranzitivnosti implikacije ili pravila *modus ponensa*. Odatle, koristeći činjenicu da su svi opadajući nizovi ordinala manjih od ε_0 konačni, što je ekvivalentno sa indukcijom do ε_0, sledi da je sistem konzistentan. Redukcija dokaza odgovara proceduri koja svodi dokaze za atomske formule bez promenljivih (te formule su naravno finitarne) na dokaze bez idealnih formula. U jednoj drugoj verziji Gentzenovog dokaza, koja je hronološki gledano prva, pokazuje se indukcijom po ordinalima manjim od ε_0 da se izvesna redukcija može izvesti za svaku dokazivu formulu; a takva redukcija se ne može izvesti za formulu koja odgovara formuli $1 = 0$. (I ova druga redukcija je u vezi sa (Cnsr).)

Gentzenov dokaz se inače izvodi argumentima koji ne koriste kvantifikaciju, tako da izuzevši transfinitnu indukciju do ε_0 oni mogu da se formalizuju u primitivno rekurzivnoj, pa prema tome i u Peanovoj aritmetici. Iz Gödelove druge teoreme o nepotpunosti sledi da se transfinitna indukcija do ε_0 ne može formalizovati u Peanovoj aritmetici (to je Gentzen i direktno proverio početkom četrdesetih godina). Bernays je pokazao da se indukcija do bilo kojeg ordinala manjeg od ε_0 može formalizovati unutar Peanove aritmetike. (To je npr. sasvim za očekivanje kod indukcije do ω^2, za koju smo videli da se svodi na dvostruku indukciju.) Tako ε_0 prirodno meri jačinu formalne Peanove aritmetike.

Ostaje pitanje, da li se indukcija do ε_0 ipak može smatrati finitističkom, u nekom smislu te reči. Kada razmatramo to pitanje treba da imamo u vidu da je indukcija do ε_0 Gentzenu potrebna samo za odlučiva svojstva, tj. samo za odlučive predikate F u formuli kojom smo gore zapisali tu indukciju. Obična indukcija do ω se u Peanovoj aritmetici pretpostavlja za ma kakve predikate.

Gentzenov metod je kasnije primenjen i na sisteme jače od formalne Peanove aritmetike koristeći ordinale α veće od ε_0, i opet se ispostavljalo da se indukcija do nekog ordinala manjeg od α može formalizovati unutar sistema. Tako je situacija vezana za Gentzenovu transfinitnu indukciju izgleda opšta pojava; mada se rezultati u ovoj oblasti, izgleda, još uvek nisu slegli.

Spomenućemo nešto o dokazu konzistentnosti za jedan sistem jači od formalne Peanove aritmetike. Neka formalni sistem za analizu bude sistem u logici drugog reda (logici koja kvantifikuje i preko predikatskih promenljivih — za razliku od logike prvog reda koja kvantifikuje samo preko individualnih promenljivih) koji od

nelogičkih termina ima samo 0 i funkciju naslednika ′, a od nelogičkih aksioma samo sledeće Peanove aksiome:

$$\forall x\,(x' \neq 0)$$

$$\forall x \forall y\,(x' = y' \rightarrow x = y).$$

U ovom sistemu predikat „x je prirodan broj“ može se definisati sledećom formulom:

$$\forall X((X0 \wedge \forall y\,(Xy \rightarrow Xy')) \rightarrow Xx).$$

Onda se mogu dokazati sve Peanove aksiome. Realni brojevi se definišu kao binarne relacije koje čine parovi prirodnih brojeva, pri čemu su drugi članovi tih parova različiti od 0: svaka takva relacija odgovara skupu racionalnih brojeva koji je levi deo jednog Dedekindovog preseka. Ovaj sistem ne pokriva celu analizu: da bi se pokrili širi delovi moderne analize potrebna je logika trećeg ili višeg reda (da bismo dobili ne samo funkcije nego i operatore nad funkcijama), i još nam treba i aksioma izbora.

Takeuti je pokazao sredinom pedesetih godina da se dokaz konzistentnosti našeg sistema za analizu svodi na dokaz eliminisanja pravila sečenja iz logike drugog reda. Razlog za to je sledeći. Ako eliminišemo sečenje, možemo pokazati da je logika drugog reda konzervativna ekstenzija logike prvog reda, pa ako bi $1 = 0$ bilo dokazivo iz gornja dva Peanova aksioma pomoću logike drugog reda, onda bi bilo dokazivo i pomoću logike prvog reda. A da je ovo poslednje nemoguće, može se pokazati gencenovskim dokazom koji je jednostavniji od dokaza konzistentnosti formalne Peanove aritmetike. Dokaz eliminisanja pravila sečenja iz logike drugog reda prvo je bio dat sredstvima teorije modela sredinom šezdesetih godina, a početkom sedamdesetih godina Girard i Prawitz dali su dokaze koji su više u gencenovskom duhu.

Ovi poslednji dokazi koriste i ideje jednog drugog dokaza konzistentnosti formalne aritmetike, koji je dao Gödel pedesetih godina. U tom dokazu Gödel se služi jednim sistemom primitivno rekurzivne aritmetike sa funkcijama višeg reda koje pripadaju svim konačnim tipovima. U tom se sistemu može interpretirati Heytingova aritmetika, pa prema tome, po već pomenutom rezultatu Gödela i Gentzena, i klasična formalna Peanova aritmetika. Snaga ovog Gödelovog sistema je na neki način ekvivalentna indukciji do ε_0.

Gentzenov dokaz konzistentnosti formalne aritmetike zasniva se na idejama koje je Gentzen izneo u svojoj tezi *Istraživanja o logičkoj dedukciji* 1934. godine. U toj tezi je data analiza logičke dedukcije kakvu niko do tada nije detaljno izveo. Ta analiza je značajna i sama za sebe, nezavisno od njene primene u rešavanju Hilbertovog drugog problema. Gentzenovom tezom je ustanovljena jedna logička disciplina koja se naziva opštom, ili gencenovskom teorijom dokaza — za razliku od Hilbertove teorije dokaza.

U opštoj teoriji dokaza ne istražuju se samo teoreme neke teorije, tj. *šta* znamo u toj teoriji, nego i dokazi tih teorema, tj. *kako* znamo to što znamo. Gentzen je razvio dva sredstva za istraživanje dokaza: sisteme prirodne dedukcije i sisteme sekvenata, koji su tesno povezani jedni sa drugima. (Govoreći o Gentzenovom dokazu konzistentnosti spomenuli smo dve verzije: u prvoj verziji koju smo spomenuli Peanova aritmetika je formalizovana kao sistem sekvenata, a u drugoj kao prirodno-dedukcijski sistem.) U sistemima prirodne dedukcije dokazi se razbijaju na atomske korake, a u svakom koraku uvodimo ili eliminišemo neku logičku konstantu. Tu je osnovni rezultat da se dokazi mogu *normalizovati*, tako što nikad uvođenje neke konstante ne prethodi njenom eliminisanju. Normalizovani dokaz se sastoji iz dva dela: u prvom eliminišemo sve logičke konstante iz premisa i dobijamo atomske formule, a u drugom te atomske formule kombinujemo uvodeći nove konstante, da bismo dobili zaključak. Normalizovani dokaz je, prema tome, direktan — on ne pravi zaobilaske preko formula koje nisu potformule premisa ili zaključaka. Ovoj teoremi o normalizaciji dokaza odgovara teorema o eliminisanju pravila sečenja u sistemima sekvenata. Tehnika eliminisanja sečenja, koju je istraživao sam Gentzen, i tehnika normalizacije prirodno-dedukcijskih dokaza, koja se razvija počevši od šezdesetih godina, najviše Prawitzovom zaslugom, predstavljaju najpoznatije tehnike u opštoj teoriji dokaza. Pomoću njih možemo da pokušamo da odgovorimo na mnoga tehnička pitanja vezana za logičke sisteme. Osim toga, pomoću ovih tehnika možemo pokušati da precizno odgovorimo i na tako opšta pitanja kao što je pitanje kada se dva dokaza u stvari svode na isto: možemo pretpostaviti da se dva dokaza (koja se mogu na određen način formalizovati) u stvari ne razlikuju ako i samo ako se oba normalizacijom svode na isti dokaz. Osim tih primena, ove tehnike iz opšte teorije dokaza imaju, kao što smo gore videli, primene i u Hilbertovoj teoriji dokaza, u dokazivanju konzistentnosti formalne

aritmetike ili analize. Redukcija u Gentzenovom dokazu konzistentnosti formalne aritmetike na izvestan način odgovara proceduri koja vodi normalizaciji ili eliminisanju sečenja. Tako se pokazuje da dokazi finitarnih formula određenog tipa ne moraju praviti zaobilaske preko idealnih formula. Ovaj rezultat je bio direktno motivisan Gentzenovim istraživanjima o prirodi logičke dedukcije.

Kreisel na jednom mestu kaže da je bar neko vreme Hilbertu glavni cilj bio da navede matematičare da se bave matematičkim dokazima kao predmetom matematičkih istraživanja — drugi Hilbertov problem i Hilbertov program je trebalo da budu samo mamac.

DODATAK A: GÖDELOVE TEOREME O NEPOTPUNOSTI

U ovom dodatku pokušaćemo da ukratko predstavimo Gödelove teoreme o nepotpunosti. Nećemo dati nikakav iscrpan tretman ovih teorema, nego ćemo samo pokušati da sugerišemo glavne ideje. U prvom odeljku, izložićemo kako izgleda formalizacija Peanove aritmetike prvog reda u hilbertovskom stilu; u drugom i trećem odeljku, biće izloženi neki elementi kodiranja; i najzad, u četvrtom odeljku, prikazaćemo teoreme o nepotpunosti. U petom odeljku, prikazaćemo jedan skorašnji rezultat u vezi sa nepotpunošću formalne aritmetike.

§ 1. Formalizacija aritmetike. *Formule* Peanove aritmetike prvog reda, koju ćemo zvati P, napravljene su na uobičajen način na jeziku L koji se sastoji od sledećih osnovnih simbola:

prebrojivo mnogo individualnih promenljivih $v_0, v_1, \ldots$;
individualne konstante 0;
funkcijske konstante naslednika $'$;
operacijskih konstanti $+, \cdot$;
logičkih konstanti $\rightarrow, \wedge, \vee, \neg, \forall, \exists, =$;
leve i desne zagrade (,).

Termi se dobijaju zatvaranjem skupa koji se sastoji od individualnih promenljivih i 0 pomoću $'$, $+$ i $\cdot$. *Numerali* se dobijaju zatvaranjem skupa 0 pomoću $'$, pri čemu je 1 skraćenica za $0'$, 2 za $0''$ itd. Skup formula, skup termâ i skup numerala su efektivno dati.

Shematska slova za formule su φ, ψ, θ, φ_1, ...; shematska slova za individualne promenljive su x, y, z, i, j, k, x_1, ...; shematska slova za terme su t, t_1, ...; a shematska slova za numerale su n, n_1, ... Shemom $\varphi(x)$ označavamo formulu u kojoj se (eventualno) x javlja slobodno, a $\varphi(t)$ se dobija iz $\varphi(x)$ supstituisanjem terma t mesto x, uz uobičajena ograničenja za supstituciju.

Teorija P ima aksiome i pravila zaključivanja koji su efektivno dati sledećim shemama:

Aksiome i pravila iskaznog računa:

1. $\varphi\to(\psi\to\varphi)$,
2. $(\varphi\to(\psi\to\theta))\to((\varphi\to\psi)\to(\varphi\to\theta))$,
3. $(\theta\to\varphi)\to((\theta\to\psi)\to(\theta\to(\varphi\wedge\psi)))$, 4. $(\varphi\wedge\psi)\to\varphi$, 5. $(\varphi\wedge\psi)\to\psi$,
6. $\varphi\to(\varphi\vee\psi)$, 7. $\psi\to(\varphi\vee\psi)$, 8. $(\varphi\to\theta)\to((\psi\to\theta)\to((\varphi\vee\psi)\to\theta))$,
9. $(\varphi\to\neg\psi)\to(\psi\to\neg\varphi)$, 10. $\neg\varphi\to(\varphi\to\psi)$, 11. $\neg\neg\varphi\to\varphi$,
12. $\dfrac{\varphi \quad \varphi\to\psi}{\psi}$.

Dodatne aksiome i pravila predikatskog računa prvog reda:

13. $\dfrac{\psi\to\varphi(x)}{\psi\to\forall x\,\varphi(x)}$,
14. $\forall x\,\varphi(x)\to\varphi(t)$,
15. $\varphi(t)\to\exists x\,\varphi(x)$,
16. $\dfrac{\varphi(x)\to\psi}{\exists x\,\varphi(x)\to\psi}$.

Pravila 13 i 16 važe pod uslovom da se x ne javlja slobodno u donjoj formuli.

17. $x=x$,
18. $y=z\to(\varphi(y)\to\varphi(z))$.

U shemi aksioma 18 formule $\varphi(y)$ i $\varphi(z)$ se dobijaju supstitucijom iz neke formule $\varphi(x)$.

Aritmetičke aksiome:

19. $\neg x'=0$,
20. $x'=y'\to x=y$,

21. $(x+0)=x$,
22. $(x+y')=(x+y)'$,
23. $(x\cdot 0)=0$,
24. $(x\cdot y')=((x\cdot y)+x)$,
25. $\forall x(\varphi(x)\to\varphi(x'))\to(\varphi(0)\to\varphi(t))$.

Ako izostavimo shemu aksioma $\neg\neg\varphi\to\varphi$, dobijamo aksiomatizaciju Heytingove aritmetike prvog reda.

Dokaz neke formule φ je konačan niz formula takav da je φ poslednja formula u tom nizu i svaka formula u nizu je ili aksioma ili se dobija iz prethodnih formula primenom nekog pravila. Može se pokazati da je skup dokaza efektivno dat. Formula φ je *teorema* akko postoji dokaz za φ.

Jezik sistema P ćemo proširiti nekim prirodnim definicijama. Tako ćemo, na primer, u nastavku koristiti veznik ekvivalencije, koji se definiše na sledeći način:

$$\varphi\leftrightarrow\psi\Leftrightarrow_{df}(\varphi\to\psi)\wedge(\psi\to\varphi);$$

koristićemo i sledeće definisane relacije:

$$t_1<t_2\Leftrightarrow_{df}\exists x(t_1+x'=t_2),$$

$$t_1\leqslant t_2\Leftrightarrow_{df}t_1<t_2\vee t_1=t_2,$$

i definicije ograničenih kvantifikatora:

$$(\forall x<t)\varphi\Leftrightarrow_{df}\forall x(x<t\to\varphi),$$

$$(\exists x<t)\varphi\Leftrightarrow_{df}\exists x(x<t\wedge\varphi),$$

(definicije za $(\forall x\leqslant t)$ i $(\exists x\leqslant t)$ su analogne ovima). Osim toga, izostavljaćemo zagrade koje bi samo otežavale čitanje: tako, na primer, nećemo uvek pisati zagrade oko terma napravljenih sa $+$ i $\cdot$.

§ 2. **Kodiranje u prirodnim brojevima.** Pod kodiranjem nekog skupa A podrazumevamo jedno $1-1$ preslikavanje $\varkappa: A\to N$, gde je N skup prirodnih brojeva. Preslikavanje $\varkappa$ naziva se kodirajućom funkcijom, a $\varkappa(a)$ se naziva *kôdom* elementa $a\in A$. Kôd nekog elementa a obično se obeležava sa $\ulcorner a\urcorner$. Iz definicije kodirajuće funkcije neposredno sledi da je A najviše prebrojiv skup. U većini slučajeva skup A je dat na efektivan način, što znači da postoji procedura,

algoritam, kojim se u konačno mnogo koraka može odrediti da li je nešto element skupa A ili nije. Isto tako, obično se zahteva da kodirajuća funkcija bude izračunljiva, tj. da se u konačno mnogo koraka može izračunati kôd $\ulcorner a \urcorner$ bilo kojeg elementa $a \in A$. Takođe, treba da bude odlučivo u konačno mnogo koraka da li je neki broj kôd nekog elementa iz A, i ako jeste, treba da bude izračunljivo kog elementa je on kôd.

Pomoću kodiranja se mogu analizirati aritmetičkim sredstvima osobine skupa A i njemu pridruženih objekata: na primer, funkcija i relacija na skupu A. Gödel je prvi koristio kodiranje za analizu nekih metamatematičkih pojmova. Kodiranjem on je predstavio u aritmetici, aritmetizovao je, logičke pojmove kao što su term, formula, dokaz, teorema, i to je bio osnovni korak u dokazima teorema o nepotpunosti. U njegovu čast kodiranje se u matematičkoj logici naziva još i *gedelizacijom*, a kôd *Gödelovim brojem*.

Razmotrimo sada sledeća dva primera kodiranja.

Primer 1 (Cantorova funkcija). Kodirajuća funkcija $\langle\ \rangle : N^2 \to N$, gde je $\langle n, m\rangle = \binom{n+m+1}{2} + n$, je 1—1 i *na*. To se može dokazati tako što sve parove prirodnih brojeva poređamo kao na sledećoj tabeli:

$$\begin{matrix} (0,1) & (0,1) & (0,2) \ldots \\ (1,0) & (1,1) & (1,2) \ldots \\ (2,0) & (2,1) & (2,2) \ldots \end{matrix}$$

i zatim ih ovako prebrojavamo: (0,0), (0,1), (1,0), (0,2), (1,1), (2,0)... Funkcija $\langle\ \rangle$ ima sve osobine uređenog para jer $\langle n_1, m_1\rangle = \langle n_2, m_2\rangle$ povlači $n_1 = n_2$ i $m_1 = m_2$. Lako je uvesti kodiranje skupova N^3, N^4 ... pomoću sledećih definicija:

$$\langle n_1, n_2, n_3\rangle =_{df} \langle\langle n_1, n_2\rangle, n_3\rangle,\ \langle n_1, n_2, n_3, n_4\rangle =_{df} \langle\langle n_1, n_2, n_3\rangle, n_4\rangle,\ \ldots$$

Primer 2. U jednom dosta uobičajenom načinu kodiranja, koji je uveo Gödel, koriste se prosti brojevi. Kod tog kodiranja glavnu ulogu igra Osnovna teorema aritmetike:

> Ako je n prirodan broj, onda postoje jedinstveni prosti brojevi $q_1, \ldots, q_k$, gde je $q_1 < q_2 < \ldots < q_k$, i jedinstveni prirodni brojevi $m_1, \ldots, m_k$ veći od 0, tako da važi $n = q_1^{m_1} \cdot \ldots \cdot q_k^{m_k}$.

Ako je $\varkappa : A \to N$ neka kodirajuća funkcija, onda se primenom ove teoreme može definisati $\ulcorner\ \urcorner$ za sve konačne nizove elemenata iz A. Na primer, ako je f konačan niz čiji su članovi $f_1, f_2, \ldots, f_k$, onda za kôd niza f možemo uzeti

$$\ulcorner f \urcorner = p_1^{\varkappa(f_1)+1} \cdot p_2^{\varkappa(f_2)+1} \cdot \ldots \cdot p_k^{\varkappa(f_k)+1}$$

gde je $p_1, p_2, \ldots, p_k$ inicijalni segment niza prostih brojeva $\geqslant 2$, tj. $p_1 = 2$, $p_2 = 3$, itd.

Zahvaljujući kodiranju, u P ćemo moći da kvantifikujemo preko konačnih nizova, a to će nam omogućiti da u P definišemo mnoge važne metamatematičke pojmove.

Sada ćemo opisati jedno kodiranje jezika L u neformalnoj aritmetici. Prvo, osnovnim simbolima jezika L pridružimo brojeve na sledeći način:

0	$'$	$+$	$\cdot$	$\rightarrow$	$\wedge$	$\vee$	$\neg$	$\forall$	$\exists$	$=$	$($	$)$	v_i
1	2	3	4	5	6	7	8	9	10	11	12	13	$20+i$

Svaka formula φ jezika L je konačan niz osnovnih simbola, kojima su pridruženi brojevi $s_1, s_2, \ldots, s_k$. Tada za kôd formule φ možemo uzeti

$$\ulcorner \varphi \urcorner = 2^{s_1} \cdot 3^{s_2} \cdot \ldots \cdot p_k^{s_k}$$

jer su brojevi osnovnih simbola veći od nule. Na primer, ako je φ formula $\forall v_0 \exists v_1 ((v_0 + v_1') = v_2)$, onda je $\ulcorner \varphi \urcorner = 2^9 \cdot 3^{20} \cdot 5^{10} \cdot 7^{21} \cdot 11^{12} \cdot \ldots \cdot 41^{22} \cdot 43^{13}$. Analogno ovome kodiramo i terme.

Kada imamo kôdove termâ i formula jezika L, možemo definisati u neformalnoj aritmetici razne aritmetičke predikate i funkcije koji odgovaraju određenim metamatematičkim pojmovima. To su, na primer, predikati *Term* i *For* za koje važi:

$Term(x)$ akko je x kôd nekog terma jezika L;

$For(x)$ akko je x kôd neke formule jezika L.

U četvrtom odeljku ćemo spomenuti neke druge predikate i funkcije koji se, takođe, mogu definisati. Koncentrisaćemo se samo na definiciju predikata *Term*. Ostale definicije se dobijaju, više ili manje, analogno.

Prvo definišemo funkciju $(y)_x = \max\{z \mid p_x^z \text{ deli } y\}$, pri čemu je p_x, kao i malopre, x-ti prost broj $\geqslant 2$. Zatim, neka je $\bar{y} = \max\{x \mid (y)_x > 0\}$. Intuitivno, $(y)_x$ je x-ti član niza $y_1, y_2, \ldots, y_k$ za $x \leqslant k$, a $\bar{y}$ je dužina tog niza, pri čemu je $y = p_1^{y_1} \cdot \ldots \cdot p_k^{y_k}$. Setimo se da je neki izraz t term jezika L akko postoje izrazi $t_1, \ldots, t_n$ takvi da je $t_n = t$ i

$$(\forall\, k \leqslant n)\,(t_k = 0 \vee t_k = v_m \vee (\exists\, i < k)\, t_k = t_i' \vee (\exists\, i < k)\,(\exists\, j < k)$$

$$(t_k = (t_i + t_j) \vee t_k = (t_i \cdot t_j))).$$

Otuda, $a \in N$ je kôd nekog terma akko postoje $a_1, \ldots, a_n \in N$ takvi da je $a_n = a$ i

$$(\forall\, k \leqslant n)\,(a_k = \ulcorner 0 \urcorner \vee a_k = \ulcorner v_m \urcorner \vee (\exists\, i < k)\,[\bar{a}_k = \bar{a}_i + 1 \wedge (a_k)_{\bar{a}_i + 1} = 2 \wedge$$

$$(\forall\, z \leqslant \bar{a}_i)\,(a_k)_z = (a_i)_z] \vee \ldots).$$

Konjunkcija u uglastim zagradama opisuje kôd terma $t_k = t_i'$: prvi konjunkt kaže da je dužina terma t_k za 1 veća od dužine terma t_i, drugi konjunkt kaže da je poslednji simbol u tom termu $'$, a treći konjunkt kaže da se termi t_k i t_i inače poklapaju. Pošto se ceo niz $a_1, \ldots, a_n$ može kodirati nekim brojem $y = p_1^{a_1} \cdot \ldots \cdot p_n^{a_n}$, definicija predikata *Term* će izgledati ovako:

$$\mathit{Term}\ (x) \Leftrightarrow_{df} \exists\, y\,((y)_{\bar{y}} = x \wedge (\forall\, k \leqslant \bar{y})\,((y)_k = 2^1 \vee (\exists\, z < (y)_k)$$

$$(y)_k = 2^{20+z} \vee (\exists\, i < k)\,[\overline{(y)_k} = \overline{(y)_i} + 1 \wedge ((y)_k)_{\overline{(y)i}+1} = 2$$

$$\wedge (\forall\, z \leqslant \overline{(y)_i})\ ((y)_k)_z = ((y)_i)_z] \vee \ldots)).$$

§ 3. Kodiranje u formalnoj aritmetici. U ovom odeljku govorićemo o tome kako izgleda kodiranje jezika L u formalnoj aritmetici P. To kodiranje je preslikavanje termâ i formula iz L u numerale, a predikati kao *Term* i *For* sada treba da budu definisani u P.

Videli smo da je u prošlom odeljku važnu ulogu igrala funkcija $(y)_x$, u čijem smo definisanju upotrebili svojstvo „biti x-ti prost broj“, tj. niz prostih brojeva. Među osnovnim simbolima sistema P nema predikata „biti x-ti prost broj“; i mada je u P lako definisati predikat „biti prost broj“, u prirodnoj definiciji predikata „biti

x-ti prost broj" naići ćemo na teškoće. U toj definiciji treba na izvestan način da kvantifikujemo preko konačnih nizova, a to znači da moramo već imati na raspolaganju nešto kao funkciju $(y)_x$. Iz ovog začaranog kruga izlaz ipak postoji. U ovom odeljku pokazaćemo kako je Gödel definisao u P funkciju koja se ponaša kao $(y)_x$. Kada imamo tu funkciju, ostale detalje u vezi sa kodiranjem možemo dobiti u P kao u prošlom odeljku, ili na neki analogan način.

Cantorova funkcija se u P može definisati pomoću sledeće jednakosti:

$$2 \cdot \langle x, y \rangle = ((x+y) \cdot (x+y)') + (2 \cdot x).$$

Lako je dokazati (indukcijom) da i u P važe ključne osobine ove funkcije. Otuda se dobija da je u P moguće definisati funkcije L i R tako da se u P može dokazati:

$$L\langle x, y \rangle = x, \qquad R\langle x, y \rangle = y, \qquad \langle Lz, Rz \rangle = z.$$

Zatim dajemo i sledeću definiciju u P:

$$\left(\frac{x}{y}\right) = z \Leftrightarrow_{df} (\exists k \leqslant x)(x = (y \cdot k) + z \wedge z < y) \vee (y = 0 \wedge z = x).$$

U P se isto tako može definisati i relacija $(x, y) = 1$ koja važi kada su x i y uzajamno prosti. Onda možemo pokazati da se sledeća teorema iz teorije brojeva može dokazati u P za svako n:

Kineska teorema o ostacima.

$$\forall x_1 \ldots \forall x_n (\forall y_1 < x_1) \ldots (\forall y_n < x_n) \left((\ldots \wedge (x_i, x_j) = 1 \wedge \ldots) \rightarrow \right.$$

$$\left. (\exists y < x_1 \cdot \ldots \cdot x_n) \left(\left(\frac{y}{x_1}\right) = y_1 \wedge \ldots \wedge \left(\frac{y}{x_n}\right) = y_n \right) \right).$$

Pomoću ove teoreme dokazujemo sledeću lemu:

Gödelova lema. Za svako n, u P se može dokazati

$$\forall y_1 \ldots \forall y_n \exists x \exists y \left(\left(\frac{y}{(x \cdot 1) + 1}\right) = y_1 \wedge \ldots \wedge \left(\frac{y}{(x \cdot n) + 1}\right) = y_n \right).$$

Dokaz. Za $i=1, \ldots, n$ neka je $x=n! \cdot \max(y_i+1)$. Tada su $(x \cdot i)+1$ po parovima uzajamno prosti, pa prema Kineskoj teoremi o ostacima postoji y tako da $\left(\frac{y}{(x \cdot i)+1}\right)=y_i$.

Funkciju $(z)_i$ sada možemo definisati u P na sledeći način:

$$(z)_i =_{df} \left(\frac{Lz}{(Rz \cdot i)+1}\right)$$

i onda možemo dokazati Gödelovu lemu i u sledećem obliku:

Gödelova lema. Za svako n, u P se može dokazati

$$\forall y_1 \ldots \forall y_n \exists y ((y)_1 = y_1 \wedge \ldots \wedge (y)_n = y_n).$$

Prema tome, u P možemo kvantifikovati preko konačnih nizova.

Kao primer primene kvantifikacije preko konačnih nizova u P dajemo definiciju eksponencijalne funkcije (ova definicija odgovara induktivnoj definiciji eksponencijalne funkcije):

$$y = x^z \Leftrightarrow_{df} \exists k ((k)_0 = 1 \wedge (\forall i < z)(k)_{i+1} = x \cdot (k)_i \wedge (k)_z = y).$$

Ova definicija je korektna jer se u P može dokazati da za svako x i z postoji jedinstveno y tako da $y=x^z$. Takođe, ako je za prirodne brojeve n_1, n_2 i n_3, $n_1 = n_2^{n_3}$, onda se u P može dokazati $n_1 = n_2^{n_3}$.

Sada se u P može definisati predikat „biti x-ti prost broj“, a takođe i predikati *Term*, *For*, i drugi predikati i funkcije. Tako smo omogućili formalnoj aritmetici da „govori o samoj sebi“. Na tom svojstvu formalne aritmetike se zasnivaju Gödelove teoreme o nepotpunosti.

§ 4. Teoreme o nepotpunosti. Pretpostavljajući da sad čitalac ima neku predstavu o kodiranju u P, pokušaćemo da prikažemo Gödelove teoreme o nepotpunosti.

Neka je T neki formalni sistem koji sadrži P, i neka $\vdash \varphi$ znači da je φ teorema sistema T. Svakoj formuli φ i svakom termu t iz T pripisuju se kodiranjem u P numerali $\ulcorner\varphi\urcorner$ i $\ulcorner t\urcorner$. Zatim, treba pokazati da se u P može definisati funkcija $sub(x, y)$ tako da se u P, pa prema tome i u T, može dokazati

$$sub(\ulcorner\varphi(x)\urcorner, n) = \ulcorner\varphi(n)\urcorner.$$

Takođe se mogu kodirati dokazi u T, i može se definisati u P binarna relacija $Prov_T$ tako da važi sledeće:

> $Prov_T(n_1, n_2)$ je dokazivo u P akko je n_1 kôd dokaza u T formule čiji je kôd n_2.

Sa definicijom

$$Pr(x) \Leftrightarrow_{df} \exists y\, Prov_T(y, x)$$

dobijamo predikat koji zadovoljava sledeće uslove:

D1. $\vdash \varphi \Rightarrow \vdash Pr(\ulcorner\varphi\urcorner)$

D2. $\vdash Pr(\ulcorner\varphi\urcorner) \rightarrow Pr(\ulcorner Pr(\ulcorner\varphi\urcorner)\urcorner)$

D3. $\vdash Pr(\ulcorner\varphi\rightarrow\psi\urcorner) \rightarrow (Pr(\ulcorner\varphi\urcorner) \rightarrow Pr(\ulcorner\psi\urcorner))$.

Za sve formalne sisteme T koji su za nas zanimljivi, uključujući i P, važi i implikacija konverzna od D1. Formula $Pr(\ulcorner\varphi\urcorner)$ se može interpretirati kao „φ je dokazivo u T“.

Teoreme o nepotpunosti zavise od sledeće leme:

Lema o dijagonalizaciji. Neka $\psi(x)$ ima samo promenljivu x slobodnu. Onda postoji formula φ bez slobodnih promenljivih tako da $\vdash \varphi \leftrightarrow \psi(\ulcorner\varphi\urcorner)$.

Dokaz. Neka $\theta(x) \Leftrightarrow_{df} \psi(sub(x, x))$ ($\theta(x)$ se zove *dijagonalizacija* od $\psi(x)$), i neka $n =_{df} \ulcorner\theta(x)\urcorner$ i $\varphi \Leftrightarrow_{df} \theta(n)$. Onda se u T može dokazati:

$$\begin{aligned}
\varphi &\leftrightarrow \theta(n),\\
&\leftrightarrow \psi(sub(n, n)),\\
&\leftrightarrow \psi(sub(\ulcorner\theta(x)\urcorner, n)),\\
&\leftrightarrow \psi(\ulcorner\theta(n)\urcorner),\\
&\leftrightarrow \psi(\ulcorner\varphi\urcorner).
\end{aligned}$$

■

Zatim primenjujemo ovu lemu uzimajući za $\psi(x)$ formulu $\neg Pr(x)$.

Prva teorema o nepotpunosti. Neka je $\vdash \varphi \leftrightarrow \neg Pr(\ulcorner\varphi\urcorner)$. Onda ako je T konzistentno,

(i) *ne* $\vdash \varphi$

(ii) *ako* $\vdash Pr(\ulcorner\varphi\urcorner) \Rightarrow \vdash \varphi$, *onda ne* $\vdash \neg\varphi$.

Dokaz. (i) Imamo

$$\vdash \varphi \Rightarrow \vdash Pr(\ulcorner\varphi\urcorner) \qquad \text{(D1)}$$
$$\Rightarrow \vdash \neg\varphi$$

što uz konzistentnost T daje *ne* $\vdash \varphi$.

(ii) Imamo

$$\vdash \neg\varphi \Rightarrow \vdash Pr(\ulcorner\varphi\urcorner)$$
$$\Rightarrow \vdash \varphi \qquad \text{(po pretpostavci)}$$

što uz konzistentnost T daje *ne* $\vdash \neg\varphi$. ∎

Kada su poznati detalji kodiranja vidi se da je φ finitarna formula. Ta formula je istinita zato što ona na izvestan način tvrdi svoju nedokazivost i zaista je nedokaziva.

Druga teorema o nepotpunosti. Neka je Con_T formula $\neg Pr(\ulcorner 1 = 0\urcorner)$. Onda ako je T konzistentno, *ne* $\vdash Con_T$.

