



UNIVERZITET U NOVOM SADU
FAKULTET TEHNIČKIH NAUKA
U NOVOM SADU



Marko-Georgije Crvenković

JEDNAKOSNA LOGIKA

MASTER RAD

Novi Sad 2021

UVOD

Jednakosna logika je deo *Matematičke logike* u kojoj postoji jedan relacijski simbol, simbol jednakosti i specijalne aksiome koje formalno opisuju osobine klasične jednakosti.

U stvari, Jednakosna logika je logička podloga formalnih računa koje pominjemo u ovom radu. Neke formalne račune spominjemo samo kao primere formalnih teorija kao što su Teorija grupa, Teorija prstena, Teorija Booleovih algebri i Teorija mreža.

Glavni deo ovog rada odnosi se na Formalnu teoriju brojeva. Kroz priču o velikanu matematike dvadesetog veka Kurtu Gödelu prikazujemo najveći rezultat aritmetike prirodnih brojeva, Teoremu nekompletnosti. U svoje vreme, dokaz ove teoreme praktično je pokazao da se čuveni program Davida Hilberta razvoja matematike dvadesetog veka ne može u celosti sprovesti.

Posledice ove teoreme u matematici i ostalim naukama su mnogobrojne. Zahvaljujući Gödelovom dokazu Teoreme nekompletnosti stvorena je nova oblast matematike, Teorija algoritama. Teorija algoritama iznedrila je Turingove mašine i od njih je put vodio do računara.

Dokazi velikih teorema samo su skicirani u ovom radu, a mogu se naći u modernim udžbenicima *Matematičke logike*.

Poseban deo rada je priča o *Srednjoškolskom problemu Tarskog*. Alfred Tarski je šezdesetih godina prošlog veka primetio da su praktično svi zakoni koji važe u Teoriji brojeva logička posledica jedanaest osnovnih zakona koje učimo u školi. Ove zakone nazivamo *HSI - High School Identities*. Posle dvadeset godina, engleski matematičar Alex Wilkie je našao identitet koji je tačan u algebri prirodnih brojeva i koji ne može da se dokaže sintaksički. U našem radu je pokazano da je formula tačna, dok teži deo dokaza, da je formula logički neizvodljiva iz *HSI* iznosi više strana i veoma je tehnički zahtevan. Ono što je dokazano u ovom radu je činjenica da postoji pet 2-elementnih modela *HSI* identiteta. Prirodno je zapitati se da li smo odabrali prave aksiome da dokažemo sve identitete, tj. da li postoji konačan skup drugih aksioma čije logičke posledice su svi identiteti Teorije brojeva. Reuben Gurevič je u jednom od svojih radova dokazao da ni jedan konačan skup aksioma u jeziku Formalne teorije brojeva ne implicira sve tačne identitete.

Najveći deo rada posvećen je Kurtu Gödelu, i njegovoj Teoremi nekompletnosti. Četrdesetih godina dvadesetog veka Gödel se našao u malom američkom mestu Princeton. Skromne kuće Princetona krile su naučne veličine koje su ostavile dubok trag u mnogim naukama. Najpoznatiji od njih, Gödelov veliki prijatelj, Albert Einstein.

Da bi se predstavio dokaz Gödelove teoreme, u prvom delu rada navedeni su osnovni elementi Matematičke logike. Ovo je preuzeto, skoro u potpunosti, iz veoma dobrog udžbenika Matematičke logike u računarstvu Predraga Janičića [22] i poznatog udžbenika Matematičke logike Slaviše Prešića [38].

Opšte je mišljenje da su najveći logičari u istoriji čovečanstva bili Aristotel, Gottlob Frege, Gödel i Tarski. Veliko je zadovoljstvo uživati u priči o njihovim životima i rezultatima.

Zahvaljujem se svom mentoru, profesorki Silviji Gilezan na pomoći i podršci pri izradi ovog rada. Zahvaljujem se članovima komisije profesor Petru Djapiću i profesor Ljubi Nedoviću na savetima i korisnim sugestijama.

Sadržaj

Uvod	i
Glava 1. Logika prvog reda	1
1.1. Sintaksa logike prvog reda	4
1.2. Semantika logike prvog reda	7
Glava 2. Formalne teorije	13
2.1. Kvantifikatorski račun prvog reda	15
Glava 3. Jednakosna logika	19
3.1. Klase algebri definisnih jednakostima	27
3.2. Srednjoškolski problem Tarskog	31
3.3. Varijeteti algebri	41
Glava 4. Gödelov univerzum	45
Glava 5. Zaključak	67
Bibliografija	69

GLAVA 1

Logika prvog reda

Matematička logika, kao nezavisna grana moderne matematike, dobila je svoj oblik na prelasku iz devetnaestog u dvadeseti vek. Napredak i brzi razvoj Matematičke logike na početku dvadesetog veka povezan je sa takozvanom krizom u osnovama matematike.

Svaki pokušaj sistematičnog predstavljanja matematike, kao i drugih nauka, vodi do problema odabira osnovnih tj. primitivnih pojmova i principa kao baze čitave prezentacije. Problem biranja i opravdanja izbora početnih podataka leži van same naučne discipline i povezan je sa filozofijom i metodologijom nauke. Sistematizacija matematike krajem devetnaestog veka dovela je do pojma *skupa* kao jedinog primarnog pojma cele matematike. Radovi Bernarda Bolzana (1781-1848), Richarda Dedekinda (1831-1916) i Georga Cantora (1845-1918) doveli su do stvaranja nove matematičke discipline, Teorije skupova.

Lepota i snaga konstrukcija te perspektiva korišćenja Teorije skupova u osnovama matematike privukle su mnoge vodeće matematičare tog vremena. Mnogo truda je uloženo u skupovno-teorijske interpretacije matematičkih i čak logičkih pojmova.

Veliki doprinos istraživanjima osnova matematičke logike dali su Gottlob Frege (1848-1925) i Bertrand Russell (1872-1970). Međutim, veliki stepen apstrakcije i *univerzalnost* pojma skupa doveli su do teškoća koje su davno bile poznate u filozofiji kada se radi sa univerzalnim pojmovima. Ovo se manifestovalo u skupovno-teorijskim *paradoksima*. Jedan od najpoznatijih skupovno-teoretskih paradoksa je *paradoks Russella*.

Da li će skup biti svoj element? Primer je skup svih skupova. S druge strane ako posmatramo skup svih skupova koji nisu svoji elementi, označimo ga sa A_0 , onda ako se zapitamo da li je $A_0 \in A_0$:

$$A_0 \in A_0 \Rightarrow A_0 \notin A_0$$

$$A_0 \notin A_0 \Rightarrow A_0 \in A_0.$$

Ovaj paradoks Russella doveo je Fregea do očajja jer je završavao svoje delo iz osnova matematike. Na sreću ovakvi paradoksi mogu da

se stvore kod *velikih* i *neprirodnih* skupova i matematičari mogu mirno da rade bez njih.

Pojava paradoksa dobrodošla je mnogim matematičarima tog vremena da ispituju osnove matematike. Pomenimo samo vodeće matematičare tog doba: Davida Hilbert (1862-1943), Henri Poincaré (1854-1912), Hermann Weyl (1885-1955).

Predlagano je nekoliko programa za *spas* matematike od *užasa* paradoksa. Svakako najpoznatiji program za *ozdravljenje* matematike je program Davida Hilberta. Njegov program je u suštini pokušaj konstrukcije takve formalizacije matematike u kojoj bi bilo moguće dokazati neprotivrečnost sistema u samom sistemu. Drugi osnovni zahtev takve formalizacije bio je zahtev da osnovna i odmah proverljiva tvrđenja o prirodnim brojevima budu tačna u toj formalizaciji. Rad Hilberta i njegovih učenika doveo je do razvoja Matematičke logike, posebno modernog aksiomatskog metoda.

Hilbertov san o uređenosti tj. formalnoj dokazivosti svih matematičkih tvrđenja, na osnovu aksioma i elementarnih pravila zaključivanja, razbio je Kurt Gödel (1906-1978) tako što je pokazao da već *obična* Teorija brojeva sadrži istinita tvrđenja koja ne možemo dokazati sredstvima Formalne teorije brojeva.

Drugi pristup osnovama matematike nastao je na kritici mnogih postavki koje se koriste u matematici bez odgovarajućeg opravdanja. Ovo se odnosi, pre svega, na neograničeno korišćenje zakona isključenja trećeg i aksiome izbora. Program konstrukcije matematike pod strogom restrikcijom korišćenja navedenih principa nazvan je *Intuicionizam*. Tvorac ovog programa je Luitzen Brouwer (1881-1966). U Rusiji, Andrej Andejevič Markov (1903-1979) i njegova škola koristili su na sistematičan način koncept *algoritma* za konstruktivno dokazivanje matematičkih tvrđenja.

Glavni rezultat aktivnosti na osnovama matematike je stvaranje Matematičke logike kao nezavisne discipline. Osnovno dostignuće Matematičke logike je razvoj moderne aksiomatske metode koju karakterišu tri stvari:

1. Eksplicitna formulacija postulata (aksioma) teorije.
2. Eksplicitna formulacija pravila zaključivanja dopustiva za neprotivrečan razvoj teorije.
3. Korišćenje sopstvenog formalnog jezika za prezentaciju svih teorema teorije koja se razmatra.

U Matematičkoj logici, prvi put u istoriji, stvoreni su tako bogati formalni jezici koji praktično omogućavaju formalizaciju svih osnovnih tvrđenja u matematici.

Bogati formalni jezici Matematičke logike i uspešno iskustvo u radu sa njima stvorili su put ka stvaranju univerzalnih računarskih mašina koje koriste različit spektar formalnih programskih jezika.

Glavni objekat istraživanja u Matematičkoj logici su različiti *računi* (Formalne teorije). Pojam računa obuhvata osnovne komponente kao:

- (a) formalni jezik računa;
- (b) aksiome računa;
- (c) pravila zaključivanja.

Koncept računa omogućava nam da damo strogu matematičku definiciju dokaza.

Drugo značajno dostignuće Matematičke logike je matematičko određivanje pojma *algoritma* tj. efektivne procedure za rešavanje problema. Napomenimo da su računarski programi u stvari kodirani algoritmi. Veliki mislilac Gottfried Leibnitz (1646-1716) je maštao o otkriću univerzalnog algoritma za rešavanje svih matematičkih problema. Alonzo Church (1903-1995) je 1936. godine pokazao da ne postoji algoritam koji bi za svako tvrđenje u aritmetici dao odgovor na pitanje:

Da li je tvrđenje tačno za sve prirodne brojeve?

Kasnije je pokazano da u sistemu čiste logike (predikatski račun) problem dokazivosti nije algoritamski rešiv.

Istraživanje računa čini *sintaksički* deo matematičke logike. Najdublja istraživanja sintaksičkog pojma dokaza u računu čine nezavisnu oblast Matematičke logike poznatu kao *Teorija dokaza*.

Zajedno sa sintaksičkom studijom računa ide semantička studija formalnih jezika Matematičke logike. Osnovni pojam semantike je pojam *istine* za izraze (formule) formalnog jezika. Klasična semantika jezika predikatskih računa čini vrlo bogatu granu Matematičke logike, *Teoriju modela*. Osnivači Teorije modela su Alfred Tarski (1901-1983) i Anatolij Maljcev (1909-1967).

Iskazni račun i predikatski račun su formalizacije logike, najstarije nauke o zakonima ljudskog mišljenja.

Na razvitak evropske matematike i mišljenja uopšte, gotovo jedino je uticala grčka matematika i filozofija. Grci su prvi našli sredstva rasuđivanja kojima se i danas služimo.

Rađanje grčke logike pada u četvrti vek pre naše ere. Prvim većim logičarima smatraju se Parmenid, Zenon, Sokrat, Platon i Euklid iz Megare. Tako kod Parmenida nailazimo na formulaciju zakona isključenja trećeg, a Zenonovi dokazi pomoću *reductio ad absurdum* (svođenje na kontradikciju) poznati su i u današnje vreme.

Vrhunac razvoja grčke logike dostignut je stvaranjem genijalnog Aristotela (384-322 pne). On je prvi uspeo da sistematizuje metode

rasuđivanja. Glavna Aristotelova teza bila je da se svako korektno rasuđivanje može svesti na sistematsku primenu malog broja određenih pravila, koja inače ne zavise od prirode objekata na koji se odnosi rasuđivanje. Aristotelov autoritet u logici bio je toliko neprikosnoven da je to čak smetalo razvoju logike. Radovi Aristotela i njegovih sledbenika nisu imali velikog uticaja na grčku matematiku.

Originalnost Grka, od samog početka njihove matematičke misli, je u svesnim pokušajima da se pronikne u logiku matematičkih dokaza. Dokazi koje nalazimo kod grčkih klasičara Euklida iz Aleksandrije, Arhimeda, Apolonija u logičkom smislu su gotovo jednaki današnjim.

Za osnivače savremene (formalne, simboličke) logike može se smatrati George Boole (1815-1864). Njegova osnovna ideja je, da prihvatajući skupovno gledište, treba neposredno operisati sa skupovima. U drugoj polovini devetnaestog veka Booleov sistem su dopunili i usavršili Augustus de Morgan (1806-1871), Charles Peirce (1839-1914) i Ernst Schröder (1841-1892).

Frege i Peirce su uveli promenljive i kvantifikatore i tako došli do podesnijeg formalizma za opisivanje matematičkog teksta. 1879. godine Frege je prvi formulisao iskazni račun kao formalnu teoriju. Njegovi se radovi odlikuju izvanrednom tačnošću. Međutim, simbolika mu je tipografski jako komplikovana i nepodesna za matematičku praksu. To je znatno umanjilo uticaj Fregea na njegove savremenike.

Danas je najviše rasprostranjen formalizovani jezik koji su uveli 1910. godine Russell i Alfred Whitehead (1861-1947) u svom kapitalnom delu *Principia Mathematica*.

Savremeni snažan razvitak Matematičke logike, sa raznovrsnom primenom, u matematici, računarstvu i mnogim drugim naukama, kao i u praksi, usmerili su svojim dostignućima najveći logičari prošlog veka David Hilbert, Alfred Tarski, Rudolf Carnap (1891-1970), Alonzo Church, Kurt Gödel, Alan Turing (1912-1954), Andrej Andejevič Markov i drugi.

Logika prvog reda, predikatska logika, znatno je izražajnije od iskazne logike. Osnovna novina u odnosu na iskaznu logiku je uvođenje kvantifikovanja, univerzalnog i egzistencijalnog. Zahvaljujući kvantifikatorima, u logici prvog reda mogu se formulisati tvrđenja koja nije moguće formulisati na jeziku iskazne logike. U okviru logike prvog reda mogu se opisati mnoge matematičke teorije.

1.1. Sintaksa logike prvog reda

Sintaksa logike prvog reda govori o njenom jeziku, a o formulama isključivo kao nizovima simbola i ne uzima u obzir njihovo značenje.

DEFINICIJA 1.1. *Logički deo jezika prvog reda čine skupovi:*

1. *prebrojiv skup promenljivih V ;*
2. *skup logičkih veznika $\{\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow\}$ pri čemu je \neg unarni veznik, a $\wedge, \vee, \Rightarrow, \Leftrightarrow$ su binarni veznici;*
3. *skup kvantifikatora $\{\forall, \exists\}$, pri čemu je \forall univerzalni kvantifikator, a \exists egzistencijalni kvantifikator;*
4. *skup logičkih konstanti $\{\top, \perp\}$;*
5. *skup pomoćnih simbola $\{(,), , \}$*

Elemente nabrojanih skupova zovemo logički simboli.

Jezik ili *signatura* \mathcal{L} sastoji se od najviše prebrojivih skupova Σ i Π koje redom nazivamo skupom funkcionalnih (operacijskih) simbola i skupom predikatskih (relacijskih) simbola, kao i od funkcije ar koja preslikava skup $\Sigma \cup \Pi$ u skup nenegativnih celih brojeva. Za $k \in \Sigma \cup \Pi$ vrednost $ar(k)$ zovemo *arnost* simbola k . Skupovi Σ i Π čine *nelogički* deo jezika prvog reda. Sve njihove elemente zovemo *nelogičkim simbolima*. Napominjemo da su svi navedeni skupovi simbola sintakse logike prvog reda disjunktni. Datu signaturu označavamo sa

$$\mathcal{L} = (\Sigma, \Pi, ar)$$

Dogovorno označavamo:

- a, b, c, \dots simbole konstanti (funkcijski simboli arnosti 0)
- f, g, h, \dots simbole operacija arnosti veće od 0;
- p, q, r, \dots predikatske simbole;
- x, y, z, \dots promenljive.

DEFINICIJA 1.2. *Skup \mathcal{L} -termova (termova) nad signaturom $\mathcal{L} = (\Sigma, \Pi, ar)$ i skupom promenljivih V je najmanji skup za koji važi:*

- *svaki simbol konstante je term;*
- *svaki simbol promenljive je term;*
- *ako je f funkcijski simbol za koji je $ar(f) = n$ i t_1, t_2, \dots, t_n su termovi, onda je i $f(t_1, t_2, \dots, t_n)$ term.*

DEFINICIJA 1.3. *Skup atomičkih formula nad signaturom $\mathcal{L} = (\Sigma, \Pi, ar)$ i skupom promenljivih V je najmanji skup za koji važi:*

- *logičke konstante \top i \perp su atomičke formule;*
- *ako je p predikatski simbol za koje je $ar(p) = n$ i t_1, t_2, \dots, t_n su termovi, onda je $p(t_1, t_2, \dots, t_n)$ atomička formula.*

DEFINICIJA 1.4. *Skup dobro zasnovanih formula nad signaturom $\mathcal{L} = (\Sigma, \Pi, ar)$ i skupom promenljivih V je najmanji skup za koji važi:*

- *svaka atomička formula je dobro zasnovana;*

- ako je A dobro zasnovana formula, onda je i $(\neg A)$ dobro zasnovana formula;
- ako su A i B dobro zasnovane formule, onda su i $(A \wedge B)$, $(A \vee B)$, $(A \Rightarrow B)$, $(A \Leftrightarrow B)$, dobro zasnovane formule;
- ako je A dobro zasnovana formula i x je promenljiva, onda su i $(\forall x)A$ i $(\exists x)A$ dobro zasnovane formule.

Umesto termina dobro zasnovane formule, \mathcal{L} -formule, pišemo kraće *formule*. Skupove formula označavamo velikim slovima grčkog alfa-beta. Ako su dve formule A i B identične kao nizovi simbola, onda to označavamo $A = B$. Ako nisu sintaksno identične, to označavamo $A \neq B$.

DEFINICIJA 1.5. *Slobodno pojavljivanje i vezano pojavljivanje promenljive u formuli definiše se na sledeći način:*

- svako pojavljivanje u atomičkoj formuli je slobodno u toj formuli;
- svako pojavljivanje promenljive koje je slobodno u A je slobodno i u $\neg A$; svako pojavljivanje promenljive koje je vezano u A je vezano i u $\neg A$;
- svako pojavljivanje promenljive koje je slobodno u A ili B je slobodno i u $A \wedge B$, $A \vee B$, $A \Rightarrow B$, $A \Leftrightarrow B$; analogno za vezano pojavljivanje;
- Svako slobodno pojavljivanje promenljive različite od x u formuli A je takođe slobodno u formuli $(\forall x)A$; svako slobodno pojavljivanje promenljive x u A je vezano u $(\forall x)A$ (tada kažemo da je x u doseg u vodećeg kvantifikatora); analogno za egzistencijalni kvantifikator.

Kažemo da je term t slobodan za promenljivu x u formuli A ako ni jedno slobodno pojavljivanje promenljive x nije u doseg kvantifikatora takvog da t sadrži odgovarajuću kvantifikovanu promenljivu.

PRIMER 1.1. U formuli $p(x, y) \Rightarrow (\forall x)q(x)$ prvo pojavljivanje promenljive x je slobodno, a drugo i treće pojavljivanje je vezano. Primitimo da je pojavljivanje x u $\forall x$ vezano.

PRIMER 1.2. U formuli $(\exists x)(p(x) \wedge (\forall x)q(x))$ četvrto pojavljivanje promenljive x je vezano i ono je u doseg kvantifikatora $\forall x$, a ne i kvantifikatora $(\exists x)$.

\mathcal{L} -formulu bez slobodnih promenljivih nazivamo *zatvorena \mathcal{L} -formula* ili *\mathcal{L} -rečenica*.

1.2. Semantika logike prvog reda

Tarski [40] je prvi precizno uveo pojam semantike 1933. godine.

DEFINICIJA 1.6. Za datu signaturu \mathcal{L} , \mathcal{L} -struktura \mathcal{D} je par $(D, I^{\mathcal{L}})$, gde je D skup, a $I^{\mathcal{L}}$ funkcija pri čemu važi sledeće:

- D je neprazan skup i zovemo ga domen, nosač ili univerzum;
- svakom simbolu konstante c iz \mathcal{L} (tj. svakom funkcijskom simbolu arnosti 0), funkcija $I^{\mathcal{L}}$ pridružuje jedan element c_I iz D ;
- svakom funkcijskom simbolu f iz \mathcal{L} za koji je $ar(f) = n$, $n > 0$, funkcija $I^{\mathcal{L}}$ pridružuje jednu totalnu (svuda definisanu na D) funkciju f_I iz D^n u D ;
- svakom predikatskom simbolu p iz \mathcal{L} za koji je $ar(p) = n$, $n > 0$, funkcija $I^{\mathcal{L}}$ pridružuje totalnu funkciju p_I iz D^n u skup $\{0, 1\}$.

Valuacija v za skup promenljivih V u odnosu na domen D je preslikavanje koje svakom elementu iz V dodeljuje jedan element iz D . Ako je $v(x_i) = d_i$, onda kažemo da je d_i vrednost promenljive x_i u valuaciji v .

Par (\mathcal{D}, v) određuje interpretaciju, tj. funkciju I_v koja preslikava skup \mathcal{L} -termova nad skupom promenljivih V u skup D , a skup \mathcal{L} -formula nad V u skup $\{0, 1\}$.

Ako su v i w valuacije za isti skup promenljivih i u odnosu na isti domen, onda sa $v \sim_x w$ označavamo da je $v(y) = w(y)$ za svaku promenljivu različitu od x . Funkcija I_v uvodi se sledećim definicijama.

DEFINICIJA 1.7. Vrednost (ili značenje) terma t u interpretaciji I_v , određenoj \mathcal{L} -strukturuom \mathcal{D} i valuacijom v , označava se sa $I_v(t)$ i definiše na sledeći način:

- ako je t simbol konstante c , onda je $I_v(t) = c_I$;
- ako je $t = f(t_1, t_2, \dots, t_n)$, $ar(f) = n$ i ako je $I_v(t_i) = d_i$, $i = 1, 2, \dots, n$ ($d_i \in D$), onda je $I_v(t) = f_I(d_1, d_2, \dots, d_n)$.

DEFINICIJA 1.8. Vrednost (ili značenje) formule A u interpretaciji I_v , određenoj \mathcal{L} -strukturuom \mathcal{D} i valuacijom v , označavamo na sledeći način:

- ako je A atomička formula \top , onda je $I_v(A) = 1$;
- ako je A atomička formula \perp , onda je $I_v(A) = 0$;
- ako je A atomička formula $p(t_1, t_2, \dots, t_n)$ pri čemu je $ar(p) = n$ i ako je $I_v(t_i) = d_i$ za $i = 1, 2, \dots, n$ (pri čemu je $d_i \in D$), onda je $I_v(A) = p_I(d_1, d_2, \dots, d_n)$;

- ako je $A = \neg B$, onda je

$$I_v(A) = \begin{cases} 0, & \text{ako je } I_v(B) = 1 \\ 1, & \text{ako je } I_v(B) = 0 \end{cases}$$

- ako je $A = B_1 \wedge B_2$, onda je

$$I_v(A) = \begin{cases} 1, & \text{ako je } I_v(B_1) = I_v(B_2) = 1 \\ 0, & \text{inače} \end{cases}$$

- ako je $A = B_1 \vee B_2$, onda je

$$I_v(A) = \begin{cases} 1, & \text{ako je } I_v(B_1) = 1 \text{ ili } I_v(B_2) = 1 \\ 0, & \text{inače} \end{cases}$$

- ako je $A = B_1 \Rightarrow B_2$, onda je

$$I_v(A) = \begin{cases} 0, & \text{ako je } I_v(B_1) = 1 \text{ i } I_v(B_2) = 0 \\ 1, & \text{inače} \end{cases}$$

- ako je $A = B_1 \Leftrightarrow B_2$, onda je

$$I_v(A) = \begin{cases} 1, & \text{ako je } I_v(B_1) = I_v(B_2) \\ 0, & \text{inače} \end{cases}$$

- ako je $A = (\exists x)B$, onda je $I_v(A) = 1$ ako postoji valuacija w sa domenom D takva da je $w \sim_x v$ i $I_w(B) = 1$; inače je $I_v(A) = 0$;
- ako je $A = (\forall x)B$, onda je $I_v(A) = 0$ ako postoji valuacija w sa domenom D takva da je $w \sim_x v$ i $I_w(B) = 0$; inače $I_v(A) = 1$.

Vidimo da $I_v(A)$ zavisi od $v(x)$ samo ako promenljiva x ima slobodno pojavljivanje u A . Specijalno, ako je A rečenica, vrednost $I_v(A)$ ne zavisi od v , pa tada umesto $I_v(A)$ pišemo $I(A)$.

DEFINICIJA 1.9. Ako je interpretacija I_v određena \mathcal{L} -strukturuom \mathcal{D} i valuacijom v i ako za formulu A važi $I_v(A) = 1$, onda kažemo da interpretacija I_v zadovoljava formulu A , da je formula A tačna u interpretaciji I_v i da je \mathcal{L} -struktura \mathcal{D} sa valuacijom v model formule A i pišemo $(\mathcal{D}, v) \models A$. Formula A je zadovoljiva u \mathcal{L} -strukturi \mathcal{D} ako postoji valuacija v takva da je $(\mathcal{D}, v) \models A$.

Ako formula nije zadovoljiva, onda kažemo da je *kontradiktorna*.

DEFINICIJA 1.10. Ako je za neku \mathcal{L} -strukturu \mathcal{D} formula A tačna za svaku valuaciju v , tj. u svakoj interpretaciji I_v , onda kažemo da je \mathcal{L} -struktura \mathcal{D} model formule A , kažemo da je formula A valjana u \mathcal{L} -strukturi \mathcal{D} i pišemo $\mathcal{D} \models A$. Ako je formula nad signaturom \mathcal{L}

valjana u svakoj \mathcal{L} -strukturi, onda za tu formulu kažemo da je valjana i to zapisujemo $\models A$.

Ako formula nije valjana, onda kažemo da je ona poreciva.

Ako nije $\mathcal{D} \models A$, onda pišemo $\mathcal{D} \not\models A$.

Za skupove formula uvodimo sledeće definicije.

DEFINICIJA 1.11. *Skup rečenica Γ je konzistentan ili zadovoljiv ako ima bar jedan model. Inače, kažemo da je nekonzistentan, nezadovoljiv, protivrečan ili kontradiktoran.*

TEOREMA 1.1. *Ako su formule A i $A \Rightarrow B$ (nad nekom signaturom \mathcal{L}) valjane, onda je i formula B valjana.*

Dokaz: Pretpostavimo suprotno da postoji \mathcal{L} -struktura \mathcal{D} i odgovarajuća interpretacija I_v u kojoj formula B nije tačna. Formula A je valjana, pa je tačna u I_v . U toj interpretaciji, onda, formula $A \Rightarrow B$ nije tačna (jer je $I_v(A) = 1$ i $I_v(B) = 0$) što protivreči pretpostavci da je formula $A \Rightarrow B$ valjana. Dakle, polazna pretpostavka je pogrešna, pa je formula B tačna u svakoj interpretaciji, tj. ona je valjana, što je trebalo dokazati. \square

TEOREMA 1.2. *Formula A nad signaturom \mathcal{L} je valjana u \mathcal{L} -strukturi \mathcal{D} ako i samo ako je formula $(\forall x)A$ valjana u \mathcal{D} .*

Dokaz: (\rightarrow) Pretpostavimo da je A valjana u \mathcal{D} i pretpostavimo da formula $(\forall x)A$ nije valjana u \mathcal{D} , tj. pretpostavimo da postoji valuacija v takva da je $I_v((\forall x)A) = 0$. Odatle sledi da postoji valuacija w za koju je $w \sim_x v$ i važi $I_w(A) = 0$, pa A nije valjana u \mathcal{D} što je u suprotnosti sa pretpostavkom. Dakle formula $(\forall x)A$ je valjana.