Dokaz. Neka φ bude kao u prošloj teoremi. Pokazaćemo da $\vdash \varphi \leftrightarrow Con_T$. U T se može dokazati

$$1 = 0 \rightarrow \varphi$$
$$Pr(\ulcorner 1 = 0\urcorner) \rightarrow Pr(\ulcorner\varphi\urcorner) \qquad \text{(D1 i D3)}$$
$$\neg Pr(\ulcorner\varphi\urcorner) \rightarrow \neg Pr(\ulcorner 1 = 0\urcorner)$$
$$\varphi \rightarrow Con_T.$$

Za konverznu implikaciju imamo da je sledeće dokazivo u T

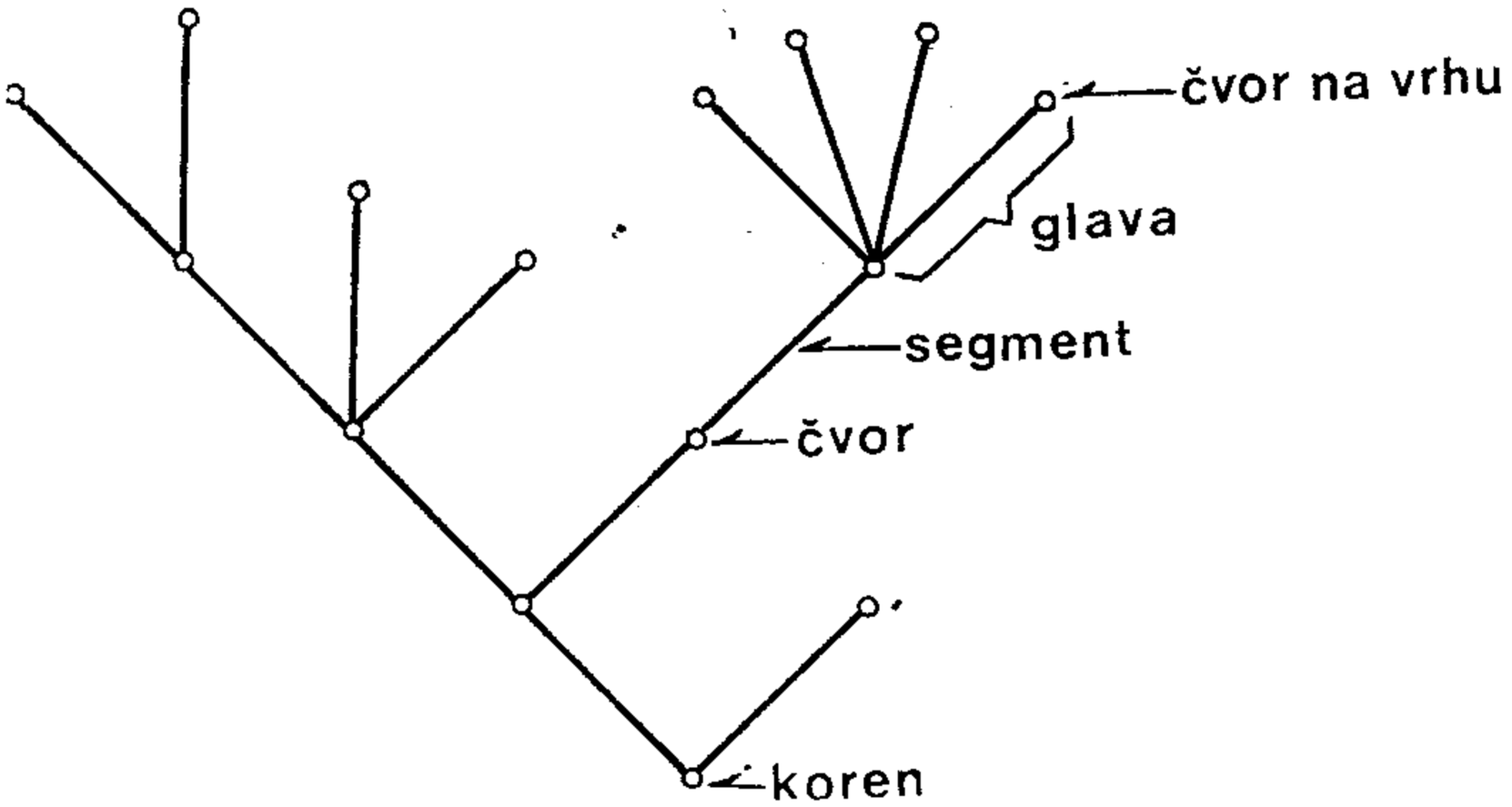
$$Pr(\ulcorner\varphi\urcorner) \rightarrow Pr(\ulcorner Pr(\ulcorner\varphi\urcorner)\urcorner) \qquad \text{(D2)}$$
$$\rightarrow Pr(\ulcorner\neg\varphi\urcorner) \qquad \text{(D1, D3 i } \vdash \neg\varphi \leftrightarrow Pr(\ulcorner\varphi\urcorner)\text{)}$$
$$\rightarrow Pr(\ulcorner\varphi \wedge \neg\varphi\urcorner) \qquad \text{(D1, D3 i logika)}$$
$$\rightarrow Pr(\ulcorner 1 = 0\urcorner) \qquad \text{(D1, D3 i logika)}$$
$$\neg Pr(\ulcorner 1 = 0\urcorner) \rightarrow \neg Pr(\ulcorner\varphi\urcorner)$$
$$Con_T \rightarrow \varphi.$$

Onda iz prve teoreme o nepotpunosti sledi *ne* $\vdash Con_T$. ∎

Formula Con_T, tj. $\neg Pr(\ulcorner 1=0 \urcorner)$, se uz interpretaciju predikata Pr koju smo gore spomenuli svodi na tvrđenje da u T nije dokazivo $1=0$, tj. na tvrđenje da je T konzistentan sistem.

§ 5. **Herkul i hidra.** U ovom odeljku predstavićemo jednu kombinatornu teoremu Parisa i Kirbya koja, iako je izraziva na jeziku formalne aritmetike, nije dokaziva u njoj. Teoreme iz kombinatorike ili teorije brojeva, koje se pozivaju na funkcije koje izvanredno brzo rastu, a koje nisu dokazive u formalnoj aritmetici, ispituju se tek u poslednjih nekoliko godina. One treba da pokažu da formalnoj aritmetici nedostaju ne samo neka čudna tvrđenja koja su izmislili logičari, kao što je φ iz prve teoreme o nepotpunosti ili Con_T, nego i teoreme koje mogu interesovati druge matematičare.

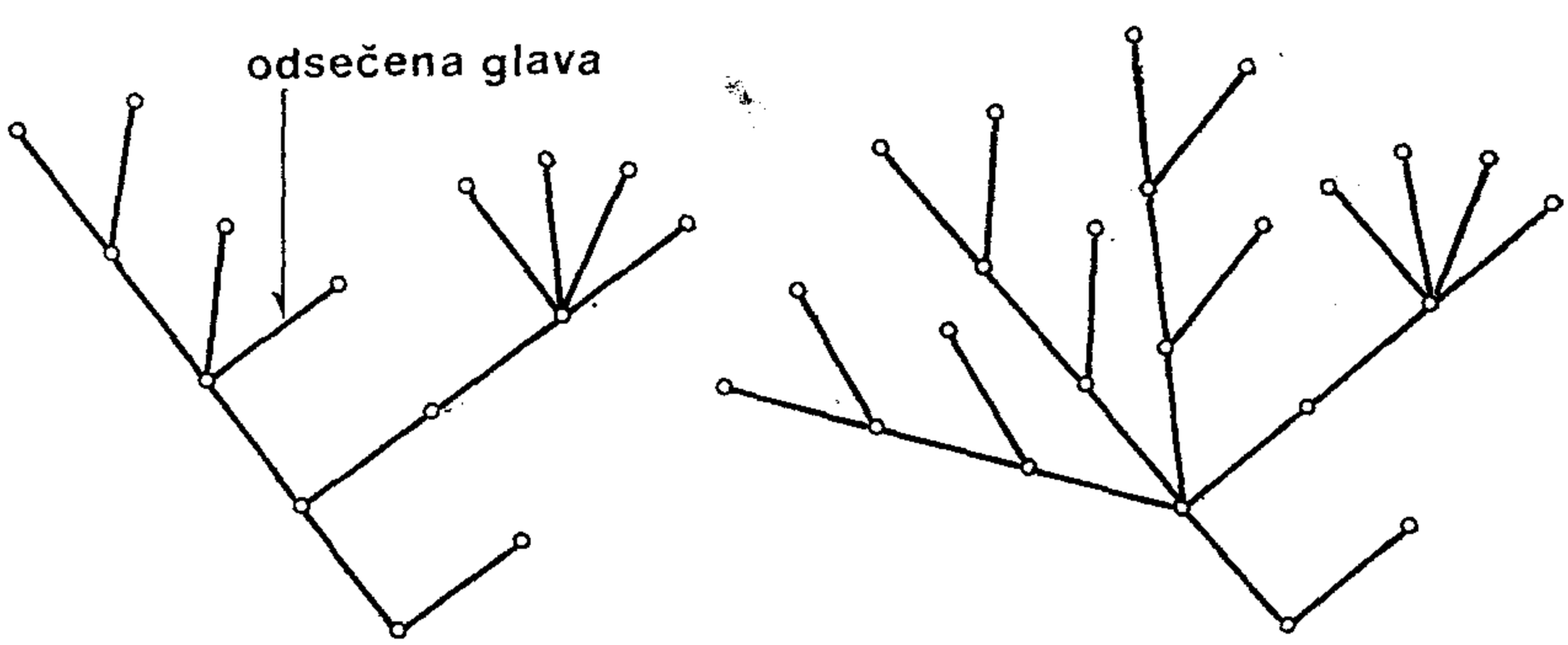
Hidra je konačno drvo, pod čime podrazumevamo konačan skup pravolinijskih *segmenata* od kojih svaki spaja dva *čvora*, tako da je svaki čvor jedinstvenim lancem segmenata povezan sa *korenom*. Znači, jedna hidra izgleda ovako:



Čvor na vrhu je čvor koji pripada samo jednom segmentu i nije koren. *Glava* hidre je čvor na vrhu zajedno sa njegovim segmentom.

Bitka između Herkula i neke date hidre se odvija ovako. U n-tom koraku bitke ($n \geqslant 1$) Herkul odseče hidri jednu glavu. Onda hidri izrastu nove glave na sledeći način. Iz čvora iz kojeg je rasla glava koja je baš odsečena vratimo se za jedan segment ka korenu. Uočimo sada drvo koje raste iz čvora do kojeg smo stigli i koje

se sastoji od segmenta preko kojeg smo se vratili i svega onoga iznad tog segmenta što je ostalo posle dekapitacije. Iz čvora do kojeg smo stigli sada izraste n novih primeraka ovog drveta. Na primer, ako u drugom koraku Herkul odseče hidri glavu označenu na slici levo, posle drugog koraka hidra će izgledati kao na slici desno:

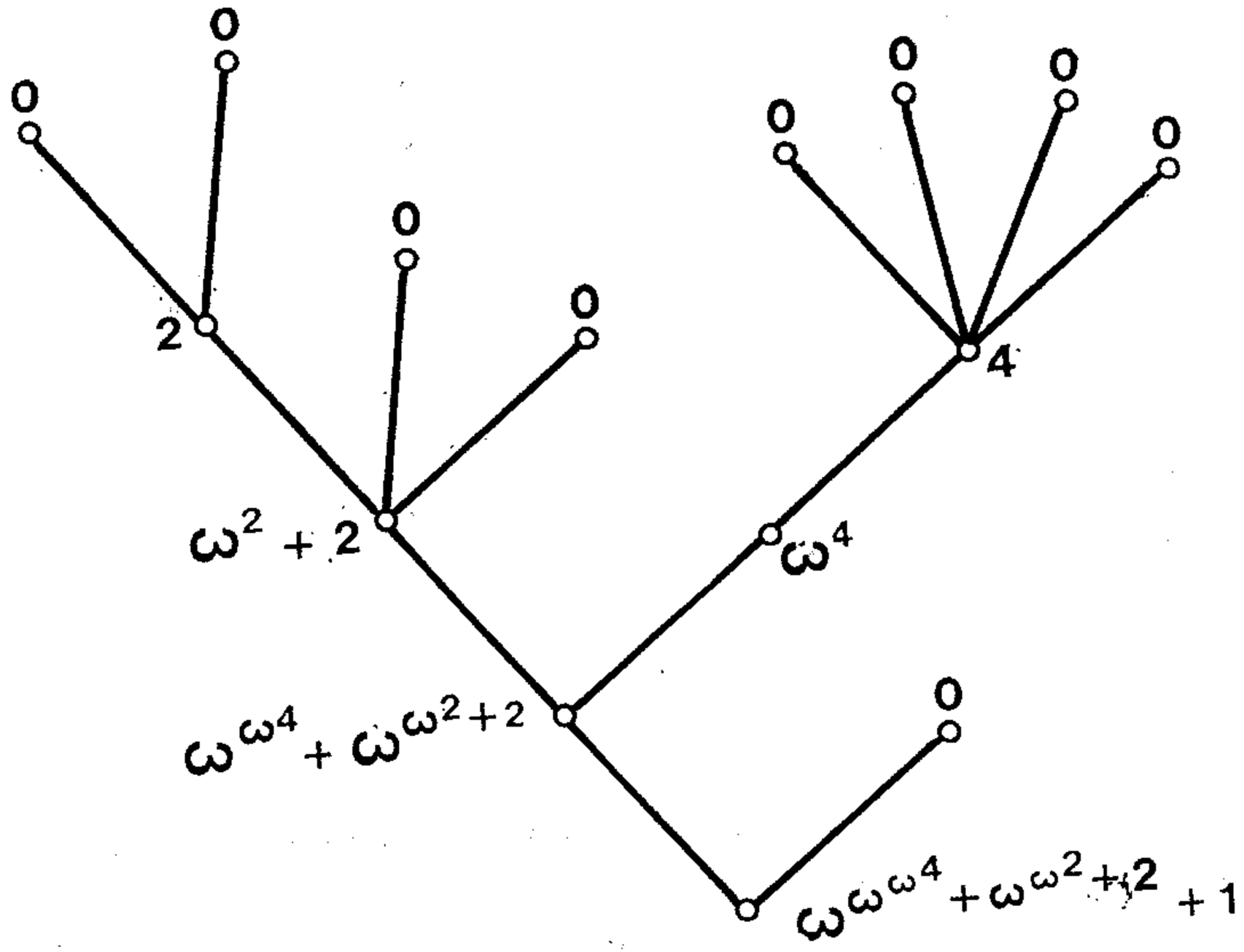


Ako je glava koja je baš odsečena rasla iz korena, ništa novo ne raste. Herkul *pobeđuje* ako posle konačno mnogo koraka od hidre ne ostaje ništa osim korena. *Strategija* je funkcija koja za svaki korak bitke određuje Herkulu koju glavu da odseče.

Ako je hidra iole složenija, vidi se da će njene glave ubrzo početi strašno da bujaju. S druge strane, vidi se i da račvanja imaju tendenciju da se tokom igre pomeraju naniže, i da hidra vremenom postaje niža, iako se strašno nagojila. Ako uočimo ovo drugo, manje će nas iznenaditi sledeća teorema:

(i) Svaka strategija omogućuje Herkulu da pobedi bilo koju hidru.

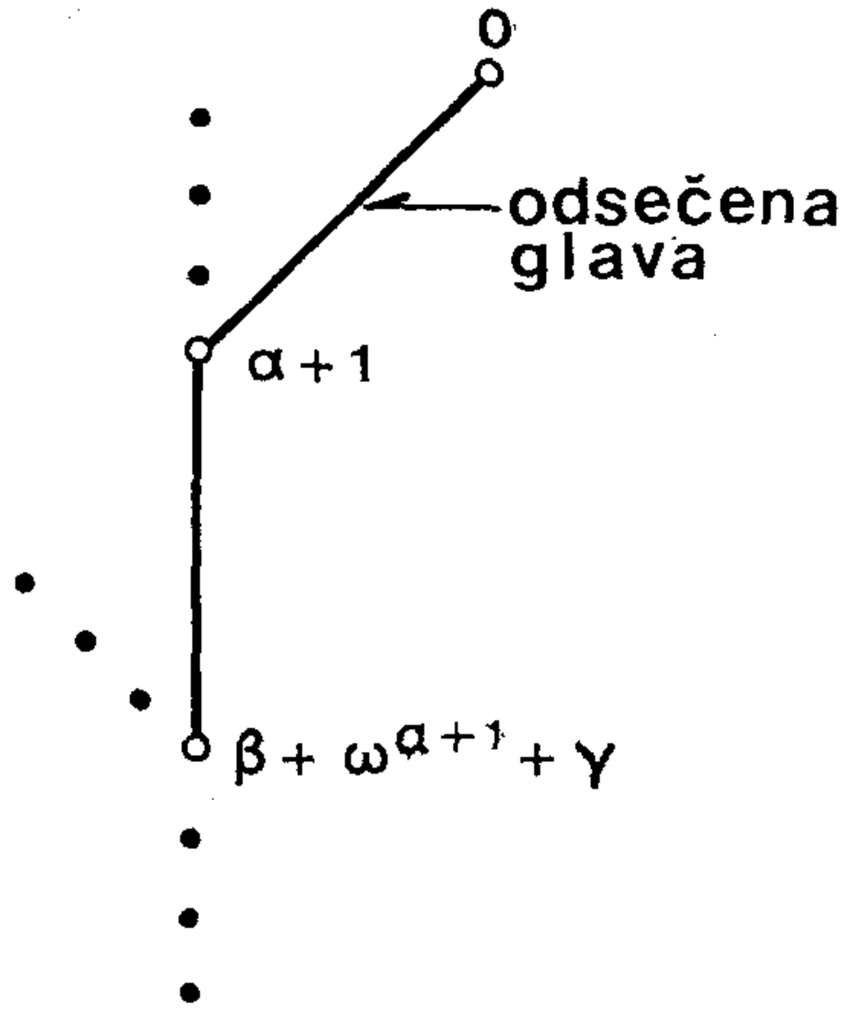
Dokaz ove teoreme se odvija ovako. Pripišimo prvo svakom čvoru date hidre jedan ordinal manji od ε_0 na sledeći način: svaki čvor na vrhu dobija 0; svaki drugi čvor dobija $\omega^{\alpha_1}+\cdots+\omega^{\alpha_n}$, gde su $\alpha_1 \geqslant \cdots \geqslant \alpha_n$ ordinali pripisani čvorovima koji su neposredno iznad našeg čvora. Ordinal hidre je ordinal koji je pripisan njenom korenu. Za hidru koju smo gore uzeli za primer dobijamo sledeće (imajući u vidu da je $\omega^0 = 1$):

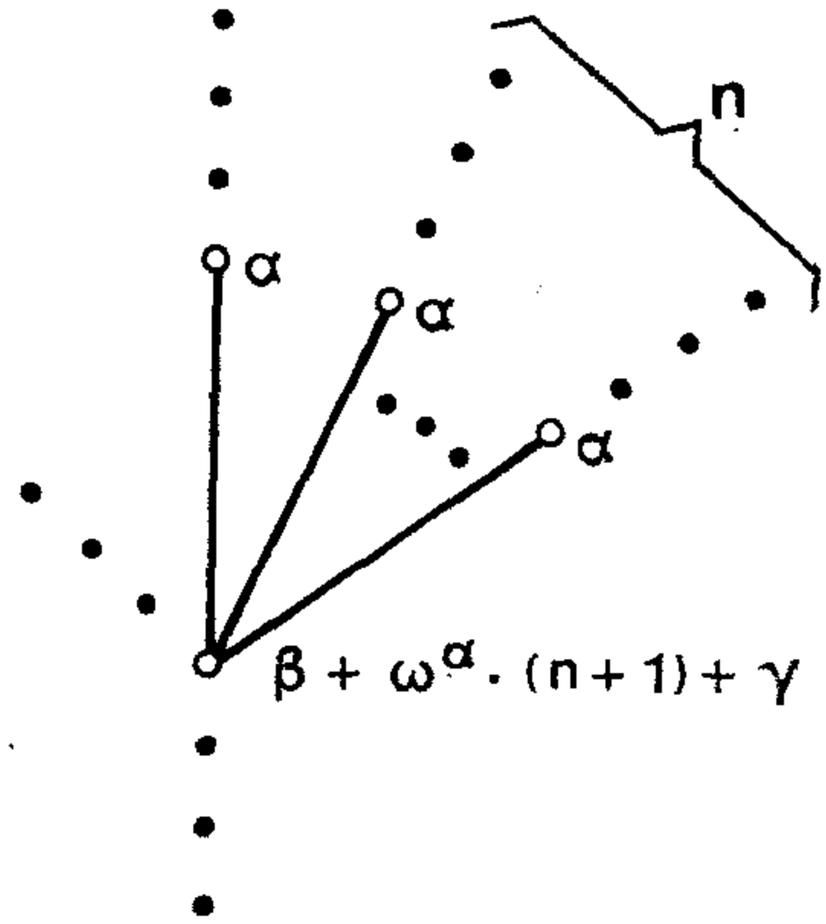


Sada je dovoljno utvrditi da je u proizvoljnoj bici ordinal hidre posle n-tog koraka manji od ordinala pre n-tog koraka. Teorema (i) onda sledi, jer su sve bitke, tj. svi opadajući nizovi ordinala, konačni. Tvrđenje da su svi opadajući nizovi ordinala manjih od ε_0 konačni je ekvivalentno sa indukcijom do ε_0.

Sasvim je lako utvrditi da se ordinal hidre smanjio ako je glava koja je baš odsečena rasla iz korena. Inače dobijamo sledeću sliku (str. 78), na kojoj je na levoj strani prikazan deo hidre pre n-tog koraka, a na desnoj odgovorajući deo posle n-tog koraka. Sada treba utvrditi da je $\omega^{\alpha+1} = \omega^\alpha \cdot \omega > \omega^\alpha \cdot (n+1)$, što povlači da se ordinal cele hidre smanjio. (Pošto je $\omega^\alpha \cdot \omega > \omega^\alpha \cdot f(n)$, gde je f bilo koja funkcija sa prirodnih brojeva na prirodne brojeve, mogli smo propisati da hidri u n-tom koraku izraste ne n novih delova, nego npr. n^n, ili n^{n^n}, ili $n^{\cdot^{\cdot^{\cdot^{n}}}}$, novih delova, i (i) bi i dalje važilo.)

Hidre se mogu kodirati prirodnim brojevima i tako možemo govoriti o bitkama između Herkula i raznih hidri na jeziku formalne aritmetike. Teoremu (i) možemo zapisati na tom jeziku ako se ograničimo na *rekurzivne* strategije, tj. strategije koje su rekurzivne





funkcije (v. Dodatak B poglavlja o desetom Hilbertovom problemu). Onda se može dokazati sledeća teorema:

(ii) Tvrđenje „Svaka rekurzivna strategija omogućuje Herkulu da pobedi bilo koju hidru“ nije dokazivo u *P*.

Ovde ne možemo da ulazimo u detalje dokaza za ovu teoremu. Ukratko, konstruiše se jedna rekurzivna strategija τ tako da je dokaz da τ vodi Herkulovoj pobedi ekvivalentan jednoj posebnoj indukciji do ε_0. Za ovu indukciju se onda pokazuje da ne može biti izvodiva u *P*.

DODATAK B: GENTZENOV DOKAZ KONZISTENTNOSTI FORMALNE ARITMETIKE

U ovom dodatku daćemo skicu Gentzenovog dokaza konzistentnosti formalne aritmetike. Radi se o verziji Gentzenovog dokaza koju smo prvo pomenuli u tekstu gore (a koja je hronološki gledano druga verzija). Mnogi tehnički detalji će u ovoj skici biti zanemareni.

§ 1. Formalizacija aritmetike pomoću sekvenata. Pretpostavimo da je dat jezik *L* kao u prošlom dodatku s tim što kao primitivne logičke konstante uzimamo samo $\wedge$, $\neg$, $\forall$, i $=$ (ostale logičke konstante se u klasičnoj logici mogu definisati pomoću ovih). *Atomske*

formule jezika L su formule bez logičkih konstanti $\wedge$, $\neg$ i $\forall$. *Stepen* neke formule je broj ovih logičkih konstanti u njoj.

Sekventi su izrazi oblika $\varphi_1, \ldots, \varphi_m \vdash \psi_1, \ldots, \psi_n$, $m \geqslant 0$, $n \geqslant 0$, gde su φ_i i ψ_j formule jezika L. Konstanta $\vdash$ se naziva *rampom*. Sekvent se interpretira kao da tvrdi da ako su sve formule sa leve strane rampe istinite, onda je bar jedna formula sa desne strane rampe istinita: zapete sa leve strane rampe odgovaraju konjunkciji, zapete sa desne strane disjunkciji, a rampa odgovara implikaciji. (Sekvent $\varphi_1, \ldots, \varphi_m \vdash \psi$ se može shvatiti kao zapis da je ψ logička posledica od $\varphi_1, \ldots, \varphi_m$, ili da se zaključak ψ može dedukovati iz premisa $\varphi_1, \ldots, \varphi_m$.) Shematska slova za konačne (uključujući i prazne) nizove formula su Γ, Δ, Θ, Ξ, Γ_1, ...

Pravila izvođenja su sledeća:

Strukturalna pravila:

slabljenje: $$\frac{\Gamma \vdash \Delta}{\varphi, \Gamma \vdash \Delta}, \qquad \frac{\Gamma \vdash \Delta}{\Gamma \vdash \Delta, \varphi};$$

kontrakcija: $$\frac{\varphi, \varphi, \Gamma \vdash \Delta}{\varphi, \Gamma \vdash \Delta}, \qquad \frac{\Gamma \vdash \Delta, \varphi, \varphi}{\Gamma \vdash \Delta, \varphi};$$

permutacija: $$\frac{\Gamma, \varphi, \psi, \Delta \vdash \Theta}{\Gamma, \psi, \varphi, \Delta \vdash \Theta}, \qquad \frac{\Gamma \vdash \Delta, \varphi, \psi, \Theta}{\Gamma \vdash \Delta, \psi, \varphi, \Theta};$$

sečenje: $$\frac{\Gamma \vdash \Delta, \varphi \quad \varphi, \Theta \vdash \Xi}{\Gamma, \Theta \vdash \Delta, \Xi}.$$

Formula φ u nekom sečenju se naziva *formulom sečenja*, a njen stepen *stepenom sečenja*.

Logička pravila:

$\wedge$: $$\frac{\Gamma \vdash \Delta, \varphi \quad \Gamma \vdash \Delta, \psi}{\Gamma \vdash \Delta, \varphi \wedge \psi}, \qquad \frac{\varphi, \Gamma \vdash \Delta}{\varphi \wedge \psi, \Gamma \vdash \Delta}, \qquad \frac{\psi, \Gamma \vdash \Delta}{\varphi \wedge \psi, \Gamma \vdash \Delta};$$

$\neg$: $$\frac{\varphi, \Gamma \vdash \Delta}{\Gamma \vdash \Delta, \neg \varphi}, \qquad \frac{\Gamma \vdash \Delta, \varphi}{\neg \varphi, \Gamma \vdash \Delta};$$

$\forall$: $$\frac{\Gamma \vdash \Delta, \varphi(x)}{\Gamma \vdash \Delta, \forall x \varphi(x)}, \qquad \frac{\varphi(t), \Gamma \vdash \Delta}{\forall x \varphi(x), \Gamma \vdash \Delta};$$

prvo pravilo za $\forall$ važi pod uslovom da se x, koje se naziva *karakterističnom promenljivom*, ne javlja slobodno u donjem sekventu. Formule logičkih pravila u kojima se javljaju logičke konstante se nazivaju *glavnim formulama* pravila.

Pravilo indukcije: $$\frac{\varphi(x),\ \Gamma\vdash\Delta,\ \varphi(x')}{\varphi(0),\ \Gamma\vdash\Delta,\ \varphi(t)}$$

koje važi pod uslovom da se *karakteristična promenljiva* x ne javlja slobodna u donjem sekventu. *Stepen indukcije* je stepen formule $\varphi(0)$.

Osnovni logički sekventi su sekventi oblika $\varphi\vdash\varphi$. *Osnovni aritmetički sekventi* su sekventi u kojima se javljaju samo atomske formule i koji za proizvoljne zamene slobodnih promenljivih numeralima postaju istiniti sekventi, uz interpretaciju sekvenata koju smo gore spomenuli. Za atomsku formulu bez promenljivih odlučivo je da li je istinita ili ne (u modelu prirodnih brojeva). Za sekvent bez slobodnih promenljivih odlučivo je da li je osnovni ili ne; za sekvent sa slobodnim promenljivima to nije uvek odlučivo — međutim, to ne utiče na naš dokaz.

Izvođenje je drvo sekvenata, gde su na vrhu osnovni sekventi, sa kojih se na niže sekvente prelazi pomoću pravila izvođenja, sve do sekventa na dnu, za koji se kaže da je *izvodljiv*. *Lanac* u nekom izvođenju je niz sekvenata koji počinje nekim sekventom na vrhu i silazi drvetom do dna izvođenja.

Može se pokazati da svakoj teoremi φ formalne Peanove aritmetike, aksiomatizovane na uobičajeni hilbertovski način kao u prošlom dodatku, odgovara izvodljiv sekvent $\vdash\varphi$. Prema tome, dovoljno je pokazati da $\vdash 1=0$ nije izvodljivo, da bismo dokazali konzistentnost formalne Peanove aritmetike. A da bismo to pokazali dokazaćemo da *prazan sekvent* $\vdash$, gde su i leva i desna strana prazne, *nije izvodljiv* — jer iz $\vdash 1=0$ i osnovnog aritmetičkog sekventa $1=0\vdash$ pomoću sečenja izvodimo prazan sekvent. (Obrnuto, iz praznog sekventa pomoću slabljenja izvodimo $\vdash 1=0$.) Izvođenje koje na dnu nema praznog sekventa se zove *korektnim*. Dokaz da su sva izvođenja korektna se sprovodi u dva koraka.

U prvom koraku se definiše *redukcija* koja svako nekorektno izvođenje pretvara u jedno drugo („jednostavnije“) nekorektno izvođenje. U drugom koraku se svakom izvođenju dodeljuje jedan *ordinal* i pokazuje se da redukcija pretvara izvođenje sa većim ordi-

nalom u izvođenje sa manjim ordinalom (time se precizira pojam „jednostavnije“ u zagradi gore). Odatle korektnost svih izvođenja sledi transfinitnom indukcijom.

§ 2. Redukcija nekorektnog izvođenja. Proizvoljno nekorektno izvođenje pripremamo za redukciju na sledeći način. Sve slobodne promenljive, osim karakterističnih, zamenimo npr. sa 0, i zatim terme bez slobodnih promenljivih zamenimo numeralima koji su im jednaki. Rezultat te pripreme će i dalje biti nekorektno izvođenje.

Zatim definišemo pojam *završetka* izvođenja. Završetak se sastoji od svih sekvenata nekog izvođenja koji se dobijaju kad krenemo od dna i zaustavimo se u svakom lancu čim naiđemo na donji sekvent nekog logičkog pravila — ti donji sekventi pripadaju završetku, gornji ne. Ako ne naiđemo na logičko pravilo idemo do vrha izvođenja. U završetku se mogu naći samo strukturalna pravila i indukcija. Zato razlikujemo dva slučaja: završetak sadrži bar jednu indukciju — u tom slučaju sprovodimo *induktivnu redukciju;* završetak ne sadrži ni jednu indukciju — u tom slučaju sprovodimo *logičku redukciju.*

§ 2.1. Induktivna redukcija. Izaberimo indukciju u završetku takvu da nema indukcije ispod nje. Ta indukcija ima oblik

$$\frac{\varphi(x),\ \Gamma \vdash \Delta,\ \varphi(x')}{\varphi(0),\ \Gamma \vdash \Delta,\ \varphi(n).}$$

U donjem sekventu se javlja numeral n, jer smo se u pripremi za redukciju oslobodili slobodnih promenjivih iz tog sekventa i zamenili terme bez promenljivih numeralima. Induktivnom redukcijom ovu indukciju pretvaramo u

$$\cfrac{\cfrac{\cfrac{\varphi(0),\ \Gamma \vdash \Delta,\ \varphi(0') \quad \varphi(0'),\ \Gamma \vdash \Delta,\ \varphi(0'')}{\varphi(0),\ \Gamma,\ \Gamma \vdash \Delta,\ \Delta,\ \varphi(0'')}\ \text{sečenje}}{\text{eventualno permutacije i kontrakcije}}}{\varphi(0),\ \Gamma \vdash \Delta,\ \varphi(0'')}$$

$$\vdots$$

$$\varphi(0),\ \Gamma \vdash \Delta,\ \varphi(n).$$

Iznad sekvenata $\varphi(0), \Gamma \vdash \Delta, \varphi(0')$ i $\varphi(0'), \Gamma \vdash \Delta, \varphi(0'')$ itd., napišemo u svakom slučaju onaj deo izvođenja koji prethodi sekventu $\varphi(x), \Gamma \vdash \Delta, \varphi(x')$ zamenjujući slobodnu promenljivu x u tom delu, gde god nije karakteristična, odgovarajućim numeralom.

Ako je n jednako 0, onda $\varphi(0), \Gamma \vdash \Delta, \varphi(0)$ dobijamo iz $\varphi(0) \vdash \varphi(0)$, eventualno koristeći strukturalna pravila.

Intuitivno, induktivna redukcija zamenjuje indukciju konačnim nizom sečenjâ.

§ 2.2. Logička redukcija. Logičkoj redukciji prethodi jedna priprema koja treba da eliminiše javljanja slabljenja i osnovnih logičkih sekvenata iz završetka bez indukcije. Pre nego što pređemo na tu pripremu uvodimo sledeće pojmove. Identične formule u gornjim i donjim sekventima pravila nazivaće se *združenima*, pri čemu je ova relacija tranzitivna. Sve formule združene sa nekom formulom u završetku čine jednu *skupinu*. Svakoj skupini u našem završetku bez indukcije odgovara jedno sečenje, tako što formule tog sečenja pripadaju skupini. To je zato što je na dnu završetka prazan sekvent, koji se mogao dobiti samo uz sečenja. Polazeći od leve formule sečenja neke skupine naviše dobijamo drvo sastavljeno od njoj identičnih formula koje se zove *leva strana skupine*: to drvo se grana ako naiđemo na kontrakciju koja se odnosila na formulu skupine; to drvo se na vrhu završava kad naiđemo na slabljenje kojim je uvedena formula skupine, ili smo stigli do kraja završetka. Sve formule iz leve strane skupine su sa desne strane rampe. Potpuno analogno se određuje komplementarna *desna strana skupine*.

Sada možemo preći na našu pripremu za logičku redukciju. Slabljenja se eliminišu iz našeg završetka tako što uzmemo neko slabljenje iznad kojeg nema slabljenja u završetku i izbrišemo njegov donji sekvent. Uz to izbrišemo i sve formule iz skupine formula združenih sa formulom koju je to slabljenje uvelo, pri čemu se mogu izgubiti i neka druga strukturalna pravila ispod slabljenja koje smo izbrisali — kada se gubi sečenje gubi se i jedan deo

izvođenja. Zatim eliminišemo osnovne logičke sekvente iz završetka. Takav se sekvent sada može javiti samo kao gornji sekvent nekog sečenja, jer kontrakcija i permutacija se na njega ne mogu primeniti. Onda je donji sekvent tog sečenja identičan sa tim osnovnim logičkim sekventom. Brišući takva sečenja dobijamo na kraju završetak bez slabljenjâ i bez osnovnih logičkih sekvenata (i bez indukcije).

Sada treba pokazati da postoji bar jedna skupina u završetku koja i u svojoj levoj i u svojoj desnoj strani sadrži bar jednu formulu koja je glavna formula nekog logičkog pravila. (Ta formula, koja je eliminisana sečenjem te skupine, je, intuitivno, formula kojom smo uveli neku logičku konstantu da bismo je zatim eliminisali, formula kojom smo napravili zaobilazak u dokazu. Taj zaobilazak pokušavamo da eliminišemo i normalizujemo dokaz.) Drugim rečima, treba pokazati da postoji pogodno mesto za našu logičku redukciju. Primetimo prvo da naše izvođenje mora sadržati bar neko logičko pravilo. Inače bi celo izvođenje bilo završetak, i to završetak samo sa atomskim formulama bez promenljivih — znači sa odlučivim formulama. Lako je pokazati da polazeći od istinitih sekvenata u takvom izvođenju ne možemo stići do praznog sekventa, koji je neistinit. Sada posmatrajmo sve lance završetka na čijim vrhovima je donji sekvent nekog logičkog pravila. Sledimo te lance od gore na dole sve dok se u sekventima na koje nailazimo nalaze formule iz skupine glavne formule logičkog pravila od kojeg smo krenuli. To jest, spustimo se do sečenja te skupine. Iz tog sečenja potiču leva i desna strana naše skupine. Tako nalazimo pogodno mesto za našu logičku redukciju.

Pre nego što pređemo na tu redukciju uvešćemo još jedan pojam. *Nivoom* nekog sekventa u izvođenju zvaćemo najveći stepen sečenjâ ili indukcija čiji donji sekvent stoji ispod tog sekventa. Ako tih sečenja i indukcija nema, nivo je 0. Pojam nivoa nam omogućuje da sečenja koja su viša tretiramo kao da uvek imaju veći ili jednak stepen od nižih sečenja. Indukcija se tu ponaša kao sečenje, jer se induktivnom redukcijom ona zamenjuje sečenjima istog stepena.