(\leftarrow) Neka je $(\forall x)A$ valjana u \mathcal{D} . To znači da za svaku valuaciju v važi $I_v((\forall x)A) = 1$. Pretpostavimo da formula A nije valjana u \mathcal{D} . Tada postoji valuacija w takva da je $I_w(A) = 0$, pa je po definiciji $I_w((\forall x)A) = 0$, što je u suprotnosti sa pretpostavkom. Dakle, formula A je valjana u \mathcal{D} . \square

TEOREMA 1.3. *Formula A je valjana ako i samo ako je formula $(\forall x)A$ valjana.*

Dokaz: (\rightarrow) Ako je formula A valjana, onda je ona valjana u svakoj \mathcal{L} -strukturi \mathcal{D} , pa je onda na osnovu teoreme 1.2, u svakoj \mathcal{L} -strukturi \mathcal{D} valjana i formula $(\forall x)A$.

(\leftarrow) Analogno važi i obrat, pa je formula A valjana ako i samo ako je formula $(\forall x)A$ valjana. \square

DEFINICIJA 1.12. *Neka je Γ skup formula nad signaturom \mathcal{L} . Kažemo da je formula A logička posledica skupa formula Γ i pišemo $\Gamma \models A$*

ukoliko za svaku \mathcal{L} -strukturu \mathcal{D} i svaku valuaciju v važi: ako za svaku formulu B iz Γ važi $(\mathcal{D}, v) \models B$, onda važi $(\mathcal{D}, v) \models A$.

Drugim rečima, kažemo da je formula A logička posledica skupa formula Γ ako je svaki model za Γ istovremeno model za A .

Ako je skup Γ konačan, tj. ako je $\Gamma = \{B_1, B_2, \dots, B_n\}$, onda pišemo $B_1, B_2, \dots, B_n \models A$. Ako je $\Gamma = \emptyset$, onda pišemo $\models A$. Ako je $\models A$, onda formula A zadovoljava svaku interpretaciju i tada je A valjana. Ako ne važi $\Gamma \models A$, onda to zapisujemo $\Gamma \not\models A$.

Na osnovu definicije logičke posledice jednostavno se dokazuje naredna teorema.

- TEOREMA 1.4. (a) Svaka valjana formula je logička posledica praznog skupa formula.
- (b) Ako je skup Γ kontradiktoran, onda je svaka formula njegova logička posledica. Specijalno, svaka formula je logička posledica $\{\perp\}$.
- (c) Ako je $\Gamma \subset \Delta$ i $\Gamma \models A$, onda je $\Delta \models A$.
- (d) Ako je formula A valjana i $\Gamma \models B$, onda je $\Gamma \setminus \{A\} \models B$.

DEFINICIJA 1.13. Kažemo da su formule A i B logički ekvivalentne i pišemo $A \equiv B$ ako je A logička posledica formule B i B je logička posledica formule A .

Tvrđenja oblika $A \equiv B$ zovemo logička ekvivalencija. Relacija \equiv je, očigledno, relacija ekvivalencije nad skupom formula. Ako za formule A_1, A_2, B_1, B_2 važi $A_1 \equiv A_2$ i $B_1 \equiv B_2$, onda lako pokazujemo da važi

- (a) $\neg A_1 \equiv \neg A_2$
 (b) $A_1 \wedge B_1 \equiv A_2 \wedge B_2$
 (c) $A_1 \vee B_1 \equiv A_2 \vee B_2$
 (d) $A_1 \Rightarrow B_1 \equiv A_2 \Rightarrow B_2$
 (e) $A_1 \Leftrightarrow B_1 \equiv A_2 \Leftrightarrow B_2$
 (f) $(\forall x)A_1 \equiv (\forall x)A_2$
 (g) $(\exists x)A_1 \equiv (\exists x)A_2$

Navodimo sledeću teoremu koja daje vezu logičke ekvivalencije i valjanosti odgovarajuće formule u signaturi \mathcal{L} .

TEOREMA 1.5. Za datu signaturu \mathcal{L} , dve \mathcal{L} -formule A i B su logički ekvivalentne ako i samo ako je formula $A \Leftrightarrow B$ valjana.

Dokaz: (\rightarrow) Pretpostavimo da važi $A \equiv B$. Sledi da za svaku \mathcal{L} -strukturu \mathcal{D} i valuaciju v , iz $(\mathcal{D}, v) \models A$ sledi $(\mathcal{D}, v) \models B$ i iz $(\mathcal{D}, v) \models B$ sledi $(\mathcal{D}, v) \models A$. Dakle, ako je $I_v(A) = 1$, onda mora biti $I_v(B) = 1$ i obratno. Ovo znači da uvek važi $I_v(A) = I_v(B)$, pa je na osnovu definicije 1.8 uvek $I_v(A \Leftrightarrow B) = 1$. Imamo da je formula $A \Leftrightarrow B$

valjana u strukturi \mathcal{D} , a kako to važi za svaku \mathcal{L} -strukturu, sledi da je formula $A \Leftrightarrow B$ valjana.

(\leftarrow) Pretpostavimo da je formula $A \Leftrightarrow B$ valjana. Onda je ona valjana u svakoj \mathcal{L} -strukturi \mathcal{D} , i odgovarajućoj interpretaciji I i biće $I(A \Leftrightarrow B) = 1$, pa će za svaku valuaciju v važiti $I_v(A \Leftrightarrow B) = 1$. Sledi da je $I_v(A) = I_v(B)$. Ovo znači da ako je $I_v(A) = 1$ onda je $I_v(B) = 1$, pa je $A \models B$. Jasno, važi i obrat $B \models A$, pa su formule A i B logički ekvivalentne. \square

Navedimo neke poznate zakone logike.

$\neg(\exists x)A \equiv (\forall x)\neg A$ - De Morganov zakon

$\neg(\forall x)A \equiv (\exists x)\neg A$ - De Morganov zakon

$(\exists x)(A \vee B) \equiv (\exists x)A \vee (\exists x)B$ - zakon distributivnosti \exists

prema \vee

$(\forall x)(A \wedge B) \equiv (\forall x)A \wedge (\forall x)B$ - zakon distributivnosti \forall

prema \wedge

$(\exists x)(A \wedge B) \equiv (\exists x)A \wedge B$ - zakon distributivnosti \exists prema \wedge

(pri čemu B ne sadrži slobodna pojavljivanja x)

$(\forall x)(A \vee B) \equiv (\forall x)A \vee B$ - zakon distributivnosti \forall prema \vee

(pri čemu B ne sadrži slobodna pojavljivanja x).

Analogan stavu iz iskazne algebre je sledeći stav. Dokaz je sličan dokazu odgovarajućeg stava iskazne algebre.

TEOREMA 1.6. *Ako su F_1, F_2, \dots, F_n zatvorene formule (rečenice), onda je*

1. $F_1, F_2, \dots, F_n \models F$ ako i samo ako $\models F_1 \wedge F_2 \wedge \dots \wedge F_n \Rightarrow F$;
2. $F_1, F_2, \dots, F_n \models F$ ako i samo ako $\models F_1 \Rightarrow (F_2 \Rightarrow \dots (F_n \Rightarrow F) \dots)$;
3. Ako je F_n zatvorena formula, onda $F_1, F_2, \dots, F_n \models F$ ako i samo ako $F_1, F_2, \dots, F_{n-1} \models F_n \Rightarrow F$.

TEOREMA 1.7. *Formula*

$$(1.1) \quad (\forall u)A(u) \Rightarrow A(t)$$

je valjana ako je A proizvoljna formula, u - promenljiva, t - term, ukoliko je term t slobodan za promenljivu u u formuli $A(u)$.

Dokaz: Pretpostavimo da formula (1.1) nije valjana. Tada pri nekoj interpretaciji I formula (1.1) ima vrednost 0. U tom slučaju formula $(\forall u)A(u)$ ima vrednost 1, dok formula $A(t)$ ima vrednost 0. Kako je term t slobodan za promenljivu u u formuli $A(u)$, odnosno kako u formuli $A(u)$ nijedno slobodno pojavljivanje promenljive u nije u oblasti dejstva bilo kog od kvantifikatora $(\forall v_i)$, $(\exists v_i)$, gde je v_i ma koja promenljiva terma t , zaključujemo da ako term t i promenljiva u

dobijaju pri interpretaciji I istu vrednost, onda će i vrednosti formula $A(u)$ i $A(t)$ biti iste. Znači, da za određenu interpretaciju i formula $A(u)$ ima vrednost 0, dok prema pretpostavci $A(u)$ ima vrednost 1 za svako u . Kontradikcija. Sledi da je formula (1.1) valjana. \square

GLAVA 2

Formalne teorije

Formalna teorija, u oznaci \mathcal{T} , određena je kad su ispunjeni sledeći uslovi.

1. Dat je najviše prebrojiv skup simbola, tzv. *osnovnih simbola* teorije \mathcal{T} .
2. U skupu svih reči sa osnovnim simbolima teorije \mathcal{T} određen je podskup, tzv. skup *formula* teorije \mathcal{T} . Dat je efektivan postupak za odlučivanje da li je neka reč formula ili nije.
3. U skupu svih formula određen je jedan podskup, čije elemente zovemo *aksiome*. Ako je još dat i efektivan postupak za odlučivanje da li je neka formula aksioma ili nije, onda \mathcal{T} zovemo *aksiomatska teorija*.
4. Dat je konačan broj *pravila izvođenja*. Svako pravilo izvođenja je izvesna relacija u skupu formula teorije \mathcal{T} . Ako je α jedno pravilo izvođenja dužine n , na primer, onda ma kakve bile formule $A_1, A_2, \dots, A_{n-1}, A_n$ postoji efektivan postupak za određivanje da li su redom formule $A_1, A_2, \dots, A_{n-1}, A_n$ u relaciji α ili nisu. Ako su redom formule A_1, \dots, A_n u relaciji α , onda kažemo da je A_n *direktna posledica* A_1, A_2, \dots, A_{n-1} po pravilu izvođenja α i pišemo

$$\frac{A_1, A_2, \dots, A_{n-1}}{A_n}.$$

Označimo redom sa $S(\mathcal{T})$, $F(\mathcal{T})$, $A(\mathcal{T})$, $R(\mathcal{T})$, skupove osnovnih simbola, formula, aksioma i pravila izvođenja teorije \mathcal{T} . Navedeni skupovi određuju formalnu teoriju, pa se teorija \mathcal{T} može striktno definisati kao

$$(S(\mathcal{T}), F(\mathcal{T}), A(\mathcal{T}), R(\mathcal{T})).$$

Umesto formalna teorija kažemo i *formalni račun*.

DEFINICIJA 2.1. *Konačan niz formula*

$$B_1, B_2, \dots, B_m$$

formalne teorije \mathcal{T} zovemo izvođenje (dedukcija, dokaz) u teoriji ako svaka formula B_i ($1 \leq i \leq m$) tog niza ispunjava uslov:

1. B_i je aksioma, ili
2. B_i je direktna posledica nekih prethodnih formula niza po izvesnom pravilu izvođenja teorije \mathcal{T} .

DEFINICIJA 2.2. Formulu B_m formalne teorije zovemo teorema u teoriji \mathcal{T} , u oznaci $\vdash_{\mathcal{T}} B_m$ ili samo $\vdash B_m$ ako postoji bar jedan niz

$$B_1, B_2, \dots, B_m$$

koji je izvođenje u teoriji \mathcal{T} . U ovom slučaju kažemo da je taj niz izvođenje (dokaz) teoreme B_m .

DEFINICIJA 2.3. Neka je \mathcal{F} neki skup formula neke formalne teorije \mathcal{T} i neka je A određena formula iste teorije. Kažemo formula A je posledica skupa formula \mathcal{F} ako postoji konačan niz formula

$$B_1, B_2, \dots, B_m, \quad B_m = A,$$

čija svaka formula B_i ispunjava uslov:

1. B_i aksioma, ili
2. $B_i \in \mathcal{F}$ ili
3. B_i je direktna posledica nekih prethodnih formula niza po izvesnom pravilu izvođenja teorije \mathcal{T} .

Ako je A posledica skupa formula \mathcal{F} , onda pišemo

$$\mathcal{F} \vdash_{\mathcal{T}} A \quad \text{ili} \quad \mathcal{F} \vdash A,$$

a elemente \mathcal{F} zovemo hipoteze (*premise, pretpostavke*). Pomenuti niz B_1, B_2, \dots, B_m zovemo izvođenje formule A iz skupa hipoteza \mathcal{F} .

Ako je \mathcal{F} konačan skup, onda umesto $\{A_1, A_2, \dots, A_n\} \vdash A$ pišemo $A_1, A_2, \dots, A_n \vdash A$.

Izvođenja iz hipoteza imaju sledeća značajna svojstva:

1. Ako je $\mathcal{F}_1 \subseteq \mathcal{F}_2$ i $\mathcal{F}_1 \vdash A$, onda $\mathcal{F}_2 \vdash A$.
2. $\mathcal{F} \vdash A$ ako i samo ako postoji konačan podskup \mathcal{F}_1 skupa \mathcal{F} takav da je $\mathcal{F}_1 \vdash A$.
3. Neka $\mathcal{F}_1 \vdash B$, gde je B proizvoljna formula iz skupa \mathcal{F}_2 . Ako je $\mathcal{F}_2 \vdash A$, onda $\mathcal{F}_1 \vdash A$.

Kažemo da je teorija \mathcal{T} neprotivrečna (konzistentna) ako ne postoji formula A teorije \mathcal{T} takva da su A i $\neg A$ teoreme teorije \mathcal{T} .

Formalne teorije obrazuju jednu klasu matematičkih teorija. Ostale matematičke teorije zovemo *obične matematičke teorije*. Za opisivanje i izgrađivanje neke formalne teorije koristi se izvesna obična matematička teorija koju zovemo *meta-teorija* te formalne teorije. Formalnu teoriju u tom slučaju zovemo i *objekat-teorija*.

Meta-teorija se izlaže korišćenjem jednog dela običnog jezika, proširenog odgovarajućom matematičkom terminologijom. Taj jezik zovemo *meta-jezik*. Na primer iskaz

formula $x + y \approx y + x$ je teorema

je u meta-jeziku Formalne teorije brojeva o kojoj će biti reči kasnije. I formalna teorija ima svoj jezik, tzv. *objekt-jezik*. To je skup čiji elementi su polazni simboli formalne teorije, reči sastavljene od tih polaznih simbola, kao i konačni nizovi tih reči. Prema tome, formule, aksiome i izvođenja pripadaju objekt-jeziku. Tvrđenje koje se odnosi na neku formalnu teoriju zovemo *meta-teorema*. Tako "formula $x + y \approx y + x$ je teorema" jeste meta-teorema.

Obične matematičke teorije izgrađuju se često na sledeći način. Polazi se od jednog skupa polaznih (osnovnih) termina i određenog skupa rečenica sa tim terminima, tzv. aksiomama. Za teoreme se uzimaju rečenice koje su tačne pri onim interpretacijama pri kojima su i aksiome tačne, isto tako, teoreme su i sve rečenice koje se dobijaju iz aksioma primenom izvesnih logičkih pravila (koja se obično ne ističu). Za prvi slučaj kažemo da se teoreme izvode *semantički*, a za drugu *sintaksički*. Kod običnih matematičkih teorija često se prepliću ta dva načina dobijanja teorema. Osim toga postoji i jak stepen intuicije o skupu. Kod formalnih teorija upotreba intuicije svodi se na neizbežan minimum.

Formalne teorije često se obrazuju sa ciljem tzv. potpunog aksiomatskog, odnosno formalnog, zasnivanja neke obične matematičke teorije. Radi toga se formalna teorija tako izabere da elementima njenog objekt-jezika odgovaraju objekti matematičke teorije, koju formalno izgrađujemo.

Interpretacija neke formalne teorije je svako preslikavanje objekt-jezika u klasu objekata neke druge matematičke teorije. Jedan od tvoraca formalnih teorija je David Hilbert. U svom programu izgrađivanja formalnih teorija postavio je zahtev korišćenja *striktne finitnosti* u meta-teoriji, odnosno nekorišćenja, na primer, aksiome izbora, aksiome beskonačnosti.

2.1. Kvantifikatorski račun prvog reda

Kvantifikatorski račun prvog reda u oznaci \mathcal{K} , jeste formalna teorija čiji su osnovni simboli i formule uvedeni u prvom delu rada u okviru logike prvog reda. Aksiome od \mathcal{K} su sledeće:

- Ax1 $A \Rightarrow (B \Rightarrow A)$;
- Ax2 $(A \Rightarrow (B \Rightarrow C)) \Rightarrow ((A \Rightarrow B) \Rightarrow (A \Rightarrow C))$;
- Ax3 $(\neg A \Rightarrow \neg B) \Rightarrow (B \Rightarrow A)$;
- Ax4 $(\forall x)A(x) \Rightarrow A(t)$,

$$\text{Ax5 } (\forall x)(A \Rightarrow B) \Rightarrow (A \Rightarrow (\forall x)B),$$

gde je term t slobodan za promenljivu x u formuli A . Pravila izvođenja ovog računa su:

(MP) Iz A i $A \Rightarrow B$ sledi B .

(Gen) Iz A sledi $(\forall x)A$, gde je x promenljiva.

Navedena pravila zovemo *modus ponens* i *generalizacija* i označavamo ih sa MP i Gen.

Primetimo da su aksiome Ax1, Ax2, Ax3 i MP aksiome i pravila izvođenja tzv. *iskaznog računa* \mathcal{P} o kome neće biti reči u ovom radu.

PRIMER 2.1. *Formula F*

$$F = \neg(\forall x)A \Rightarrow \neg(\forall x)\neg\neg A,$$

sa proizvoljnom formulom A , predstavlja jednu teoremu računa \mathcal{K} .

Dokažimo ovo sledećim nizom formula.

- (1) $(\forall x)\neg\neg A \Rightarrow \neg\neg A$ Ax4
- (2) $\neg\neg A \Rightarrow A$ (izvod teoreme iskaznog računa)
- (3) $((\forall x)\neg\neg A \Rightarrow A) \Rightarrow ((\neg\neg A \Rightarrow A) \Rightarrow ((\forall x)\neg\neg A \Rightarrow A))$ (izvod teoreme računa \mathcal{P})
- (4) $(\neg\neg A \Rightarrow A) \Rightarrow ((\forall x)\neg\neg A \Rightarrow A)$ (iz (1) i (3) po MP)
- (5) $((\forall x)\neg\neg A \Rightarrow A)$ (iz (2) i (4) po MP)
- (6) $(\forall x)((\forall x)\neg\neg A \Rightarrow A)$ (iz (5) po Gen)
- (7) $(\forall x)((\forall x)\neg\neg A \Rightarrow A) \Rightarrow ((\forall x)\neg\neg A \Rightarrow (\forall x)A)$ Ax5
- (8) $(\forall x)\neg\neg A \Rightarrow (\forall x)A$ (iz (6) i (7) po MP)
- (9) $((\forall x)\neg\neg A \Rightarrow (\forall x)A) \Rightarrow (\neg(\forall x)A \Rightarrow \neg(\forall x)\neg\neg A)$ (izvod teoreme računa \mathcal{P})
- (10) $\neg(\forall x)A \Rightarrow \neg(\forall x)\neg\neg A$ (iz (8) i (9) po MP).

Napomenimo da su teoreme iskaznog računa \mathcal{P} tautologije pa je svaka zamena iskaznih slova formulama računa \mathcal{K} teorema. (3) i (9) su u stvari, izvodi aksioma \mathcal{P} . (2) je tautologija u \mathcal{P} .

Pogledajmo nekoliko teorema računa \mathcal{K} koje nisu izvodi formula računa \mathcal{P} .

$$(\forall x)(\forall y)A \Leftrightarrow (\forall y)(\forall x)A$$

$$(\forall x)A \Rightarrow (\exists x)A$$

$$(\forall x)(A \wedge B) \Leftrightarrow (\forall x)A \wedge (\forall x)B$$

$$A(t) \Rightarrow (\exists x)A(x) \quad t \text{ je slobodan za } x \text{ u } A$$

$$(\exists x)(\forall y)A \Rightarrow (\forall y)(\exists x)A$$

$$((\forall x)(B \Rightarrow C) \wedge (\forall x)(A \Rightarrow B)) \Rightarrow (\forall x)(A \Rightarrow C)$$

$$(((\forall x)(C \Rightarrow B) \wedge (\forall x)(C \Rightarrow A)) \wedge (\exists x)C) \Rightarrow (\exists x)(A \wedge B)$$

U formalnom zasnivanju običnih matematičkih teorija osnovni značaj ima formulski jezik kvantifikatorskog računa \mathcal{K} . Pri tome, aksiome odgovarajuće formalne teorije su određene formule računa \mathcal{K} . Do njih se dolazi *prevođenjem* teksta prirodnog jezika na formulski jezik računa \mathcal{K} .

PRIMER 2.2. *Tekst:*

1. *Svi racionalni brojevi su realni.*
2. *Nijedan racionalan broj nije realan.*
3. *Neki racionalni brojevi su realni.*
4. *Neki racionalni brojevi nisu realni.*

U formalnoj teoriji realnih brojeva prevod ovog teksta glasi:

1. $(\forall x)(Q(x) \Rightarrow R(x)).$
2. $(\forall x)(Q(x) \Rightarrow \neg R(x)).$
3. $(\exists x)(Q(x) \wedge R(x)).$
4. $(\exists x)(Q(x) \wedge \neg R(x)).$

Jasno, $Q(x)$ i $R(x)$ interpretiramo redom: x je racionalan broj i x je realan broj.

Koristeći teoremu 1.1 prvog poglavlja i činjenicu da je svaka aksioma kvantifikatorskog računa \mathcal{K} valjana formula, lako se dokazuje sledeća teorema.

TEOREMA 2.1. *(Saglasnost teorije \mathcal{K}). Ako je formula teorema teorije \mathcal{K} , onda je ona valjana.*

Teorema 2.1 je obrat *Teoreme kompletnosti* koju je u svojoj doktorskoj tezi 1930. godine dokazao Kurt Gödel. Da bismo dokazali Teoremu kompletnosti, koristićemo sledeću teoremu.

TEOREMA 2.2. *Ako teorija \mathcal{T} ima model, onda je \mathcal{T} neprotivrečna.*

Dokaz: Pretpostavimo suprotno, tj. pretpostavimo da postoji formula A takva da su A i $\neg A$ teoreme teorije \mathcal{T} . Na osnovu teoreme 2.1 formule A i $\neg A$ su valjane što je nemoguće, (na osnovu definicije semantike logike prvog reda). \square

Potpunost ili kompletnost teorije \mathcal{K} dokazaćemo na sledeći način.

TEOREMA 2.3. *(Kompletnost teorije \mathcal{K}) Ako je formula A valjana, onda je ona teorema teorije \mathcal{K} .*

Dokaz: (skica) Dovoljno je razmatrati zatvorene formule jer za svaku formulu F važi da je valjana ako i samo ako je valjana formula $(\forall x)F$. Neka je formula A zatvorena i valjana. Pretpostavimo da A nije teorema teorije \mathcal{K} . Neka je \mathcal{K}' teorija dobijena dodavanjem $\neg A$

kao aksiome teoriji \mathcal{K} . Dokažimo da je teorija \mathcal{K}' neprotivrečna (konzistentna). Pretpostavimo da je teorija \mathcal{K}' protivrečna. Tada postoji formula B takva da važi

$$\vdash_{\mathcal{K}'} B \quad \text{i} \quad \vdash_{\mathcal{K}'} \neg B.$$

Formula $B \Rightarrow (\neg B \Rightarrow A)$ je izvod tautologije iskaznog računa \mathcal{P} pa je teorema teorije \mathcal{K}' , jer u \mathcal{K}' mogu da se dokažu sve teoreme teorije \mathcal{K} .

Iz $\vdash_{\mathcal{K}'} B, \vdash_{\mathcal{K}'} \neg B$ i $\vdash_{\mathcal{K}'} B \Rightarrow (\neg B \Rightarrow A)$ dvostrukom primenom MP dobija se $\vdash_{\mathcal{K}'} A$. $\neg A$ je aksioma \mathcal{K}' , pa je $\neg A \vdash_{\mathcal{K}} A$. Slično iskaznom računu \mathcal{P} , u \mathcal{K} važi *Teorema dedukcije* (koju nismo naveli u ovom radu) pa imamo $\vdash_{\mathcal{K}} \neg A \Rightarrow A$. Formula $(\neg A \Rightarrow A) \Rightarrow A$ je izvod tautologije iz \mathcal{P} , pa je teorema računa \mathcal{K} . Iz $\vdash_{\mathcal{K}} \neg A \Rightarrow A$ i $\vdash_{\mathcal{K}} (\neg A \Rightarrow A) \Rightarrow A$ primenom MP dobija se $\vdash_{\mathcal{K}} A$. Kontradikcija sa pretpostavkom da A nije teorema računa \mathcal{K} . Sledi da je \mathcal{K}' neprotivrečna. Poznati stav logike prvog reda kaže da svaka neprotivrečna teorija ima model (prebrojiv). Dakle, \mathcal{K}' ima model \mathcal{D} . Kako je $\neg A$ aksioma teorije \mathcal{K}' , ona je valjana u \mathcal{D} . A je valjana formula, valjana je i u \mathcal{D} . Međutim, nemoguće je da su A i $\neg A$ istovremeno valjane u \mathcal{D} . Kontradikcija. Sledi da je A teorema teorije \mathcal{K} . \square

Sledeću teoremu dokazao je 1930. godine Gödel.

TEOREMA 2.4. (*Teorema kompaktnosti*) *Teorija \mathcal{T} ima model ako i samo ako svaka konačna teorija $\mathcal{T}' \subseteq \mathcal{T}$ ima model.*

Dokaz:

\mathcal{T} ima model $\Leftrightarrow \mathcal{T}$ je neprotivrečna

\Leftrightarrow svaka konačna teorija $\mathcal{T}' \subseteq \mathcal{T}$ je neprotivrečna

\Leftrightarrow svaka konačna teorija $\mathcal{T}' \subseteq \mathcal{T}$ ima model.

\square

Teorema kompaktnosti ima mnoge primene u matematici. Na primer, teorema daje tzv. *nonstandardne modele* teorije brojeva, realnih brojeva, itd. O ovom će biti reči kasnije.

Prema formalističkom gledištu zasnivanje neke matematičke teorije ne sme da se temelji na intuiciji, već je potrebno stvoriti aksiomatsku bazu i tada je matematička istina jedino što proizilazi iz aksioma bez obzira na značenja takvog tvrđenja. Jezikom formula predikatskog računa uvode se razne tzv. aksiomatske teorije skupova. Te teorije su specijalni kvantifikatorski račun. Međutim, ni za jednu od poznatih aksiomatskih teorija ne znamo da li je neprotivrečna.

GLAVA 3

Jednakosna logika

Specijalni kvantifikatorski račun prvog reda je formalna teorija čije su formule neke od formula računa \mathcal{K} , one u kojima učestvuju samo neke određene ali ne nužno i sve konstante, operacijska i relacijska slova. Aksiome specijalnog računa su, pre svega, one koje proističu iz shema aksioma Ax1, Ax2, Ax3, Ax4, Ax5 i drugo, izvesne *specijalne aksiome*, koje su formule računa \mathcal{K} . Jedina pravila izvođenja su MP i Gen.

Kvantifikatorski račun prvog reda sa jednakošću, je svaki specijalni kvantifikatorski račun prvog reda koji među predikatskim (relacijskim) slovima ima jedno slovo dužine 2, označeno sa \approx . Umesto $\approx (t_1, t_2)$ piše se $t_1 \approx t_2$, i koji među specijalnim aksiomama ima i sledeće formule:

$$t_1 \approx t_1, t_1 \approx t_2 \Rightarrow t_2 \approx t_1, (t_1 \approx t_2 \wedge t_2 \approx t_3) \Rightarrow t_1 \approx t_3,$$

$$(t_1 \approx t'_1 \wedge t_2 \approx t'_2 \wedge \dots \wedge t_j \approx t'_j) \Rightarrow f_i^j(t_1, t_2, \dots, t_j) \approx f_i^j(t'_1, t'_2, \dots, t'_j),$$

$$(t_1 \approx t'_1 \wedge t_2 \approx t'_2 \wedge \dots \wedge t_j \approx t'_j) \Rightarrow R_i^j(t_1, t_2, \dots, t_j) \approx R_i^j(t'_1, t'_2, \dots, t'_j),$$

gde su $t_1, t_2, \dots, t_j, t'_1, t'_2, \dots, t'_j$ termini, f_i^j, R_i^j su operacijska i relacijska slova tog računa.

Jednakosna teorija je specijalni kvantifikatorski račun prvog reda sa jednakošću čije specijalne aksiome su, pored gore navedenih, i formule oblika $t_1 \approx t_2$, koje zovemo *identiteti*.