Sad prelazimo na logičku redukciju. Izaberimo jednu skupinu u našem završetku i u toj skupini izaberimo sa svake strane jednu formulu na vrhu koja je glavna formula nekog logičkog pravila. Posmatrajmo slučaj kada je glavna konstanta u toj formuli $\forall$ (preostali slučajevi sa $\wedge$ i $\neg$ su analogni, i nećemo ih posebno razmatrati). Izvođenje onda izgleda ovako:

$$\dfrac{\begin{array}{c}\vdots\\ (x)\\ \vdots\\ \Gamma_1 \vdash \Delta_1, \varphi(x)\end{array}}{\Gamma_1 \vdash \Delta_1, \forall x \varphi(x)} \qquad \dfrac{\begin{array}{c}\vdots\\ \vdots\\ \varphi(n), \Gamma_2 \vdash \Delta_2\end{array}}{\forall x \varphi(x), \Gamma_2 \vdash \Delta_2}$$

početak završetka

$$\text{nivo } \rho \quad \dfrac{\Gamma \vdash \Delta, \forall x \varphi(x) \qquad \forall x \varphi(x), \Theta \vdash \Xi}{\Gamma, \Theta \vdash \Delta, \Xi}$$

sečenje skupine

$$\begin{array}{l}\text{nivo } \rho \\ \text{nivo } \sigma < \rho\end{array} \quad \dfrac{\begin{array}{c}\vdots\\ \Gamma_3 \vdash \Delta_3\end{array}}{\vdash}$$

prazni sekvent.

Zahvaljujući pripremi za redukciju term n u $\varphi(n)$ mora biti numeral. Pošto je nivo praznog sekventa 0, a nivo gornjih sekvenata sečenja naše skupine bar 1, mora postojati sekvent $\Gamma_3 \vdash \Delta_3$.

Logičkom redukcijom ovo izvođenje pretvaramo u:

$$
\begin{array}{cc}
\begin{array}{c}
\vdots\,(n) \\
\dfrac{\Gamma_1 \vdash \Delta_1, \varphi(n)}{\Gamma_1 \vdash \varphi(n), \Delta_1, \forall x\,\varphi(x)}\ \text{slabljenje i eventualno permutacije}
\end{array}
&
\begin{array}{c}
\vdots \\
\dfrac{\varphi(n), \Gamma_2 \vdash \Delta_2}{\forall x\,\varphi(x), \Gamma_2 \vdash \Delta_2}
\end{array}
\end{array}
$$

$$
\begin{array}{cc}
\begin{array}{c}
\vdots\,(x) \\
\dfrac{\Gamma_1 \vdash \Delta_1, \varphi(x)}{\Gamma_1 \vdash \Delta_1, \forall x\,\varphi(x)}
\end{array}
&
\begin{array}{c}
\vdots \\
\dfrac{\varphi(n), \Gamma_2 \vdash \Delta_2}{\forall x\,\varphi(x), \Gamma_2, \varphi(n) \vdash \Delta_2}\ \text{slabljenje i eventualno permutacije}
\end{array}
\end{array}
$$

$$
\text{nivo } \rho \quad \dfrac{\Gamma \vdash \varphi(n), \Delta, \forall x\,\varphi(x) \qquad \forall x\,\varphi(x), \Theta \vdash \Xi}{\Gamma, \Theta \vdash \varphi(n), \Delta, \Xi}
\qquad
\dfrac{\Gamma \vdash \Delta, \forall x\,\varphi(x) \qquad \forall x\,\varphi(x), \Theta, \varphi(n) \vdash \Xi}{\Gamma, \Theta, \varphi(n) \vdash \Delta, \Xi} \quad \text{nivo } \rho
$$

$$
\dfrac{
\dfrac{\text{nivo } \rho \quad \dfrac{\vdots}{\Gamma_3 \vdash \varphi(n), \Delta_3}}{\Gamma_3 \vdash \Delta_3, \varphi(n)}\ \text{eventualno permutacije}
\qquad
\dfrac{\dfrac{\vdots}{\Gamma_3, \varphi(n) \vdash \Delta_3} \quad \text{nivo } \rho}{\varphi(n), \Gamma_3 \vdash \Delta_3}\ \text{eventualno permutacije}
}{
\Gamma_3, \Gamma_3 \vdash \Delta_3, \Delta_3
}\ \text{novo sečenje}
$$

$$
\dfrac{\Gamma_3, \Gamma_3 \vdash \Delta_3, \Delta_3}{\Gamma_3 \vdash \Delta_3}\ \text{eventualno permutacije i kontrakcije} \qquad \text{nivo } \sigma
$$

$$
\dfrac{\vdots}{\vdash}
$$

Na prvi pogled izgleda kao da je novo izvođenje kompleksnije od starog. Sada imamo dva sečenja sa formulom $\forall x \varphi(x)$. (Ta sečenja se moraju i dalje tolerisati jer je moguće da se $\forall x \varphi(x)$ ne javlja samo na mestima koja smo naznačili, tj. skupina te formule se može granati na obe strane. Da nema tog grananja mogli bismo izvršiti redukciju tako što bi se izbeglo pojavljivanje formule $\forall x \varphi(x)$ izostavljanjem logičkih pravila i primenjivanjem sečenja sa formulom $\varphi(n)$.) Ali oba puta oslobodili smo se jednog logičkog pravila iznad sečenja. To će nam omogućiti da svaki deo izvođenja iznad gornjih sekvenata novog sečenja bude ocenjen kao manje kompleksan od odgovarajućeg dela starog izvođenja, tj. dela iznad $\Gamma_3 \vdash \Delta_3$. Međutim, sad se još javlja i novo sečenje iznad $\Gamma_3 \vdash \Delta_3$. Poenta je da to sečenje ima manji stepen od starog sečenja. Naš je cilj da iskoristimo ove činjenice da bismo redukcijom smanjili ordinal izvođenja.

§ 3. **Ordinali.** Ordinale koje ćemo koristiti uvodimo ovako:

skup S_0 čini ordinal 0,

skup S_1 čine ordinali $0, \omega^0, \omega^0 + \omega^0, \ldots$, tj. $0, 1, 2, \ldots$, tj. svi ordinali ispod ω,

skup S_2 čine ordinali ispod ω^ω,

skup S_3 čine ordinali ispod $(\omega^{\omega^\omega}$ (tj. $\omega^{(\omega^\omega)}$), itd.

Ordinali svih skupova S_k, gde je k prirodan broj, su manji od ε_0. Kanonski, svaki ordinal skupa S_{k+1}, osim 0, se može predstaviti kao

$$\omega^{\alpha_1} + \omega^{\alpha_2} + \cdots + \omega^{\alpha_m},$$

gde α_i pripada skupu S_k, $\alpha_1 \leqslant \alpha_2 \leqslant \cdots \leqslant \alpha_m$, i m je prirodan broj $\geqslant 1$. Odsada nadalje, stalno ćemo govoriti o ordinalama koji su kanonski predstavljeni. Ako je $\alpha = \omega^{\gamma_1} + \cdots + \omega^{\gamma_m}$ i $\beta = \omega^{\delta_1} + \cdots + \omega^{\delta_n}$, $m \geqslant 1$, $n \geqslant 1$, onda je $\alpha < \beta$ kada kod prvog γ_i i δ_j koji nisu jednaki, $\gamma_i < \delta_j$.

Prirodna suma dva ordinala različita od nule se definiše ovako. Neka α i β budu kao malopre; onda se prirodna suma $\alpha\#\beta$ dobija uređivanjem $m+n$ članova ω^{γ_i} i ω^{δ_j} po veličini i umetanjem znaka $+$ između tih članova. Lako se vidi da je $\#$ komutativno, da je $\alpha\#\beta>\alpha$, i da $\alpha_1<\alpha_2$ povlači $\alpha_1\#\beta<\alpha_2\#\beta$.

Ordinali se pripisuju izvođenjima na sledeći način. Svaki sekvent i svako pravilo u nekom izvođenju dobija ordinal polazeći od vrha prema dnu, i to ovako. Svaki sekvent na vrhu izvođenja dobija ordinal 1 (tj. ω^0). Ako su već određeni ordinali gornjih sekvenata nekog pravila, ordinal tog pravila se određuje na sledeći način. U slučaju strukturalnih pravila, to će biti ordinal gornjeg sekventa, osim u slučaju sečenja, kada je to prirodna suma ordinalâ gornjih sekvenata. U slučaju logičkih pravila, ordinalu gornjeg sekventa se dodaje $+1$, ili ako ima dva gornja sekventa, većem od ta dva ordinala se dodaje $+1$. I najzad, u slučaju indukcije, ako je ordinal gornjeg sekventa $\omega^{\alpha_1}+\cdots+\omega^{\alpha_m}$, onda je ω^{α_1+1} ordinal pravila. Kada znamo ordinal α nekog pravila, ordinal donjeg sekventa tog pravila se određuje ovako: ako je nivo donjeg sekventa isti kao nivo gornjeg (ili gornjih), onda je ordinal donjeg sekventa α; ako je njegov nivo manji za 1, onda je taj ordinal ω^α; ako je manji za 2, onda je taj ordinal ω^{ω^α}; itd. Ordinal izvođenja je jednak ordinalu sekventa na dnu izvođenja.

Sada treba da pokažemo da redukcija opisana u prošlom odeljku smanjuje ordinal izvođenja.

Posmatrajmo prvo induktivnu redukciju. Pretpostavimo da je ordinal gornjeg sekventa indukcije $\omega^{\alpha_1}+\cdots+\omega^{\alpha_m}$. Ordinal pravila je onda ω^{α_1+1}, i to je i ordinal donjeg sekventa, jer njegov nivo ne može biti manji od nivoa gornjeg sekventa — stepen formule $\varphi(0)$, koji je i stepen indukcije, je jednak stepenu sečenja čija je formula $\varphi(0)$ i koje se javlja u izvođenju ispod te indukcije. Ako sada pogledamo deo izvođenja kojim smo zamenili indukciju, na vrhu opet imamo ordinale $\omega^{\alpha_1}+\cdots+\omega^{\alpha_m}$. Osim toga, svi sekventi u tom delu imaju isti nivo, tj. nivo sekvenata indukcije. Ordinal sekventa na dnu tog dela je, prema tome, jednak prirodnoj sumi svih ordinala $\omega^{\alpha_1}+\cdots+\omega^{\alpha_m}$. Pošto ta suma u kanonskoj notaciji ima oblik $\omega^{\alpha_1}+\ldots$, ona je manja od ω^{α_1+1}. Ovo smanjenje ordinala čuva se do dna izvođenja, jer ispod su samo strukturalna pravila, a ako je $\alpha_1<\alpha_2$, onda je $\omega^{\alpha_1}<\omega^{\alpha_2}$, i $\alpha_1\#\beta<\alpha_2\#\beta$. Prema tome, smanjio se i ordinal celog izvođenja. Ako je n u indukciji jednako 0, u novom izvođenju $\varphi(0),\ \Gamma\vdash\Delta,\varphi(0)$ ima ordinal 1.

Pošto je u starom izvođenju ordinal ovog sekventa bio bar ω^1, opet dobijamo smanjenje.

Intuitivno treba da bude jasno zašto je za indukciju vezan ordinal ω^{α_1+1}. Ordinal ω^{α_1+1} je jednak $\omega^{\alpha_1}\cdot\omega$ — on je limit konačnih prirodnih suma ordinalâ $\omega^{\alpha_1}+\cdots+\omega^{\alpha_m}$. Te prirodne sume odgovaraju konačnim nizovima sečenjâ kojima zamenjujemo indukciju.

Posmatrajmo sada logičku redukciju. Kao i u prošlom odeljku, koncentrisaćemo se samo na slučaj sa logičkom konstantom $\forall$ (ostali slučajevi se tretiraju analogno). Ordinali pravila kojima se dobijaju sekventi $\Gamma_3\vdash\varphi(n)$, Δ_3 i $\Gamma_3, \varphi(n)\vdash\Delta_3$ u novom izvođenju — te ordinale označavamo sa α_1 i α_2 — moraju biti manji od ordinala α koji pripada pravilu kojim je dobijeno $\Gamma_3\vdash\Delta_3$ u starom izvođenju. Razlog za to je u tome što je u delovima izvođenja iznad ta dva nova sekventa i u delu izvođenja iznad starog sekventa $\Gamma_3\vdash\Delta_3$, nivo svih sekvenata isti (neposredno iznad on je ρ), a po jedno logičko pravilo koje je povećavalo ordinal je izbačeno i zamenjeno strukturalnim pravilima koja ne utiču na ordinal. Isto tako, $\Gamma_3\vdash\Delta_3$ u novom izvođenju ima isti nivo $\sigma<\rho$ kao i u starom izvođenju. I sekvent $\Gamma_3, \Gamma_3\vdash\Delta_3, \Delta_3$, iz kojeg se $\Gamma_3\vdash\Delta_3$ dobija eventualno permutacijama i kontrakcijama, ima nivo σ. Nivo τ gornjih sekvenata novog sečenja zadovoljava $\rho>\tau\geqslant\sigma$. Desna nejednakost je trivijalna, a da je $\rho>\tau$ pokazuje se na sledeći način. Po definiciji τ je maksimum broja σ i broja koji je stepen formule $\varphi(n)$. Ako je $\tau=\sigma$, onda je $\tau<\rho$ pošto je $\sigma<\rho$; a ako je τ jednak stepenu formule $\varphi(n)$, onda je $\tau<\rho$, jer je stepen formule $\varphi(n)$ manji od stepena formule $\forall x\varphi(x)$ — ρ je veće ili jednako tom drugom stepenu.

Pretpostavimo da je razlika između ρ, τ i σ minimalna, tj. $\rho-1=\tau=\sigma$. U starom izvođenju, pravilo kojim smo dobili $\Gamma_3\vdash\Delta_3$ ima ordinal α, pa prema tome $\Gamma_3\vdash\Delta_3$ ima ordinal ω^α. U novom izvođenju, odgovarajuća pravila imaju ordinale α_1 i α_2 (koji su oba manji od α) i prema tome gornji sekventi novog sečenja imaju ordinale ω^{α_1} i ω^{α_2}, a sekvent $\Gamma_3\vdash\Delta_3$ ispod tog novog sečenja ima ordinal $\omega^{\alpha_1}+\omega^{\alpha_2}$ (pretpostavljamo da je npr. $\alpha_1\geqslant\alpha_2$). Ovaj poslednji ordinal je manji od ω^α zato što je $\alpha_1<\alpha$. Pošto se ovo smanjenje prenosi do dna izvođenja, smanjuje se i ordinal izvođenja. Ako je razlika između ρ, τ i σ veća od minimalne, nejednakost

$$\omega^\alpha>\omega^{\alpha_1}+\omega^{\alpha_2}$$

se zamenjuje nejednakošću

$$\begin{matrix} \omega^{\alpha} & & \omega^{\alpha_1} & & \omega^{\alpha_2} \\ \cdot & & \cdot & & \cdot \\ \cdot & & \cdot & & \cdot \\ \cdot & & \cdot & & \cdot \\ \omega & & \omega & + & \omega \\ \cdot & & \cdot & & \cdot \\ \cdot & & \cdot & & \cdot \\ \cdot & & \cdot & & \cdot \\ \omega & > & \omega & & \end{matrix}$$

Sada se vidi kako smo iskoristili činjenice o logičkoj redukciji spomenute na kraju prošlog odeljka. U novom izvođenju jedan deo starog izvođenja se sad javlja dva puta u novom ruhu, ali oba puta nešto pojednostavljen izostavljanjem jednog logičkog pravila. Naravno, može se desiti da je $\alpha < \alpha_1 + \alpha_2$, iako je $\alpha_1 < \alpha$ i $\alpha_2 < \alpha$. Ali zato je $\omega^{\alpha} > \omega^{\alpha_1} + \omega^{\alpha_2}$. (Isto to bismo dobili i sa prirodnim brojevima kad mesto ω stavimo neki broj $\geqslant 3$.) Do ove poslednje nejednakosti ćemo doći kad napravimo korak koji odgovara uvođenju novog sečenja sa manjim stepenom.

(Da smo dokazivali konzistentnost sistema bez pravila indukcije, mogli smo mesto ordinala ω da svuda stavimo npr. 3, i koristimo običnu indukciju mesto transfinitne indukcije.)

Ovim je dokazano da se ordinal izvođenja praznog sekventa smanjuje redukcijom. Odatle transfinitnom indukcijom sledi korektnost svih izvođenja, i time je dokazana konzistentnost formalne aritmetike.

BIBLIOGRAFSKE BELEŠKE

U knjizi [Browder 1976], gde se u engleskom prevodu može naći Hilbertovo predavanje sa svetskog matematičkog kongresa 1900. godine, nalazi se i jedan esej o drugom Hilbertovom problemu od Kreisela (u tom eseju Kreisel kaže ono što spominjemo na kraju prvog dela ovog poglavlja). Glavni Hilbertovi radovi koji se tiču njegovog programa su prevedeni na engleski u knjizi [van Heijenoort 1967].

Gödelove teoreme o nepotpunosti se često prikazuju u udžbenicima matematičke logike (v. npr. [Mendelson 1964]).

Gentzenovi radovi se mogu naći u engleskom prevodu u knjizi [Gentzen 1969]. Prawitzovi radovi [1971] i [1981] daju dobar pregled rezultata i u Hilbertovoj teoriji dokaza (koja se tamo zove *reduktivnom*) i u opštoj teoriji dokaza, i sadrže reference za gotovo sve o čemu smo u ovom poglavlju govorili.

O Herkulu i hidri se govori u članku Kirbya i Parisa [1982]. Okvir za ovaj članak daju Smoryńskovi popularni članci [1980] i [1983].

III DESETI HILBERTOV PROBLEM

Problem rešivosti diofantovskih jednačina

Uvod

Deo Hilbertovog predavanja[1] koje se odnosi na ovaj problem glasi:

10Hp „10. *Ispitivanje rešivosti neke diofantovske jednačine.*
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.“

U vreme kada je Hilbert postavio ovaj problem, nisu postojala odgovarajuća matematička sredstva za njegovo rešavanje. Naime u formulaciji 10Hp pominje se “...postupak kojim se može odlučiti, *koristeći konačan broj operacija...*“. Ukoliko takav postupak (algoritam, efektivna procedura) zaista postoji, svako eksplicitno navođenje jednog takvog postupka daje definitivno rešenje za 10Hp. Problem nastaje onda kada ni jedan takav algoritam ne može da se navede, odnosno kada se sumnja da on zaista postoji. Jer svaki dokaz koji se odnosi na neki pojam podrazumeva primenu određenih matematičkih sredstava, što pretpostavlja da dati pojam treba da bude dovoljno formalizovan. Algoritam kao matematički pojam nije postojao u ono vreme, on se pojavio tek tridesetih godina kada je K. Gödel uveo pojam rekurzivnih funkcija. Neposredno po

---

[1] [Hilbert 1900]

uvođenju formalnog pojma algoritma, analizirani su mnogobrojni drugi sistemi koji su definisali pojam efektivne izračunljivosti. Ispostavilo se da svi predloženi algoritamski sistemi određuju istu klasu aritmetičkih funkcija, koje se danas najčešće nazivaju rekurzivnim funkcijama (ukoliko je njihov domen skup prirodnih brojeva N), ili parcijalno rekurzivnim funkcijama (ukoliko se za njihove domene dopuste podskupovi prirodnih brojeva). S obzirom da se dobijala uvek ista klasa izračunljivih funkcija, A. Church je postavio ovu hipotezu 1936. god:

> *Churchova teza.* Klasa rekurzivnih funkcija jednaka je klasi intuitivno izračunljivih funkcija.

Ukoliko se Churchova teza prihvati, dokaz da ne postoji efektivan postupak koji rešava dati problem, svodi se na dokaz da ne postoji rekurzivna funkcija sa nekim precizno utvrđenim osobinama. Sa ovakvim pretpostavkama J. Robinson, M. Davis i H. Putnam su 50-tih i 60-tih godina pripremili 10Hp za rešenje, da bi ga mladi matematičar J. Matijasevič 1970. god. definitivno negativno rešio. Naime, on je dokazao da postupak o kojem Hilbert govori u svojem problemu ne postoji.

Ubuduće, u ovom paragrafu, često ćemo koristiti relaciju zadovoljenja, u oznaci $\models$. Reč je o relaciji između struktura i formula kojom se iskazuje važenje neke formule φ u nekoj strukturi A. Ako je A neka operacijsko-relacijska struktura, $\varphi(x_1, \ldots, x_n)$ formula jezika strukture A i ako su $a_1, \ldots, a_n \in \mathrm{A}$ vrednosti dodeljene promenljivima $x_1, \ldots, x_n$, onda

$$A \models \varphi(a_1, \ldots, a_n)$$

označava da je formula $\varphi(a_1, \ldots, a_n)$ *tačna* ili *istinita* u strukturi A. Kvantori su u tom slučaju ograničeni na domen A strukture A, dok se vrednosti operacijskih i relacijskih simbola koji se pojavljuju u φ izračunavaju već kako su definisani (interpretirani) u strukturi A.

U rešavanju 10Hp značajnu ulogu imaju dve strukture, prsten celih brojeva $Z = (\mathrm{Z}, +, \cdot, 0, 1)$, i struktura prirodnih brojeva $N = (\mathrm{N}, +, \cdot, 0, 1)$, jer se ispostavlja da je rešavanje 10Hp u ovim dvema strukturama ekvivalentno. Dakle, ovde je Z skup celih brojeva, tj. $\mathrm{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$, dok je $\mathrm{N} = \{0, 1, 2, \ldots\}$ skup prirodnih brojeva. Operacije $+$ i $\cdot$ su uobičajene operacije sabiranja i množenja brojeva.

Deseti Hilbertov problem ekvivalentan je problemu u kojem se kao rešenja traže *prirodni* brojevi, Jer:

1. (i) svaki postupak koji daje sva celobrojna rešenja daje automatski i sva pozitivna celobrojna rešenja;
(ii) u 10 Hp traži se odlučivost za formule oblika

$$Z \vDash \exists\, x,\, y\, P(x,\, y) = 0\ ^{2};$$

slično pitanje za strukturu prirodnih brojeva izgleda

$N \vDash \exists\, x,\, yP(x,\, y) = 0$, odnosno $Z \vDash (\exists\, x,\, y \in \mathrm{N})\, P(x,\, y) = 0$;

ova druga formula može se izraziti rečenicom prvog reda u Z:

$$Z \vDash \exists\, x,\, y\, (P(x,\, y) = 0 \wedge x \geqslant 0 \wedge y \geqslant 0)$$

što je, koristeći Lagrangeovu teoremu: x je prirodan broj akko $Z \vDash \exists\, x_1\, x_2\, x_3\, x_4\ \ x = x_1^2 + x_2^2 + x_3^2 + x_4^2$ (tj. svaki prirodan broj jednak je zbiru kvadrata neka četiri cela broja), ekvivalentno sa

$$Z \vDash \exists\, x,\, x_1,\, x_2,\, x_3,\, x_4,\, y,\, y_1,\, y_2,\, y_3,\, y_4\, (P(x,\, y)^2 +$$

$$+ (x - x_1^2 - x_2^2 - x_3^2 - x_4^2)^2 + (y - y_1^2 - y_2^2 - y_3^2 - y_4^2)^2 = 0);$$

2. (i) svaki postupak A koji daje nenegativna celobrojna rešenja može se modifikovati do nekog postupka A' koji daje sva celobrojna rešenja; naime, A' se sastoji iz primene postupka A na jednačine

$$P(x,\, y) = 0,\ P(-x,\, y) = 0,\ P(x,\, -y) = 0,\ P(-x,\, -y) = 0$$

s obzirom da je

(ii) $Z \vDash \exists\, x,\, y\ P(x,\, y) = 0$ akko $Z \vDash \exists\, x,\, y\, (x \geqslant 0 \wedge y \geqslant 0 \wedge (P(x,\, y) = 0 \vee \cdots \vee P(-x,\, -y) = 0))$;

3. pitanje kojem domenu (N ili Z) pripadaju koeficijenti polinoma je irelevantno, jer za svaki polinom P sa celobrojnim koefi-

---

[2] Dakle, ovaj zapis čita se jednostavno:

Postoje celi brojevi x i y takvi da je $P(x,\, y) = 0$.

cijentima postoje polinomi Q i R sa koeficijentima u skupu prirodnih brojeva takvi da

$$Z \models P(x_1, \ldots, x_n) = 0 \text{ akko } N \models Q(x_1, \ldots, x_n) = R(x_1, \ldots, x_n).$$

Dakle, u odnosu na rešenje, *10 Hp (Z) i 10 Hp (N)* su potpuno ekvivalentni u svim relevantnim aspektima:

$$(H)\begin{cases} 1^\circ & \text{što se tiče domena koeficijenata polinoma;} \\ 2^\circ & \text{postupka za nalaženje korena jednačina;} \\ 3^\circ & \text{postupka za dokaz egzistencije korena polinoma.} \end{cases}$$

Ovde treba da navedemo još nekoliko napomena.

Aspekti (H) nisu neka pitanja specifična samo za deseti Hilbertov problem, jer se ona mogu postaviti za bilo koju jednačinu nad bilo kojim domenom. Naime, to su glavni uslovi od interesa kod bilo kojih jednačina.

Deseti Hilbertov problem odnosi se na 3° *u* (H). Pitanje 2° je, donekle, neposredno rešivo, jer postoji trivijalan algoritam za nalaženje korena (u N, a slično i u Z). Taj postupak glasi ovako:

nabrajati sve n-torke prirodnih brojeva $(d_1, \ldots d_n)$ u leksikografskom poretku i zatim proveriti da li je $P(d_1, \ldots, d_n) = 0$.

Ako jednačina $P(x_1, \ldots, x_n) = 0$ ima rešenje u N, onda se ono ovim *postupkom sigurno nalazi.* Problem nastaje onda kada ta jednačina nema rešenja, jer očigledno je da se tada ovaj proces pretraživanja nikad ne završava. Deseti Hilbertov problem se onda može i ovako razumeti: ako je data diofantovska jednačina $p(x_1, \ldots x_n) = 0$, *dokle treba izvoditi ovaj postupak?* Dakle, 10 Hp je ekvivalentan sa problemom da se efektivno odredi $d_p \in N$ takav da je dovoljno sprovesti navedeni postupak samo za

$$d_1, \ldots, d_n \leqslant d_p.$$

Drugim rečima, ako je p_n niz svih polinoma sa celobrojnim koeficijentima, *da li postoji izračunljiva funkcija* h tako da za sve $n \in N$ važi:

$$(\exists\, x_1 \ldots x_n)\, p_m(x_1, \ldots, x_n) = 0 \Rightarrow (\exists\, x_1 \ldots x_n \leqslant h(m))\, p_m(x_1, \ldots, x_n) = 0.$$

Odgovor je, kao što ćemo videti, ne. Ovaj problem granice sada ćemo objasniti na nekoliko primera.

Kod diofantovske jednačine $x^2+y^2=25$ sva rešenja u skupu prirodnih brojeva N su (0, 5), (3, 4), (4, 3), (5, 0), prema tome, možemo uzeti da je $d_p=5$. Procena ove granice bitno se ne menja ni u slučaju jednačine

$$x^2+y^2=a, \text{ gde je } a \text{ neki prirodan broj.}$$

Naime, očigledno je da možemo uzeti $d_p=[\sqrt{a}]+1$.

Pellova jednačina

$$x^2-(a^2-1)y^2=1$$

ima beskonačno mnogo rešenja u N za svaki prirodan broj $a>0$, ali možemo uzeti $d_p=a$, jer je jedno rešenje ove jednačine $(a, 1)$.

Nedavno je Faltings dokazao da za svaki prirodan broj $n\geqslant 3$ diofantovska jednačina

$$x^n+y^n=z^n$$

ima najviše konačno mnogo rešenja u N. Ali do sada nema procene eventualnog rešenja ove diofantovske jednačine, niti da li uopšte ima rešenja za neko $n\geqslant 3$. Prema tome, za sada se ne zna neka efektivna granica $g(n)=d_{pn}$ za niz polinoma

$$p_n(x)=x^n+y^n-z^n,$$

pa prema tome pitanje čuvene Fermatove hipoteze još uvek ostaje otvoreno.

Kasnije, u ovom članku, videćemo kako se može konstruisati niz polinoma $p_n(x_1, \ldots, x_k)$ za koje ne postoji odgovarajuća efektivna granica $g(n)=d_{pn}$.

Diofantovski i drugi aritmetički skupovi

Svakom polinomu p sa koeficijentima u skupu prirodnih brojeva N može se pridružiti jedan skup, algebarska mnogostrukost polinoma p:

$$M_p=\{(d_1, \ldots, d_n)\in N^n:\ p(d_1, \ldots, d_n)=0\}.$$

Ovi skupovi su jednostavne prirode. Na primer, za svaku n-torku $(d_1, \ldots, d_n)\in N^n$ možemo odlučiti da li je $(d_1, \ldots, d_n)\in M_p$,

dovoljno je da sračunamo vrednost $p(d_1, \ldots, d_n)$. Primećujemo da smo se ovde ograničili na domen prirodnih brojeva, a to možemo u skladu sa uvodnim napomenama.

Neka je $\mathscr{A}$ klasa algebarskih mnogostrukosti. Ova familija skupova zatvorena je u odnosu na neke skupovne operacije, na primer:

$$X, Y \in \mathscr{A} \Rightarrow X \cap Y,\ X \cup Y \in \mathscr{A},\ M_p \cap M_q = M_{p^2+q^2},\ M_p \cup M_q = M_{pq}.$$

Ali familija $\mathscr{A}$ nije zatvorena za sve skupovne operacije, na primer, za komplementiranje. Recimo, za skup $A = N - \{0\} = \{x \in N: x \neq 0\} = \{x \in N: x = 0\}^c$ imamo $A \notin \mathscr{A}$ (jer ne postoji polinom jedne promenljive čiji su koreni svi pozitivni prirodni brojevi). Dalje, ako je $A = M_p$ imamo ovaj niz ekvivalencija:

$$\begin{aligned} x_1, \ldots, x_n \in A^c &\Leftrightarrow p(x_1, \ldots, x_n) \neq 0 \\ &\Leftrightarrow p(x_1, \ldots, x_n) > 0 \\ &\Leftrightarrow \exists y\, p(x_1, \ldots, x_n) = y + 1. \end{aligned}$$

Dakle, u ovom slučaju komplementiranje je u vezi sa egzistencijalnim kvantorom, odnosno projekcijom, jer A^c je projekcija algebarske mnogostrukosti polinoma $(p(x_1, \ldots, x_n) - y - 1)^2$.

Evo nekoliko primera algebarskih mnogostrukosti:

1° svaki konačan skup $X = \{a_1, \ldots, a_n\}$ je skup rešenja jednačine $(x - a_1) \ldots (x - a_n) = 0$; dakle X je algebarska mnogostrukost;

2° Pitagorine trojke, rešenja diofantovske jednačine $x^2 + y^2 = z^2$, čine jednu algebarsku mnogostrukost;

3° skup svih rešenja neke diofantovske jednačine $p(x_1, \ldots, x_n) = 0$ je algebarska mnogostrukost;

4° ako je (S) sistem diofantovskih jednačina

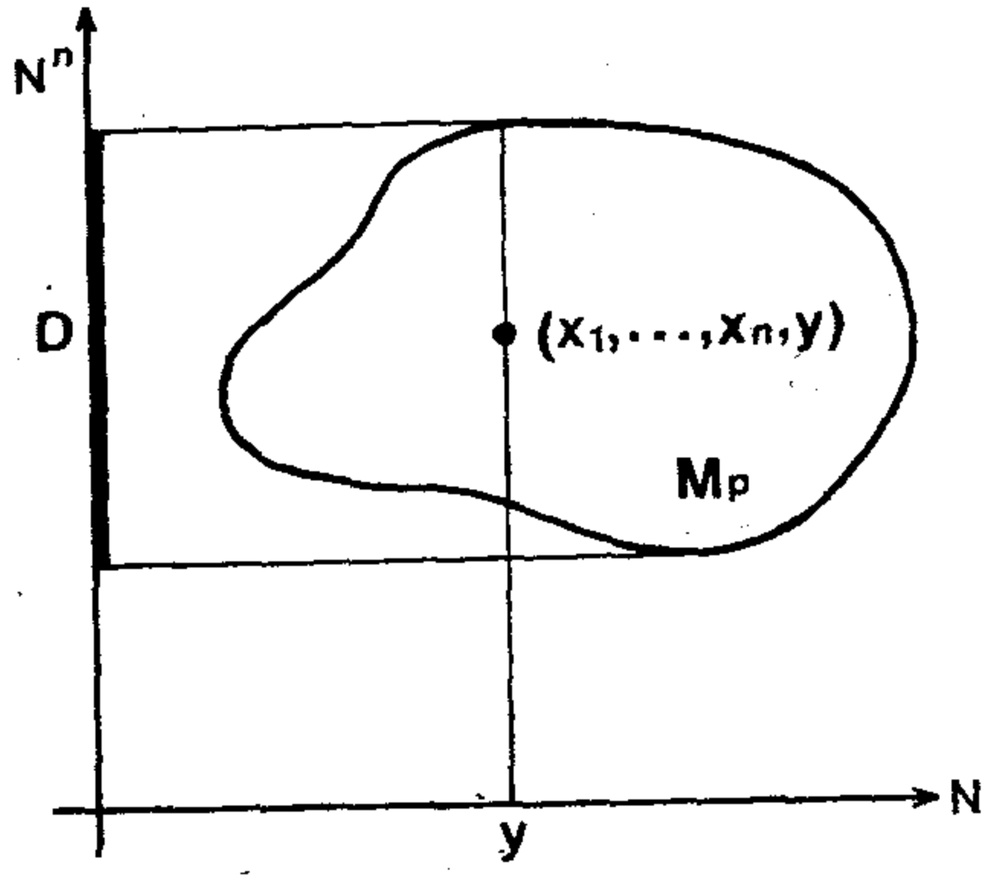
$$\begin{aligned} p_1(x_1, \ldots, x_n) &= 0 \\ &\vdots \\ p_k(x_1, \ldots, x_n) &= 0 \end{aligned}$$

tada je skup A rešenja ovog sistema, takođe, algebarska mnogostrukost, jer je $A=\{(x_1, \ldots, x_n)\colon p(x_1, \ldots, x_n)=0\}$ gde je $p=p_1^2+\cdots+p_n^2$.

Polazeći od algebarskih mnogostrukosti, mogu se izgraditi mnogi zanimljivi aritmetički skupovi složenije strukture. Neka je M_p algebarska mnogostrukost polinoma $p(x_1, \ldots, x_n, y)$ i neka je D skup

$$\{x\in N\colon \exists y\, p(x_1, \ldots, x_n\, y)=0\}.$$

Tada



$$(x_1, \ldots, x_n)\in D \text{ akko } \exists y\,(x_1, \ldots, x_n, y)\in M_p$$

tj. $D = proj_y M_p$.

Definicija. Skup $X\subseteq N^k$ je *diofantovski,* ako je X dobijen iz neke algebarske mnogostrukosti primenom nekog konačnog broja projekcija.

Neka je $\mathcal{D}$ klasa svih diofantovskih skupova. Da li se ovi skupovi mogu opisati na neki drugi način pogodan za rešenje desetog Hilbertovog problema? Mogu, i upravo to je dokazao *J.* Matijasevič. U opisu klase $\mathcal{D}$ koriste se sledeće vrste aritmetičkih skupova, koje inače imaju važnu ulogu u teoriji izračunljivih funkcija.

Klasa Δ_0 je najmanja klasa aritmetičkih skupova zatvorena u odnosu na ove operacije: $\cup$, $\cap$, ^{c} i koja sadrži ove skupove:

— sve konačne skupove prirodnih brojeva,

— grafove elementarnih aritmetičkih funkcija, tj. onih aritmetičkih funkcija koje se mogu dobiti kao konačne kompozicije funkcija $+$, $\cdot$, $'$, 0.