U slučaju kvantifikatorskih računa prvog reda sa jednakošću uvodimo i tzv. *normalni model* tog računa. To je model u kome se relacijsko slovo \approx interpretira kao jednakost.

Neka su \mathcal{D}_1 i \mathcal{D}_2 modeli računa \mathcal{S} koji imaju redom domene D_1 i D_2 i neka su $d_1, d_2, \dots, d_n \in D_1$. Kažemo da su modeli *izomorfni* ako postoji preslikavanje $f : D_1 \rightarrow D_2$ tako da su ispunjeni uslovi:

1. Ako su relacije R_1 i R_2 interpretacije istog slova dužine n , onda važi $R_1(d_1, d_2, \dots, d_n)$ je tačno ako i samo ako $R_2(f(d_1), \dots, f(d_n))$ je tačno.
2. Ako su operacije g_1 i g_2 interpretacije istog operacijskog slova dužine n , onda važi $g_1(d_1, d_2, \dots, d_n) = d$ ako i samo ako $g_2(f(d_1), \dots, f(d_n)) = f(d)$.
3. Ako su elementi a_1 i a_2 interpretacije istog simbola konstante, onda važi $f(a_1) = a_2$.

Za račun \mathcal{S} kažemo da je *kategoričan* ako su svi njegovi modeli izomorfni.

Kažemo da je \mathcal{S} *neprotivrečan* ako u tom računu ne postoje dve formule A i $\neg A$ takve da su obe teoreme tog računa.

Ako postoji efektivna procedura za utvrđivanje da li je data formula teorema računa (teorije) \mathcal{S} , onda kažemo da je račun \mathcal{S} *odlučiv*, a inače kažemo da je *neodlučiv*.

Svaki od specijalnih računa u vezi je sa izvesnom (neformalnom) matematičkom teorijom. U nekim slučajevima to znači da je, po našem verovanju, model računa \mathcal{S} određen odgovarajućom matematičkom teorijom.

Elementarna teorija grupa \mathcal{G} je specijalan račun prvog reda koji ima relacijsko slovo R_1^2 , u drugoj oznaci \approx , operacijsko slovo f_1^2 i konstantu a_1 . Umesto $f_1^2(t_1, t_2)$ i a_1 pišemo $t_1 + t_2$ i 0 . Specijalne aksiome su

$$\begin{aligned} x + (y + z) &\approx (x + y) + z \\ x + 0 &\approx x \\ (\forall x)(\exists y)(x + y &\approx 0) \\ x &\approx x \\ x \approx y &\Rightarrow y \approx x \\ (x \approx y \wedge y &\approx z) \Rightarrow x \approx z \\ (x_1 \approx y_1 \wedge x_2 &\approx y_2) \Rightarrow x_1 + x_2 \approx y_1 + y_2 \end{aligned}$$

Ovo je račun sa jednakošću. Jedan (normalni) model računa \mathcal{G} određuju

1. Domen je skup celih brojeva.
2. Operacije sabiranja kao interpretacija simbola $+$.
3. Broj 0 kao interpretacija simbola 0 .

Napomenimo da su računi \mathcal{K} i \mathcal{G} neprotivrečni što se lako pokazuje svođenjem na iskazni račun \mathcal{P} koji je neprotivrečan.

Jedna od naših centralnih tema u ovom radu je *Formalna teorija brojeva*.

Formalna teorija brojeva je specijalni račun prvog reda u oznaci \mathcal{N} , koji ima jedno relacijsko slovo R_1^2 , konstantu a_1 i operacijska slova f_1^1, f_1^2, f_1^3 . Umesto $R_1^2, a_1, f_1^1(t_1), f_1^2(t_1, t_2), f_1^3(t_1, t_2)$ pišemo $\approx, 0, t_1', t_1 + t_2, t_1 \cdot t_2$. Specijalne aksiome računa \mathcal{N} jesu:

- (i) $(x \approx y \wedge y \approx z) \Rightarrow x \approx z$
- (ii) $x \approx y \Leftrightarrow x' \approx y'$
- (iii) $x' \not\approx 0 \quad (\neg x' \approx 0)$
- (iv) $x + 0 \approx x$
- (v) $x + y' \approx (x + y)'$
- (vi) $x \cdot 0 \approx 0$

- (vii) $x \cdot y' \approx x + x \cdot y$
 (viii) $(A(0) \wedge (\forall x)(A(x) \Rightarrow A(x'))) \Rightarrow (\forall x)A(x)$,

gde je $A(x)$ proizvoljna formula računa \mathcal{N} . Poslednju formulu zovemo *Aksioma indukcije*. To je u stvari shema-aksioma, jer $A(x)$ može biti proizvoljna formula. Imamo sledeće: ako su $A(0)$ i $(\forall x)(A(x) \Rightarrow A(x'))$ teoreme računa \mathcal{N} , onda je i formula $(\forall x)A(x)$ teorema računa \mathcal{N} . Drugim rečima važi sledeće

$$A(0), (\forall x)(A(x) \Rightarrow A(x')) \vdash (\forall x)A(x).$$

Primetimo da data shema važi za samo prebrojivo mnogo aksioma, dok se matematička indukcija za prirodne brojeve sastoji iz neprebrojivog skupa aksioma (jer se odnosi na sve podskupove skupa prirodnih brojeva). Navedimo bez dokaza neke teoreme računa \mathcal{N} . One su posledica skupa navedenih specijalnih aksioma i aksioma računa \mathcal{K} .

$$\begin{aligned} t_1 \approx t_1, t_1 \approx t_2 \Rightarrow t_2 \approx t_1, (t_1 \approx t_2 \wedge t_2 \approx t_3) \Rightarrow t_1 \approx t_3, \\ (t_1 \approx t_2 \wedge t_3 \approx t_4) \Rightarrow t_1 + t_3 \approx t_2 + t_4, \\ (t_1 \approx t_2 \wedge t_3 \approx t_4) \Rightarrow t_1 \cdot t_3 \approx t_2 \cdot t_4, \end{aligned}$$

gde su t_1, t_2, t_3, t_4 , proizvoljni termovi. Vidimo da je račun \mathcal{N} račun sa jednakošću.

$$\begin{aligned} 0 \cdot t_1 \approx 0, 0 + t_1 \approx t_1, t'_1 \cdot t_2 \approx t_1 + t_1 \cdot t_2, \\ t_1 + t_2 \approx t_2 + t_1, t_1 \cdot t_2 \approx t_2 \cdot t_1, t'_1 + t_2 \approx (t_1 + t_2)', \\ t_1 + (t_2 + t_3) \approx (t_1 + t_2) + t_3, t_1 \cdot (t_2 + t_3) \approx t_1 \cdot t_2 + t_1 \cdot t_3, \\ (t_1 \cdot t_2) \cdot t_3 \approx t_1 \cdot (t_2 \cdot t_3) \\ t_1 + t_2 \approx t_1 + t_3 \Rightarrow t_2 \approx t_3, \\ t_1 + t_2 \approx 0 \Rightarrow (t_1 \approx 0 \wedge t_2 \approx 0) \\ (t_1 \neq 0 \wedge t_2 \cdot t_1 \approx t_3 \cdot t_1) \Rightarrow t_2 \approx t_3, \end{aligned}$$

gde su t_1, t_2, t_3 , proizvoljni termovi. Ove teoreme odgovaraju poznatim svojstvima koje, po našem uverenju, imaju prirodni brojevi $0, 1, 2, 3, \dots$. Da ne bude zabune, u navedenim teoremama računa \mathcal{N} operacijske simbole $+, \cdot, 0$ interpretirali smo obično simbolima $+, \cdot, 0$. Označavamo termove $0, 0', 0'', 0''', \dots$ dogovorno sa $0, \bar{1}, \bar{2}, \bar{3}, \dots$ i zovemo ih *numerali*. U daljem tekstu numerale ćemo zvati *pozitivni celi brojevi*

Uvodimo sledeće definicije:

$$\begin{aligned} t_1 < t_2 \text{ je zamena za } (\exists u)(u \neq 0 \wedge t_1 + u = t_2) \\ t_1 \leq t_2 \text{ je zamena za } t_1 < t_2 \vee t_1 = t_2 \\ t_1 > t_2 \text{ je zamena za } t_2 < t_1 \\ t_1 \geq t_2 \text{ je zamena za } t_2 \leq t_1 \\ t_1 | t_2 \text{ je zamena za } (\exists u)(t_2 \approx t_1 \cdot u), \end{aligned}$$

gde su t_1, t_2 termovi i gde je u prva promenljiva u nizu $x, y, z, x_1, y_1, z_1, \dots, x_n, y_n, z_n \dots$ koja ne učestvuje u t_1 ni u t_2 . Tada su sledeće formule teoreme računa \mathcal{N} :

$$\begin{aligned}
t_1 + \bar{1} &\approx t'_1, \quad t_1 \cdot \bar{1} \approx t_1, \quad t_1 \cdot \bar{2} \approx t_1 + t_1 \\
t_1 \cdot \bar{3} &\approx (t_1 + t_1) + t_1, \dots \\
t_1 + t_2 \approx \bar{1} &\Rightarrow (t_1 \approx 0 \wedge t_2 \approx \bar{1}) \vee (t_1 \approx \bar{1} \vee t_2 \approx 0) \\
t_1 \cdot t_2 \approx \bar{1} &\Rightarrow (t_1 \approx \bar{1} \wedge t_2 \approx \bar{1}) \\
0 < \bar{1}, \quad \bar{1} < \bar{2}, \quad \bar{2} < \bar{3}, \dots \\
\neg(t_1 < t_1), \quad (t_1 < t_2 \wedge t_2 < t_3) &\Rightarrow t_1 < t_3 \\
t_1 < t_2 &\Rightarrow t_1 + t_3 < t_2 + t_3 \\
t_1 \leq t_2 &\Rightarrow (t_1 + t_3 \leq t_2 + t_3) \\
(t_1 \leq t_2 \wedge t_2 < t_3) &\Rightarrow t_1 < t_3 \\
t_1 \leq t'_1 \\
t_1 \approx t_2 \vee t_1 < t_2 \vee t_1 > t_2 \\
t_1 \leq t_2 \vee t_2 \leq t_1 \\
t_1 \not\approx 0 &\Leftrightarrow t_1 > 0 \\
(t_1 > 0 \wedge t_2 > 0) &\Rightarrow t_1 \cdot t_2 > 0 \\
(t_1 \leq t_2 \wedge t_2 \leq t_1) &\Rightarrow t_1 \approx t_2,
\end{aligned}$$

t_1, t_2 i t_3 su termovi. Naravno, navedeni skup teorema se lako može proširiti sve novim i novim teoremama, inspirišući se onim što smatramo da ispunjavaju prirodni brojevi $0, 1, 2, 3, \dots$. Važe poznate binomne formule

$$\begin{aligned}
(x + y)^2 &\approx x^2 + 2xy + y^2, \\
(x + y)^3 &\approx x^3 + 3x^2y + 3xy^2 + y^3, \\
&\vdots
\end{aligned}$$

Jasno, x^3 je zamena za $(x \cdot x) \cdot x$ itd, što je jednoznačno određeno prema gornjim teoremama.

Sve ovo iskazano navodi na pomisao da račun \mathcal{N} dobro odgovara sistemu naših prirodnih brojeva, odnosno da mu potpuno opisuje sva svojstva. Istina je mnogo komplikovanija. O ovome će biti reči kasnije.

Verujemo da skup prirodnih brojeva $0, 1, 2, 3, \dots$ u odnosu na operacije sabiranja, množenja i $'$ za koju je $x' = x + 1$, čini normalni model računa \mathcal{N} , ako se njegovi simboli $+, \cdot, '$ intepretiraju kao pomenute operacije i ako se konstanta 0 interpretira kao broj 0 . Skup prirodnih brojeva zovemo *standardni model*. Svaki drugi neizomorfni

sa njim normalni model računa \mathcal{N} zovemo *nestandardni* model računa \mathcal{N} . Videćemo da takvi modeli postoje. Verujući da je standardni model model računa \mathcal{N} , zaključujemo da je račun \mathcal{N} neprotivrečan jer je svaki specijalni kvantifikatorski račun prvog reda, koji ima model, neprotivrečan.

Postoji dokaz neprotivrečnosti računa \mathcal{N} , bez poziva na model, jedino pomoću meta-teorije koji sadrži veliki deo teorije skupova (teoriju ordinalnih brojeva). Prvi takav dokaz dao je Gerhard Gentzen (1909-1945) 1936. godine.

TEOREMA 3.1. *Neprotivrečan račun sa jednakošću ima konačan ili prebrojiv model.*

Dokaz se bazira na stavu koji kaže da svaki neprotivrečan specijalni kvantifikatorski račun \mathcal{S} prvog reda ima prebrojiv model \mathcal{M} . Dokaz ovog stava je izostavljen jer je tehnički zahtevan i prevazilazi glavnu temu ovog rada. Relacija \approx , prema definiciji računa sa jednakošću, ima svojstva

$$x \approx x, \quad x \approx y \Rightarrow y \approx x, \quad (x \approx y \wedge y \approx z) \Rightarrow x \approx z.$$

Ovo znači da je \approx relacija ekvivalencije u modelu \mathcal{M} . Označimo sa \bar{a} klasu ekvivalencije elementa a , a sa $\bar{\mathcal{M}}$ skup svih klasa ekvivalencije. Skup $\bar{\mathcal{M}}$ je konačan ili prebrojiv. Neka su f, R interpretacije u modelu \mathcal{M} redom za operacijski simbol f dužine (arnosti) m i relacijsko slovo R dužine n . U skupu $\bar{\mathcal{M}}$ definišemo operaciju

$$\begin{aligned} \bar{f}(\bar{a}_1, \bar{a}_2, \dots, \bar{a}_m) &= \overline{f(a_1, a_2, \dots, a_m)} \\ \bar{R}(\bar{a}_1, \bar{a}_2, \dots, \bar{a}_n) &= \overline{R(a_1, a_2, \dots, a_n)}. \end{aligned}$$

Neposredno zaključujemo da je $\bar{\mathcal{M}}$ normalni model računa \mathcal{S} , smatrajući da su \bar{f}, \bar{R} interpretacije f i R i da je interpretacija ma koje konstante a jednaka \bar{a} .

Pretpostavimo da je standardni model model računa \mathcal{N} . Koristeći teoremu 3.1 dokazujemo sledeće.

TEOREMA 3.2. *Račun \mathcal{N} ima nestandardni model.*

Dokaz: Formiramo novi račun \mathcal{N}' dodavanjem konstante a_2 i aksioma

$$a_2 \not\approx 0, \quad a_2 \not\approx \bar{1}, \quad a_2 \not\approx \bar{2}, \dots, a_2 \not\approx \bar{n}, \dots$$

U aksiome ubrajamo i aksiome koji proističu iz Ax1 - Ax5 tako što dozvoljavamo mogućnost da u formuli $A(x)$ figuriše i konstanta a_2 . Račun \mathcal{N}' je neprotivrečan. Zaista, ako je obrnuto, tj. \mathcal{N}' protivrečan, onda u njemu postoji izvođenje B_1, B_2, \dots, B_n za neku njegovu formulu $A \wedge \neg A$.

Neka je \bar{m} jedan numeral koji ne učestvuju u tom izvođenju i neka je B'_1, B'_2, \dots, B'_n niz formula koji se dobija kad se u izvođenju B_1, B_2, \dots, B_n a_2 zameni u svakoj formuli sa \bar{m} . Taj niz je izvođenje neke formule $A' \wedge \neg A'$. Kako je \mathcal{N} po pretpostavci neprotivrečan račun, dolazimo do kontradikcije. Dakle, račun \mathcal{N}' ima normalni model \mathcal{M} . Taj model nije izomorfan sa standardnim modelom, jer ne postoji nijedan broj koji je različit od svih prirodnih brojeva. \square

Račun \mathcal{N} se u literaturi naziva *Peanova aritmetika* (Giuseppe Peano (1858-1932)). Aksiomatizacija aritmetike je provedena polovinom 19. veka, a poznata je kao *Peanova aksiomatika*. Dva su izvora Peanove aksiomatike. Sam Peano kaže da je imao veliku korist od rada Dedekinda [4] (prevod ovog rada je objavio Matematički institut SANU, [5]) i da se obilato služio radom Hermanna Grassmana (1809-1877), u stvari knjigom [14]. Upravo je Grassmann izdvojio osnovne aritmetičke pojmove dovoljne za građenje deduktivnog sistema aritmetike. Tema njegovog rada su zapravo celi brojevi. Lako se uočava kako se Grassmannova metoda može prilagoditi izgradnji teorije prirodnih brojeva.

Dedekindov rad je nešto više od aksiomatike. Koji osnovni pojmovi i koja njihova svojstva omogućuju izgradnju deduktivnog sistema aritmetike nije Dedekindovo osnovno pitanje. Njegovo osnovno pitanje je bilo: Šta je broj? Njega ne zadovoljava intuicija prirodnog broja, ali ne zato što je varljiva i nesigurna, nego zato što je smatrao da je može svesti na jednu bitniju intuiciju - logičku intuiciju, koja i jeste pretpostavka svake deduktivne nauke.

Aksiomatika se pojavljuje tamo gde je intuicija poljuljana i nesigurna, tamo gde je treba staviti pod vlast logike.

Pre ili kasnije, sva matematička znanja postaju predmetom aksiomatske metode. Interesnatno je da se aksiomatizacija geometrije dogodila dve hiljade godina pre aritmetičke aksiomatizacije. Izgleda da su razlozi kasne aksiomatizacije aritmetike prilično jasni. Naime, pojam, prirodnog broja i upotreba aritmetičkih operacija toliko su jasni da nije bilo nikakve potrebe da se još jasnije ekspliciraju i ograniče upotrebom aksioma.

Intuicija prostora bila je teško poljuljana učenjem Elejaca koji su se neposredno suprotstavili logici, dokazujući nemogućnost deljenja prostora. Setimo se Zenonove priče o Ahilu i kornjači. Grčka se misao prilagodila logici. Možemo reći da osećamo da su neka tvrđenja o prostornim odnosima istinita, ali smo potpuno svesni varljivosti naših intuicija i zato ih podređujemo logici.

Peano je izvanredno dobro upozorio na varljivost intuicije odnosno dobro upozorio na varljivost shvatanja osnovnih matematičkih entiteta konstruišući krivu koja ispunjava dvodimenzionalnu oblast.

Nekoliko reči o indukciji. Blaise Pascal (1623-1662) je posle 1654. godine eksplicitno formulisao dva pravila za dokaz indukcijom, osnovu (bazu) i indukcijski korak (indukcijsku hipotezu). Ovi rezultati su publikovani 1665. godine. Ova tehnika se malo koristila. Primeri se mogu naći kod Pier de Fermata (1601-1665) i povremeno kod Leonharda Eulera (1707-1783). Kada je imenovana kao takva, ono što zovemo indukcija pripisivano je Jacobu Bernoulliju (1655-1705) i zvala se *prelaz od n ka $n + 1$* ili Bernoullijev metod. Krajem 18. veka Abraham Kästner (1719-1800) skreće pažnju na indukciju i neko vreme indukcija dobija ime *Kästnerov* metod. Carl Jacobi (1804-1851) 1826. godine, govoreći o nekim rezultatima Karla Gaussa (1777-1855), govori da Gauss koristi Kästnerov metod dokazivanja. 1830. godine George Peacock (1791-1858) naziva indukciju *demonstrativna indukcija*. De Morgan naziva indukciju *Matematička indukcija*.

1889. godine Peano štampa rad *Arithmetices principia, nova methodo exposita*. Neki istoričari insistiraju na nazivu *Dedekind-Peano aksiome*. Poznati logičar, Hao Wang (1921-1995), na primer, je tvrdio da je sam Peano rekao da je svoje aksiome preuzeo od Dedekinda. Kao izvor svog tvrđenja Wang uzima Philipa Jourdaina (1879-1919) iz 1912. [24]. Međutim, Jourdain ništa slično ne tvrdi u navedenom radu. Jourdain samo tvrdi da Peano priznaje da je imao veliku korist od Dedekindovog eseja, [26].

Pojavom paradoksa u Teoriji skupova, otkrivenih od strane Cesare Burali-Fortija (1861-1931) i Russella, Peano kaže:

Ali dokaz da je sistem aksioma aritmetike, ili geometrije, neprotivrečan nije po mom mišljenju neophodan. Mi ne stvaramo aksiome proizvoljno, mi radije podrazumevamo kao aksiome najjednostavnije propozicije koje nalazimo, eksplicitno napisane ili implicitno, u našem tretiranju aritmetike ili geometrije. Naša analiza principa ovih nauka sastoji se u reduciranju opštih tvrđenja na minimalan broj neophodnih i dovoljnih uslova. Sistem aksioma aritmetike ili geometrije zadovoljen je idejom broja ili tačke, podržan od strane bilo koga ko piše aritmetiku ili geometriju. Imamo ideju broja, dakle broj postoji.

Ovo su upravo platonističke ideje o matematičkom svetu ideja koji po Platonu postoji. Najpoznatiji platonista, bar u jednom periodu svog života, bio je Gödel.

Pokažimo, na primer, da je u Formalnoj teoriji brojeva,

$$\bar{2} + \bar{2} \approx \bar{4}.$$

Dokaz bi mogao da izgleda ovako:

$$\begin{aligned}
\bar{2} + \bar{2} &\approx \bar{2} + \bar{1}' && \text{(po definiciji jer je } \bar{2} \approx \bar{1}') \\
&\approx (\bar{2} + \bar{1})' && \text{(primenom specijalnog aksioma (v))} \\
&\approx (\bar{2} + 0')' && \text{(jer je } \bar{1} \approx 0') \\
&\approx ((\bar{2} + 0)')' && \text{(primenom (v), } x \text{ je } \bar{2}, y \text{ je } 0) \\
&\approx (\bar{2}')' && \text{(primenom } x + 0 \approx x, x \text{ je } \bar{2}) \\
&\approx (\bar{3}') && \text{(jer je } \bar{2}' \approx \bar{3}) \\
&\approx \bar{4} && \text{(jer je } \bar{3}' \approx \bar{4}).
\end{aligned}$$

Ova činjenica se često koristi u običnom govoru da se naglasi sigurnost, odnosno preciznost matematike.

Pogledajmo tvrđenje

$$0 + x \approx x,$$

gde je x ma koji numeral. Napomenimo da komutativnost nije specijalni aksiom, pa ne možemo da koristimo aksiomu (iv). Dokaz izgleda ovako:

Neka je $\mathcal{O}(x)$ oznaka za formulu $0 + x \approx x$. Koristimo indukciju. Baza indukcije je $0 + 0 \approx 0$, što je tačno na osnovu (iv) za $x = 0$. Indukcijski korak Formule $\mathcal{O}(x)$ i $\mathcal{O}(x')$ redom glase:

$$0 + x \approx x, \quad 0 + x' \approx x'.$$

Koristeći prvu kao hipotezu, neposredno dobijmo

$$\begin{aligned}
0 + x' &\approx (0 + x)' && \text{(prema (v))} \\
&\approx x' && \text{(indukcijska hipoteza, odnosno formula} \\
&&& \mathcal{O}(x) = 0 + x \approx x),
\end{aligned}$$

pa je jednakost $0 + x' \approx x'$ dokazana. Na osnovu (viii) imamo

$$\mathcal{O}(0) \wedge (\forall x)(\mathcal{O}(x) \Rightarrow \mathcal{O}(x')) \Rightarrow (\forall x)\mathcal{O}(x),$$

pa je navedeno tvrđenje teorema \mathcal{N} . Ovde smo izostavili formalni dokaz, koji pored specijalnih aksioma koristi i pravila izvođenja i aksiome kvantifikatorskog računa, koje važe u svim teorijama, kao univerzalni zakoni logike.

Koristeći prethodno, dokazujemo zakon komutativnosti za \mathcal{N} :

$$x + y \approx y + x.$$

Označimo ovu formulu sa $C(y)$. Tada $C(0)$ glasi $x + 0 \approx 0 + x$ i to je tačan identitet. Polazeći od $C(y)$ za $C(y')$ imamo

$$\begin{aligned} x + y' &\approx (x + y)' \quad (\text{po (v)}) \\ &\approx (y + x)' \quad (\text{po } C(y), \text{ tj. induksijskoj hipotezi}) \\ &\approx y' + x \quad (\text{jer se lako dokazuje } x' + y \approx (x + y)'). \end{aligned}$$

Pored principa matematičke indukcije navodimo ekvivalente ovog principa koje u ovom radu nećemo dokazivati.

$$[A(0) \wedge (\forall x)((\forall y < x)A(y) \Rightarrow A(x))] \Rightarrow (\forall x)A(x).$$

Ovo je tzv. princip *potpune matematičke indukcije*. Drugi ekvivalent principa indukcije glasi

Svaki neprazan podskup S skupa \mathbb{N} prirodnih brojeva ima minimalni element.

Naravno, sve ovo je izrečeno u meta-jeziku teorije \mathcal{N} .

Jednakost je izraz koji se koristi za termove bez promenljivih interpretiranih u domenu modela. Ovo je nasleđeno iz starih radova iz oblasti logike. Radi se o *identitetima*.

3.1. Klase algebri definisnih jednakostima

Algebra A je uređen par (A, \mathcal{F}) , gde je $A \neq \emptyset$ neprazan skup, a \mathcal{F} konačan ili beskonačan skup operacija (preslikavanja) na A . Neka je

$$f : \underbrace{A \times A \times \dots \times A}_n \rightarrow A.$$

Kažemo da je f n -arna operacija algebre A . Identiteti su formule oblika

$$t_1 \approx t_2,$$

koje interpretirane u modelu A postaju tačne jednakosti. Ovakve formule se zovu *zakoni* u klasama algebri. Na primer

$$(x + y) + z \approx x + (y + z)$$

je zakon asocijativnosti koji važi u algebri $\mathbf{N} = (\mathbb{N}, +, \cdot)$, tj. u prirodnim brojevima. Navodimo primere algebri koje su upravo određene svojim zakonima.

Prsteni. Označimo sa \mathcal{R} teoriju prstena u jeziku $\mathcal{L}_{\mathcal{R}} = \{+, \cdot, -, 0, 1\}$, gde su $+$ i \cdot binarni operacijski znaci, $-$ unarna i $0, 1$ nularne operacijske konstante. Aksiome su

- R1. $x + 0 \approx x$ (aditivna jedinica)
- R2. $x + (-x) \approx 0$ (aditivan inverz)
- R3. $x + y \approx y + x$ ($+$ je komutativan)
- R4. $x + (y + z) \approx (x + y) + z$ ($+$ je asocijativan)

- R5. $x \cdot 1 \approx x$ (desna multiplikativna jedinica)
 R6. $1 \cdot x \approx x$ (leva multiplikativna jedinica)
 R7. $x \cdot (y \cdot z) \approx (x \cdot y) \cdot z$ (\cdot asocijativnost)
 R8. $x \cdot (y + z) \approx (x \cdot y) + (x \cdot z)$ (leva distributivnost)
 R9. $(x + y) \cdot z \approx (x \cdot z) + (y \cdot z)$ (desna distributivnost)

Sve algebre $\mathbf{R} = (R, +, \cdot, -, 0, 1)$ koje zadovoljavaju aksiome računa \mathcal{R} zovu se prstenovi. R1. - R9. se zovu *skup aksioma* ili skup *definišućih relacija*. To su zakoni koje zadovoljavaju svi prsteni. Primitimo da su R1., R2., R3., R4. zakoni koji određuju da li je neka struktura aditivna (komutativna) grupa. R5, R6. i R7. određuju tzv. *klasu monoida*.

Najočigledniji primeri prstena dolaze iz brojevni struktura i matrica.

- (beskonačni brojevni sistemi) $(\mathbb{Z}, +, \cdot, -, 0, 1)$, $(\mathbb{Q}, +, \cdot, -, 0, 1)$, $(\mathbb{R}, +, \cdot, -, 0, 1)$, $(\mathbb{C}, +, \cdot, -, 0, 1)$ - radi se o prstenima celih brojeva, racionalnih brojeva, realnih brojeva, kompleksnih brojeva.
- (konačni brojevni sistemi) $(\mathbb{Z}_n, +, \cdot, -, 0, 1)$ prsten celih brojeva modulo n .
- $(\mathbb{Z}[i], +, \cdot, -, 0, 1)$, gde je $i = \sqrt{-1}$. Ovaj prsten se naziva Gaussov prsten celih brojeva. Elementi Gaussovog prstena celih brojeva izgledaju ovako:

$$\{m + in \mid m, n, \in \mathbb{Z}\}.$$

- $(M_{n \times n}(\mathbb{R}), +, \cdot, -, O, E)$ prsten matrica formata $n \times n$ sa realnim sadržajem (realnih matrica).