Klasa Δ_1 je najmanja klasa aritmetičkih skupova takva da ispunjava ove uslove:

1° $\Delta_0 \subseteq \Delta_1$;

2° klasa Δ_1 je zatvorena za skupovne operacije $\cup$, $\cap$, ^{c};

3° klasa Δ_1 je zatvorena za ograničene projekcije, tj. ako je $X \in \Delta_1$ i ako je $Y = \{(x, z): (\exists\, y \leqslant z)\ (x, y) \in X\}$, onda $Y \in \Delta_1$;

4° ako su neki skup X i njegov komplement X^c projekcije nekih Δ_1 skupova, onda je i X Δ_1 skup.

Graf eksponencijalne funkcije $y = x^z$ je Δ_1 skup ali ne i Δ_0, jer ova funkcija raste brže od svake Δ_0 funkcije.

Klasu Σ_1 skupova definišemo kao mnoštvo projekcija Δ_1 skupova.

Jasno je da aritmetičke formule opisuju aritmetičke skupove u strukturi prirodnih brojeva. Ako neka formula φ opisuje Δ_0 skup onda kažemo da je φ Δ_0 formula. Na sličan način se uvode Δ_1 i Σ_1 formule. Negacija Σ_1 formule naziva se Π_1 formulom. Postoji dalja klasifikacija aritmetičkih formula, odnosno skupova. Na taj način se dobija aritmetička hijerarhija Σ_n, Π_n skupova i formula. Kada je reč o skupovima ona se dobija uzastopnom primenom operacija projekcije i komplementiranja na Δ_1 skupove, dok se aritmetička hijerarhija formula dobija primenom egzistencijalnog kvantora i logičke operacije negacije na Δ_1 formule. Zbog svoje važnosti Δ_1 i Σ_1 skupovi nose zasebna imena. Tako, Δ_1 skupovi nazivaju se rekurzivnim, dok se Σ_1 skupovi nazivaju rekurzivno nabrojivim skupovima.

Važe ovi klasični rezultati:

R1° (uz Churchovu tezu) za neki aritmetički skup X postoji efektivan postupak kojim se za proizvoljan prirodan broj n utvrđuje da li je $n \in X$ akko $X \in \Delta_1$;

R2° neki skup $X \subseteq N$ može se efektivno izlistati, tj. mogu se efektivno nabrojati njegovi elementi akko $X \in \Sigma_1$;

R3° postoji skup $K \in \Sigma_1 - \Delta_1$.

Dakle, K je Σ_1 ali ne i Δ_1 skup. Ta se činjenica može iskazati i ovako: K je rekurzivno nabrojiv skup koji nije rekurzivan.

Primeri. 1. Skup prirodnih brojeva je Δ_1 skup, tj. $N \in \Delta_1$.

2. Ako je $\pi_n = c_0.\, c_1\, c_2 \cdot \cdot \cdot c_n$ prvih n decimala broja π, onda je skup $\{10^n \pi_n : n \in N\}$ Δ_1 skup.

3. Skup svih kôdova dokaza u Peanovoj aritmetici je Δ_1 skup.

4. Skup S svih kôdova teorema Peanove aritmetike je Σ_1 skup. Jedna od najdubljih teorema matematičke logike je ova Gödelova teorema: U R3° se može uzeti da je $K = S$. Otuda imamo ove važne posledice rezultata o kojima je bilo reči u prethodnom poglavlju. Prva je da ne postoji efektivan postupak kojim se za proizvoljuu formulu formalne aritmetike odlučuje da li je teorema Peanove aritmetike. Druga je da Peanova aritmetika P nije potpuna; drugim rečima, postoje rečenice jezika formalne aritmetike koje nisu teoreme u P, a nisu ni njihove negacije.

5. (H. Putnam) Diofantovski skupovi mogu se opisati na jednostavan način. Naime, neka je S skup svih prirodnih brojeva a za koje jednačina $p(a, z_1, \ldots, z_n) = 0$ ima rešenja po $z_1, \ldots, z_n$. Neka je $Q(x, z_1, \ldots, z_n) = (x+1)\,(1 - p(x, z_1, \ldots, z_n)^2) - 1$. Tada je S upravo skup svih nenegativnih vrednosti polinoma Q.

Rešenje

Osnovna činjenica koja povezuje diofantovske skupove i izračunljive skupove je ovaj

Osnovni rezultat. $\mathcal{D} = \Sigma_1$

Prema definiciji diofantovskih i Σ_1 skupova neposredno sledi $\mathcal{D} \subseteq \Sigma_1$. Što se tiče inkluzije $\Sigma_1 \subseteq \mathcal{D}$, M. Davis i J. Robinson sveli su problem na to da se dokaže da je graf eksponencijalne funkcije $z = x^y$ diofantovski skup. Odnosno, da postoji diofantovska jednačina čija celobrojna rešenja rastu eksponencijalnom brzinom. J. Matijasevič je 1970. naveo sistem diofantovskih jednačina čija su rešenja Fibonaccievi brojevi[1]. Preciznije rečeno, J. Matijasevič je dokazao sledeće tvrđenje:

[1] Fibonaccievi brojevi najjednostavnije se definišu rekurentnom formulom $f_{n+2} = f_n + f_{n+1}$ uz početne uslove $f_0 = 0$, $f_1 = 1$. Otuda nalazimo da je $f_2 = 1$, $f_3 = 2$, $f_4 = 3$ itd. Važi $f_n = (((1+\sqrt{5})/2)^n - ((1-\sqrt{5})/2)^n)/\sqrt{5}$, dakle članovi Fibonaccievog niza rastu eksponencijalnom brzinom.

Teorema. Relacija $D=\{(v, u)\in N^2:\ v=f_{2u}\}$ je diofantovska relacija sa eksponencijalnim rastom.

Da niz $v=f_{2u}$ raste eksponencijalnom brzinom sledi na osnovu eksplicitne formule za Fibonacciev niz. Glavni deo tvrđenja, da je D diofantovska relacija, sledi na osnovu sledeće leme, centralne u Matijasevičevom radu:

Lema. $v=f_{2u}$ akko postoje pozitivni celi brojevi a, z, g, h, m, x, y takvi da

$$u\leqslant v<1,$$

$$a^2-az-z^2=1,$$

$$g^2-2gh-4h^2=1,$$

a^2 deli g,

$$m=3+(4h+g)h,$$

$$x^2-mxy+y^2=1,$$

$u=r(x, a)$, $r(x, a)$ je ostatak dobijen deljenjem broja x brojem a,

$v=r(x, 4h+g)$.

Zanimljivo je da se u dokazu ove leme koriste u osnovi elementarna svojstva Fibonaccievog niza. Ubrzo po Matijasevičevom dokazu, Čudnovski je pokazao da i rešenja Pellove jednačine obrazuju diofantovski skup koji raste eksponencijalnom brzinom.

Pellova jednačina. $x^2+(a^2-1)y^2=1 \qquad (a>0).$

Rešenje Pellove jednačine data su sa

$$x_n(a)+y_n(a)\sqrt{a^2-1}=(a+\sqrt{a^2-1})^n.$$

Negativno rešenje desetog Hilbertovog problema.

Prema osnovnom rezultatu R 3° postoji skup $K\in\Sigma_1-\Delta_1$. Kako je $\mathcal{D}=\Sigma_1$, to znači da je $K\in\mathcal{D}$. Dakle, postoji polinom $p(x, y_1, \ldots, y_n)$ takav da

$$K=\{a\in N:\ \exists y_1 \ldots y_n\, p(a, y_1, \ldots, y_n)=0\}.$$

Ako bi postojao algoritam kojim se za proizvoljan polinom utvrđuje da li ima korene, onda bismo tim postupkom mogli da utvrdimo da li jednačina

$$p(a, y_1, \ldots, y_n) = 0$$

ima celobrojno rešenje, i to za proizvoljan $a \in N$. Dakle, postojao bi efektivan postupak kojim se utvrđuje pripadnost skupu K, a to bi prema osnovnom rezultatu $R\,1°$ značilo da je K odlučiv skup, tj. Δ_1 skup, što je kontradikcija.

Primetimo da je ovo rešenje desetog Hilbertovog prodlema dato u jačoj formi, jer se pokazuje da ne postoji postupak rešavanja već za jednu jednoparametarsku familiju diofantovskih jednačina.

Posledice

1° Neka P označava skup prostih brojeva. Tada je P diofantovski skup, jer $P \in \Delta_1 \subsetneq \Sigma_1$. Prema rezultatu H. Putnama, P je skup svih nenegativnih vrednosti nekog polinoma. Taj polinom izgleda ovako (ima 26 promenljivih i dvadesetpetog je stepena):

$$(k+2)\,(1-(wz+h+j-q)^2-((gk+2g+k+1)\,(h+j)+h-z)^2-$$
$$(2n+p+q+z-e)^2-(16\,(k+1)^3\,(k+2)\,(n+1)^2+1-f^2)^2-$$
$$(e^3\,(e+2)\,(a+1)^2+1-o^2)^2-((a^2-1)\,y^2+1-x^2)^2-$$
$$(16r^2\,y^4\,(a^2-1)+1-u^2)^2-(((a+u^2\,(u^2-a))^2-1)\,(n+4\,dy)^2+1-$$
$$(x+cu)^2)^2-(n+L+v-y)^2-((a^2-1)\,L^2+1-m^2)^2-(ai+k+1-$$
$$L-i)^2-(p+L\,(a-n-1)+b\,(2\,an+2\,a-n^2-2\,n-2)-m)^2-$$
$$(q+y\,(a-p-1)+s\,(2\,ap+2\,a-p^2-2\,p-2)-x)^2-$$
$$(z+pL\,(a-p)+t\,(2\,ap-p^2-1)-pm)^2).^1$$

Ovim je istovremeno rešen jedan stari problem iz teorije brojeva: da se nađe algebarski izraz čije su vrednosti upravo svi prosti brojevi.

---

[1] [Jones et al. 1976]

2° *Fermatova hipoteza* glasi:

(*F*) jednačina $x^n+y^n=z^n$ nema rešenja po x, y, z u $N-\{0\}$ za $n\geqslant 3$.

Osim toga, eksponencijalna funkcija je diofantovskog tipa (tj. njen graf); dakle postoji polinom q takav da

$$a=b^c \text{ akko } \exists u_1 \ldots u_n\, q(a, b, c, u_1, \ldots, u_n)=0.$$

Prema tome, Fermatova hipoteza ekvivalentna je sa tvrđenjem da ova diofantovska jednačina nema rešenja za prirodan broj n:

$$q(v,\ x+1,\ n+3, u_1, \ldots, u_n)^2+q(w,\ y+1,\ n+3,\ u_1, \ldots, u_n)^2+$$

$$q(v+w,\ z+1,\ n+3,\ u_1, \ldots, u_n)^2=0.$$

3° *Goldbachova hipoteza* da je svaki prirodan broj n, $n\geqslant 3$, zbir dva prosta broja ekvivalentna je sa tvrđenjem da diofantovska jednačina

$$p_G(z_1, \ldots, z_n)=z_0$$

nema rešenja, gde je p_G jedan tačno utvrđen polinom.

4° *Riemannova hipoteza* o raspodeli nula ζ funkcije

$$\zeta(s)=\sum_n n^{-s}$$

ekvivalentna je sa tim da diofantovska jednačina $p_R=0$ nema rešenja, gde je p_R jedan tačno utvrđen polinom.

5° Svaki definabilni aritmetički skup nastaje iz neke algebarske mnogostrukosti primenom konačnog broja operacija komplementiranja i projekcije.

6° Sledeći primer interesantan je zbog svoje primene u matematičkoj logici, kao i zbog neobičnih i unekoliko paradoksalnih misli koje nastaju u kontekstu ove primene. Koristićemo se prethodnim poglavljem, u stvari Dodatkom A o Gödelovim teoremama o nepotpunosti, u kojem se između ostalog govori o kodiranju pojmova iz teorije dokaza, kao što su formula, dokaz, teorema, neprotivrečnost i slično.

Za teoriju T iz §4 pomenutog dodatka, ovde ćemo uzeti neku teoriju skupova; to će obično biti neka ekstenzija teorije *ZFC* (Zermelo-Fraenkelove teorije skupova), koja danas sigurno ima centralnu ulogu u zasnivanju matematike.

Podsetimo se da je $Prov_T(u, v)$ predikat sa značenjem „u je kôd dokaza u T formule čiji je kôd v“. Ako je T aksiomatska teorija, tj. ako T ima odlučiv skup aksioma, onda se za svaki konačan niz formula može odlučiti da li je on dokaz u teoriji T. Otuda je lako izvesti da je $Prov_T$ odlučiv predikat dakle, prema R1° to je Δ_1 predikat. Rečenica Con_T je formalizacija u aritmetici pojma neprotivrečnosti. Naime, Con_T iskazuje da se u T ne može dokazati apsurd, tj.

$$Con_T \Leftrightarrow \neg \exists x \; Prov_T(x, \ulcorner 0 = 1 \urcorner).$$

Iz ovakve definicije forrmule Con_T, i s obzirom na definiciju Σ_1 i Π_1 formula, neposredno nalazimo da je Con_T Π_1 formula. Prema osnovnom rezultatu o diofantovskim skupovima, sledi da postoji polinom $S(x_0, x_1, \ldots, x_n)$ takav da u N važi:

$$Con_T \Leftrightarrow \neg \exists x_0 \ldots x_n \; S(x_0, \ldots, x_n) = 0, \qquad \text{tj.}$$

$$Con_T \Leftrightarrow \quad \forall x_0 \ldots x_n \; S(x_0, \ldots, x_n) \neq 0. \tag{1}$$

U daljem razmatranju pretpostavljamo, kao što je to uobičajeno, da je ZFC neprotivrečna teorija, kao i da je naša metateorija takođe ZFC teorija. Tada, prema drugoj Gödelovoj teoremi o nepotpunosti u ZFC se ne može dokazati Con_{ZFC}, tj.

$$ne\ ZFC \vdash Con_{ZFC}, \qquad \text{odnosno}$$

$$ne\ ZFC \vdash \forall x_0 \ldots x_n \in N \; S(x_0, \ldots, x_n) \neq 0 \tag{2}$$

i to možemo ovako da protumačimo: u ZFC ne možemo dokazati da diofantovska jednačina $S(x_0, \ldots, x_n) = 0$ nema celobrojnih rešenja.

S obzirom na pretpostavku da je ZFC neprotivrečna teorija, to onda u ZFC nije dokaziva ni negacija formule Con_T, tj.

$$ne\ ZFC \vdash \neg Con_T, \qquad \text{odnosno}$$

$$ne\ ZFC \vdash \exists x_0 \ldots x_n \in N \; S(x_0, \ldots, x_n) = 0. \tag{3}$$

Drugim rečima, u ZFC ne možemo dokazati da diofantovska jednačina $S(x_0, \ldots, x_n) = 0$ ima celobrojna rešenja.

Dakle, prema (2) i (3) ove teorije su neprotivrečne:

$$ZFC + \neg Con_T, \qquad ZFC + Con_T.$$

Otuda sledi, da postoje dva modela, neka su to $\mathfrak{M}$ i $\mathfrak{N}$ takvi da

$\mathfrak{M} \models$ „Diofantovska jednačina $S(x_0, \ldots, x_n) = 0$ ima celobrojna rešenja“

$\mathfrak{N} \models$ „Diofantovska jednačina $S(x_0, \ldots, x_n) = 0$ nema celobrojna rešenja“

Svaki model teorije skupova istovremeno je i model, „univerzum“, matematike (bar njenog većeg dela), pa se mogu postaviti ova, pomalo naivna pitanja. Naime, koje vrste je univerzum radne matematike? Ovo pitanje ima smisla za jednog matematičara platonistu, jer za njega je matematika kategorična, a to znači da on smatra da živi u jednom izabranom modelu matematike.

Vrlo je jednostavno konstruisati proceduru kojom se traže celobrojni koreni diofantovske jednačine $S(x_0, \ldots, x_n) = 0$. Naime, lako je konstruisati program, tako što će se proveravati da li je $S(d_0, \ldots, d_n) = 0$ prolazeći redom kroz sve $n+1$-torke $d_0, \ldots, d_n$ prirodnih brojeva.

U modelu $\mathfrak{N}$ računar, koristeći prethodnu proceduru, nikad neće prestati sa radom, jer odgovarajuća diofantovska jednačina nema rešenja. Sa modelom $\mathfrak{M}$ situacija je nešto drugačija. Jer diofantovska jednačina $S(x_0, \ldots, x_n) = 0$ sada ima rešenje, dakle računar će posle nekog vremena pronaći jedno rešenje ove jednačine. Ovde se može postaviti sledeće zanimljivo pitanje: da li se trenutak prestanka rada računara, odnosno pronalaženja prvog rešenja jednačine po opisanoj proceduri može nekako proceniti? Upravo se u ovom pitanju krije glavno iznenađenje!

Zaista, pretpostavimo da je $d_0, \ldots, d_n$ jedno rešenje diofantovske jednačine $S(d_0, \ldots, d_n) = 0$ koje pripada skupu prirodnih brojeva u $\mathfrak{M}$. Ako pretpostavimo da su $d_0, \ldots, d_n$ konačni prirodni brojevi (gledajući na njih van modela $\mathfrak{M}$), onda se lako izvodi ne samo da je $\mathfrak{M} \models S(d_0, \ldots, d_n) = 0$, već i $S(d_0, \ldots, d_n) = 0$. S obzirom na ekvivalenciju (1), imali bismo $\neg Con_{ZFC}$, što bi značilo da je *ZFC* protivrečna teorija, suprotno uvedenoj pretpostavci. Dakle, rešenje $d_0, \ldots, d_n$ *nije konačno*, tj. bar jedan od brojeva $d_0, \ldots, d_n$ je beskonačan prirodan broj u $\mathfrak{M}$. Iz toga, naravno, automatski sledi, da skup prirodnih brojeva u $\mathfrak{M}$ sadrži kao pravi podskup skup interpretacija numerala 0, 1, 2, ...

U modelu $\mathfrak{M}$ važi $\neg Con_{ZFC}$, tj. u $\mathfrak{M}$ postoji element w koji je kôd dokaza u *ZFC* za apsurd. Dakle, model $\mathfrak{M}$ teorije *ZFC* tvrdi

da je *ZFC* protivrečna teorija, odnosno da *ZFC* nema model. Ovaj paradoks je ipak prividan, jer argumentacijom kao u prethodnom pasusu nalazimo da *w* nije konačan broj, pa dokaz za apsurd čiji je kôd *w*, nije finitarnog karaktera.

Dakle, razrešenje paradoksa smo našli u tome da u radnoj matematici nema beskonačno velikih prirodnih brojeva. Ali trag sumnje ostaje, jer, na primer, Leibniz ne samo da je verovao u beskonačne prirodne brojeve, već je na osnovu njih stvorio jednu od najvećih građevina matematike, infinitezimalni račun. Danas je analiza Leibnizovskog tipa oživljena u nestandardnoj analizi u okviru koje su na potpuno konzistentan način zasnovane beskonačno male veličine i beskonačno veliki prirodni brojevi. Uostalom, H. J. Keisler kaže: „One (aktuelne infinitezimale) postoje za mene bar koliko i realni brojevi, jer se za dokaz njihove egzistencije ne koriste naročito jača sredstva nego što je to slučaj sa realnim brojevima."

U vezi sa diofantovskom jednačinom $S(x_0, \ldots, x_n) = 0$ mogu se uočiti i neki drugi zanimljivi problemi. Na primer, zamislimo igru između dva igrača *A* i *B* definisanu ovako:

Igrači *A* i *B* naizmenično biraju *n*-torke prirodnih brojeva i proveravaju da li su one rešenja jednačine $S(x_0, \ldots, x_n) = 0$. Pobeđuje onaj igrač koji prvi naiđe na rešenje ove jednačine.

U univerzumu $\mathfrak{N}$ nijedan igrač ne pobeđuje i igra traje bez kraja, iz jednostavnog razloga što diofantovska jednačina $S(x_0, \ldots, x_n) = 0$ nema rešenja u modelu $\mathfrak{N}$. U univerzumu $\mathfrak{M}$ igra je odlučiva, ali do pobede jednog od igrača dolazi tek posle beskonačno duge igre!

Na kraju dolazimo do centralnog pitanja: za koji od modela $\mathfrak{M}$, $\mathfrak{N}$ treba da se odlučimo u radnoj matematici. Zanimljivo je da se ovo pitanje može raspraviti kada se pođe od nekih osobina kardinalnih brojeva. Naime, u teoriji skupova vrlo su popularne aksiome koje postuliraju egzistenciju velikih kardinalnih brojeva (nedostižnih i još većih, kao što su, na primer, merljivi kardinali). Ako φ označava jednu takvu aksiomu (u koje, između ostalog, veruje određen broj matematičara koji se bave teorijom skupova), onda važi:

$$ZFC + \varphi \vdash Con_{ZFC}.$$

Drugim rečima, u $ZFC + \varphi$ diofantovska jednačina $S(x_0, \ldots, x_n) = 0$ nema rešenja. Ali s druge strane, iz Gödelovih teorema o nepotpunosti lako je izvesti da se u *ZFC* ne može dokazati $Con_{ZFC+\varphi}$,

pa i ako se ima pretpostavka Con_{ZFC}. Dakle, uvođenje ovakvih aksioma ima donekle *ad hoc* karakter.

Ipak senka sumnje pada na ovo rešenje, jer pažljivom analizom aksioma koje postuliraju postojanje velikih kardinala nailazimo na još neka pitanja koja nemaju tako jednostavan odgovor. Naime, jedna takva aksioma postulira egzistenciju nekakvih objekata koji u skupovnoj hijerarhiji leže vrlo visoko, ali izlazi da oni ipak odlučuju neka jednostavna aritmetička svojstva, kao što je rešivost diofantovskih jednačina. S druge strane, aritmetičke osobine odnose se na objekte koji leže vrlo nisko u skupovnoj hijerarhiji, pa se postavlja prirodno pitanje koji su to dugi hodnici koji povezuju tako različite objekte.

Dolazimo do toga, da ne postoje neki posebni dovoljni razlozi za prihvatanje bilo kojeg od modela $\mathfrak{M}$, $\mathfrak{N}$. Jer, odlučivanje za jedan od tih modela $\mathfrak{M}$, $\mathfrak{N}$ svodi se na pitanje rešivosti diofantovske jednačine $S(x_0, \ldots, x_n)=0$. Da li to znači da iz verovanja da je ova jednačina rešiva sledi da je ovu jednačinu moguće rešiti?

DODATAK A: DOKAZ MATIJASEVIČEVE TEOREME

U ovom dodatku dokazaćemo Matijasevičevu teoremu:

Aritmetički skup X je diofantovski akko je X Σ_1 skup.

U prethodnom delu teksta bilo je već reči o ovoj teoremi, i pri tome smo se uverili da ona ima centralnu ulogu u razrešenju desetog Hilbertovog problema. Mada je dokaz ove teoreme u osnovi elementaran, on je dosta dug, ima puno tehničkih detalja, ali, isto tako, sadrži i veoma duhovite i oštroumne ideje. U osnovi dokaz se izvodi tako što se postepeno pokazuje da se diofantovskim skupovima mogu opisati sve složeniji skupovi, dok se najzad ne obuhvate svi Σ_1 skupovi. S obzirom na dužinu, kao i na mogućnost postepene redukcije, ovaj dokaz je podeljen na više pomoćnih tvrđenja — lema. Mnoga od ovih tvrđenja su i sama interesantna, a osim toga, imaju primenu i van dokaza Matijasevičeve teoreme.

Radi kraćeg zapisivanja koristićemo sledeću notaciju: simbol $\vec{x}$ stoji umesto $x_1, \ldots, x_n$ za neki prirodan broj n. Otuda, $\vec{x}\in A$ je kraći zapis za $x_1, \ldots, x_n\in A$, dok $\forall\vec{x}\varphi$ označava formulu $\forall x_1, \ldots \forall x_n \varphi$.

Podsećamo da, pod ograničenim kvantorom podrazumevamo kvantore vida $\forall x<y$, $\exists x<y$.

Lema 1. Za svaku Σ_1-formulu $\varphi(\vec{x})$ postoji formula ψ bez kvantora i ograničeni kvantori $Q_1 z_1<y_1, \ldots, Q_m z_m<y_m$ tako da važi;

$$N \models \forall \vec{x}(\varphi(\vec{x}) \leftrightarrow \exists \vec{v} Q_1 z_1<y_1 \ldots Q_m z_m<y_m \psi(\vec{x}, \vec{y}, \vec{z}, \vec{v})).$$

Dokaz ove leme u osnovi je sličan dokazu poznate teoreme o preneksnoj normalnoj formi[1], s tim da se koristi sledeća shema koja važi u formalnoj aritmetici, teoriji P, dakle i u strukturi prirodnih brojeva:

(R) $$(\forall x<y)(\exists z)\varphi \rightarrow (\exists v)(\forall x<y)(\exists z<v)\varphi.$$

Detaljnije, dokaz se izvodi indukcijom po složenosti formule, na primer broju logičkih znakova, koristeći shemu (R) i veći broj jednostavnih valjanih formula[2].

Lema 2. Neka je φ Σ_1 formula. Tada postoji polinom p sa celobrojnim koeficijentima takav da

$$N \models \forall \vec{x}(\varphi(\vec{x}) \leftrightarrow \exists \vec{y} Q_1 z_1<v_1 \cdots Q_m z_m<v_m p(\vec{x}, \vec{y}, \vec{z}, \vec{v}) = 0)$$

gde su $O_i z_i<v_i$ ograničeni kvantori.

Dokaz. Prema prethodnoj lemi postoji formula ψ bez kvantora tako da je

$$N \models \forall \vec{x}(\varphi \leftrightarrow \exists \vec{u} Q_1 v_1<W_1 \cdots Q_m v_m<w_m \psi),$$

gde su $Q_i v_i<w_i$ ograničeni kvantori. Prema teoremi o konjunktivnoj normalnoj formi postoje formule ψ_i, tako da važi ekvivalencija

---

[1] Teorema o preneksnoj normalnoj formi tvrdi da je svaka formula ekvivalentna formuli kod koje kvantori prethode drugim logičkim i nelogičkim znacima koji učestvuju u izgradnji formule. Npr.: $\forall x \exists y (x=y+z+z \wedge x \geqslant u)$ je u preneksnoj normalnoj formi, dok $\forall x \exists y (x \geqslant y) \wedge \exists u (x \geqslant u)$ to nije

[2] kao što su $\exists x \varphi \vee \exists x \psi \leftrightarrow \exists x (\varphi \vee \psi)$, $\forall x \varphi \vee \forall y \psi \leftrightarrow \forall x \forall y (\varphi \vee \psi)$ ako se x ne javlja u ψ i y u φ, itd.

$\psi \leftrightarrow \bigwedge_{i<n} \psi_i$, gde je svaka formula ψ_i disjunkcija nekih jednakosti i nejednakosti, recimo: ψ_i je

$$u_1 = v_1 \vee \cdots \vee u_k = v_k \vee u_1' \neq v_1' \vee \cdots \vee u_p' \neq v_p'.$$

Dalje, u teoriji P važe sledeće ekvivalencije:

$A = B \leftrightarrow (A - B)^2 = 0$

$A = 0 \vee B = 0 \leftrightarrow AB = 0$

$A = 0 \wedge B = 0 \leftrightarrow A^2 + B^2 = 0$

$A \neq 0 \leftrightarrow \exists y\,(A = y + 1)$

($z = (A - B)^2$ akko $z + 2AB = A^2 + B^2$, dakle funkcija $(A, B) \mapsto (A - B)^2$ je definabilna u P)

$(\exists x < y)\,\exists z\,\theta \leftrightarrow \exists x\,\exists z\,\exists u\ (x + u + 1 = y \wedge \theta)$.

Koristeći prve četiri ekvivalencije dokazuje se da postoje polinomi p_i, koji su takvi da važe ove ekvivalencije u N:

$$\psi_i \leftrightarrow \exists \vec{Y}^i\ (p_i = 0), \qquad i < n.$$

Koristeći shemu (R) i petu po redu ekvivalenciju, nalazimo da je za neke ograničene kvantore Q_i

$$\varphi \leftrightarrow \exists \vec{u} Q_1 z_1' < v_1' \cdots Q_s z_s' < v_s' \exists \vec{Y}^1 \cdots \vec{Y}^t\ (p_1 = 0 \wedge \cdots \wedge p_t = 0)$$

$$\leftrightarrow \exists \vec{u} \exists \vec{y} Q_1 z_1 < v_1 \cdots Q_m z_m < v_m\ (p = 0)$$

gde je $p = p_1^2 + \cdots + p_t^2$.

Formule vida $\exists \vec{x}\, p(\vec{x}, \vec{y}) = 0$ nazivaćemo D-formulama. Prema dokazu prethodne leme neposredno nalazimo da je skup D-formula zatvoren za primenu logičkih operacija konjunkcije, disjunkcije, egzistencijalnog kvantora i ograničenog egzistencijalnog kvantora. Drugim rečima, ako su φ i ψ D formule, tada je $\varphi \wedge \psi$ D-formula, a slično važi i za ostale pomenute logičke operacije.

Formule vida $\exists \vec{y} Q \vec{z} < \vec{v}\, p(\vec{x}, \vec{y}, \vec{z}, \vec{v}) = 0$ nazovimo M-formulama. S obzirom na Lemu 2 dokaz Matijasevičeve teoreme biće završen onda kada dokažemo da je svaka M-formula takođe i D-formula. Dalje, uverili smo se da je skup D-formula zatvoren u odnosu na neke logičke operacije. Otuda nije teško izvesti da je dovoljno pokazati

da je skup *D-formula* zatvoren u odnosu na primenu ograničenog kvantora $\forall x<y$. Upravo ova činjenica predstavlja jezgro dokaza Matijasevičeve teoreme, i njen dokaz nikako nije trivijalan.

Neka je $p(\vec{x}, \vec{k}, \vec{y})$ polinom sa celobrojnim koeficijentima. Označimo sa d stepen polinoma p i neka je C zbir apsolutnih vrednosti koeficijenata polinoma p. Definišemo formulu ψ na sledeći način:

$$\psi(\vec{x}, y) =_{df} \forall k \leqslant y \, \exists \vec{y} \, p(\vec{x}, k, \vec{y}) = 0$$

Sledeći rezultat svodi odnos između *M*-formula i *D*-formula na razmatranje osobina nekoliko jednostavnih aritmetičkih funkcija.

Lema 3. Ako su formule 1°—3° *D*-formule, tada je i ψ takođe *D-f*ormula, gde

$$1^\circ \ z = y^x, \quad 2^\circ \ y = x!, \quad 3^\circ \ x_1/x_2 = \binom{x_3/x_4}{x_5} \wedge x_3 \geqslant x_4 \, x_5.$$

Ovde je $\binom{x}{y} = x(x-1)\cdot\cdot\cdot(x-y+1)/y!$

Dokaz. Uvešćemo sledeće formule čije su promenljive $\vec{x}$, y, Y, N, K, $\vec{Y}$.

$$\psi_1 =_{df} N \geqslant C(x_1 \cdot\cdot\cdot x_n y Y)^d \wedge Y < Y_1 \wedge \cdot\cdot\cdot \wedge Y < Y_m,$$

$$\psi_2 =_{df} 1 + K \cdot N! = \prod_{k=1}^{y} (1 + k \cdot N!),$$

$$\psi_3 =_{df} p(x_1, \ldots, x_n, K, Y_1, \ldots, Y_m) = 0 \mod (1 + K \cdot N!),$$

$$\psi_{i+3} =_{df} \prod_{j \leqslant Y} (Y_i - j) = 0 \mod (1 + K \cdot N!), \ i = 1, \ldots, m; \ m \text{ je broj promenljivih } Y_i.$$

Značenja nekih formula su sledeća:

ψ_1: N je jedna gornja granica za vrednost polinoma p u tački $(\vec{x}, y, \vec{y})$, ako je $y, y_i < Y$;

ψ_2: izabran je „veliki modul“; negde kasnije formula $p=0$ biće zamenjena formulom $p=0 \mod m$.

Formulu ψ' definišemo sa: $\psi' =_{df} \bigwedge_i \psi_i$.

Dokazujemo da u strukturi prirodnih brojeva važi sledeća ekvivalencija:

$$\psi \leftrightarrow \exists Y \exists N \exists K \exists \vec{Y}\ \psi'.$$

Označimo desnu stranu ove ekvivalencije sa ψ''. Najpre dokazujemo implikaciju $\psi \rightarrow \psi''$. Stoga, pretpostavimo da je za neke prirodne brojeve $\vec{a}$, b ispunjeno $N \models \psi [a_1, \ldots, a_n, b]$, Prema izboru formule ψ, za svaki $k \leqslant b$ postoje $b_{1k}, \ldots, b_{mk}$ takvi da je $p(a_1 \ldots, a_n, k, b_{1k}, \ldots, b_{mk}) = 0$.

Neka je $\mathbf{Y} = \max(b, \max_{i,k} b_{ik})$, i izaberimo $\mathbf{N} \geqslant C(a_1 \ldots a_n b \mathbf{Y})^d$.

Ako je $1 \leqslant k < k' \leqslant b$, tada su $1 + k \cdot \mathbf{N}!$, $1 + k' \cdot \mathbf{N}!$ uzajamno prosti, pa prema Kineskoj teoremi o ostacima (v. Dodatak A drugog poglavlja) postoje $\mathbf{Y}_i$, tako da je $\mathbf{Y}_i = b_{ik} \mod (1 + k \cdot \mathbf{N}!)$, $k = 1, \ldots, b$. Brojevi $\mathbf{Y}_i$ mogu se izabrati proizvoljno velikim, pa za odgovarajuće $\mathbf{Y}_i$ imamo

$$N \models \psi_1 [\vec{a}, b, \mathbf{Y}, \vec{\mathbf{Y}}].$$

Vrednost promenljive K je jedinstveno određena u formuli ψ_2, tj. postoji tačno jedno $\mathbf{K}$ tako da je $\mathbf{N} \models \psi_2 [b, \mathbf{K}, \mathbf{N}]$. Kako je $b_{ik} \leqslant \mathbf{Y}$, to se $\mathbf{Y}_i - b_{ik}$ pojavljuje u $\prod_{j \leqslant \mathbf{Y}} (\mathbf{Y}_i - j)$. Takođe, prema izboru $\mathbf{Y}_i$, ako je $k \leqslant b$, onda $1 + k \cdot \mathbf{N}!$ deli $\mathbf{Y}_i - b_{ik}$; dakle $\prod_{j < \mathbf{Y}} (\mathbf{Y}_i - j) = 0 \mod (1 + k \cdot N!)$ za sve $k \leqslant b$.

S obzirom da su za različite $k < b$ brojevi $1 + k \cdot \mathbf{N}!$ uzajamno prosti, sledi:

$$\prod_{j < \mathbf{Y}} (\mathbf{Y}_i - j) = 0 \mod \prod_{k=1}^{b} (1 + k \cdot \mathbf{N}!), \quad \text{tj.} \quad N \models \psi_{i+3} [b, \mathbf{Y}, \mathbf{N}, \mathbf{K}, \mathbf{Y}_i].$$

Najzad, ako je $k \leqslant b$, onda je $(1 + K \cdot \mathbf{N}!) - (1 + k \cdot \mathbf{N}!) = 0 \mod (1 + k \cdot \mathbf{N}!)$, pa kako su $\mathbf{N}!$ i $1 + k \cdot \mathbf{N}!$ uzajamno prosti, to sledi:

$$K = k \mod (1 + k \cdot N!).$$

Dakle, koristeći $\mathbf{Y}_i = b_{ik} \bmod (1 + k \cdot N!)$, imamo

$$p(a_1, \ldots, a_n, k, b_{1k}, \ldots, b_{mk}) = p(a_1, \ldots, a_n, \mathbf{K}, Y_1, \ldots, Y_m).$$

Sada dokazujemo implikaciju $\psi'' \to \psi$. Stoga pretpostavimo: $N \vDash \psi'[a, b, \mathbf{Y}, \mathbf{N}, \mathbf{K}, \mathbf{Y}]$ za neke $a, b, \mathbf{Y}, \mathbf{N}, \mathbf{K}, \mathbf{Y}$. Cilj nam je da odredimo takve b_{ik} da je:

$$p(a_1, \ldots, a_n, k, b_{1k}, \ldots, b_{mk}) = 0, \qquad k = 1, \ldots, b.$$

Neka su p_k proizvoljni prosti brojevi koji dele $1 + k \cdot \mathbf{N}!$, i neka je b_{ik} ostatak dobijen deljenjem broja p_k brojem $\mathbf{Y}_i$; tada imamo:

Ako je $N \vDash \psi_3[\vec{a}, \mathbf{K}, \vec{\mathbf{Y}}]$ onda je $p(\vec{a}, k, b_{1k}, \ldots, b_{mk}) = 0$ za sve $k \leqslant b$.

Dalje, pokazujemo da je $|p(a, k, b_{,1k}, \ldots, b_{mk})| < p_k$. Kako je $N \vDash \psi_2[b, \mathbf{K}, \mathbf{N}]$, to onda p_k deli $1 + \mathbf{K} \cdot \mathbf{N}!$. Prema definiciji formule ψ_{i+3} sledi: $\prod_{j \leqslant \mathbf{Y}} (\mathbf{Y}_i - j) = 0 \bmod p_k$. S obzirom da je p_k prost broj, postoje $j_0 \leqslant \mathbf{Y}$, $u \in N$ tako da je $\mathbf{Y}_i - j_0 = up_k$. Kako je za neki v $\mathbf{Y}_i = vp_k + b_{ik}$, to sledi $v \geqslant u$, i takođe $(v-u)p_k + b_{ik} = j_0 \leqslant \mathbf{Y}$. Otuda je $b_{ik} \leqslant \mathbf{Y}$. Dakle,

$$|p(a, k, b_{1k}, \ldots, b_{mk})| \leqslant \sum_i |c_i a_1^{i_1} \cdot \ldots \cdot a_n^{in} \cdot k^{in+1} b_{1k}^{in+2} \cdot \ldots \cdot b_{mk}^{in+m+1}|$$
$$\leqslant \left(\sum_i |c_i|\right) \cdot (a_1 \cdot \ldots \cdot a_n b\mathbf{Y})^d = C(a_1 \cdot \ldots \cdot a_n b\mathbf{Y})^d \leqslant N.$$

S obzirom da p_k deli $1 + k \cdot N!$ sledi $N < p_k$, dakle

$$p(a, k, b_{1k}, \ldots, b_{mk}) < p_k, \quad \text{pa} \quad p(a, k, b_{1k}, \ldots, b_{mk}) = 0.$$

Uvodeći neke pomoćne promenljive, lako je uočiti da su formule ψ_i D-formule, ako su to ove formule:

$$y = x!, \qquad z = \prod_{k \leqslant y} (1 + kx), \qquad z = \prod_{j \leqslant y} (x - j).$$

Ali kako je

$$\prod_{k \leqslant y} (1 + kx) = x^y \cdot y! \binom{1/x + y}{y} \qquad \prod_{j \leqslant y} (x - j) = y! \binom{x-1}{y}.$$

to je ovim lema dokazana. ■

Dakle, prethodnom lemom dokaz Matijasevičeve teoreme je redukovan na to da se dokaže da su formule (odnosno grafovi odgovarajućih funkcija)

$$z = y^x, \quad y = x!, \quad z = \binom{y}{x}$$

diofantovske. Ali taj rezultat je bio poznat i pre nego što se pojavio Matijasevičev dokaz, naime do ovoga su došli još J. Robinson, M. Davis i H. Putnam. U nastavku ovog dodatka pokazaćemo da su grafovi eksponencijalne funkcije i faktorijel funkcije diofantovski skupovi, i to onako kako su to uradili Matijasevič i Čudnovski.

Podsećamo da je Pellova jednačina ova diofantovska jednačina po x, y

$x^2 - dy^2 = 1$, d je pozitivan ceo broj nije potpun kvadrat.

Nije teško pokazati sledeću činjenicu:

Lema 4. Ako je (x_1, y_1) ono rešenje Pellove jednačine kod kojeg je x_1 najmanji pozitivan ceo broj, onda su sva rešenja ove jednačine data sa

$$x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n, \qquad n \text{ je ceo broj.}$$

Na primer, ako je $x + \sqrt{dy}$ rešenje Pellove jednačine, tada je i $x - \sqrt{dy}$ rešenje iste jednačine, jer

$$x - \sqrt{dy} = (x - \sqrt{dy})/(x^2 - y^2 d) = 1/(x + \sqrt{dy}).$$

Ovde ćemo posebno razmatrati rešenja ove Pellove jednačine

$$x^2 - (a^2 - 1)y^2 = 1. \tag{P}$$

Rešenja ove Pellove jednačine označićemo sa $(x_n(a), y_n(a))$. Tada je opšte rešenje diofantovske jednačine (P) dato sa

$$x_n(a) + y_n(a)\sqrt{a^2 - 1} = (a + \sqrt{a^2 - 1})^n.$$

Lema 5 (glavna lema). Skup $E = \{(y, n, a): y = y_n(a), a > 1\}$ je diofantovski.

Dokaz. Razmotrimo sledeći niz formula:

$$\psi_1 = {}_{df} y \geqslant n \wedge a > 1,$$

$$\psi_2 = {}_{df} x^2 - (a^2 - 1)\, y^2 = 1,$$

$$\psi_3 = {}_{df} y' = 0 \mod 2\, x^2\, y^2,$$

$$\psi_4 = {}_{df} x'^2 - (a^2 - 1)\, y'^2 = 1,$$

$$\psi_5 = {}_{df} A = a + x'^2 (x'^2 - a),$$

$$\psi_6 = {}_{df} x_1^2 - (A^2 - 1)\, y_1^2 = 1,$$

$$\psi_7 = {}_{df} y_1 - y = 0 \mod x'^2,$$

$$\psi_8 = {}_{df} y_1 = n \mod 2\, y.$$

Primetimo da su sve formule ψ_i diofantovske. Sada dokazujemo jednakost $E = \{(y, n, a)\colon \exists\, x', y', x_1, y_1, x, A \bigwedge_{i \leqslant 8} \psi_i\}$. U dokazu ovog fakta koristićemo sledećih nekoliko tvrđenja. Većina njih se dokazuje indukcijom.

1° $\forall\, k > 1\; y_k(a) = k \mod (a-1)$.

2° $a = b \mod c \to y_n(a) = y_n(b) \mod c$.

3° $y_i(a) = y_j(a) \mod x_n(a) \wedge a > 1 \to i = j \mod 2n \vee i = -j \mod 2n$.

4° Ako $y_i(a)^2$ deli $y_j(a)$ onda $y_i(a)$ deli j.

Najpre dokazujemo ovu inkluziju

(1) $$E \subseteq \{(y, n, a)\colon \exists\, x', y', x_1, y_1, A, x \bigwedge_i \psi_i\}.$$

Pretpostavimo da je $(y, n, a) \in E$. Indukcijom po n lako se dokazuje da je $y_n(a) \geqslant n$, ukoliko je $a > 1$, $n > 1$. Prema Lemi 4 postoji jedinstven prirodan broj n takav da je $x = x_n(a)$ rešenje za ψ_2. Za neki Y izaberimo $y' = Y \cdot 2\, x^2\, y^2$ tako da je ψ_3 zadovoljeno. Dalje, izaberimo jedinstveno rešenje $X = x'$ diofantovske jednačine $X^2 - (a^2 - 1)\,(2\, x^2\, y^2)\, Y^2 = 1$. Na taj način je zadovoljena i formula ψ_4. Vrednost konstante A je određena na jedinstven način formulom ψ_5. Najzad, izaberimo za (x_1, y_1) n-to rešenje u jednačini ψ_6.

Na ovaj način su određene sve konstante u formulama $\psi_1 - \psi_6$. Ostaje da se proveri da li su ispunjene formule ψ_7 i ψ_8.

Za ovako izabrane konstante, s obzirom na formulu ψ_3, imamo $y'^2 = 0 \mod 2y$, dakle, prema ψ_4, $x'^2 = 1 \mod 2y$. Dalje, prema formuli ψ_5 $A = a + 1 \cdot (1-a) \mod d\, 2y$, tj. $A = 1 \mod 2y$. Dakle, prema 1° važi $y_n(A) = n \mod (A-1)$, pa kako $2y$ deli $A-1$ sledi $y_n(A) = n \mod 2y$. S obzirom da je $y_1 = y_n(A)$ imamo $y_1 = n \mod 2y$, tj. ψ_8 važi.

Prema formuli ψ_5 važi $A = a \mod x'^2$, dakle, koristeći 2°, $y_n(A) = y_n(a) \mod x'^2$, tj. $y_1 = y \mod x'^2$, pa i formula ψ_7 važi. Ovim smo dokazali inkluziju (1) Sada dokazujemo inkluziju u obrnutom smeru.

Dakle, treba dokazati da ako brojevi $a, x, y, n, x', y', x, y, A$ zadovoljavaju $\psi_1 - \psi_8$, onda je n indeks rešenja (x, y) Pellove jednačine, tj. da je $(x, y) = (x_n(a), y_n(a))$.

Neka su N, N', N_1 redom indeksi rešenja $(x, y), (x', y'), (x_1, y_1)$. Treba da dokažemo $n = N$. Kao i u slučaju dokaza inkluzije (1) nalazimo:

$A = 1 \mod 2y$ (prema ψ_5),

$y_1 = N_1 \mod 2y$ (prema 1°). Takođe,

$y_1 = n \mod 2y$ (prema (ψ_8), odakle

$N_1 = n \mod 2y$. Dalje,

$A = a \mod x'^2$ (prema ψ_5),

$y_1 = y_{N_1}(A) = y_{N_1}(a) \mod x'^2$ (prema 2° i ψ_5). Dalje,

$y = y_N(a) = y_1 \mod x'^2$ (prema ψ_7), odakle

$y_N(a) = y_{N_1}(a) \mod x'^2$.

Prema 3° sledi (birajući $i = N$, $j = N_1$, $n = N'$)

$$N = \pm N_1 \mod 2N'. \tag{2}$$

$y_N(a)^2$ deli $y_{N'}(a)$ (prema ψ_3), odakle, koristeći 4°,

$y_N(a)$ deli N', tj. y deli N'.

$N = \pm N_1 \mod 2N'$ (prema (2)).

Najzad, $y \geqslant n$ (prema ψ_1) i $y \geqslant N$ (jer $y = y_N(a)$), odakle sledi $N = n$. ■

Sada dokazujemo:

Lema 6. Graf funkcije $y = a^n$ je diofantovski skup.

Dokaz. Neka je $E_0 = \{\langle y, n, a\rangle: a > 1 \wedge y = a^n\}$. Dovoljno je dokazati da je E_0 diofantovski skup.

*A*ko je $a > 1$ tada je lako dokazati indukcijom po n da je $(2a-1)^n \leqslant y_{n+1}(a) \leqslant (2a)^n$.

Otuda za $N \geqslant 1$ važi:

$$a^n(1-1/(2Na))^n = (2aN-1)^n/(2N)^n \leqslant y_{n+1}(Na)/y_{n+1}(N) \leqslant$$

$$(2Na)^n/(2N-1)^n = a^n(1-1/(2N))^{-n}.$$

Otuda za dovoljno veliko N imamo:

$$(1-1/(2N))^{-1}-1 < 1/a^n, \quad 1-(1-1/(2Na))^n < 1/a^n.$$

Dakle za dovoljno veliko N važi:

$$a^n = [y_{n+1}(Na)/y_{n+1}(N)].$$

Prema tome, skup E_0 je projekcija skupa E_1 čiji su elementi trojke $\langle y, n, a\rangle$, i koji je definisan formulom

$$a > 1 \wedge 0 \leqslant y_{n+1}(N)\, y - y_{n+1}(Na) < y_{n+1}(N) \wedge N > \text{const.},$$

gde const. označava jednu donju granicu za N, na primer to može biti $4n(y+1)$. Stoga je:

$$y = a^n \wedge a > 1 \leftrightarrow \exists N\,(a > 1 \wedge 0 \leqslant y_{n+1}(N)\, y - y_{n+1}(Na) <$$

$$y_{n+1}(N) \wedge 4n(y+1) < N).$$

Primetimo da je E_1 diofantovski skup, s obzirom na Lemu 5 i definirajuću formulu θ (desna strana gornje ekvivalencije):

$$\theta(a, n, N, y) \leftrightarrow \exists y'\, y''\,(y' = y_{n+1}(N) \wedge y'' = y_{n+1}(Na) \wedge \ldots).$$ ■

Sada dokazujemo da su binomna funkcija i faktorijel funkcija, takođe, diofantovske.

Lema 7. Neka je ψ ova formula: $r=\binom{n}{k}\wedge n\geqslant k$. Tada je skup $\{(r, k, n)\colon \psi\}$ diofantovski.

Dokaz. Neka je $r(x, y)$ funkcija ostatka, tj. $r(x, y)$ je ostatak dobijen deljenjem broja x brojem y. Tada važi ova implikacija:

$$u\geqslant n^k\rightarrow\binom{n}{k}=r\,(u,\,[(u+1)^n/u^k]) \tag{1}$$

Zaista, ova činjenica neposredno sledi iz identiteta:

$$(u+1)^n/u^k=\sum_{\mathrm{i}=\mathrm{k}+1}^{n}\binom{n}{i}u^{i-k}+\binom{n}{k}+\sum_{i=0}^{k-1}\binom{n}{i}u^{i-k}.$$

Dalje, neka su formule $\psi_1-\psi_5$ definisane na sledeći način:

$$\psi_1=_{df}u>n^k;\ \ \psi_2=_{df}v=[(u+10)^n/u^k];\ \ \psi_3=_{df}r=v\ \mathrm{mod}\ \mathrm{u};$$
$$\psi_4=_{df}r<u;\ \ \psi_5=_{df}n\geqslant k.$$

Koristeći (1) nalazimo $\psi\leftrightarrow\exists\,u,\,v\,(\psi_1\wedge\psi_2\wedge\cdots\wedge\psi_5)$. Formule $\psi_1-\psi_5$ su diofantovske, pa kako su one zatvorene za primenu egzistencijalnog kvantora, to je i ψ diofantovska formula. ■

Lema 8. Formula $\psi=_{df}m=k!$ je diofantovska.

Dokaz. Uvodimo sledeće formule:

$$\psi_1=_{df}n>(2\,k)^{k+1};\quad \psi_2=_{df}m=\left[n^k/\binom{n}{k}\right].$$

S obzirom na implikaciju:

$$k>0\wedge n>(2\,k)^{k+1}\rightarrow k!=\left[n^k/\binom{n}{k}\right],$$

imamo $\psi\leftrightarrow\exists\,n\,(\psi_1\wedge\psi_2)$. ■

Lema 9. Neka je ψ ova formula: $x/y=\binom{u/v}{w}\wedge u>vw$,

i neka je $S=\{(x, y, u, v, w)\colon \psi\}$. Tada je S diofantovski skup.

Dokaz. Razvijanjem funkcije $(1+a^{-2})^{u/v}$ u binomni Taylorov red, i odgovarajućim procenjivanjem, nalazimo:

Ako je $a>0$ ceo broj takav da je $a=0 \bmod (v^w \cdot w!)$ i $a>2^{u-1} u^{w+1}$, onda

$$\binom{u/v}{w} = a^{-1}[a^{2w+1}(1+a^{-2})^{u/v}] - a[a^{2w-1}(1+a^{-2})^{u/v}].$$

Dalje, neka su formule $\psi_1 - \psi_4$ uvedene na sledeći način:

$$\psi_1 =_{df} a=0 \bmod (v^w \cdot w!); \quad \psi_2 =_{df} a>2^{u-1} u^{w+1}$$

$$\psi_3 =_{df} u_1/u_2 = a^{-1}[a^{2w+1}(1+a^{-2})^{u/v}];$$

$$\psi_4 =_{df} v_1 = a[a^{2w-1}(1+a^{-2})^{u/v}].$$

Tada je

$$\psi \leftrightarrow \exists u_1 u_2 v_1 a (\psi_1 \wedge \psi_2 \wedge \psi_3 \wedge \psi_4),$$

dakle formula ψ je diofantovska. ■

Sada je dokaz Matijasevičeve teoreme neposredna posledica Lema 3, 6, 8 i 9.

DODATAK B: TEORIJA EFEKTIVNE IZRAČUNLJIVOSTI

§ 1. Uvod. Ideja efektivne izračunljivosti nastala je relativno nedavno, tridesetih godina, ali to nije smetalo da se ovaj pojam uvrsti među najvažnije doprinose praktičnoj kulturi modernog naučnog života. Jer, uvođenje takvog tehničkog pojma nije dovelo samo do značajnih otkrića u logici, mada je to bio prvobitni cilj, već se ispostavilo da ova teorija predstavlja vitalno intelektualno sredstvo u izgradnji modela složenih sistema. Verovatno se najvažnije primene nalaze u računarstvu i računarima, ali se, isto tako, značajne primene ove teorije mogu naći u raspravljanju pitanja iz biologije, psihologije, lingvistike, filozofije i naravno matematike.

U ovom dodatku izložićemo neke od glavnih ideja teorije izračunljivosti, s ciljem da se bolje razumeju drugo i treće poglavlje ove knjige, ali i da se bar donekle potvrde navodi izrečeni u prethodnom pasusu.

Glavni pojam ove teorije je pojam algoritma ili efektivne procedure. Najjednostavnije rečeno, pod algoritmom se podrazumeva efektivan postupak koji primenjen na klasu reči nad nekim alfabe-

tom (te reči se nazivaju *ulazima*) eventualno daje odgovarajuće izlazne reči (tj. *izlaze*). Dakle, algoritam je procedura za izračunavanje neke funkcije. Primeri takvih postupaka su poznati praktično u svim oblastima matematike. Spomenimo neke:

1° sabiranje i množenje prirodnih brojeva,

2° Euklidov algoritam za određivanje najvećeg zajedničkog delioca dva prirodna broja,

3° diferenciranje elementarnih funkcija,

4° rešavanje pojedinih klasa diferencijalnih jednačina,

5° postupci za ispitivanje tautologičnosti iskaznih formula.

Svi ovi i drugi postupci izračunavanja imaju sledeće zajedničke osobine koje se mogu smatrati neophodnim, da bi se isvesna procedura smatrala efektivnom (naravno, ovde se pretpostavlja jedna idealna situacija; tako npr. u sledećim uslovima reč „postoji“ ima upravo ono značenje koje ima u matematici):

1. svaki algoritam dat je kao *konačan niz instrukcija*;
2. postoji *računsko sredstvo*, koje interpretira i izvodi instrukcije algoritma;
3. postoji *memorijski prostor* u kojem se čuvaju (privremeno ili stalno) svi podaci koji se javljaju prilikom izračunavanja;
4. izračunavanje po datom algoritmu je *diskretne prirode*, dakle izvodi se korak po korak i bez korišćenja neprekidnih metoda ili analognih sredstava;
5. izračunavanje po datom algoritmu je *determinisano*, tj. izvodi se bez korišćenja slučajnih metoda ili sredstava; dakle, ponovljene primene algoritama na iste ulazne veličine proizvode iste izlazne veličine;
6. ne postoje *nikakva ograničenja* na veličinu ulaza, broj instrukcija, veličinu memorije, kao ni na dužinu računa koji se izvodi za konkretan ulaz;
7. algoritam *ne mora davati rezultat za sve ulaze*; izračunavanje pomoću algoritama može, dakle, da se nikad ne završi.*

---

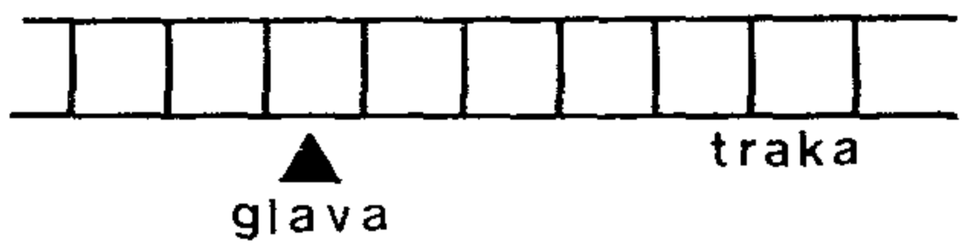
* Zahvaljujem se Miodragu Kapetanoviću što mi je sugerisao ovu tačku.

8. ipak, u sledećem smislu postoji granica u mogućnostima računskih sredstava: ispostavlja se da postoji *univerzalan algoritam* koji simulira izračunavanje po svakom algoritmu;
9. algoritama i objekata na kojima se oni izvode ima *prebrojivo mnogo*, ali ne i više;
10. algoritmi, ulazni i izlazni simboli mogu se *efektivno kodirati* u skupu prirodnih brojeva.

Polazeći od ovih uslova predloženo je više formalnih sistema u okviru kojih se definiše i analizira matematičkim sredstvima pojam efektivne izračunljivosti. Dajemo pregled nekih od njih.

§ **2. Turingove mašine.** Tridesetih godina počinje nagli razvoj logike. Gödel, Church, Tarski, Kleene, Post i drugi proučavaju formalizovane sisteme i iz tih radova i radova Alana Turinga[1] nastaje matematički pojam efektivne izračunljivosti. Turing konstruiše 1935. god. jedan apstraktan model izračunljivosti koji po njemu nosi naziv algoritamski sistem Turingovih mašina. Ovo otkriće zanimljivo je jer je dalo teorijski okvir za projektovanje i stvaranje računara koji se mogu programirati (von Neumann i njegove kolege), kao i formalnih programskih jezika. Dajemo jedan neformalan opis Turingovih mašina.

Turingova mašina je mehaničko sredstvo kojem je pridružen memorijski prostor u vidu trake koja se beskrajno pruža ulevo i udesno. Traka je podeljena na prostore jednake veličine koji se nazivaju ćelijama. Nad trakom se nalazi glava mašine koja se u svakom momentu nalazi nad nekom ćelijom trake. Traka može da se kreće ulevo i udesno i to u jednom koraku pomeranje se vrši najviše za jednu ćeliju. Najzad mašina vrši sledeće radnje:



— briše sadržaj ćelije nad kojom se glava nalazi;
— eventualno, briše i upisuje nov simbol iz unapred datog alfabeta A;
— vrši pomeranje trake za jednu ćeliju ulevo ili udesno.

[1] [Turing 1937]

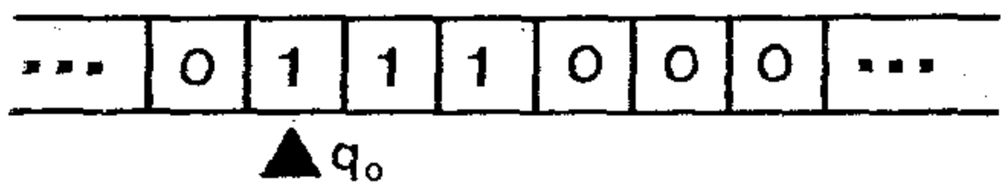
Dok je aktivna, mašina izvodi samo jednu od nabrojanih operacija u jedinici vremena, i jedna takva operacija naziva se računskim korakom. Posle svakog izvedenog koraka mašina se nalazi u jednom od stanja iz unapred datog konačnog skupa stanja S. Rad mašine izvodi se prema instrukcijama iz nekog utvrđenog konačnog niza instrukcija koji nazivamo *programom*. Svaka instrukcija izgleda ovako:

(1) $pXYq$

gde su p, q stanja, tj. $p, q \in S$, dok je X simbol alfabeta A, a Y takođe simbol iz proširenog alfabeta $A \cup \{L, R\}$, gde $L, R \notin A$. Instrukcijom (1) izražava se pravilo, da ukoliko se mašina nalazi u stanju p i ako je sadržaj ćelije koju glava ispituje simbol X, onda mašina upisuje u tu ćeliju simbol Y ili vrši pomeranje trake ulevo ili udesno, a zatim prelazi u stanje q. Pomeranje trake ulevo vrši se ako je $Y = L$, dok se pomeranje udesno izvodi ako je $Y = R$. Najzad, alfabet S sadrži specijalan znak, neka je to simbol 0, čije je značenje sledeće:

ako je $X = 0$, onda je sadržaj ispitivane ćelije prazan;
ako je $Y = 0$, onda se sadržaj ispitivane ćelije briše.

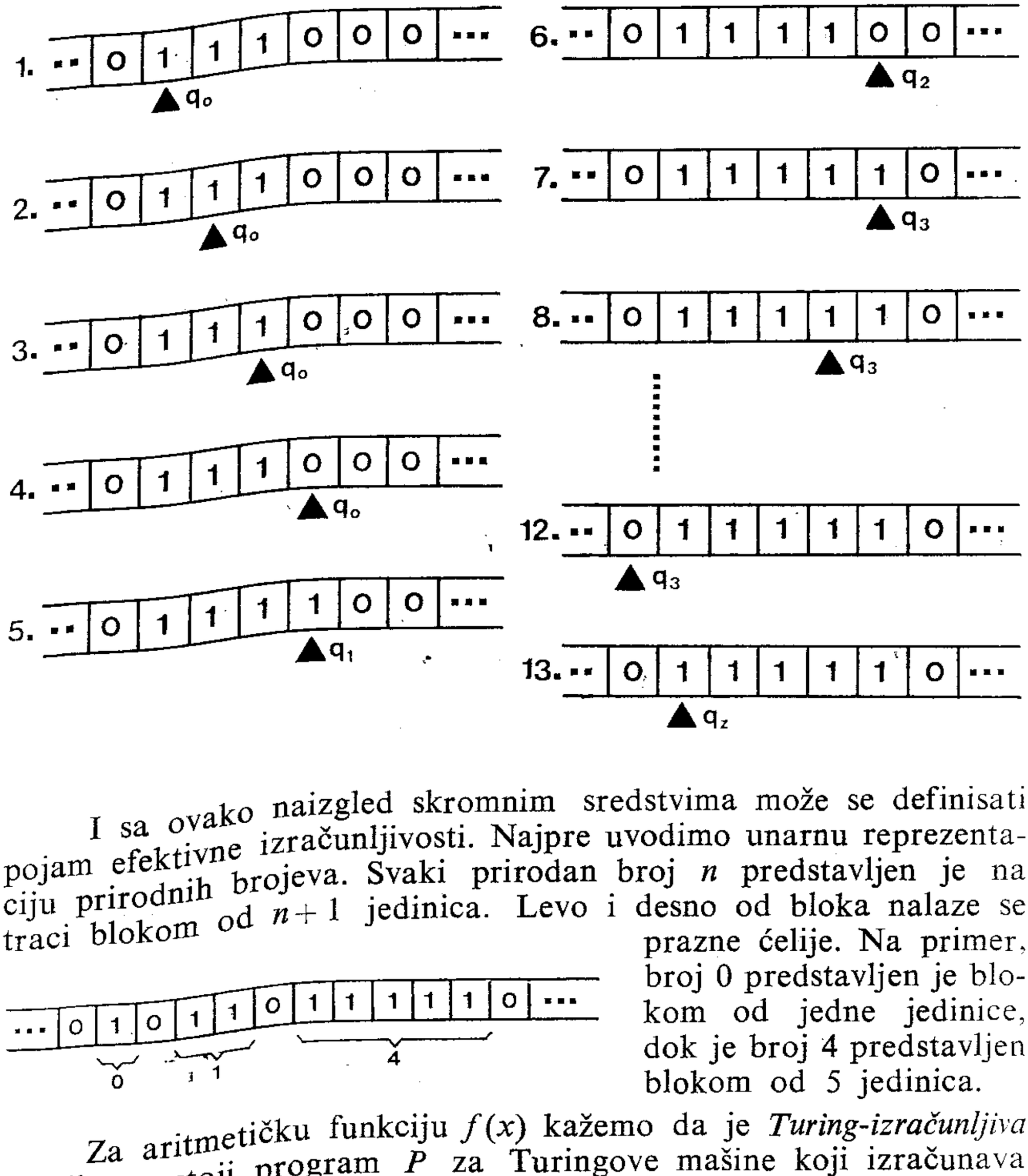
Ovde ćemo se ograničiti na slučaj najjednostavnijeg alfabeta, tj. uzećemo da je $A = \{0, 1\}$. Mada izbor ovakvog alfabeta može da izgleda kao veliko ograničenje, ispostavlja se da računske mogućnosti takve mašine nisu manje od Turingovih mašina sa proizvoljno velikim alfabetom. Stanja mašine označićemo sa $q_0, q_1, \ldots$. Među njima razlikujemo početno stanje, neka je to q_0 i završno stanje q_z. Dakle, na početku rada mašina se nalazi u stanju q_0, a ukoliko se nađe u stanju q_z onda ona prestaje sa radom.



$q_0\,1\,Lq_0$
$q_0\,01\,q_1$
$q_1\,1\,Lq_2$
$q_2\,01\,q_3$
$q_3\,1\,Rq_3$
$q_3\,0\,Lq_z$

Evo jednog primera programa za Turingove mašine. Neka je na traci konfiguracija kao na slici, tj. blok jedinica smešten između dve nule. Treba napisati program koji će dopisati dve jedinice s desna na taj blok i vratiti glavu na početak bloka. Kao što vidimo taj program ima šest instrukcija.

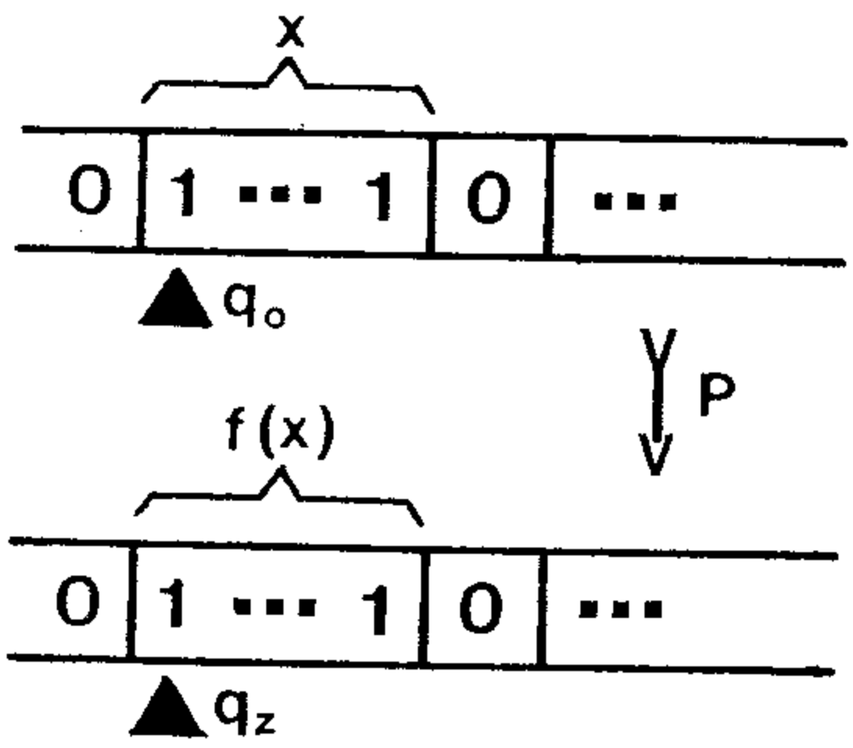
Izračunavanje po ovom programu prikazano je u sledećem nizu konfiguracija, odakle se vidi u svakom koraku sadržaj trake, kao i stanje u kojem se mašina nalazi:



I sa ovako naizgled skromnim sredstvima može se definisati pojam efektivne izračunljivosti. Najpre uvodimo unarnu reprezentaciju prirodnih brojeva. Svaki prirodan broj n predstavljen je na traci blokom od $n+1$ jedinica. Levo i desno od bloka nalaze se prazne ćelije. Na primer, broj 0 predstavljen je blokom od jedne jedinice, dok je broj 4 predstavljen blokom od 5 jedinica.

Za aritmetičku funkciju $f(x)$ kažemo da je *Turing-izračunljiva* ukoliko postoji program P za Turingove mašine koji izračunava vrednosti funkcije f na sledeći način:
u početnom stanju q_0 glava mašine nalazi se na prvoj ćeliji bloka jedinica kojim je u unarnoj notaciji predstavljena ulazna vrednost x,

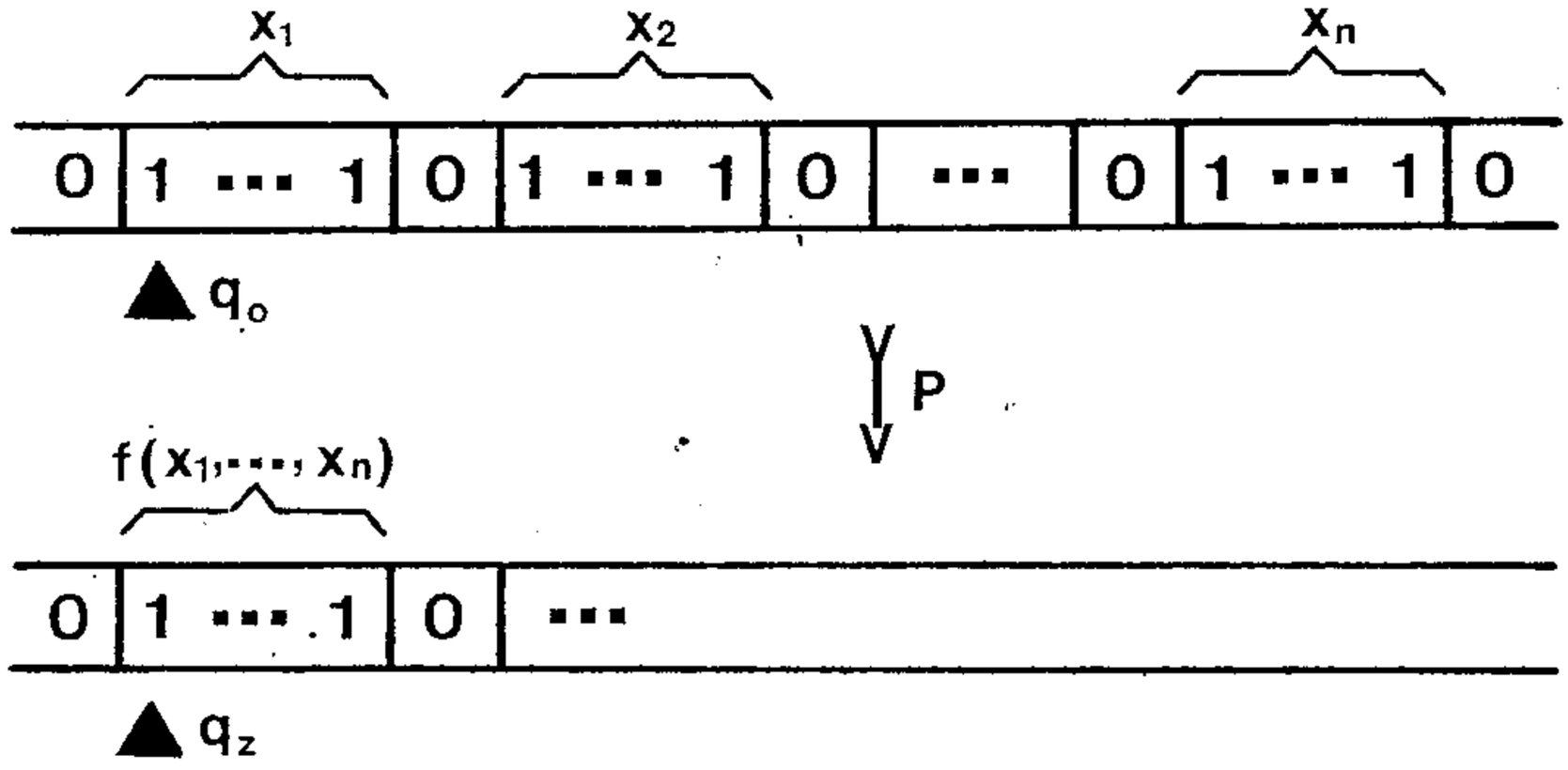
argument x, argument funkcije f; po izvršenom programu P, glava mašine nalazi se nad prvom ćelijom bloka jedinica koji predstavlja vrednost $f(x)$, takođe u unarnoj notaciji.