Booleove algebre. (George Boole (1818-1865)) Označimo klasu svih Booleovih sa \mathcal{BA} . Jezik teorije Booleovih algebri dat je sa $\mathcal{L}_{\mathcal{BA}} = \{\wedge, \vee, ', 0, 1\}$, gde su \wedge i \vee binarni operacijski simboli, $'$ je unarni simbol i 0, 1 konstante. Teorija \mathcal{BA} je data sledećim aksiomama.

- B1. $x \vee y \approx y \vee x$ (\vee komutativna)
 B2. $x \wedge y \approx y \wedge x$ (\wedge komutativna)
 B3. $x \vee (y \vee z) \approx (x \vee y) \vee z$ (asocijativnost \vee)
 B4. $x \wedge (y \wedge z) \approx (x \wedge y) \wedge z$ (asocijativnost \wedge)
 B5. $x \wedge (x \vee y) \approx x$ (zakon apsorpcije za \wedge)
 B6. $x \vee (x \wedge y) \approx x$ (zakon apsorpcije za \vee)
 B7. $x \wedge (y \vee z) \approx (x \wedge y) \vee (x \wedge z)$ (distributivnost \wedge u odnosu na \vee)
 B8. $x \vee x' \approx 1$
 B9. $x \wedge x' \approx 0$
 B10. $x \vee 1 \approx 1$
 B11. $x \wedge 0 \approx 0$

Sve algebre $\mathbb{B} = (B, \vee, \wedge, ', 0, 1)$ koje zadovoljavaju aksiome \mathcal{BA} zovu se Booleove algebre. Jedna od interesantnih teorema o Booleovim algebrama je ona koja kaže da nosači konačnih Booleovih algebri moraju biti kardinalnosti stepena 2, tj. mogu imati 1, 2, 4, 8, ... itd. elemenata, ali ne mogu imati 3 elementa ili 12 itd.

Konačne algebre predstavljamo tzv. tablicama operacija Arthura Cayleya (1821-1895), kada je reč o unarnim i binarnim operacijama. Manje se koriste Cayleyjeve tablice za operacije arnosti veće od 3.

$$\mathcal{B}_2 \quad \begin{array}{c|cc} \vee & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 1 \end{array} \quad \begin{array}{c|cc} \wedge & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 1 \end{array} \quad \begin{array}{c|c} ' & \\ \hline 0 & 1 \\ 1 & 0 \end{array}$$

$$\mathcal{B}_4 \quad \begin{array}{c|cccc} \vee & 0 & 1 & a & b \\ \hline 0 & 0 & 1 & a & b \\ 1 & 1 & 1 & 1 & 1 \\ a & a & 1 & a & 1 \\ b & b & 1 & 1 & b \end{array} \quad \begin{array}{c|cccc} \wedge & 0 & 1 & a & b \\ \hline 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & a & b \\ a & 0 & a & a & 0 \\ b & 0 & b & 0 & b \end{array} \quad \begin{array}{c|c} ' & \\ \hline 0 & 1 \\ 1 & 0 \\ a & b \\ b & a \end{array}$$

Primetimo da se komutativnost algebre u Caylyjevim tablicama ispoljava kao simetrija u odnosu na *glavnu dijagonalu* tablice. Interesantno je da nemamo još uvek jednostavan geometrijski prikaz asocijativnosti. Najpoznatiji primeri Booleovih algebri su skupovne Booleove algebre. To su algebre oblika

$$\mathbf{Su}(U) = (Su(U), \cup, \cap, ', \emptyset, U)$$

gde je \cup interpretacija \vee , \cap interpretacija \wedge , komplement interpretacija $'$ i \emptyset , U redom prazan skup i ceo skup U , kao interpretacije 0 i 1. Često je lakše proveriti valjanost nekih zakona Booleovih algebri na skupovima nego sintaksički tražiti izvođenja. Naime, ako zakon ne važi, to se lakše konstatuje preko skupova, koristeći John Vennove (1834-1923) dijagrame. Algebre koje imaju samo jednu binarnu operaciju nazivaju se *grupoidi*. Odmah primećujemo da je broj četvoroelementnih grupoida

$$4^{16} = 4294967296.$$

Naravno, postavlja se pitanje koliko ima neizomorfnih grupoida. Što se zakona tiče, u algebri se izomorfne algebre poistovećuju. Na primer grupoidi dati tablicama

$$\begin{array}{c|cc} & a & b \\ \hline a & a & a \\ b & a & b \end{array} \quad \begin{array}{c|cc} & a & b \\ \hline a & a & b \\ b & b & b \end{array}$$

su jasno izomorfni. Drugim rečima, drugi grupoid smo mogli predstaviti tablicom

$$\begin{array}{c|cc} & b & a \\ \hline b & b & b \\ a & b & a \end{array}$$

Neki skup aksioma, za bilo koju klasu algebri, nazivamo *nezavisan*, ako se nijedan aksiom datog skupa ne može dobiti kao sintaksička posledica preostalog skupa aksioma.

Najmanji skup identiteta neke algebre, čija sintaksička posledica su svi zakoni date algebre, se naziva *baza identiteta* algebre. U primerima koje smo naveli, sem \mathbf{N} , baze identiteta su konačne. Da li postoje konačne algebre sa beskonačnom bazom identiteta? Odgovor je potvrđan. Pronađeno je nekoliko najjednostavnijih binarnih algebri čiji nosači imaju samo 3 elementa i koje nemaju konačnu bazu identiteta. Evo nekoliko primera:

$$\begin{array}{c|ccc} G_1 & a & b & c \\ \hline a & a & b & b \\ b & b & b & c \\ c & b & c & c \end{array} \quad \begin{array}{c|ccc} G_2 & a & b & c \\ \hline a & a & c & b \\ b & c & b & c \\ c & b & c & c \end{array} \quad \begin{array}{c|ccc} G_3 & a & b & c \\ \hline a & a & b & b \\ b & c & b & c \\ c & b & c & c \end{array}$$

Interesantno je da sva tri navedena grupoida zadovoljavaju zakon $x^2 \approx x$, dok su G_1 i G_2 još i komutativni. Više o ovome može se videti u radu [23]. Svi dvoelementni grupoidi imaju konačnu bazu identiteta. Ovo je dokazao Roger Lyndon (1917-1988), [29]. Prvi troelementni grupoid sa beskonačnom bazom identiteta pronašao je V. L. Murskii 1970. godine.

Ako grupoid zadovoljava zakon asocijativnosti onda ga nazivamo *polugrupa* ili *semigrupa*. Najmanja polugrupa koja nema konačnu bazu identiteta ima 6 elemenata. Ovu polugrupu pronašao je P. Perkins u radu [36]. Sve polugrupe koje imaju manje od 6 elemenata imaju konačnu bazu. Ovo je dokazao Avraham Trahtman (1944-) u radu [42].

Sve konačne grupe imaju konačne baze identiteta. Ovo su dokazali S. Oates i M.B. Powell u radu [32].

Takođe, svi konačni prsteni imaju konačnu bazu identiteta. Ovo su dokazali R.L.Kruse u radu [25] i I.V. Lvov u radu [28].

O problemima konačnosti baze identiteta možemo se informisati iz knjige profesora Petra Markovića [35]. Grana algebre koja se bavi problemima vezanim za zakone algebarskih struktura i mnogim drugim pitanjima vezanim za logiku i filozofiju algebre naziva se *Univerzalna algebra*.

Postavlja se pitanje da li data konačna algebra \mathbf{A} ima konačnu bazu identiteta. Alfred Tarski je 1960-tih godina postavio pitanje:

Da li postoji algoritam koji, kada je efektivno data konačna algebra \mathbf{A} , odlučuje da li \mathbf{A} ima konačnu bazu identiteta (i moguće da nađe bazu, ako postoji).

Vodeći matematičar u oblasti Univerzalne algebre Ralph McKenzie (1941-) je dokazao u radu [31] da takav algoritam ne postoji. Dokaz se bazira na neodlučivosti *holting* problema Turingove mašine tj. nerešivosti problema zaustavljanja proizvoljne Turingove mašine.

3.2. Srednjoškolski problem Tarskog

Centralni deo ovog rada je tzv. *Srednjoškolski problem Tarskog*, u originalu *Tarski's High School Algebra Problem*.

Šezdesetih godina prošlog veka Alfred Tarski je primetio da postoji samo jedanaest osnovnih identiteta koji važe u algebri pozitivnih celih brojeva \mathbf{N}^+ i čija posledica bi bili svi zakoni koji važe na \mathbf{N}^+ . Ove zakone učimo u osnovnoj i srednjoj školi. Tarski ih je nazvao *High School Identities*, skraćeno *HSI* :

- (1) $x + y \approx y + x$
- (2) $x + (y + z) \approx (x + y) + z$
- (3) $x \cdot 1 \approx x$
- (4) $x \cdot y \approx y \cdot x$
- (5) $x \cdot (y \cdot z) \approx (x \cdot y) \cdot z$
- (6) $x \cdot (y + z) \approx x \cdot y + x \cdot z$
- (7) $1^x \approx 1$
- (8) $x^1 \approx x$
- (9) $x^{y+z} \approx x^y \cdot x^z$
- (10) $(x \cdot y)^z \approx x^z \cdot y^z$
- (11) $(x^y)^z \approx x^{y \cdot z}$.

Identiteti (1) do (6) se označavaju sa \overline{HSI} i uključuju samo operacijske simbole $+$, \cdot , 1 .

DEFINICIJA 3.1. *Neka je \mathcal{L} jezik $\mathcal{L} = \{+, \cdot, \uparrow, 1\}$. Algebra \mathbf{A} koja zadovoljava identitete (1) - (11) naziva se *HSI-algebra*. Umesto $a \uparrow b$ pišaćemo a^b .*

Primetimo da je $\mathbf{N}^+ = (\mathbf{N}^+, +, \cdot, \uparrow, 1)$, gde je \mathbf{N}^+ skup pozitivnih celih brojeva, *HSI-algebra*.

DEFINICIJA 3.2. *Neka je $\overline{\mathcal{L}} = \{+, \cdot, 1\}$. $\overline{\mathcal{L}}$ -algebra \mathbf{A} koja zadovoljava \overline{HSI} naziva se \overline{HSI} -algebra.*

U \overline{HSI} ili *HSI*-algebri \mathbf{A} pišemo n umesto $\underbrace{1 + 1 + \dots + 1}_n$.

Jasno, $\overline{\mathbf{N}^+} = (\mathbf{N}^+, +, \cdot, 1)$ je \overline{HSI} -algebra. Takođe, ako je \mathbf{A} HSI -algebra, onda je $\overline{\mathbf{A}} = (A, +, \cdot, 1)$, gde su $+$, \cdot , 1 isti kao u \mathbf{A} , \overline{HSI} -algebra.

U stvari, identiteti HSI izolovani su u poznatom radu [4], Dedekinda iz 1888. godine. Dedekind je dokazao da oni slede iz Peanovih aksioma.

Kada govorimo o HSI identitetima, važi sledeće:

- (i) Postoji mnogo vrlo malih modela HSI .
- (ii) Postoje tačni identiteti u \mathbf{N}^+ koji se ne mogu izvesti iz HSI .

Kad radimo sa jednakosnom teorijom čiji je model $\overline{\mathbf{N}^+}$ imamo korisnu činjenicu da svaki $\overline{\mathcal{L}}$ -term t ima prostu *normalnu formu* $v(t)$, koju zovemo *polinom*. Sve normalne forme tj. svi polinomi su posledice \overline{HSI} .

- TEOREMA 3.3. (a) *Jednakosna teorija čiji su specijalni aksiomi (1)-(6) je odlučiva.*
 (b) *Svi identiteti koji važe u $\overline{\mathbf{N}^+}$ mogu se izvesti iz \overline{HSI} .*

Dokaz: (a) Neka je $t_1 \approx t_2$ identitet u jeziku $\overline{\mathcal{L}}$. Pomoću \overline{HSI} (1)-(6) odredimo normalne forme $v(t_1)$ i $v(t_2)$. Tada, ako je $v(t_1) = v(t_2)$, identitet $t_1 \approx t_2$ je posledica (1)-(6). Ako je $v(t_1) \neq v(t_2)$ identitet $t_1 \approx t_2$ se ne može izvesti iz (1)-(6).

(b) Neka je Σ skup $\overline{\mathcal{L}}$ -identiteta koji se mogu izvesti iz \overline{HSI} . Kako je $\overline{\mathbf{N}^+}$ model od \overline{HSI} , sledi da je Σ podskup svih identiteta koji važe u $\overline{\mathbf{N}^+}$. Neka $t_1 \approx t_2$ važi u $\overline{\mathbf{N}^+}$. Koristeći \overline{HSI} možemo naći normalne forme za t_1 i t_2 i to onda daje izvođenje za $t_1 \approx t_2$. \square

Međutim, kada gledamo HSI i \mathbf{N}^+ nemamo više takvih normalnih formi. Situacija postaje mnogo komplikovanija zbog operacije \uparrow .

Prirodni modeli od \overline{HSI} su pozitivni racionalni i realni brojevi. Međutim, kad tražimo prirodne modele od HSI ove mogućnosti nestaju. Na primer, pozitivni racionalni brojevi nisu zatvoreni za stepenovanje \uparrow . $\sqrt{2}$ nije racionalan broj.

U literaturi je kao prvi relevantan rad koji se odnosi na Problem Tarskog rad [6].

Srednjoškolski problem Tarskog glasi:

Da li su svi identiteti koji važe u algebri \mathbf{N}^+ sintaksička posledica HSI ?

Odgovor je negativan. Problem je rešio Alex J. Wilkie (1948-), 1980. godine u rukopisu [45]. Wilkie je pronašao formulu u jeziku \mathcal{L} koja je tačna u \mathbf{N}^+ , ali ne može da se izvede iz HSI . Navodimo

Wilkiev identitet $W(x, y)$:

$$\begin{aligned} & ((1+x)^y + (1+x+x^2)^y)^x \cdot ((1+x^3)^x + (1+x^2+x^4)^x)^y \approx \\ & ((1+x)^x + (1+x+x^2)^x)^y \cdot ((1+x^3)^y + (1+x^2+x^4)^y)^x. \end{aligned}$$

Da bismo videli da je ovaj identitet tačan u \mathbf{N}^+ primetimo sledeće

$$\begin{aligned} 1+x^3 & \approx (1+x) \cdot (1-x+x^2) \\ 1+x^2+x^4 & \approx (1+x+x^2) \cdot (1-x+x^2) \end{aligned}$$

Označimo sa $A = 1+x$, $B = 1+x+x^2$, $C = 1-x+x^2$. Tada Wilkijev identitet postaje

$$\begin{aligned} & (A^y + B^y)^x \cdot ((A \cdot C)^x + (B \cdot C)^x)^y \approx \\ & (A^x + B^x)^y \cdot ((A \cdot C)^y + (B \cdot C)^y)^x, \end{aligned}$$

što je očigledno tačno, tj. leva i desna strana su identične. Naime, leva i desna strana Wilkiejevog identiteta pomnožena je sa C^{xy} .