Program (1) izračunava vrednosti funkcije $f(x) = x + 2$. Dakle, ova funkcija je Turing-izračunljiva.

Funkcije sa više argumenata se izračunavaju na sličan način kao funkcije jednog argumenta. U slučaju funkcija od n argumenata reprezentacija argumenata i vrednosti funkcije prikazana je na slici.

U Turing-izračunljive funkcije spadaju razne aritmetičke funkcije: sabiranje i množenje prirodnih brojeva, polinomne funkcije,



niz prostih brojeva, zatim karakteristične funkcije skupova: parnih brojeva, prostih brojeva, kôdova formula Peanove aritmetike, kôdova dokaza u Peanovoj aritmetici. Evo programa za računanje zbira prirodnih brojeva:

$q_0\ 1\ Lq_0$

$q_0\ 01\ q_1$

$q_1\ 1\ Rq_1$

$q_1\ 0\ Lq_2$

$q_2\ 10\ q_3$

$q_3\ 0\ Lq_z$

Očigledno je da instrukcija ima najviše prebrojivo mnogo, pa kako su programi za Turingove mašine konačni nizovi instrukcija, sledi da i programa ima tačno prebrojivo mnogo. Otuda sledi da Turing-izračunljivih funkcija ima ne više od prebrojivo mnogo. Podsetimo se, takođe, da aritmetičkih funkcija ima kontinuum mnogo.

Turing-izračunljive funkcije dele se na totalne i parcijalne. Kod totalnih funkcija vrednosti funkcija definisane su za sve vrednosti argumenata, dok kod parcijalnih to ne mora da bude slučaj. Na primer, jedan program za izračunavanje prazne funkcije ima samo jednu instrukciju:

$$q_0\, 1\, 1\, q_0.$$

Prema ovom programu (instrukciji) mašina nikad ne prestaje da radi.

Da bismo uveli univerzalnu Turingovu mašinu, najpre se mora uvesti neko kodiranje Turingovih mašina. Ukoliko se ograničimo na alfabet {0, 1}, jedna mogućnost je ova: kôdovi simbola 0, 1, L, R su redom 1, 2, 3, 4, dok je kôd instrukcije $I = q_i XYq_j$:

$$k(I) = 2^i\, 3^{k(X)}\, 5^{k(Y)}\, 7^j,$$

gde su $k(X)$, q_i, $k(Y)$ kôdovi simbola X, Y. Ako je $P = I_1 I_2 \cdot \cdot \cdot I_n$ jedan program, možemo uzeti da je kôd programa P:

$$\ulcorner P \urcorner = 2^{k(I_1)}\, 3^{k(I_2)} \ldots p_n^{k(I_n)}.$$

gde je $2, 3, \ldots, p_n, \ldots$ niz prostih brojeva. Najzad sve programe možemo urediti ovako:

$$P \prec Q \text{ akko } \ulcorner P \urcorner < \ulcorner Q \urcorner,$$

pa se u tom uređenju svi programi mogu efektivno nabrojati u niz:

$$P_0 \prec P_1 \prec P_2 \cdot \cdot \cdot$$

Tada se u P_n broj n naziva *indeksom* programa P. Očigledno je da se za svaku Turingovu mašinu može efektivno odrediti njen indeks, kao i da se za svaki prirodan broj n takođe može efektivno konstruisati Turingova mašina P_n.

Uvedimo i ovu notaciju: ako je P program i x prirodan broj, tada $P(x) \downarrow y$ znači „program P za ulaz x u konačno mnogo koraka daje izlaz y“, i tada kažemo da $P(x)$ konvergira ka y.

Simbol $P(x)\downarrow$ znači da P za ulaz x daje neki izlaz, dok $P(x)\uparrow$ označava da nije $P(x)\downarrow$, i tada kažemo da P divergira za ulaz x. Slična je notacija u slučaju više argumenata.

Pod *univerzalnom* Turingovom mašinom podrazumevamo program U sa osobinom:

$$P_n(x)\downarrow y \Rightarrow U(n, x)\downarrow y$$

$$P_n(x)\uparrow \quad \Rightarrow U(n, x)\uparrow .$$

Važi sledeće tvrđenje koje opravdava uslov 8 iz liste osobina efektivne izračunljivosti:

Teorema. Postoji univerzalna Turingova mašina.

Ako je $\varphi(x_1, \ldots, x_n)$ neki aritmetički predikat, onda kažemo da je φ *odlučiv* ukoliko je njegova karakteristična funkcija:

$$k_\varphi(x_1, \ldots, x_n) = \begin{cases} 1 & \text{ako je } \varphi(x_1, \ldots, x_n) \\ 0 & \text{ako nije } \varphi(x_1, \ldots, x_n) \end{cases}$$

Turing-izračunljiva. Ukoliko se neki problem može formalizovati ili prevesti na neki aritmetički predikat, tada kažemo da je taj problem odlučiv ako je odgovarajuća karakteristična funkcija Turing-izračunljiva. Na primer, da li je zadovoljeno:

„n je paran broj“,

„n je prost broj“,

„polinom $p(x)$ sa racionalnim koeficijentima ima racionalne korene“,

„niz simbola s je formula formalne aritmetike“

su odlučivi problemi, jer su odgovarajući aritmetički predikati odlučivi. Sada navodimo primer jednog neodlučivog problema.

Problem zaustavljanja (Halting problem). Neka je k karakteristična funkcija predikata $U(n, x)\downarrow$ gde je U univerzalna Turingova mašina. Tada važi:

$$U(n, x)\downarrow \Rightarrow k(n, x) = 1$$

$$U(n, x)\uparrow \Rightarrow k(n, x) = 0.$$

Dokazujemo da k nije Turing-izračunljiva funkcija. Pretpostavimo suprotno. Tada je i funkcija h definisana ovako:

$$h(n, x) = \begin{cases} \uparrow & \text{ako je } k(n, x) = 1 \\ 1 & \text{ako je } k(n, x) = 0. \end{cases}$$

takođe Turing-izračunljiva, jer se na osnovu programa za funkciju k lako konstruiše i program za funkciju h. Neka je P_m program koji izračunava funkciju h. Tada na osnovu osobina programa U i funkcija k i h nalazimo:

$$U(m, m)\downarrow \Rightarrow k(m, m) = 1 \Rightarrow h(m, m)\uparrow$$

$$U(m, m)\uparrow \Rightarrow k(m, m) = 0 \Rightarrow h(m, m)\downarrow,$$

što u oba slučaja daje protivrečnost. Dakle, funkcija k nije izračunljiva pa ni problem zaustavljanja vezan za predikat

$$U(n, x)\downarrow$$

čije je značenje „Turingova mašina sa indeksom n za ulaz x prestaje sa radom posle konačno mnogo koraka“, nije odlučiv.

Ovaj problem ima važnu ulogu u teoriji efektivne izračunljivosti, jer se neodlučivost mnogih drugih problema dokazuje na osnovu neodlučivosti problema zaustavljanja.

Naravno, u prethodnom „negativnom“ rešenju problema zaustvljanja, pojam odlučivosti precizno je određen. Dokazati da je neki problem odlučiv, u ovom kontekstu znači konstruisati određenu Turingovu mašinu, dok se dokaz da neki problem nije odlučiv svodi na dokaz da jedna određena funkcija (karakteristična funkcija problema) nije Turing-izračunljiva. S tim u vezi, postavlja se jedno pitanje koje nije doduše u potpunosti matematičkog karaktera: Da li je izračunljivost u intuitivnom smislu obuhvaćena sistemom izračunljivosti Turingovih mašina? Odgovor donekle daje

Churchova teza. Klasa intuitivno izračunljivih funkcija poklapa se sa klasom Turing-izračunljivih funkcija.

Dakle, ova teza tvrdi da je sistemom Turing-izračunljivih funkcija obuhvaćen u potpunosti pojam efektivine izračunljivosti. Kao što ovo pitanje nije u potpunosti matematičkog karaktera, ni sama teza nije sasvim matematičkog karaktera. Potvrda za tezu nalazi se u činjenici da do danas nijedan sistem izračunljivosti nije dao širu klasu izračunljivih funkcija od klase Turing-izračunljivih funkcija.

Najzad spomenimo da se sistem Turingovih mašina može uvesti na strožijem matematičkom jeziku. Naime, ako je $A=\{0, 1\}$, za proširen alfabet možemo uzeti skup $\{0, 1, 2, 3\}$ gde su simboli L i R redom zamenjeni brojevima 2,3. Za stanja možemo uzeti samo prirodne brojeve, pa se programi mogu definisati kao preslikavanja konačnih podskupova skupa $N \times A$ u skup $\{0, 1, 2, 3\} \times N$.

§ 3. Rekurzivne funkcije. Zanimljivo je pitanje da li se klasa Turing-izračunljivih funkcija može opisati na „algebarski" način, tj. da li se ona može dobiti koristeći određene operacije nad aritmetičkim funkcijama polazeći od nekih jednostavnih funkcija. To je moguće, a odgovarajuće operacije nad funkcijama su: supstitucija, rekurzija i minimizacija. Do kraja ovog paragrafa ograničavamo se na klasu aritmetičkih funkcija.

Supstitucija. Neka su $g(x_1, \ldots, x_n)$, $h_1(x_1, \ldots, x_m), \ldots, h_n(x_1, \ldots, x_m)$ aritmetičke funkcije. Funkcija f dobijena je supstitucijom iz funkcija $g, h_1, \ldots, h_n$ akko za sve $x_1, \ldots, x_m \in N$ važi

$$f(x_1, \ldots, x_m) \cong g(h_1(x_1, \ldots, x_m), \ldots, h_n(x_1, \ldots, x_m)).$$

Ovde simbol $\cong$ ima sledeće značenje: ako su $f(x)$, $g(x)$ neke aritmetičke funkcije, onda $f(x) \cong g(x)$ znači da je vrednost $f(x)$ definisana akko je definisana vrednost $g(x)$, i ako je $f(x)$ definisano, onda je $f(x)=g(x)$.

Postoje dve vrste rekurzije:

Primitivna rekurzija sa parametrima. Ako je f neka m-arna parcijalna (aritmetička) funkcija i h $(m+2)$-arna parcijalna funkcija, tada je $(m+1)$-arna funkcija g dobijena primitivnom rekurzijom pomoću funkcija f i h ukoliko je g definisana na sledeći način:

$$g(x_0, \ldots, x_{m-1}, 0) \cong h(x_0, \ldots, x_{m-1})$$

$$g(x_0, \ldots, x_{m-1}, y+1) \cong h(x_0, \ldots, x_{m-1}, y, g(x_0, \ldots, x_{m-1}, y)).$$

Ulogu parametara ovde imaju promenljive $x_0, \ldots, x_{m-1}$.

Primitivna rekurzija bez parametara. Ako je a prirodan broj i h parcijalna funkcija sa dva argumenta, tada je unarna funkcija g

dobijena rekurzijom pomoću konstante a i funkcije h na sledeći način:

$$g(0) = a$$
$$g(x+1) \cong h(x, g(x)), \qquad x \in N.$$

Minimizacija. Neka je f $(m+1)$-arna parcijalna funkcija. Tada se m-arna parcijalna funkcija g dobija iz f minimizacijom, ukoliko za sve prirodne brojeve $x_0, \ldots, x_{m-1}$ važi:

$g(x_0, \ldots, x_{m-1}) =$ najmanji y takav da $(\forall z < y)((x_0, \ldots, x_{m-1}, z) \in$ Domen (f) i $f(x_0, \ldots, x_{m-1}, y) = 0)$.

Tada pišemo:

$$g(x_0, \ldots, x_{m-1}) = \mu y (f(x_0, \ldots, x_{m-1}, y) = 0).$$

Klasa parcijalno rekurzivnih funkcija je presek svih klasa A parcijalnih funkcija takvih da:

(1) A sadrži funkciju naslednik $x \mapsto x+1$, $x \in N$, i projekcijske funkcije $U_i^n: (x_0, \ldots, x_{n-1}) \mapsto x_i$, $(i < n)$, $x_0, \ldots, x_{n-1} \in N$;

(2) A je zatvorena za operacije supstitucije, primitivne rekurzije i minimizacije.

Dakle, A je najmanja klasa parcijalnih funkcija za koju važi (1) i (2). Centralna teorema o klasi parcijalno rekurzivnih funkcija je ova teorema karakterizaćije Turing-izračunljivih funkcija.

Teorema. Neka parcijalna funkcija f je Turing-izračunljiva akko je f parcijalno rekurzivna funkcija.

Prema tome, sistem parcijalno rekurzivnih funkcija takođe predstavlja jedan formalni sistem efektivne izračunljivosti. Sa ovim tvrđenjem završavamo ovaj dodatak, uz napomenu da postoje i mnogi drugi sistemi efektivne izračunljivosti, o kojima se čitalac može informisati u literaturi.

BIBLIOGRAFSKE BELEŠKE

1. Prvi koraci u rešavanju desetog Hilbertovog problema učinjeni su još 50-tih godina. Najvažniji rezultati iz tog vremena sadržani su u sledećim radovima: [Robinson 1952], [Davis 1953] i [Davis et al. 1961].

2. Kompletno rešenje desetog Hilbertovog problema dao je J. Matijasevič 1970. god. To rešenje je sadržano u radu [Матиясевич

1970]. Ovde treba uvrstiti i rad G. V. Čudnovskog [1970] koji je dao nešto drugačije rešenje.

3. Formulacija desetog Hilbertovog problema je vrlo jednostavna i stoga je taj problem zanimljiv široj matematičkoj publici. Rešenje, mada ingeniozno, sadrži mnoge u osnovi elementarne detalje. Osim toga, Matijasevičevo rešenje po primenama i posledicama u logici i aritmetici daleko prevazilazi sam 10Hp. To je, verovatno razlog što postoji više prikaza ovog rešenja namenjenih široj matematičkoj publici. U najzanimljivije i veoma kompletne prikaze ove vrste spadaju [Davis 1973] i [Манин 1980]. U članku M. Davisa, J. Matijaseviča i J. Robinson *Hilbert's tenth problem. Diophantine equations: positive aspects of a negative solution*, u knjizi [Browder 1976], analizira se veoma detaljno značaj rešenja 10Hp za neke druge veoma poznate i još uvek otvorene probleme u matematici.

4. Za potpuno razumevanje formulacije i rešenja 10Hp potrebno je da je čitalac donekle upoznat sa teorijom rekurzivnih funkcija. O tome se nešto više može saznati npr. u knjigama [Cutland 1980] i [Rogers 1967].

5. Rešenje 10Hp naročito je značajno za teoriju modela formalne aritmetike. Reč je o nestandardnim modelima (dakle neizomorfnim strukturi prirodnih brojeva), za koje je interesovanje poraslo u 70-tim godinama. Posebno zanimanje za ovu temu nastaje posle otkrića J. Parisa 1978. god. aritmetičkog iskaza „sa matematičkim sadržajem" (radi se o jednoj finitarnoj verziji Ramseyeve teoreme) koji je istinit a nedokaziv u formalnoj aritmetici. Do tada su svi poznati neodlučivi aritmetički iskazi bili metamatematičkog karaktera. Na ovu temu je objavljeno nekoliko stotina članaka, a čitalac se o tome može dosta brzo informisati u člancima Smoryńskog, J. Parisa i L. Harringtona u knjizi [Barwise 1978]. Postoje i veoma zanimljiva predavanja, koja doduše nisu tako lako dostupna (ali oni najzainteresovaniji ipak ih mogu naći) od J. Parisa, W. Mareka i C. Smoryńskog.

6. U našoj zemlji takođe postoji zanimanje za modele aritmetike; uostalom to potvrđuje ova knjižica. Na ovu temu pisali su Ž. Mijajlović i M. Kapetanović u knjizi [Mihaljinec et al. 1984]. Autor ovog poglavlja 1982. god. održao je u okviru Seminara za matematičku logiku jednogodišnji kurs o modelima aritmetike, i tom prilikom izložio je rešenje za 10Hp. Zabeleške sa ovih predavanja takođe postoje.

IV SEDAMNAESTI HILBERTOV PROBLEM

Problem predstavljivosti pozitivno definitnih racionalnih formi kao suma kvadrata

Uvod[1]

Ovaj problem, takođe, ima jednostavnu formulaciju. Racionalna funkcija $f=g/h$ nad poljem racionalnih brojeva Q (ili poljem realnih brojeva R) je *pozitivno definitna* ukoliko važi:

$$\forall\, x \in R\,(h(x) \neq 0 \;\Rightarrow\; f(x) \geqslant 0).$$

Tada sedamnaesti Hilbertov problem glasi:

17 Hp Ako je f pozitivno definitna racionalna funkcija nad poljem Q ili R, da li je f onda zbir kvadrata nekih racionalnih funkcija?

Već se sam Hilbert bavio tim problemom i nekim sličnim problemima. Na primer, 11. problem sa Hilbertove liste odnosi se na aritmetičku teoriju kvadratnih formi. Takođe, Hilbert je 1883. godine pozitivno rešio 17 Hp u slučaju da racionalna funkcija f ima 2 argumenta. Ovaj problem se, naravno, može formulisati i za polinome, ali Hilbert je još 1888. godine pokazao da je takva formulacija problema, na neki način, nužna. Naime, on je dokazao da postoje pozitivno definitni polinomi nad poljem realnih brojeva koji nisu konačne sume kvadrata nekih polinoma. Doduše, ovaj Hilbertov dokaz bio je indirektne i nekonstruktivne prirode, tj. Hilbert nije naveo konkretan polinom takve vrste[2]. Mada Hilbert nije bio prvi koji je koristio ovakve dokaze, on je svakako bio prvi matematičar koji je ukazao na duboki značaj i vrednost tak-

---

[1] Značenje simbola $\models$ i nekih drugih simbola čitalac može naći u prethodnom poglavlju.

[2] Motzkin je 1966. god. dao primer takvog polinoma: $p(x, y)=1+x^4 y^2+ + x^2 y^4-3 x^2 y^2$.

vih dokaza u matematici. Naravno, takvi dokazi primljeni su na dramatičan način u ondašnjoj matematičkoj sredini, jer to je bilo vreme strogog i doslednog formalizma u tradicionalnom značenju te reči. Nije bilo neobično da se nađu formule koje su tekle iz stranice u stranicu u nekom od časopisa iz tog vremena, ili kako su govorili matematičari u kasnijim vremenima „one su bile uporedive jedino sa formulama koje opisuju kretanje meseca".

U tom novom hilbertovskom duhu naročito je poznato njegovo rešenje takozvanog Gordanovog problema. Danas je to rešenje poznato kao:

Hilbertova teorema o bazi. Ako je F polje, tada je u prstenu polinoma $F[x_1, \ldots, x_n]$ svaki ideal konačno generisan.

To znači sledeće: ako je S bilo koji podskup prstena $F[x_1, \ldots, x_n]$, tada postoje neki polinomi $f_1, \ldots, f_k$ nad poljem F takvi da je svaki polinom $g \in S$ linearna kombinacija polinoma $f_1, \ldots, f_k$.

Prsteni sa osobinom da su svi ideali nad njima konačno generisani nazvani su kasnije Noetherinim, po Emmy Noether, koja je svoju naučnu karijeru započela kao asistent kod Hilberta. (Zanimljivo je da je u početku njene asistenture Hilbert dobrim delom nju izdržavao, jer Noether nije bila zvanično primljena za asistenta, i pored Hilbertovog angažovanja.) Danas, Hilbertova teorema o bazi predstavlja jednu od osnovnih teorema algebarske geometrije.

Koliko su Hilbertovi dokazi bili neobični najbolje pokazuju komentari ondašnjih matematičaia. Na primer, Lindemann za metode mladog Hilberta kaže da su „unheimlich"[1]. Doduše, to nije bio prvi slučaj u istoriji matematike da se matematičari sa nekom dozom strahopoštovanja odnose prema rešenjima nekog svog savremenika. Tako se još za Arhimeda govorilo „da mu rešenja šapuću bogovi". Sam Gordan kaže: „To nije matematika, to je teologija." Ova rečenica kao da je predviđala novo vreme i nov pristup matematici, i može se slobodno reći da ona odzvanja sve do danas u matematici, dugo pošto je i sam Gordanov rad pao u zaborav.

Bez obzira na konzervativnost matematičke sredine, i za ono vreme neobičan Hilbertov pristup, kod ondašnjih matematičara

[1] nelagodni, neprijatni, ili slobodnije prevedeno, zastrašujući.

postojala je objektivnost i naučno poštenje, i tako je Hilbert ubrzo postao docent u Getingenu, i ušao u najuži krug izabranih matematičara svog doba. U tome mu je pomogao Felix Klein koji se i sam proslavio već u 23. godini, kada je održao svoje pristupno predavanje za profesuru u Erlangenu, danas poznato kao Erlangenski program.

Mada je mladi Hilbert išao svojim putem koji se prilično razlikovao od Kroneckerove filozofije konkretnog i konstruktivnog, Kroneckerove ideje o aritmetičkom kontinuumu puno su uticale na Hilberta, što se može videti bilo po nekim Hilbertovim radovima, bilo u formulaciji drugog problema sa njegove čuvene liste.

O algebarskom rešenju

Imajući u vidu razne metode rešavanja, u 17. Hilbertovom problemu ima nekoliko delova koji se mogu preciznije formulisati. U svim formulacijama značajnu ulogu ima pojam realno zatvorenog polja. Pre navođenja definicije, podsetimo se da $F[x_1, \ldots, x_n]$ označava prsten polinoma nad poljem F, dok $F(x_1, \ldots, x_n)$ označava polje racionalnih izraza nad F s promenljivama $x_1, \ldots, x_n$.

Definicija. Polje F je *realno zatvoreno* akko:

1° svaki polinom $p \in F[x]$ neparnog stepena ima koren u F;

2° za sve $x_1, \ldots, x_n \in F$, $x_1^2 + \cdots + x_n^2 = 0$ povlači $x_1 = 0, \ldots, x_n = 0$;

3° $\forall x \exists y (y^2 = x \vee y^2 = -x)$.

Uslov 3° definicije kazuje da se u F može uvesti funkcija korenovanja za nenegativne elemente, dok se uslov 1° odnosi na neku vrstu neprekidnosti polinomnih funkcija u realno zatvorenim poljima.

Primeri realno zatvorenih polja su polje realnih brojeva i polje realnih algebarskih brojeva.

Jedna od najvažnijih osobina bilo kojeg realno zatvorenog polja F je da se ono može urediti na *jedinstven* način, tj. postoji jedinstveno uređenje $\leqslant$ domena F tako da je $(F, \leqslant)$ uređeno polje. Uređenje $\leqslant$ može se uvesti ovako:

$$\forall x, y \in F (y \leqslant x \leftrightarrow \exists z\, x = y + z^2). \qquad (I)$$

Za ovako uvedenu relaciju $\leqslant$ važe:
aksiome linearnog uređenja

$$x\leqslant x, \quad x\leqslant y\wedge y\leqslant x\to x=y, \quad x\leqslant y\wedge y\leqslant z\to x\leqslant z, \quad x\leqslant y\vee y\leqslant x;$$

aksiome saglasnosti:

$$x\leqslant y\to x+z\leqslant y+z, \quad x\leqslant y\wedge 0\leqslant z\to xz\leqslant yz.$$

Provera ovih aksioma u strukturi $(F, \leqslant)$ je jednostavna; na primer, za osobinu antisimetričnosti to izgleda ovako:

Neka za $x, y\in F$ važi $x\leqslant y$, $y\leqslant x$. Tada za neke $u, v\in F$ važi $y=x+u^2$, $x=y+v^2$, odakle $x=x+u^2+v^2$. Odavde, prema uslovu 2° definicije nalazimo $u=0$, $v=0$, tj. $x=y$.

S druge strane, neka je $(F, \leqslant)$ uređeno realno zatvoreno polje. Ukoliko uređenje $\leqslant$ zadovoljava uslov (**I**), to znači da u polju F postoji jedinstveno uređenje.

Neka (L) označava aksiome linearnog uređenja i aksiome saglasnosti. Dokazujemo da u realno zatvorenom polju F uslov (L) povlači (I). Najpre pokažimo da u F važi:

(1) $0\leqslant x\to \exists y \;\; y^2=x$.

Kako je $0^2=0$ to (1) dokazujemo za slučaj $0<x$. Na osnovu aksioma (L) lako se pokazuje da je $0<x^2$ i $-x<0$. Prema uslovu 3° definicije realno zatvorenih polja postoji $y\in F$ tako da je $y^2=x$ ili $y^2=-x$. Ako je $y^2=-x$ onda $y^2<0$, što je kontradikcija, dakle $y^2=x$, tj. (1) važi.

Ako je $x\leqslant y$ onda $y=x+(y-x)=x+u^2$, jer prema (1) postoji u, tako da je $u^2=y-x$, dakle (L) povlači (I).

Kod uređenih polja moguće je govoriti o stalno pozitivnim ili pozitivno definitnim polinomima i racionalnim funkcijama. Takvi polinomi su, na primer, zbirovi kvadrata proizvoljnih polinoma. Ima i drugih primera pozitivno definitnih racionalnih funkcija. Recimo, $q(x, y)=1/(x^2+y^2)$. Primetimo da se q može predstaviti kao zbir kvadrata nekih racionalnih funkcija:

$$q(x, y)=\left(\frac{x}{x^2+y^2}\right)^2+\left(\frac{y}{x^2+y^2}\right)^2,$$

što ide u prilog potvrdnog odgovora na 17 Hp.

Ovaj primer ima jednostavnu generalizaciju za one racionalne funkcije koje nastaju kao količnici zbirova kvadrata polinoma. Tako, $q=(x_1^2+\cdots+x_n^2)/(y_1^2+\cdots+y_m^2)$ je pozitivno definitna, i može se predstaviti kao zbir kvadrata nekih racionalnih izraza:

$$q=\frac{(x_1^2+\cdots+x_n^2)(y_1^2+\cdots+y_m^2)}{(y_1^2+\cdots y_m^2)^2}=\frac{x_1^2y_1^2+x_1^2y_2^2+\cdots+x_n^2y_m^2}{(y_1^2+\cdots+y_m^2)^2}$$

odakle

$$q=\sum_{i,j}\left(\frac{x_iy_j}{y_1^2+\cdots+y_m^2}\right)^2.$$

Pojam pozitivne definitnosti polinoma može se na sledeći način proširiti na bilo koje polje:

Ako je $F=(\mathrm{F},+,\circ,\leqslant 0,1)$ uređeno polje i $f\in F[x]$, onda se definicija pozitivne definitnosti uvodi kao i ranije.

Ako je $F=(\mathrm{F},+,\circ,\leqslant,0,1)$ bilo koje polje, onda je $f\in F[x]$ pozitivno definitan ukoliko je f pozitivno definitan u svim raširenjima (ekspanzijama) polja F do uređenog polja $(F,\leqslant)$.

Sada se u vezi sa 17 Hp prirodno postavljaju pitanja da li je tačno:

H_1 — neka je F realno zatvoreno polje; ako je $f\in F(x)$ pozitivno definitna, tada je za neki prirodan broj n racionalna forma f zbir kvadrata nekih racionalnih formi nad F;

H_2 — iskaz H_1 važi ukoliko se otkloni pretpostavka da je F realno zatvoreno;

H_3 — ako je iskaz H_1, odnosno H_2, tačan, onda postoji neka granica za broj n sabiraka koja zavisi jedino od broja promenljivih u funkciji f, a ne i od same funkcije.

Svakako najznačajniji prilog rešavanju ovog problema pripada Emilu Artinu koji je takođe bio jedno vreme asistent i Hilbertov kolega u Getingenu[1]. Naime on je 1926. god. dokazao:

1° H_1 važi;

2° H_2 važi pod uslovom da je svako uređenje polja F arhimedovsko.

[1] Kako je E. Artin bio Jevrejin, on je zbog nacističkih progona prebegao 30-tih godina u SAD. Hilbert je takođe jedno vreme bio pod istragom policije zbog sumnje da je Jevrejin, a sve to zbog svog imena, David. Ispostavilo se da je on ipak Nemac.

Artinovo rešenje se zasnivalo na tzv. Artin-Schreirovoj teoriji formalno-realnih polja, za razliku od Hilbertovog, u osnovi konstruktivnog dokaza u slučaju racionalnih funkcija od dva argumenta. Pored toga, Artin u svom dokazu koristi Sturmovu teoremu o broju korena polinoma u datom intervalu.

Kasnije su objavljeni i neki drugi dokazi, koji su bili manje više konstruktivnog karaktera[2]. Dokaz u kojem se koriste metode matematičke logike razmatraćemo u sledećem odeljku.

Što se tiče problema H_3, E. Landau[3] je dokazao ovo tvrđenje za slučaj polja racionalnih brojeva:

svaka pozitivno definitna racionalna funkcija $f \in Q(x)$ je suma najviše 8 kvadrata racionalnih funkcija nad Q.

Pourchet[4] je proširio ove rezultate na ma koje algebarsko realno polje, i to za racionalne funkcije sa jednim argumentom, s tim da je rešio i H_3 za taj slučaj. Naime, on je dokazao da je 5 najbolja granica u problemu H_3. Najzad, na osnovu Artinove teorije, H_2 važi za polje racionalnih brojeva Q bez ograničenja na broj promenljivih.

Osim toga, postoje negativni rezultati. Dubois[5] je dokazao da H_2 ne važi u proizvoljnim poljima. Naime, on je konstruisao uređeno polje F i pozitivno definitan polinom p nad F koji nije predstavljiv kao zbir kvadrata nekih racionalnih izraza nad F. Dakle, u slučaju H_2 nužne su neke dodatne pretpostavke. Problem H_2 je u potpunosti rešen metodama matematičke logike.

Najzad, Tsen, Lang, Ax i Pfister[6] dokazali su da je $n = 2^k$ gornja granica u H_3 za realno zatvorena polja (k je broj promenljivih). U vezi sa ovim postoje još uvek neki otvoreni problemi, kao što su:

1° Da li je 2^k najbolja granica u H_3?

2° Odrediti najbolju granicu u H_3 za slučaj polja racionalnih brojeva Q.

---

[2] [Habicht 1940], [Kreisel 1957].
[3] [Landau 1906].
[4] [Pourchet 1971].
[5] [Dubois 1967]
[6] [Tsen 1936], [Lang 1965], [Pfister 1971].

Neki algebarski rezultati

Rešenje problema H_1 za racionalne funkcije jedne promenljive nad poljem realnih brojeva R je veoma jednostavno.

Neka je $p(x)$ realan, pozitivno definitan polinom. Kako je $p>0$, to onda $p(x)$ nema realnih nula. Otuda se kompleksni koreni polinoma p javljaju u parovima, jer ako je $z=a+bi$ koren polinoma p, to je i $\bar{z}=a-bi$. Stoga, imamo ovu faktorizaciju polinoma p u polju kompleksnih brojeva:

$$p(x)=(x-u_1)(x-\bar{u}_1)\ldots(x-u_n)(x-\bar{u}_n),$$

gde su $u_1, \ldots, u_n$ (kompleksni) koreni polinoma p. Neka je

$$m(x)=(x-u_1)(x-u_2)\ldots(x-u_n).$$

S obzirom da za proizvoljne kompleksne brojeve u, v važi

$$\overline{u+v}=\bar{u}+\bar{v}, \quad \overline{u\cdot v}=\bar{u}\cdot\bar{v}, \quad \text{i} \quad (\forall x\in R)\,\bar{x}=x,$$

za $x\in R$ sledi:

$$\overline{m(x)}=(x-\bar{u}_1)(x-\bar{u}_2)\ldots(x-\bar{u}_n).$$

Ako je $u(x)=\mathrm{Re}(m(x))$, $v(x)=\mathrm{Im}(m(x))$, onda su u, v polinomi nad R i važi:

$$p(x)=m(x)\cdot\overline{m(x)}=(u+vi)(u-vi)=u^2+v^2,$$

dakle $p(x)$ je zbir kvadrata polinoma.

U rešavanju 17 Hp značajnu ulogu ima pojam formalno realnih polja. Stoga navodimo nekoliko najznačajnijih osobina ovih polja u vidu grupe teorema.

Definicija. Polje F je *formalno realno* akko u F važi:

$$x_1^2+\cdots+x_n^2=0\rightarrow x_1=0\wedge\cdots\wedge x_n=0$$

Svako podpolje polja realnih brojeva je formalno realno. Na primer, takvo je polje racionalnih brojeva. Polje kompleksnih brojeva nije formalno realno, jer ako je i imaginarna jedinica tada u tom polju važi $i^2+i^2=0$. Sledećim tvrđenjem opisana su sva formalno realna polja.

Teorema 1. Polje F je formalno realno akko F ima proširenje do nekog uređenog polja.

Dajemo skicu dokaza ove teoreme. Neka je P_0 najmanji podskup od F takav da važi:

1° $a\in F\to a^2\in P_0$,

2° $a, b\in P_0\to a+b,\ ab\in P_0$.

Lako je proveriti da je $P_0=\{a_1{}^2+\cdots+a_n{}^2 : n\in N,\ a_1,\ldots,a_n\in F\}$. Tada $-1\notin P_0$, jer bi inače za neke $a_1,\ldots,a_n\in F$ važilo $-1=a_1{}^2+\cdots+a_n{}^2$, tj. $1^2+a_1{}^2+\cdots+a_n{}^2=0$, što je suprotno definiciji formalno realnih polja.

Dalje, neka je $\mathscr{P}$ mnoštvo svih podskupova $P\subseteq F$ takvih da je $P_0\subseteq P$ i $-1\notin P$. Tada je $P_0\in\mathscr{P}$, tj. $\mathscr{P}$ je neprazna familija. Ako je $L\subseteq\mathscr{P}$ lanac (u odnosu na inkluziju) nije teško proveriti da skup $S=\bigcup_{P\in L} P$, takođe, pripada familiji $\mathscr{P}$. Prema tome, ispunjeni su uslovi Zornove leme, dakle u familiji $\mathscr{P}$ postoji maksimalan element S. Koristeći uslov maksimalnosti, pokazuje se da za svaki $x\in F$ važi $x\in S$ ili $-x\in S$. Tada relacija $\leqslant$ skupa F definisana sa $x\leqslant y$ ako $y-x\in S$ predstavlja jedno uređenje polja F. Prema konstrukciji vidimo da je S skup nenegativnih elemenata uređenja $\leqslant$.

Zanimljivo je da se realno zatvorena polja mogu opisati upravo kao ona uređena polja u kojima polinomi imaju neke osobine neprekidnih funkcija. To kazuje sledeće tvrđenje.

Teorema 2. Realno zatvorena polja su upravo ona formalno realna polja koja se mogu urediti tako da za svaki $p\in F[x]$ važi:

ako za neke $a, b\in F$ važi $p(a)<0<p(b)$, onda polinom $p(x)$ ima koren u intervalu $(a, b)_F$.

Realno zatvorena polja imaju sličnu ulogu u klasi formalno realnih polja, kao što algebarski zatvorena polja imaju u klasi svih polja. O tome govori sledeća teorema.

Teorema 3. Svako uređeno polje F ima realno zatvorenje $\overline{F}$, tj. takvo polje $\overline{F}$ da važi:

1° $\overline{F}$ je algebarsko proširenje polja F (što znači da je svaki $a\in\overline{F}$ koren nekog polinoma nad F);

2° $\overline{F}$ je realno zatvoreno polje.

Odnos između realno zatvorenih polja i algebarski zatvorenih polja iskazan je ovom teoremom[1].

Teorema 4. Ako je F realno zatvoreno polje, onda je $F[\sqrt{-1}]$ algebarski zatvoreno polje.

U vezi sa prethodnom teoremom setimo se da za polje kompleksnih brojeva C važi $C=R[\sqrt{-1}]$.

Najzad, sledeća činjenica je od interesa i za sledeći paragraf.

Teorema 5. Neka je F realno zatvoreno polje i neka racionalna funkcija $f\in F(x)$ nije suma kvadrata nekih drugih racionalnih funkcija. Tada postoji uređeno polje $(F(x), \leqslant)$ u kojem je $f<0$.

Naravno, u prethodnoj teoremi f nije pozitivno definitna u $(F(x), \leqslant)$, jer je $f(a)<0$, gde je a polinom x.

Dokaz prethodne teoreme izvodi se tako što se najpre izabere skup $P\subseteq F(x)$, takav da P bude skup nenegativnih elemenata u budućem uređenju. Za to je dovoljno da P zadovoljava sledeće uslove:

1° $g^2\in P$ za $g\in F(x)$,

2° skup P je zatvoren za operacije $+$ i $\cdot$,

3° $-f\in P$,

4° $-1\notin P$,

5° za svaki $g\in F(x)$ važi $g\in P$ ili $-g\in P$.

Konstrukcija skupa P izvodi se ovako. Neka je P_0 najmanji podskup skupa $F(x)$ koji zadovoljava uslove 1°—3°. Otuda lako sledi da $-1\notin P_0$. Koristeći aksiomu izbora nalazi se maksimalan skup P koji zadovoljava uslove 1°—4°. Naime, uoči se kolekcija S svih podskupova skupa $F(x)$ koji zadovoljavaju uslove 1°—4°. Familija S je neprazna jer $P_0\in S$. Tada, prema Zornovoj lemi, sledi da S ima maksimalan element P (u odnosu na inkluziju $\subseteq$). Onda se jednostavno proverava da P pored uslova 1°—4° takođe zadovoljava i uslov 5°.

Spomenimo da se slična konstrukcija izvodi i u drugim situacijama, na primer kod uređenih Abelovih grupa.

---

[1] Polje K je algebarski zatvoreno ukoliko svaki polinom nad K stepena $\geqslant 1$ ima koren u K. Glavni primeri algebarski zatvorenih polja su polje kompleksnih brojeva i polje algebarskih brojeva.

Logika i 17 Hp

Dok su Tarski i Gödel uveli matematiku u logiku, za Abrahama Robinsona i A. Maljceva može se reći da su uveli logiku u matematiku. Jer, danas verovatno najznačajnije primene logike u drugim matematičkim oblastima, nestandardna analiza i modelsko-teoretska algebra, potiču od A. Robinsona. A. Maljcev je dao prvi priloge takve vrste u algebri još 1936. Zanimljivo je da se A. Robinson bavio primenjenom matematikom u aeronautici pre i za vreme drugog svetskog rata. Doktorirao je 1949. iz matematičke logike.

Robinsonovo rešenje 17 Hp metodima matematičke logike, preciznije metodima teorije modela, predstavlja vrlo značajan prilog modelsko-teoretskoj algebri.

U osnovi, Robinsonovo rešenje se zasniva na metodu eliminacija kvantora i pojmu modelske potpunosti. Modelska potpunost predstavlja modelsko-teoretski pandan eliminaciji kvantora, a osim toga, ovaj pojam se može shvatiti kao jedan princip prenosa, što je za primene u algebri od prevashodnog značaja.

Definicija. Teorija T u predikatskom računu prvog reda dopušta eliminaciju kvantora ukoliko za svaku formulu φ teorije T postoji formula ψ bez kvantora u jeziku teorije T tako da važi:

$$T \vdash \varphi \leftrightarrow \psi.$$

Logičku osnovu modelsko-teoretskog rešenja 17 Hp čini sledeće tvrđenje.

Teorema 6. (A. Tarski, 1949) Teorija uređenih realno zatvorenih polja dopušta eliminaciju kvantora.

Teorije koje dopuštaju eliminaciju kvantora imaju ovu, vrlo zanimljivu osobinu:

(*) Svaka teorija koja dopušta eliminaciju kvantora je modelski potpuna.

Da bismo bliže objasnili ovaj pojam, pretpostavimo da je T proizvoljna teorija prvog reda jezika L. Dalje, neka su A, B, takođe proizvoljne operacijsko-relacijske strukture (modeli) istog jezika. Model A je *elementaran podmodel* modela B, odnosno B je elementarno proširenje modela A, ukoliko su ispunjeni sledeći uslovi:

1° A je podmodel modela B;

2° za svaku formulu $\varphi\vec{x}$ jezika L i sve $\vec{a}\in A$ važi

$$A\models\varphi(\vec{a}) \quad \text{akko} \quad B\models\varphi(\vec{a}).$$

Da je A podmodel modela B zapisujemo ovako: $A\prec B$.

Definicija. Teorija T je *modelski potpuna* akko za proizvoljna dva modela A, B teorije T važi: ako je A podmodel modela B, onda je A elementaran podmodel modela B.

Sa ovom definicijom modelske potpunosti nije teško dokazati tvrđenje (*). Zaista, pretpostavimo da teorija T dopušta eliminaciju kvantora i neka su A, B modeli teorije T. Dalje, pretpostavimo da je A podmodel modela B i neka je $\varphi(\vec{x})$ proizvoljna formula jezika teorije T. Najzad, uzmimo da je

$$A\models\varphi(\vec{a}), \quad \vec{a}\in A.$$

Kako teorija T dopušta eliminaciju kvantora, to postoji formula ψ bez kvantora, takođe, u jeziku teorije T, tako da važi $T\vdash\varphi\leftrightarrow\psi$. S obzirom da je A model teorije T, to je onda

$$A\models\forall x(\varphi(x)\leftrightarrow\psi(x)),$$

odakle sledi $A\models\psi(\vec{a})$. Po pretpostavci A je podmodel modela B i $\psi(\vec{a})$ je formula bez kvantora, odakle sledi $B\models\psi(\vec{a})$.

Sada, slično kao u prethodnom razmatranju, nalazimo

$$B\models\forall\vec{x}(\varphi(\vec{x})\leftrightarrow\psi(\vec{x})),$$

odakle $B\models\varphi(\vec{a})$.

Dakle, dokazali smo da $A\models\varphi(\vec{a})$ povlači $B\models\varphi(\vec{a})$ za bilo koju formulu $\varphi(\vec{x})$ i $\vec{a}\in A$. Na sličan način se dokazuje da važi implikacija u drugom smeru.

Uočićemo da je do sada simbol $f(\vec{x})$ imao dvostruku ulogu. Naime, $f\in F(\vec{x})$ i $f<0$ znači „da je element f u polju $F(\vec{x})$ manji od nule“. Osim toga, $F\subseteq F(\vec{x})$, pa koeficijenti racionalne funkcije f leže takođe u polju $F(\vec{x})$. Stoga je $f(x)$ racionalna forma i nad poljem $F(\vec{x})$. Ako je;

$$f(x)=\sum_{\alpha}a_{\alpha}x_1^{\alpha_1}\ldots x_n^{\alpha_n}$$

onda se ova racionalna funkcija nad $F(\vec{x})$ radi razlikovanja od elementa f može beležiti ovako:

$$f(\vec{X}) = \sum_{\alpha} a_{\alpha} x_1^{\alpha_1} \ldots x_n^{\alpha_n}.$$

Dakle, domen promenljivih $x_1, \ldots x_n$ je F, dok je domen za promenljive $X_1, \ldots, X_n$ skup racionalnih izraza $F(\vec{x})$. Primetićemo da su $x_1, \ldots, x_n$ onda elementi skupa $F(\vec{x})$, dok to $X_1, \ldots, X_n$ nisu. Naravno, uvođenje novih promenljivih $X_1, \ldots, X_n$ nije obavezno; iz konteksta je jasno koje se značenje simbola $f(\vec{x})$ podrazumeva.

Rešenje 17 Hp za polje realnih brojeva R. (A. Robinson, 1955)

Neka je $f \in R(\vec{x})$ i pretpostavimo da f nije suma kvadrata; tada, prema Teoremi 5, postoji uređenje polja racionalnih funkcija $R(\vec{x})$ tako da je u tom polju $f < 0$. Neka je $(\bar{R}(\vec{x}), \leqslant)$ realno algebarsko zatvorenje polja $(R(\vec{x}), \leqslant)$; ono postoji prema Teoremi 3. Tada, takođe, $f < 0$ i u ovom polju, odakle

$$(\bar{R}(\vec{x}), \leqslant) \models \exists \vec{x} f(\vec{x}) < 0. \qquad (1)$$

Ovde smo koristili činjenicu da svako realno zatvoreno polje ima *jedinstveno* raširenje do uređenog polja, pa otuda sledi da je $(R, \leqslant)$ podmodel modela $(\bar{R}(\vec{x}), \leqslant)$.

Označimo sa T teoriju uređenih realno zatvorenih polja. Prema teoremi Tarskog teorija T dopušta eliminaciju kvantora; dakle prema (*), teorija T je takođe modelski potpuna. Prema ovoj osobini teorije T i (1) imamo:

$$(R, \leqslant) \models \exists \vec{x} f(x) < 0,$$

tj. racionalna funkcija f nije pozitivno definitna.

DODATAK: ELIMINACIJA KVANTORA

U ovom dodatku želimo da ostvarimo dva cilja. Prvi se odnosi na jedan postupak eliminacije kvantora blizak eliminaciji kvantora za teoriju uređenih realno zatvorenih polja koji smo koristili u ovom poglavlju. Naime, dokazaćemo da teorija algebarski zatvorenih polja dopušta eliminaciju kvantora. Dokaz ove teoreme je nešto jednostavniji nego što je to slučaj sa realno zatvorenim poljima, pa je to razlog što smo ovaj dokaz izabrali.

U drugom delu razmatraćemo čuveni Hilbertov *Nullstellensatz*, jednu od osnovnih teorema algebarske geometrije. I ovaj Hilbertov rezultat može se dobiti logičkim metodama, kao što je to pokazao A. Robinson. Zanimljivo je da su prvi i drugi deo dodatka u neposrednoj vezi, jer eliminacija kvantora za teoriju algebarski zatvorenih polja predstavlja glavnu poentu u ovom logičkom dokazu Hilbertovog *Nullstellensatza*. Čitalac može ovde naći, takođe, i nekoliko teorema i metoda koje se koriste u modelsko-teoretskoj algebri, disciplini koja je nastala spajanjem ideja i metoda algebre i logike.

§ 1. Eliminacija kvantora za teoriju algebarski zatvorenih polja. Aksiome teorije algebarski zatvorenih polja čine aksiome polja i ovaj niz aksioma:

$$\exists x (y_0 + y_1 x + \cdots + y_n x^n = 0) \vee y_n = 0, \quad n = 1, 2, \ldots$$

Prema tome, ovim aksiomama se iskazuje da svaki polinom stepena $\geqslant 1$ ima koren. Označimo sa T teoriju polja a sa T^* teoriju algebarski zatvorenih polja. Tada su polje kompleksnih brojeva C i polje algebarskih brojeva primeri modela teorije T^*.

Primeri eliminacije kvantora za teoriju T^* poznati su odavno u klasičnoj algebri. Jedan od najpoznatijih, kojim ćemo se i ovde koristiti je teorema o rezolventi.

Definicija. Neka su: $a(x) = \sum_{i \leqslant m} a_i x^i$, $b(x) = \sum_{j \leqslant n} b_j x^j$ kompleksni polinomi. *Rezolventa polinoma* a i b je determinanta

$$\operatorname{Res}(a, b) = \begin{vmatrix} a_0 & a_1 & \cdots & a_m & 0 & \cdots & 0 \\ 0 & a_0 & a_1 & \cdots & a_m & & 0 \\ & & & \vdots & & & \\ 0 & \cdots & & a_0 & a_1 & \cdots & a_m \\ b_0 & b_1 & \cdots & b_n & 0 & \cdots & 0 \\ 0 & b_0 & b_1 & \cdots & b_n & \cdots & 0 \\ & & & \vdots & & & \\ 0 & \cdots & & b_0 & b_1 & \cdots & b_n \end{vmatrix}$$

Dakle $\operatorname{Res}(a, b)$ je determinanta reda $m+n$, gde su m i n redom stepeni polinoma a i b.

Primer. $$\operatorname{Res}(2x+1,\ x^2+x-1) = \begin{vmatrix} 2 & 1 & 0 \\ 0 & 2 & 1 \\ 1 & 1 & -1 \end{vmatrix} = -5.$$

Glavno svojstvo rezolvente iskazano je ovim tvrđenjem:

Teorema 7. Kompleksni polinomi a, b imaju zajednički koren u polju kompleksnih brojeva C akko $\mathrm{Res}(a, b) = 0$.

Drugačije rečeno, ako su a i b polinomi redom stepena m i n, onda:

$$(1) \qquad \exists x\,(a(x) = 0 \wedge b(x) = 0) \leftrightarrow \mathrm{Res}(a, b) = 0.$$

Rezolventa dvaju polinoma može se definisati na isti način u bilo kojem polju, odnosno u okviru teorije T. Tada Teorema 2 ostaje na snazi u T^*, odnosno ona je teorema teorije T^*. Dokaz je potpuno isti kao u slučaju polja kompleksnih brojeva.

Neka su $a(x) = y_m + y_{m-1}x + \cdots + y_0 x^m$, $b(x) = z_n + z_{n-1}x + \cdots + z_0 x^n$ polinomi, gde su $y_0, \ldots, y_m, z_0, \ldots, z_n$ promenljive. Uvedimo ove polinome:

$$a_0(x) = a(x),\ a_1(x) = y_m + \cdots + y_{m-1}x^{m-1},\ a_m(x) = y_m,$$

i na sličan način polinome $b_i(x)$. Tada, prema Teoremi 7, imamo

$$(2) \qquad \exists x(a(x) = 0 \wedge b(x) = 0) \leftrightarrow$$

$$\bigvee_{\substack{i<m\\ j<n}} (sta_i = m - i \wedge stb_j = n - j \wedge \mathrm{Res}(a_i, b_j) = 0) \vee \bigwedge_{i,\,j} (y_i = 0 \wedge z_j = 0) \leftrightarrow$$

$$\bigvee_{\substack{i<m\\ j<n}} (y_0 = 0 \wedge \ldots \wedge y_{i-1} = 0 \wedge y_i \neq 0 \wedge z_0 = 0 \wedge \ldots \wedge z_{j-1} = 0 \wedge z_j \neq 0$$

$$\wedge\ \mathrm{Res}(a_i, b_j) = 0) \vee \bigwedge_{i,\,j} (y_i = 0 \wedge z_j = 0).$$

Razmotrimo još dva jednostavna slučaja eliminacije kvantora. S obzirom da je svako algebarski zatvoreno polje beskonačno (koreni polinoma $(x - x_0)(x - x_1) \ldots (x - x_n) + 1$ su različiti od $x_0, \ldots, x_n$) za polinom $a(x) = \sum_i y_i x^i$ imamo

$$(3) \qquad \exists x\,(a(x) \neq 0) \leftrightarrow y_0 \neq 0 \vee \cdots \vee y_n \neq 0.$$

Sada ćemo pokazati da se eliminacija kvantora u formuli

$$(4) \qquad \exists x\,(a(x) = 0 \wedge b(x) \neq 0)$$

svodi na slučaj (2). Najpre primetimo da je $b(x) \neq 0 \leftrightarrow \exists y\ yb(x) - 1 = 0$, i da se y javlja kao faktor u svakom članu polinoma $yb(x) - 1$, osim u slobodnom članu. Ako promenljivu y izaberemo tako da se ne javlja u formuli $a(x) = 0 \wedge b(x) = 0$, onda je

$$\exists x\,(a(x) = 0 \wedge b(x) \neq 0) \leftrightarrow \exists y \exists x\,(a(x) = 0 \wedge yb(x) - 1 = 0).$$

Prema (2) formula $\exists x\,(a(x) = 0 \wedge yb(x) - 1 = 0)$ ekvivalentna je disjunkciji $\varphi_1 \vee \ldots \vee \varphi_k$ koja ne sadrži kvantore, i svaka formula φ_j za $j < k$ je vida (za odgovarajući polinom b_j')

$$y_0 = 0 \wedge \ldots \wedge y_{i-1} = 0 \wedge y_i \neq 0 \wedge z_0 y = 0 \wedge \ldots \wedge z_{j-1} y = 0 \wedge z_j y \neq 0 \wedge$$
$$\operatorname{Res}(a_i,\ b_j') = 0.$$

Kako je $\exists x \bigvee_i \varphi_i \leftrightarrow \bigvee_i \exists x \varphi_i$ valjana formula, to je dovoljno izvesti eliminaciju kvantora u formuli $\exists y \varphi_i$. Lako se možemo uveriti da je za to dovoljno eliminisati egzistencijalni kvantor u formuli

$$\exists y\,(y \neq 0 \wedge \operatorname{Res}(a_i, b_j') = 0)$$

odnosno u formuli vida

$$\exists y\,(y \neq 0 \wedge m(y) = 0), \quad m(y) \text{ je polinom.}$$

Neka je $m(y) = m_0 + m_1 y + \ldots m_k y^k$. Tada se neposredno proverava da je

$$\exists y\,(y \neq 0 \wedge m(y) = 0) \leftrightarrow \bigvee_{i<j} m_i \neq 0 \wedge m_j \neq 0).$$

Sada prelazimo na opšti slučaj eliminacije kvantora u teoriji T^*. Neka je φ bilo koja formula teorije T. Prema teoremi o preneksnoj normalnoj formi (videti prethodno poglavlje) formula φ ekvivalentna je formuli u preneksnoj normalnoj formi

$$Q_1 x_1 \ldots Q_n x_n \psi$$

gde je ψ formula bez kvantora. Koristeći valjanu formulu $\forall x \alpha(x) \leftrightarrow \leftrightarrow \neg \exists x \neg \alpha(x)$, kao i to da nas eliminacija kvantora u formuli $\neg \varphi$ vodi do istog rezultata za formulu φ, možemo pretpostaviti da je Q_n egzistencijalni kvantor.

Dalje, prema teoremi o disjunktivnoj normalnoj formi postoje formule $\psi_1, \ldots, \psi_k$ tako da je

$$\psi \leftrightarrow \psi_1 \vee \ldots \vee \psi_k$$

i svaka formula ψ_i je konjunkcija formula oblika $u=0$, $v\neq 0$. Pri tome smo koristili činjenicu da je svaki term jezika teorije polja jednak nekom polinomu. Kako je $v_1\neq 0\wedge\ldots\wedge v_n\neq 0\leftrightarrow v_1 v_2\ldots v_n\neq 0$, to se može uzeti da je svaki disjunkt ψ_i vida

$$a_1=0\wedge\ldots\wedge a_m=0\wedge b\neq 0.$$

S obzirom na valjanu formulu $\exists x\bigvee_i\psi_i\leftrightarrow\bigvee_i\exists x\psi_i$, izlazi da je dovoljno da se navede postupak eliminacije kvantora za formule oblika

$$\exists x(a_1=0\wedge\ldots\wedge a_m=0\wedge b\neq 0). \tag{5}$$

Neka je $\lambda_i x^{n_i}$ član najvišeg stepena polinoma $a_i(x)$, $i=1,\ldots,m$, i neka je $n_\theta=m+\sum_i n_i$. Odredićemo formule θ_1 i θ_2 vida (5) tako da je $\theta\leftrightarrow\theta_2\vee\theta_2$ i $n_{\theta_1}, n_{\theta_2}<n_\theta$ ukoliko je $n_\theta>1$ i $m\geqslant 2$.

Najpre pretpostavimo da je $n_1=0$. Onda je

$$\theta\leftrightarrow a_1=0\wedge\exists x(a_2=0\wedge\ldots\wedge a_m=0\wedge b\neq 0)$$

pa zato pretpostavimo da je $n_1\neq 0$ i $n>1$. Možemo takođe uzeti da je $n_2\leqslant n_1$. Neka je $a_1'=\lambda_2 a_1-\lambda_1 x^{n_1-n_2}a_2$, $a_2'=a_2-\lambda_2 x^{n_2}$. Tada je

$$\theta\leftrightarrow(\lambda_2=0\wedge\exists x(a_1=0\wedge a_2'=0\wedge\ldots\wedge a_m=0\wedge b\neq 0)\vee$$

$$\lambda_2\neq 0\wedge\exists x(a_1'=0\wedge a_2=0\wedge\ldots\wedge a_m=0\wedge b\neq 0).$$

Sada je očigledno da za formulu θ_1 možemo izabrati prvi disjunkt, a za formulu θ_2 drugi disjunkt desne strane ove ekvivalencije. Na ovaj način je definisana rekurzivna procedura za eliminisanje kvantora kojom se dolazi do slučajeva (2) i (3), a kako se ovi rešavaju to smo već opisali.

Odavde odmah možemo izvesti nekoliko posledica koje se odnose na teoriju algebarski zatvorenih polja, T^*:

1° Ako je φ bilo koja rečenica teorije polja, to ni formula ψ bez kvantora, a za koju je $T^*\vdash\varphi\leftrightarrow\psi$, nema slobodnih promenljivih. S obzirom da je jezik teorije polja $\{+,\circ,0,1\}$, to se lako uveravamo da se za formulu ψ može uzeti formula oblika $n=0$, gde je $n=1+\cdots+1$ (n puta). Ako su $p_1,\ldots,p_k$ svi prosti faktori broja n, onda je

$$T^*\vdash n=0\leftrightarrow p_1=0\vee\ldots\vee p_k=0.$$

Odavde proizilazi da su sva kompletna proširenja teorije T^* teorije oblika $T_p = T^* \cup \{p = 0\}$ (p je prost broj), tj. teorije algebarski zatvorenih polja karakteristike p.

2° S obzirom da se za sve formule $n = 0$, $n \neq 0$ očigledno može odlučiti da li su one teoreme teorije T^*, to se isto može i za svaku rečenicu teorije T^*. Dakle, teorija algebarski zatvorenih polja je odlučiva.

Zanimljivo je da teorija polja nije odlučiva.

§ 2. Hilbertov Nullstellensatz. U prethodnom delu videli smo da su teorije koje dopuštaju eliminaciju kvantora modelski potpune. Otuda imamo:

Princip prenosa za algebarski zatvorena polja. Neka su F i K algebarski zatvorena polja i neka je $F \subseteq K$. Dalje, neka su $f_1, \ldots, f_k \in F[x_1, \ldots, x_n]$. Ako sistem jednačina:

$$f_1 = 0, \quad f_2 = 0, \ldots, f_k = 0, \tag{1}$$

ima rešenja u K, onda on ima rešenja i u F.

Ova činjenica može se iskazati i u formalizmu algebarske geometrije. U tom novom obliku glavnu ulogu ima pojam algebarskog varijeteta, pa stoga dajemo njegovu definiciju.

Varijetet nad poljem F generisan polinomima $f_1, \ldots, f_k$ je skup svih rešenja sistema jednačina (1).

Taj varijetet označavamo sa $V_F(f_1, \ldots, f_k)$. Dakle, princip prenosa za algebarski zatvorena polja u ovom novom formalizmu izgleda:

ako je $F \subseteq K$, onda $V_K(f_1, \ldots, f_k) \neq \varnothing \Rightarrow V_F(f_1, \ldots, f_k) \neq \varnothing$.

U sledećih nekoliko redova podsetićemo se na definiciju ideala prstena. Doduše, Hilbertov *Nullstellensatz* može se ispričati i bez tog pojma, ali on će nam biti potreban u njegovom dokazu. Pored toga, Hilbertov *Nullstellensatz* ima zanimljivu posledicu koja se odnosi na osobine algebarskih varijeteta.

Definicija. Ideal prstena $(P, +, \cdot, 0, 1)$ je svaki skup $I \subseteq P$ za koji važi:

1° $(I, +, 0)$ je podgrupa grupe $(P, +, 0)$.

2° $\{ix : i \in I, x \in P\} \subseteq I$, $\{xi : i \in I, x \in P\} \subseteq I$, tj. $IP \subseteq I$, $PI \subseteq I$.

Na primer, skup parnih brojeva je ideal prstena celih brojeva. Opštije, za svaki prirodan broj m, $mZ=\{mx : x\in Z\}$ je ideal prstena celih brojeva Z.

Ako su $a_1, \ldots, a_n$ elementi prstena P, onda postoji najmanji ideal tog prstena koji sadrži ove elemente, to je

$$\{x_1 a_1 + \cdots + x_n a_n : x_1, \ldots, x_n \in P\}.$$

Ovaj ideal označavaćemo sa $I(a_1, \ldots, a_n)$. Slično, ako je S bilo koji podskup prstena P, onda ideal generisan skupom S, u oznaci $I(S)$, je najmanji ideal koji sadrži skup S. Lako se možemo uveriti da je

$$I(S)=\{x_1 s_1 + \cdots + x_n s_n : s_1, \ldots, s_n \in S,\ x_1, \ldots, x_n \in P,\ n\in N\}.$$

U proučavanju algebarskih podskupova stepena F^n nekog polja F glavnu ulogu ima prsten polinoma $F[x_1, \ldots, x_n]$, kao i njegovi ideali. Na primer, možemo pokušati da uopštimo pojam algebarskog varijeteta. Ako je S bilo koji podskup prstena $F[x_1, \ldots, x_n]$ možemo uzeti da je $V_F(S)$ skup svih korena svih polinoma iz S, tj.

$$V_F(S)=\{(x_1, \ldots, x_n)\in F^n : (\forall f\in S)\ f(x_1, \ldots, x_n)=0\}.$$

Lako se možemo uveriti da je

$$V_F(S)=V_F(I(S)).$$

Ali na osnovu Hilbertove teoreme o bazi možemo zaključiti da je dovoljno proučavati konačno generisane varijetete. Zaista, prema ovoj teoremi $I(S)$ je konačno generisan, što znači da je za neke polinome $f_1, \ldots, f_k$ ispunjena jednakost $I(S)=I(f_1, \ldots, f_k)$, odakle

$$V_F(S)=V_F(f_1, \ldots, f_k).$$

Sada navodimo fundamentalnu teoremu algebarske geometrije *Hilbertov Nullstellensatz*. Neka su $f, g_1, \ldots, g_k$ polinomi nad poljem F sa promenljivama $x_1, \ldots, x_n$. Pretpostavimo da u nekom algebarski zatvorenom proširenju K polja F važi:

sva rešenja sistema $g_1=0, \ldots, g_k=0$ su i rešenja jednačine $f=0$, tj.

$$V_K(g_1, \ldots, g_k)\subseteq V_K(f).$$

Tada za neki prirodan broj m polinom f^m je linearna kombinacija polinoma $g_1, \ldots, g_k$, tj. postoje polinomi $h_1, \ldots, h_k \in F[x_1, \ldots, x_n]$ takvi da je $f^m = h_1 g_1 + \cdots + h_k g_k$, odnosno $f^m \in I(g_1, \ldots, g_k)$.

Za princip prenosa može se reći da je algebarsko-logičkog karaktera. Osim toga, u dokazu Hilbertovog *Nullstdllensatza*, isto tako, važnu ulogu ima ova fundamentalna teorema teorije polja.

Teorema 8. Svako polje je sadržano u nekom algebarski zatvorenom polju.

Neki slučajevi ove teoreme su nam dobro poznati, bar kad je reč o brojevnim poljima. Naime, svako brojevno polje je sadržano u algebarski zatvorenom polju: to je polje kompleksnih brojeva. Ali ovo tvrđenje je već manje očigledno ukoliko je reč o nekim drugim poljima, na primer konačnom polju $Z_p = (Z_p, +_p, \cdot_p, 0, 1)$, $Z_p = \{0, 1, \ldots, p-1\}$, gde je p prost broj, a $+_p$, $\cdot_p$ aritmetičke operacije po modulu p.

Navodimo skicu dokaza Teoreme 8 u kojem se na jednom mestu koriste metodi matematičke logike, tačnije teorija modela. Ali najpre moramo izvesti još neke osobine ideala u prstenima. Od sada pa do kraja, pretpostavljamo da prsteni o kojima govorimo sadrže jedinicu. Zapazićemo da prsten polinoma $F[x_1, \ldots, x_n]$ nad poljem F sadrži jedinicu, to je konstantni polinom 1. Za ideal I prstena P kažemo da je *pravi* ako je $I \neq P$. Lako se možemo uveriti da je I pravi ideal akko $1 \notin I$.

Definicija. Pravi ideal I prstena P je *maksimalan* akko I nije sadržan ni u jednom širem pravom idealu prstena P.

Na primer ideal pZ je maksimalan u prstenu celih brojeva Z.

Teorema 9. Svaki pravi ideal prstena P sadržan je u nekom maksimalnom idealu istog prstena.

Dokaz. Neka je $\mathcal{S}$ kolekcija svih pravih ideala prstena P koji sadrže ideal I. Ako je $\mathcal{L}$ lanac ideala iz $\mathcal{S}$ u odnosu na $\subseteq$, onda je $\cup \mathcal{L}$ takođe ideal koji pripada $\mathcal{S}$ i koji je širi od svakog člana iz $\mathcal{L}$. Otuda prema Zornovoj lemi $\mathcal{S}$ ima maksimalan član J (u odnosu na $\subseteq$). Tada je J maksimalan ideal prstena P koji sadrži I. ∎

Ako je P prsten i I neki njegov ideal, tada se može konstruisati nov prsten iz ova dva objekta. Članovi domena tog novog

prstena su razredi $I+x=\{i+x: i\in I\}$, dok su operacije među razredima definisane ovako:

$$(I+x)+(I+y)=I+(x+y), \quad (I+x)(I+y)=I+xy.$$

Nije teško pokazati da su definicije ovih operacija korektne i da je $P/I=(P/I, +, \circ, 0, 1)$ takođe prsten, gde je P/I skup svih razreda $I+x$, $x\in P$. Ova nova algebarska struktura naziva se *količničkim prstenom*. Preslikavanje $\psi: P\to P/I$ koje svakom $x\in P$ dodeljuje njegov razred $I+x$ je homomorfizam ovih prstena, tj. za sve $x, y\in P$ važi

$$\psi(x+y)=\psi(x)+\psi(y), \quad \psi(xy)=\psi(x)\psi(y).$$

Dakle P/I je homomorfna slika prstena P. Homomorfizam ψ naziva se *kanonskim*.

Zanimljivu osobinu imaju maksimalni ideali prstena:

Teorema 10. Neka je P komutativan prsten i neka je J maksimalan ideal tog prstena. Tada je P/J polje.

Dokaz. Primetimo da je $\mathbf{O}$ u P/J u stvari skup J. Zaista, $\mathbf{O}=J+0=J$. Neka je $a\in P$ i $J+a\neq 0$. To znači $a\notin J$, pa kako je J maksimalan ideal, ideal I generisan skupom $J\cup\{a\}$ je nepravi, tj. $I=P$, pa je otuda $1\in I$. Takođe, lako se proverava da je $\mathbf{I}=\{i+xa: x\in P, i\in I\}$. Kako je $1\in I$, to za neke $b\in P$, $i\in J$ važi $1=i+ba$. Ako je $\psi: P\to P/I$ kanonski homomorfizam, onda imamo:

$$I=\psi(1)=\psi(i+ba)=\psi(i)+\psi(b)\psi(a)=(I+b)(I+a),$$

jer je $\psi(i)=0$. Dakle, $I+b$ je inverzni element za $I+a$ u odnosu na množenje u prstenu P/I. ■

Ideja dokaza Teoreme 8 sastoji se u tome da se osnovno polje postepeno proširuje tako da u novodobivenom polju neki polinomi imaju koren. Proširivanje se vrši sve dok ne postanu rešive sve algebarske jednačine $f=0$, $stf\geqslant 1$. Najpre ćemo rešiti najjednostavniji slučaj.

Lema. Neka je F polje i $p\in F[x]$, $stp\geqslant 1$. Tada postoji polje K koje proširuje F i u kojem p ima koren.

Dokaz. Neka je J ideal prstena $F[x]$ koji je generisan polinomom p. Prema Teoremi 9 postoji maksimalan ideal I koji sadrži J, dok je prema Teoremi 10 P/I polje. Neka je $\psi: F[x]\to F[x]/I$ kanonski

homomorfizam. Ako je $a \in F$, onda je a istovremeno konstantni polinom čija je vrednost a. Ako su $a, b \in F$ dve različite konstante onda $\psi(a) \neq \psi(b)$, jer bi inače imali $\psi(a-b)=0$, tj. $a-b \in I$, što znači da p deli $a-b$, a to je moguće jedino ako je $a=b$, jer je $stp \geqslant 1$. Otuda se polje F *utapa* u $F[x]/I$, pa se može izvršiti identifikacija elementa a i $I+a$, tj. uzećemo da je $\psi(a)=a$ za sve $a \in F$.

Kako je $p \in I$, onda je $\psi(p)=0$, dok je za $a \in F$ $\psi(a)=a$, pa za $p(x)=\sum_i a_i x^i$ imamo:

$$\mathbf{O}=\psi(p)=\psi\left(\sum_i a_i x^i\right)=\sum_i \psi(a_i)\,\psi(x)^i=\sum_i a_i (I+x)=p(I+x)$$

tj. $I+x$ je koren polinoma p u polju $F[x]/I$. ■

Koristeći ovu lemu lako može da se dokaže ovo tvrđenje:

Tvrđenje. Ako je F polje i $p_1, \ldots, p_n \in F[x]$. $stp_1, \ldots, stp_n \geqslant 1$, tada postoji polje K koje sadrži polje F i u kojem svaki od ovih polinoma ima koren.

Zaista, prema Lemi postoje polja $K_1, \ldots, K_n$ tako da je

$$F \subseteq K_1 \subseteq K_2 \subseteq \ldots \subseteq K_n$$

i svaki polinom p_i ima koren u polju K_i. Tada svaki od polinoma $p_1, \ldots, p_n$ ima koren u polju K_n.

Dokaz Teoreme 8 može se izvesti na više načina. U klasičnim, „čisto algebarskim" dokazima koristi se neka eksplicitna forma aksiome izbora: oni uglavnom predstavljaju infinitarno raširenje rasuđivanja korišćenog u dokazu prethodnog tvrđenja. Ovom prilikom koristićemo se jednom teoremom iz matematičke logike, koja je svakako najviše korišćena u primenama logike u algebri. To je:

Teorema kompaktnosti. Ako je T skup rečenica[1] nekog jezika prvog reda L, sa osobinom da svaki konačan podskup od T ima model, onda postoji model A teorije T (tj. A zadovoljava svaku rečenicu iz T):

---

[1] *Rečenica* je svaka zatvorena formula, tj. formula koja nema slobodnih promenljivih. Skup T ćemo zvati *teorijom*, a elemente skupa T *aksiomama* teorije T.

Dokaz Teoreme 8. Neka je $F=(\mathrm{F}, +, \cdot, 0, 1)$ bilo koje polje. Konstruisaćemo teoriju T koja će zadovoljavati ove uslove:

1° svaki model teorije T je polje;

2° svaki model teorije T sadrži izomorfnu kopiju polja F; dakle, bez gubljenja opštosti možemo pretpostaviti da svaki model teorije T sadrži kao potpolje polje F;

3° ako je K model teorije T, tada svaki polinom stepena $\geqslant 1$ sa koeficijentima u polju F ima koren u K.

S obzirom na ove uslove, izgled aksioma teorije T je u potpunosti određen. Naime, pretpostavićemo da se T sastoji iz ove tri grupe aksioma:

1′. sve aksiome polja;

2′. u ovoj grupi se nalaze rečenice koje opisuju strukturu polja F; otuda jezik teorije polja $\{+, \cdot, 0,1\}$ širimo novim elementima, naime simbolima konstanti $\underline{a}$ (simbol konstante $\underline{a}$ često nazivamo *imenom* elementa a) za svaki $a\in F$. Kada se ovi simboli interpretiraju u polju-modelu teorije T, onda upravo te konstante čine domen izomorfne kopije polja F. Aksiome koje opisuju strukturu polja F su jednakosti i različitosti vida

$$\underline{a}+\underline{b}=\underline{c}, \quad \underline{a}\cdot\underline{b}=\underline{c}, \quad \underline{a}\neq\underline{b}, \qquad a, b\in F$$

kad god je ispunjeno

$$a+b=c, \qquad a\cdot b=c, \qquad a\neq b$$

(napomenimo da se aksiome ovog tipa nazivaju *dijagramom* modela);

3′. u ovim aksiomama dalje se širi jezik $\{+, \cdot, 0,1\}\cup\{\underline{a}: a\in F\}$ novim simbolima konstanata; za svaki polinom $p\in F[x]$, $stp\geqslant 1$, uvodi se nov simbol konstante c_p; taj simbol konstante u interpretaciji biće koren polinoma p; otuda su i aksiome ove grupe formule vida

$$p(c_p)=0.$$

Dakle, jezik teorije T definitivno izgleda ovako:

$$\{+, \cdot, 0,1\}\cup\{\underline{a}: a\in F\}\cup C$$

gde je $C=\{c_p: p\in F[x]\}$, $stp\geqslant 1$. Ovim je teorija u potpunosti određena. Ako je $S\subseteq T$ konačan podskup, onda S ima model. Zaista,

ako su $p(c_{p_1}) = 0, \ldots, p(c_{p_n}) = 0$ aksiome grupe 3′ koje pripadaju skupu S, onda model K za S postoji prema *Tvrđenju*. Simboli konstanata $c_{p_1}, \ldots, c_{p_n}$ interpretiraju se redom upravo kao koreni polinoma $p_1, \ldots, p_n$ u polju K. Tada, prema teoremi kompaktnosti teorija T ima model; neka je to

$$K = (\mathrm{K}, +, \cdot, 0, 1, b_a, d_p)\, a \in F,\ c_p \in C.$$

Dakle, model K pored operacija $+$ i $\cdot$ ima „mnogo“ konstanti, to su b_a, d_p. Ove konstante su redom interpretacije simbola $\underline{a}$, c_p. S obzirom na prvu grupu aksioma struktura (K, $+$, $\cdot$, 0, 1) je polje. S obzirom na drugu grupu aksioma teorije T, polje F se utapa u polje K; utapanje je preslikavanje $\psi : a \mapsto b_a$. Na primer, $u \neq v \Rightarrow \psi(u) \neq \psi(v)$, jer ako je $u \neq v$ onda je $\underline{u} \neq \underline{v}$ aksioma teorije T, pa kako je K model teorije T ista rečenica važi u K; dakle za interpretacije simbola $\underline{u}$, $\underline{v}$ (to su b_u, b_v) važi $b_u \neq b_v$, tj. $\psi(u) \neq \psi(v)$. Slično, ako je za $u, v, w \in \mathrm{K}$ $w = u + v$, onda je $\underline{w} = \underline{u} + \underline{v}$ aksioma teorije T, pa otuda $b_w = b_u + b_v$, tj.

$$\psi(u + v) = \psi(w) = b_w = b_u + b_v = \psi(u) + \psi(v).$$

Slično važi $\psi(u \cdot v) = \psi(u) \cdot \psi(v)$ za $u, v \in K$, pa je ψ homomorfizam. Otuda možemo izvršiti identifikaciju elemenata a i b_a, tj. možemo uzeti da je F potpolje polja K. Naravno ovo se može malo strože obrazložiti. Nije teško dokazati da postoji polje L tako da je $F \subseteq L$ i $K \cong L$. Prema tome, i L se može raširiti do modela teorije T izborom nekih konstanata iz domena L.

Najzad, prema trećoj grupi aksioma svaki polinom p, $stp \geqslant 1$, nad poljem F ima koren u K (ovde koristimo pretpostavku da je F potpolje polja K).

Sada konstruišemo ovaj lanac polja:

$$F \subseteq K_1 \subseteq K_2 \subseteq \ldots$$

gde svaki polinom nad K_i stepena $\geqslant 1$ ima koren u K_{i+1}, što je moguće prema prethodnom. Tada je unija $K = \bigcup_i K_i$ ovih polja algebarski zatvorena i $F \subseteq K$. ∎

Dokaz Hilbertovog Nullstellensatza. Neka je F polje i neka su $f, g_1, \ldots, g_k \in F[x_1, \ldots, x_n]$. Pretpostavimo da je

$$V_K(g_1, \ldots, g_k) \subseteq V_K(f) \tag{1}$$

u nekom algebarski zatvorenom raširenju K polja F. Neka je x_0 promenljiva različita od promenljivih $x_1, \ldots, x_n$ i neka je $g_0 = 1 - x_0 f$. Iz uslova (1) neposredno dobijamo da je

$$V_K(g_0, \ldots, g_k) = \varnothing . \tag{2}$$

Po principu prenosa za algebarski zatvorena polja, i za svako drugo algebarski zatvoreno polje L koje sadrži F takođe je ispunjeno

$$V_L(g_0, \ldots, g_k) = \varnothing . \tag{3}$$

Dokažimo da za ideal $I = I_F(g_0, \ldots g_k)$ prstena $F[x_0, \ldots, x_n]$ koji je generisan elementima $g_0, \ldots, g_n$ važi $I = F[x_0, \ldots, x_n]$. Pretpostavimo suprotno; tada je po Teoremi 9, I sadržan u nekom maksimalnom idealu J prstena $F[x_0, \ldots, x_n]$. No, onda je po Teoremi 10, $F[x_0, \ldots, x_n]/J$ polje koje sadrži polje F. Osim toga, svi polinomi iz ideala J imaju zajednički koren; dakle i polinomi $g_0, \ldots, g_n$ imaju zajednički koren u $F[x_0, \ldots, x_n]/J$. Po Teoremi 8, polje $F[x_0, \ldots, x_n]/J$ je sadržano u nekom algebarski zatvorenom polju L, a u tom polju je $V_L(g_0, \ldots, g_k) \neq \varnothing$, suprotno uslovu (3). Prema tome, $I = F[x_0, \ldots, x_n]$, pa $1 \in I$. To znači da postoje polinomi $q_0, q_1, \ldots, q_k \in F[x_0, \ldots, x_n]$ takvi da je

$$1 = q_0(1 - x_0 f) + q_1 g_1 + \cdots + q_n g_n .$$

Ukoliko se umesto promenljive x_0 stavi $1/f$, posle sređivanja, nalazimo prirodan broj m i neke polinome $h_1, \ldots, h_k$ tako da je

$$f^m = h_1 g_1 + \cdots + h_k g_k .$$

§ 3. Realno zatvorena polja. Ovde ćemo dokazati neke važnije teoreme iz teorije realnih polja, koje se spominju u rešenju sedamnaestog Hilbertovog problema. Ove teoreme predstavljaju deo tzv.

Artin-Schreirove teorije realnih polja i pomoću njih se takođe može rešiti 17 Hp, na algebarski način. Osim toga, ove teoreme nalaze primene i u drugim oblastima matematike, naročito u algebarskoj geometriji i nestandardnoj analizi. Spomenućemo da je svaki model nestandardne analize jedno realno algebarski zatvoreno polje.

Glavna teorema ove oblasti je već pomenuta teorema iz prvog dela:

Teorema 1. Svako formalno realno polje ima realno algebarsko zatvorenje.

Dokaz. Najpre dokažimo sledeće:

(1) svako formalno realno polje F sadržano je u nekom maksimalnom formalno realnom polju koje je algebarsko nad F.

Da bismo dokazali (1), neka je F formalno realno polje i neka je $\overline{F}$ algebarsko zatvorenje ovog polja. Tada je svako algebarsko proširenje polja F izomorfno nekom podpolju polja $\overline{F}$. Dakle, u traženju maksimalnog formalno realnog polja koje je algebarsko nad F možemo se ograničiti na potpolja polja $\overline{F}$. Zato neka je $\mathcal{F}$ familija svih formalno realnih potpolja polja $\overline{F}$ koja sadrže F. Kako je $F\in\mathcal{F}$, to je $\mathcal{F}$ neprazna familija. S druge strane, lako se proverava da su za $\mathcal{F}$ ispunjeni uslovi Zornove leme; naime, svaki lanac $\mathcal{L}\subseteq\mathcal{F}$ ima gornje ograničenje. Dakle, po ovoj lemi postoji maksimalan element $K\in\mathcal{F}$, i to je onda maksimalno formalno realno polje koje sadrži F i koje je algebarsko nad F. Za polje K primećujemo da važi:

(2) polje $\overline{F}$ je algebarsko zatvorenje polja K;

(3) ako je L formalno realno polje koje je algebarsko proširenje polja K, onda je $L=K$.

Tvrđenje (3) sledi na osnovu maksimalnosti polja K u familiji $\mathcal{F}$ i (2). Jer ukoliko je L kao u (3), onda zbog (2) postoji polje L_1 tako da je $K\subseteq L_1\subseteq\overline{F}$ i izomorfizam $\varphi: L_1\cong L$, $\varphi\restriction K=id_K$. No tada je $K=L_1$, odakle i $K=L$.

Sada dokazujemo ovo, samo po sebi zanimljivo, tvrđenje:

(4) ako je L formalno realno polje koje nema pravo algebarsko proširenje do nekog formalno realnog polja, onda je L realno zatvoreno.

Dokaz ove činjenice lako se izvodi na osnovu sledeće leme (ubuduće, svako polje L koje zadovoljava uslove iz (4) nazivaćemo maksimalnim realnim poljem):

Lema. Neka je L formalno realno polje. Tada važi:

1° ako je $a \in L$, onda je $L(\sqrt{a})$ ili $L(\sqrt{-a})$ formalno realno polje. Ako je a zbir kvadrata u L, onda je $L(\sqrt{a})$ realno polje. Ako $L(\sqrt{a})$ nije formalno realno polje, onda je $-a$ zbir kvadrata u polju L;

2° ako je $f(x)$ nesvodljiv polinom neparnog stepena n nad poljem L i ako je a koren polinoma f, onda je $L(a)$ formalno realno polje.

Dokaz leme. 1° Neka je $a \in L$. Ako je a kvadrat u L, onda je $L(\sqrt{a}) = L$, prema tome $L(\sqrt{a})$ je formalno realno jer je polje L takvo. Pretpostavimo da a nije kvadrat u L. Ako polje $L(\sqrt{a})$ nije realno, to onda za neke $u_i, v_i \in L$ važi:

$$-1 = \sum_i (u_i + v_i \sqrt{a})^2 = \sum (u_i^2 + 2 u_i v_i \sqrt{a} + v_i^2 a).$$

Kako su 1 i a linearno nezavisni nad poljem L, to sledi:

$$-1 = \sum_i u_i^2 + a \sum_i v_i^2.$$

Ako je a suma kvadrata u polju L, onda dolazimo do kontradikcije. Ukoliko to nije slučaj, onda:

$$-a = (1 + \sum_i u_i^2) / \sum_i v_i^2,$$

odakle lako izlazi da je $-a$ zbir kvadrata (videti prvi deo, što prema prethodnom znači da je $L(\sqrt{-a})$ formalno realno polje.

U dokazu drugog dela leme koristićemo sledeće pomoćno tvrđenje:

(*) neka je polje K, proširenje polja L, p nesvodljiv polinom nad L i q proizvoljan polinom nad L. Ako je a koren polinoma p, q u K, tada q deli p.

Dokaz tvrđenja (∗). Najpre dokažimo da je $st(p) \leqslant st(q)$. Zato pretpostavimo da je q polinom najmanjeg stepena koji ispunjava uslove tvrđenja, i neka su m, r polinomi takvi da važi:

$$p = mq + r, \quad st(r) < st(q).$$

Ali tada je $r(a) = 0$, pa r ispunjava uslove tvrđenja. S obzirom na izbor polinoma q sledi da je r nula—polinom, tj. $p = mq$. Kako je p nesvodljiv nad L, to je m konstanta i $st(q) = st(p)$.

Sada se vratimo na dokaz samog tvrđenja (∗). Neka su u, v polinomi takvi da važi

$$q = up + v, \ st(v) < st(p).$$

Kako je $v(a) = 0$, prema prethodnom dokazu nalazimo da je v nula-polinom, odakle $q = up$.

Ovim je tvrđenje (∗) dokazano.

Sada smo u mogućnosti da dokažemo 2°.

2° Pretpostavimo suprotno, da $L(a)$ nije formalno realno, i neka je f polinom najmanjeg neparnog stepena n sa tom osobinom. Otuda sledi da je za neke polinome h_i nad L ispunjeno

$$-1 = \sum_i h_i(a)^2.$$

gde su stepeni polinoma h_i manji od n. Kako je a koren polinoma $1 + \sum_i h_i(x)^2$, a isto tako i nesvodljivog polinoma $f(x)$, to prema tvrđenju (∗) polinom $f(x)$ deli $1 + \sum_i h_i(x)^2$. Dakle, postoji polinom $g(x)$ nad L takav da važi:

$$-1 = \sum_i h_i(x)^2 + g(x) f(x).$$

Stepen polinoma $\sum_i h_i(x)^2$ je paran broj $i > 0$, jer bi inače -1 bio zbir kvadrata u L. Očigledno je da je ovaj stepen $\leqslant 2n-2$. Dalje, f je neparnog stepena, pa je g onda takođe neparnog stepena $\leqslant n-2$. Ako je b koren polinoma g, onda je -1 suma kvadrata u polju $L(\mathrm{b})$. Ali kako je $st(g) < st(f)$, to imamo kontradikciju prema izboru polinoma f.

Ovim je lema dokazana.

Sada je tvrđenje (4) neposredna posledica leme. Naime, ukoliko L ne bi bilo realno zatvoreno polje, po ovoj lemi ono bi imalo neko pravo algebarsko proširenje do formalno realnog polja, što se protivi maksimalnosti polja L.

Najzad, možemo da završimo dokaz teoreme. Ona je sada direktna posledica konstrukcije polja K i tvrđenja (3) i (4). ■

Važna strukturna teorema teorije formalno realnih polja je Teorema 4 iz prvog dela. Prema ovoj teoremi, algebarsko zatvorenje nekog realno zatvorenog polja F dobija se dodavanjem imaginarne jedinice, tj. $\bar{F}=F(\sqrt{-1})$. Dokaz ovog tvrđenja ovde ne navodimo; on se može naći u našoj literaturi, npr. u [Božović, Mijajlović 1983]. Zato ćemo navesti glavne posledice:

Teorema 2. Neka je F realno zatvoreno polje, tada:

1° F je maksimalno realno polje;

2° svaki nesvodljiv polinom nad F je najviše drugog stepena.

Dokaz. 1° Neka je K realno algebarsko proširenje polja F. Tada, kao što smo videli u dokazu Teoreme 1, možemo uzeti da je:

$$F\subseteq K\subseteq\bar{F}=F(\sqrt{-1}).$$

Aditivni deo polja $\bar{F}$ je vektorski prostor nad poljem F dimenzije 2. Isto tako, aditivni deo polja K je vektorski prostor nad poljem F, odakle sledi $K=F$ ili $K=\bar{F}$. Ali $K\neq F$ jer $0=1^2+i^2$, pa $K=\bar{F}$.

2° Ovaj dokaz se ne razlikuje od dokaza istog tvrđenja za polinome nad poljem realnih brojeva. ■

Jednostavna posledica Teoreme 2 je da je svaki polinom nad nekim realno zatvorenim poljem L proizvod linearnih i nesvodljivih kvadratnih polinoma. Ako je:

$$p(x)=a\prod_i(x-\alpha_i)\prod_j((x-\beta_j)^2+\lambda_j)$$

jedno takvo razlaganje, onda je $\lambda_j>0$. Odavde odmah sledi dokaz Weierstrassove teoreme za polinome (Teorema 2, prvi deo, § 3). Naime, prema ovom razlaganju polinoma p, p može da menja znak jedino u okolini nekog svog korena. Odavde izlazi veliki deo analize u realnim poljima, na primer Rolleova teorema za polinome, kao i Sturmova teorema o oceni broja korena polinoma u nekom intervalu.

§ 4. Sturmov algoritam. Eliminacija kvantora u teoriji algebarski zatvorenih polja može se izvršiti na nešto drugačiji način nego što smo to uradili u ovom dodatku. Naime, ako je F algebarski zatvoreno polje i ako su f i g polinomi nad F sa promenljivom x, tada u slučaju da f i g imaju neki zajednički koren a, najveći zajednički delilac polinoma f i g je stepena $\geqslant 1$ (jer $x-a$ deli f i g). Drugim rečima

$$\exists x\,(f(x)=0 \wedge g(x)=0) \leftrightarrow st\,NZD(f, g)\geqslant 1.$$

Nalaženje polinoma $NZD(f, g)$ može se izvršiti Euklidovim algoritmom. Za utvrđene polinome f i g taj proces se završava u konačno mnogo koraka, odnosno njegova dužina esencijalno zavisi jedino od stepena polinoma f i g. Otuda se možemo lako uveriti da se ovaj algoritam opisuje jednom formulom bez kvantora, tj. ako je:

$$f=q_1 g+m_2,\ g=q_2 m_2+m_3,\ m_2=q_3 m_3+m_4,\ \ldots,\ m_{i-2}=$$

$$=q_{i-1} m_{i-1}+q_i,\ m_{i-1}=q_i m_i \quad stf>stg>stm_2>\ldots>stm_i,$$

onda je

$$(1)\qquad \exists x\,(f(x)=0 \wedge g(x)=0) \leftrightarrow f=q_1 g+m_1 \wedge \ldots\ m_{i-1}=q_i m_i \wedge z\neq 0$$

gde je z koeficijent uz najviši stepen promenljive x u m_i. Drugi detalji dokaza su kao u § 1 ovog dodatka. Primetićemo da desna strana ove ekvivalencije ne sadrži kvantore.

Sa metodološkog stanovišta, postupak eliminacije kvantora za teoriju uređenih realno zatvorenih polja sličan je prethodnom za algebarski zatvorena polja, i kao što se ovaj zasniva na Euklidovom algoritmu, tako se taj postupak za uređena realno zatvorena polja može izvesti na osnovu Sturmovog algoritma.

Sturmova teorema. Neka je $p(x)$ realan polinom i neka je $p_0, p_1, \ldots, p_r$ niz realnih polinoma definisanih na sledeći način:

1° $p_0=p$;

2° $p_1=p'$ (prvi izvod od p);

3° za sve $0<i<r$ postoji polinom q_i takav da je

$$p_{i-1}=p_i q_i-p_{i+1}, \quad \text{gde je} \quad p_{i+1}\neq 0 \ \text{i}\ stp_{i+1}<stp_i$$

drugim rečima, q_i je količnik, a $-p_{i+1}$ ostatak dobijen deljenjem polinoma p_{i-1} polinomom p_i;

4° $p_{r-1} = p_r q_r$.

Neka je $d(a)$ broj promena znakova u nizu $p_0(a), \ldots, p_r(a)$ (nule se pritom ignorišu).

Neka su a i b realni brojevi koji nisu koreni polinoma p, i neka je $a<b$. Tada je broj korena polinoma p (ne računajući višestrukost korena) u intervalu $[a, b]$ jednak $d(a)-d(b)$.

Sada ćemo ilustrovati primenu Sturmove teoreme u eliminaciji kvantora na primeru jedne formule teorije uređenih polja. Primenom Sturmove teoreme odmah dobijamo

$$\exists x\,(a<x \wedge x<b \wedge p(x)=0) \leftrightarrow d(a)>d(b).$$

Osim toga, na sličan način kao kod formule (1), koristeći Sturmovu teoremu možemo naći formulu ψ bez kvantora tako da je:

$$d(a)>d(b) \leftrightarrow \psi.$$

Na ovaj način je eliminisan kvantor u formuli

$$\exists x\,(a<x<b \wedge p(x)=0).$$

Dalje se redukcija izvodi slično kao kod algebarski zatvorenih polja. Pri tome, može biti zgodno da se koristi ova ekvivalencija:

$$p_1=0 \wedge \ldots \wedge p_n=0 \leftrightarrow p_1^2+\ldots+p_n^2=0$$

(primetimo da ova formula nije teorema teorije algebarski zatvorenih polja).

Slično kao kod algebarski zatvorenih polja imamo ove posledice za teoriju T uređenih realno zatvorenih polja:

1° teorija T je kompletna;

2° teorija T je odlučiva.

BIBLIOGRAFSKE BELEŠKE

1. Prvi i glavni korak u rešavanju 17Hp predstavlja rad [Artin 1927].

2. Artin-Schreirova teorija formalno-realnih polja, na koju se odnosi §3 Dodatka, detaljno je prikazan u knjizi [Lang 1965].

3. Dokaz Hilbertove teoreme o bazi može se naći, na primer, u poznatoj knjizi [Artin 1955].

4. Zanimljiv pregled istorije 17Hp može se naći u članku A. Pfisera: *Hilbert's seventeenth problem and related problems on definite orms* u knjizi [Browder 1976]. U tom članku ovaj problem se analizira više sa algebarskog stanovišta, dok se Robinsonovo rešenje samo ovlaš pominje. Osim toga, ovaj rad je interesantan jer se u njemu navode i nekoliko otvorenih problema u vezi sa 17Hp.

5. U radu [Robinson 1955] nalazi se rešenje 17Hp opisanim metodima matematičke logike.

6. Eliminacija kvantora u teoriji algebarski zatvorenih polja i teoriji uređenih realno zatvorenih polja, kao i neke detaljnije analize koje proističu iz ovih postupaka, mogu se naći u knjizi [Kreisel, Krivine 1971]. Spomenimo da je decembra 1976. S. Vujošević prikazao ove metode na Seminaru za matematičku logiku. Ovde smo se između ostalog koristili i zabeleškama koje su ostale sa tih predavanja. Između metoda za eliminaciju kvantora u ovom poglavlju i u knjizi [Kreisel, Krivine 1971] postoje neke razlike. Tako na primer umesto dela u kojem se koristi rezolventa polinoma, u toj knjizi se koristi jedna lema koja se odnosi na deljivost polinoma.

7. Dokaz teoreme o rezolventi polinoma može se naći u knjizi [Kurepa 1965].

8. Kompletno rešenje 17Hp nalazi se takođe u [Cherlin 1976]. Ova knjiga je zanimljiva i zbog drugih primena logike u analizi algebarskih struktura (p-adska polja, tela, moduli, Abelove grupe).

9. Jedan od najvažnijih i najboljih udžbenika iz teorije modela je knjiga [Chang, Keisler 1973].

10. Problem eliminacije kvantora može se razmatrati u teoriji modela i sa nešto drugačijeg stanovišta. U tom drugom pristupu naročito važnu ulogu imaju dijagrami modela (o tome se nešto malo govorilo i u ovom poglavlju), zatim jedna specifična i važna vrsta modela — zasićeni modeli, i najzad elementarna utapanja modela. Ovakav pristup je manje jednostavan, ali su zato ovako dobijeni rezultati dublji. O ovom pristupu čitalac se može informisati u knjizi [Sacks 1972]. Autor ovog poglavlja održao je nekoliko predavanja na ovu temu 1976. i 1977. na Seminaru za matematičku logiku.

11. U članku [Mijajlović 1981] primenjena je teorija modela u tzv. infinitarnoj teoriji Galoisa. Članak se u stvari najvećim delom odnosi na proces kompletiranja polja do algebarski zatvorenih polja.

12. U knjizi [Božović, Mijajlović 1983] jedno poglavlje odnosi se na teoriju Galoisa. Tu se čitalac može detaljnije upoznati sa teorijom polja kao i glavnim aparatom ove teorije, teorijom grupa.

13. U članku [Motzkin 1967] daje se primer polinoma koji je pozitivno definitan ali nije konačna suma kvadrata nekih drugih polinoma. Ovaj primer pomenut je u fusnoti na početku ove glave.

BIBLIOGRAFIJA

[1900] C. Angus Scott, A report on the Páris Congress of Mathematicians, *Bulletin of the American Mathematical Society 6 (November)*.

[1927] E. Artin, Über die Zerlegung definiter Funktionen in Quadrate *Abhandlungen aus dem mathematischen Seminar der Universität Hamburg* 5, 100—115.

[1955] E. Artin, *Elements of Algebraic Geometry*, Courant Institute of Mathematical Sciences, New York University, New York.

[1977] J. Barwise (ed.), *Handbook of Mathematical Logic*, North-Holland, Amsterdam [ruski prevod: *Справочная книга по математической логике*, Наука, Москва 1983].

[1977] J.L. Bell, *Boolean-valued Models and Independence Proofs in Set Theory*, Oxford University Press, Oxford.

[1964] P. Benacerraf, H. Putnam (eds), *Philosophy of Mathematics*, Blackwell, Oxford.

[1967] P. Bernays, David Hilbert, *u The Encyclopedia of Philosophy*, P. Edwards (ed.), Macmillan, New York, vol. 3, 496—504.

[1971] G. Boolos, The iterative conception of set, *The Journal of Philosophy* 68, 215—231.

[1983] N. Božović, Ž. Mijajlović, *Uvod u teoriju grupa*, Naučna knjiga, Beograd.

[1976] F.E. Browder (ed.), *Mathematical Developments Arising from Hilbert's Problems*, Proceedings of Symposia in Pure Mathematics 28, American Mathematical Society, Providence R.I.

[1973] C.C. Chang, H.J. Keisler, *Model Theory*, North-Holland, Amsterdam [ruski prevod: *Теория моделей*, Мир, Москва 1977],

[1976] G. Cherlin, *Model-Theoretic Algebra: Selected Topics*, Lecture Notes in Mathematics 521, Springer, Berlin.

[1980] N.J. Cutland, *Computability: An Introduction to Recursive Function Theory*, Cambridge University Press, Cambridge [ruski prevod: *Вычислимость: введение в теорию рекурзивных функций*, Мир, Москва 1983].

[1970] Г. В. Чудновский, Диофантовы предикаты, *Успехи математических наук* 25, 185—186.

[1953] M. Davis, Aritmetical problems and recursively enumerable predicates, *The Journal of Symbolic Logic* 18, 33—41.

[1961] M. Davis, H. Putnam, J. Robinson, The decision problem for exponential diophantine equations, *Annals of Mathematics* 74, 425—436.

[1973] M. Davis, Hilbert's tenth problem is unsolvable, *American Mathematical Monthly* 80, 233—269.

[1976] J. Dieudonné, Mathématiques vides et mathématiques significatives, *u Langage et pensée mathématiques*, Actes du Colloque International, Centre Universitaire de Luxembourg, 273—297.

[1967] D.W. Dubois, Note on Artin's solution of Hilbert's 17th problem, *Bulletin of the American Mathematical Society* 73, 540—541.

[1893] G. Frege, *Grundgesetze der Arithmetic*, Jena [delimičan engleski prevod: *The Basic Laws of Aritmetic*, University of California Press, Berkeley Cal. 1964].

[1969] G. Gentzen, *The Collected Papers of Gerhard Gentzen*, North-Holland, Amsterdam.

[1940] K. Gödel, *The Consistency of the Continuum Hypothesis*, Princeton University Press, Princeton N.J.

[1940] W. Habicht, Über die Zerlegung strikte definiter Formen in Quadrate, *Comentarii Mathematici Helvetii* 12, 317—322.

[1967] J. van Heijenoort (ed.), *From Frege to Gödel: A Source Book in Mathematical Logic, 1879—1931*, Harvard University Press, Cambridge Mass.

[1899] D. Hilbert, *Grundlagen der Geometrie*, Teubner, Leipzig [srpsko-hrvatski prevod: *Osnove geometrije*, Srpska akademija nauka, Beograd 1957].

[1900] D. Hilbert, Mathematische Probleme, *Göttinger Nachrichten*, 253—297, *i Archiv der Mathematik und Physik* 3. reihe, 1 (1901), 44—63, 213—237 [engleski prevod u Browder 1976].

[1928] D. Hilbert, W. Ackermann, *Grundzüge der theoretischen Logik*, Springer, Berlin [engleski prevod: *Principles of Mathematical Logic*, Chelsea, New York 1950].

[1932] D. Hilbert, S. Cohn-Vossen, *Anschaulische Geometrie*, Springer, Berlin [engleski prevod: *Geometry and the Imagination*, Chelsea, New York 1952; ruski prevod: *Наглядная геометрия*, Наука, Москва 1981].

[1934] D. Hilbert, P. Bernays, *Grundlagen der Mathematik*, Springer, Berlin [ruski prevod: *Основания математики*, Наука, Москва 1979].

[1978] T. Jech, *Set Theory*, Academic Press, New York.

[1976] J.P. Jones, D. Sato, H. Wada, D. Wiens, Diophantine representation of the set of prime numbers, *American Mathematical Monthly* 83, 449—464.

[1982] L. Kirby, J. Paris, Accessible independence results for Peano Arithmetic, *Bulletin of the London Mathematical Society* 14, 285—293.

[1957] G. Kreisel, Hilbert's 17th problem, *Summaries of Talks Presented at the Summer Institute of Symbolic Logic*, Cornell University, 313—320.

[1971] G. Kreisel, J.-L. Krivine, *Elements of Mathematical Logic: Model Theory*, North-Holland, Amsterdam.

[1972] J.-L. Krivine, *Théorie axiomatique des ensembles*, Presse Universitaire de France, Paris, *drugo izdanje* [srpskohrvatski prevod: *Aksiomatička teorija skupova*, Školska knjiga, Zagreb 1978].

[1980] K. Kunen, *Set Theory*, North-Holland, Amsterdam.

[1965] Đ. Kurepa, *Viša algebra I*, Školska knjiga, Zagreb.

[1965] S. Lang, *Algebra*, Addison-Wesley, Reading Mass. [ruski prevod: *Алгебра*, Мир, Москва 1968].

[1906] E. Landau, Über die Darstellung definiter Funktionen durch Quadrate, *Mathematische Annalen* 62, 272—285.

[1980] Ю. И. Манин, *Вычислимое и невычислимое*, Советское радио, Москва.

[1970] Ю. В. Матиясевич, Диофантовость перечислимых множеств, *Доклады Академии Наук СССР* 191, 279—282.

[1964] E. Mendelson, *Introduction to Mathematical Logic*, Van Nostrand, New York [ruski prevod: *Введение в математическую логику*, Наука, Москва 1976].

[1984] M. Mihaljinec, S. Prešić, K. Šeper, Ž. Mijajlović, *O brojevima*, Školska knjiga, Zagreb.

[1981] Ž. Mijajlović, Completions of models and Galois theory, *Algebarska konferencija u Novom Sadu*, Univerzitet u Novom Sadu, 19—26.

[1967] T.S. Motzkin, The arithmetic-geometric inequality, *u Inequalities*, O. Shish (ed.), Academic Press, New York, 205—224.

[1971] A. Pfister, Quadratic forms over fields, *u Proceedings of Symposia in Pure Mathematics* 20, American Mathematical Society, Providence R.I., 150—160.

[1971] Y. Pourchet, Sur la représentation en somme de carrés des polynomes à une indeterminée sur un corps de nombres algébriques, *Acta Arithmetica* 19, 86—104.

[1971] D. Prawitz, Ideas and results in proof theory, *u Proceedings of the Second Scandinavian Logic Symposium*, J.E. Fenstad (ed.), North-Holland, Amsterdam, 235—307.

[1981] D. Prawitz, Philosophical aspects of proof theory, *u Contemporary Philosophy: A New Survey*, vol. 1, G. Fløistad, G.H. von Wright (eds), Nijhoff, The Hague, 235—277.

[1970] C. Reid, *Hilbert*, Springer, Berlin.

[1955] A. Robinson, On ordered fields and definite functions, *Mathematische Annalen* 130, 257—271.

[1952] J. Robinson, Existential definability in arithmetic, *Transactions of the American Mathematical Society* 72, 437—449.

[1967] H. Rogers, Jr, *Theory of Recursive Functions and Effective Computability*, McGraw-Hill, New York [ruski prevod: *Теория рекурзивных функций и эффективная вычислимость*, Мир, Москва 1972].

[1972] G. Sacks, *Saturated Model Theory*, Benjamin, Reading Mass. [ruski prevod: *Теория насыщенных моделей*, Мир, Москва 1976].

[1967] J.R. Shoenfield, *Mathematical Logic*, Addison-Wesley, Reading Mass. [ruski prevod: *Математическая логика*, Наука, Москва 1975].

[1971] J.R. Shoenfield, Unramified forcing, *u Axiomatic Set Theory* D. Scott (ed.), Proceedings of Symposia in Pure Mathematics 13, American Mathematical Society, Providence R.I., 357—380, [za ruski prevod v. Shoenfield 1967].

[1980] C. Smoryński, Some rapidly growing functions, *The Mathematical Intelligencer* 2, 149—154.

[1983] C. Smoryński, "Big" news from Archimedes to Friedmann, *Notices of the American Mathematical Society* 30, 251—256.

[1936] C. Tsen, Zur Stufentheorie der Quasi-algebraisch-Abgeschlossenheit kommutativer Körper, *Journal of the Chinese Mathematical Society* 1, 81—92.

[1937] A. Turing, On computable numbers, with an application to the *Entscheidungsproblem*, *Proceedings of the London Mathematical Society*, 2nd series, 42, 230—265.

[1944] H. Weyl, David Hilbert and his mathematical work, *Bulletin of the American Mathematical Society* 50, 612—654 [preštampano u Reid 1970].

INDEKS

Ž. Mijajlović Z. Marković, K. Došen: HILBERTOVI PROBLEMI I LOGIKA ● Prvo izdanje, 1986. godina ● Izdavač: ZAVOD ZA UDŽBENIKE I NASTAVNA SREDSTVA, Beograd, Obilićev venac 5/I ● Glavni i odgovorni urednik: mr VOJISLAV MITIĆ ● Urednik: GLIŠA NEŠKOVIĆ ● Likovni urednik: BOŽIDAR AREŽINA ARIŠ ● Lektor: DUŠICA TRIFUNOVIĆ ● Korektor: KOREKTURA ZAVODA ZA UDŽBENIKE ● Grafički urednik: MIRKO MARKOVIĆ ● Obim: 10½ štamparskih tabaka ● Format: 14×20 cm ● Tiraž: 2 000 primeraka ● Rukopis predat u štampu juna 1985. godine ● Štampanje završeno februara 1986. godine ● Štampa: BIGZ, Bulevar vojvode Mišića 17