Međutim, ovaj identitet se ne može izvesti iz *HSI*. Problem je polinom $C = 1-x+x^2$. Naravno, znak oduzimanja, $-$, u C nije u jeziku \mathcal{L} . Pitanje je da li možda postoji neko drugo C koje bi bilo u jeziku \mathcal{L} . Wilkie je pokazao da ne postoji. Nepostojanje C ne znači da se identitet ne može dokazati na neki drugi način semantički ili čak sintaksički. Wilkie je pokazao da se njegov identitet nikako ne može izvesti iz *HSI*.

Čovek koji je na elementaran način približio problem genijalnog Alfreda Tarskog široj publici je profesor Univerziteta Waterloo u Kanadi Stanley Burris, u radu [2]. Pre ovog rada S. Burris i S. Lee su objavili interesantan rad [1] u kome su navedeni mali modeli *HSI* identiteta. Sledio je rad [3] u kome je konstruisana algebra u kojoj su važili *HSI*, a nije važio Wilkijev identitet $W(x, y)$ i koja je imala 12 elemenata.

Postavlja se pitanje da li su nas pogrešno učili u školi, odnosno da li postoji neki drugi konačan skup aksioma iz kojih bismo izveli sve zakone algebre pozitivnih celih brojeva. Odgovor je negativan. R. Gurevič je 1990. u radu [16] dokazao da takav skup ne postoji. Preciznije rečeno, Gurevič je pokazao sledeće:

Neka je $\mathcal{L} = \{\text{termovi signature } (+, \cdot, \uparrow, 1)\}$ i $K = \{(t \approx u) | t, u \in \mathcal{L} \text{ i } \mathbf{N}^+ \models t \approx u\}$.

Za bilo koji konačan $S \subset K$ postoji identitet (Wilkiejevog tipa) $(t \approx u) \in K$, od jedne promenljive, takav da se $t \approx u$ ne može izvesti iz S .

Formule koje je koristio Gurevič liče na $W(x, y)$. Neka je

$$A = 1+x, B_n = 1+x+x^2+\dots+x^{n-1}, C_n = 1+x^n,$$

$$D_n = 1 + x^2 + x^4 + \cdots + x^{2n-2}.$$

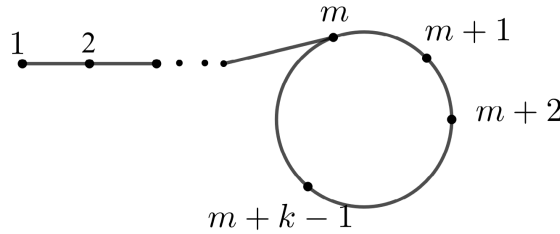
TEOREMA 3.4. *Za svaki konačan skup $S \subset K$ postoji neparno $n \geq 3$ takvo da se identitet*

$$(A^{2^x} + B_n^{2^x})^x \cdot (C_n^x + D_n^x)^{2^x} \approx (A^x + B_n^x)^{2^x} \cdot (C_n^{2^x} + D_n^{2^x})^x$$

ne može izvesti iz S .

Mada je Gurevičev dokaz o ne konačnoj aksiomatizabilnosti uglavnom elementaran, u jednom trenutku morao je da pređe u kompleksnu ravan i ispituje analitička produženja kompleksnih funkcija oko singulariteta.

Mi ćemo u ovom radu posmatrati male modele HSI koje su ispitali Burris i Lee u radu [1]. Svaki model od HSI ima najmanji podmodel, naime, podalgebru generisanu konstantom 1. Elementi podmodela su baš $1, 2, \dots$, gde je $2 := 1 + 1$, $3 := 2 + 1$, itd. Kako ovi elementi uključuju 1 i zatvoreni su za sabiranje, množenje i stepenovanje, zovemo ih *celi brojevi modela*. Ako je skup celih brojeva beskonačan, onda imamo kopiju od \mathbf{N}^+ . Međutim, ako u modelu važi $m \approx m + k$, m, k su celi brojevi modela, onda je skup celih brojeva konačan i model izgleda kao na slici 3.1.



SLIKA 3.1. Konačan model identiteta $m \approx m + k$

U opštem slučaju, pored celih brojeva, model može da ima elemente koji nisu celi brojevi.

Ako je data algebra $\mathbf{A} = (A, \mathcal{F})$ i relacija ekvivalencije \sim na skupu A koja je saglasna sa operacijama iz \mathcal{F} , tzv. kongruencija, onda algebra $\mathbf{A}/\sim = (A/\sim, \mathcal{F})$ zadovoljava sve identitete algebre \mathbf{A} . Algebra \mathbf{A}/\sim se zove *faktor struktura*. Operacije na A/\sim se prirodno definišu. Na primer, ako je $+$ $\in \mathcal{F}$, onda je $a/\sim + b/\sim := (a + b)/\sim$. Algebra \mathbf{A}/\sim se zove *količnička algebra* algebre \mathbf{A} . Sve količničke algebre \mathbf{A}/\sim

zadovoljavaju sve zakone identitete algebre \mathbf{A} . Sledeće dve algebre su količničke algebre algebre \mathbf{N}^+ i zadovoljavaju *HSI*.

$$\begin{array}{c|cc} + & 1 & 2 \\ \hline 1 & 2 & 2 \\ 2 & 2 & 2 \end{array} \quad \begin{array}{c|cc} \cdot & 1 & 2 \\ \hline 1 & 1 & 2 \\ 2 & 2 & 2 \end{array} \quad \begin{array}{c|cc} \uparrow & 1 & 2 \\ \hline 1 & 1 & 1 \\ 2 & 2 & 2 \end{array}$$

$$\begin{array}{c|cc} + & 1 & 2 \\ \hline 1 & 2 & 1 \\ 2 & 1 & 2 \end{array} \quad \begin{array}{c|cc} \cdot & 1 & 2 \\ \hline 1 & 1 & 2 \\ 2 & 2 & 2 \end{array} \quad \begin{array}{c|cc} \uparrow & 1 & 2 \\ \hline 1 & 1 & 1 \\ 2 & 2 & 2 \end{array}$$

Naravno, ove algebre zadovoljavaju sve identitete (zakone) \mathbf{N}^+ kao količničke algebre.

Međutim, prema Burrisu, za sledeću malu algebru ne znamo da li zadovoljava sve zakone \mathbf{N}^+ , tj. ne znamo da li je količnička algebra algebre \mathbf{N}^+ .

$$\begin{array}{c|cc} + & 1 & a \\ \hline 1 & 1 & 1 \\ a & 1 & a \end{array} \quad \begin{array}{c|cc} \cdot & 1 & a \\ \hline 1 & 1 & a \\ a & a & a \end{array} \quad \begin{array}{c|cc} \uparrow & 1 & a \\ \hline 1 & 1 & 1 \\ a & a & 1 \end{array}$$

U radu [1] dokazana je sledeća teorema.

TEOREMA 3.5. *Postoji tačno pet 2-elementnih HSI algebri, do na izomorfizam i one su date sledećim tablicama:*

$$\begin{array}{c} 1. \end{array} \begin{array}{c|cc} + & 1 & a \\ \hline 1 & 1 & 1 \\ a & 1 & a \end{array} \quad \begin{array}{c|cc} \cdot & 1 & a \\ \hline 1 & 1 & a \\ a & a & a \end{array} \quad \begin{array}{c|cc} \uparrow & 1 & a \\ \hline 1 & 1 & 1 \\ a & a & 1 \end{array}$$

$$\begin{array}{c} 2. \end{array} \begin{array}{c|cc} + & 1 & a \\ \hline 1 & 1 & 1 \\ a & a & a \end{array} \quad \begin{array}{c|cc} \cdot & 1 & a \\ \hline 1 & 1 & a \\ a & a & a \end{array} \quad \begin{array}{c|cc} \uparrow & 1 & a \\ \hline 1 & 1 & 1 \\ a & a & a \end{array}$$

$$\begin{array}{c} 3. \end{array} \begin{array}{c|cc} + & 1 & a \\ \hline 1 & 1 & a \\ a & a & a \end{array} \quad \begin{array}{c|cc} \cdot & 1 & a \\ \hline 1 & 1 & a \\ a & a & a \end{array} \quad \begin{array}{c|cc} \uparrow & 1 & 2 \\ \hline 1 & 1 & 1 \\ a & a & a \end{array}$$

$$\begin{array}{c} 4. \end{array} \begin{array}{c|cc} + & 1 & 2 \\ \hline 1 & 2 & 2 \\ 2 & 2 & 2 \end{array} \quad \begin{array}{c|cc} \cdot & 1 & 2 \\ \hline 1 & 1 & 2 \\ 2 & 2 & 2 \end{array} \quad \begin{array}{c|cc} \uparrow & 1 & 2 \\ \hline 1 & 1 & 1 \\ 2 & 2 & 2 \end{array}$$

$$\begin{array}{c} 5. \end{array} \begin{array}{c|cc} + & 1 & 2 \\ \hline 1 & 2 & 1 \\ 2 & 1 & 2 \end{array} \quad \begin{array}{c|cc} \cdot & 1 & 2 \\ \hline 1 & 1 & 2 \\ 2 & 2 & 2 \end{array} \quad \begin{array}{c|cc} \uparrow & 1 & 2 \\ \hline 1 & 1 & 1 \\ 2 & 2 & 2 \end{array}$$

Dokaz. Prvo tražimo sve moguće 2-elementne *HSI* algebre. Takve algebre imaju jedan ili dva cela broja. Dakle, moguće su sledeći slučajevi.

I $\boxed{1 + 1 \approx 1}$ Iz (6) i (9) *HSI* dobijamo

$$x + x \approx x \quad x \cdot x \approx x.$$

Prema tome Cayleyjeve tablice ovakvih *HSI* algebri izgledaju ovako.

$$\begin{array}{c|cc} + & 1 & a \\ \hline 1 & 1 & b \\ a & b & a \end{array} \quad \begin{array}{c|cc} \cdot & 1 & a \\ \hline 1 & 1 & a \\ a & a & a \end{array} \quad \begin{array}{c|cc} \uparrow & 1 & a \\ \hline 1 & 1 & 1 \\ a & a & c \end{array} \quad 1^a \approx a \quad (7) \text{ HSI}$$

Ovo nam daje najviše 4 mogućnosti. Ako za b biramo 1, onda imamo dve mogućnosti za c . Analogno ako za b biramo a . Sve ovo nam daje algebre 1., 2. i 3. i algebru

$$\begin{array}{c|cc} + & 1 & a \\ \hline 1 & 1 & a \\ a & a & a \end{array} \quad \begin{array}{c|cc} \cdot & 1 & a \\ \hline 1 & 1 & a \\ a & a & a \end{array} \quad \begin{array}{c|cc} \uparrow & 1 & a \\ \hline 1 & 1 & 1 \\ a & a & 1 \end{array}$$

Međutim, ova algebra ne zadovoljava (9) *HSI* jer je $a^{1+a} = a^a = 1$ ali $a^1 \cdot a^a = a \cdot 1 = a$.

II $\boxed{1 + 1 \not\approx 1}$ Svi elementi algebre su celi brojevi. Postoje tačno dve 2-elementne celobrojne *HSI* algebre i to su 4. i 5. Sada se lako pokazuje da ovih pet algebri zadovoljavaju *HSI* identitete i nisu izomorfne. \square

Što se tiče 3-elementnih *HSI*-algebri Burris i Lee navode sledeće. Ako je A konačan neprazan skup od n elemenata, onda postoji n^{n^2} binarnih algebri. Primenjujući *HSI* identitete (1), (3), (4), (7) i (8) mogu se 3-elementne algebre svesti na formu

$$\begin{array}{c|ccc} + & 1 & a & b \\ \hline 1 & c & d & e \\ a & d & f & g \\ b & e & g & h \end{array} \quad \begin{array}{c|ccc} \cdot & 1 & a & b \\ \hline 1 & 1 & a & b \\ a & a & i & j \\ b & b & j & k \end{array} \quad \begin{array}{c|ccc} \uparrow & 1 & a & b \\ \hline 1 & 1 & 1 & 1 \\ a & a & l & m \\ b & b & n & o \end{array}$$

Broj algebri koje treba testirati u ovom slučaju je 3^{13} tj. oko 1600000. Opet se pristupa ispitivanju celih brojeva ovih algebri. Na kraju dobijamo tačno 44 3-elementne *HSI*-algebre. Pre trideset godina trebalo je S. Burrisu i S. Leeju šest meseci da nađu sve 4-elementne i 5-elementne *HSI* algebre. Danas bi za to bilo potrebno nekoliko sekundi.

Drugačija je priča kada se traže *HSI*-algebre u kojima ne važi $W(x, y)$. Modeli koje smo naveli nisu takvi. Napomenimo da je R. Gurevič u radu [17] dao 59-elementnu *HSI*-algebru u kojoj ne važi $W(x, y)$.

Poslednji rad koji smo našli na temu kompjuterskog pretraživanja *HSI*-algebri u kojima ne važi $W(x, y)$ napisao je J. Zhang sa Instituta za softver Kineske akademije nauka [46]. Kako je Zhang naveo u tekstu rada, eksperimentalni rezultati pokazuju da takav model mora imati bar 11 elemenata. Po svemu sudeći, model *HSI*-algebre u kojoj ne važi $W(x, y)$ i koji ima 12 elementa je najmanji mogući model. J. Zhang i H. Zhang su 1995. godine razvili sistem za konstrukciju modela SEM (System for Enumerating Models) u radu [47] pomoću koga proveravaju na malim modelima *HSI*-algebri da li važi $W(x, y)$. Da koriste SEM i ispituju da li postoji 4-elementna Gurevič-Burrisova *HSI*-algebra, koja ne zadovoljava $W(x, y)$ daju se sledeći inputi.

4.

$$s(x, y) = s(y, x).$$

$$s(x, s(y, z)) = s(s(x, y)z).$$

$$p(x, 1) = x.$$

$$p(x, y) = p(y, x)$$

$$p(x, p(y, z)) = p(p(x, y)z).$$

$$e(1, x) = 1.$$

$$e(x, 1) = x.$$

$$e(x, s(y, z)) = p(e(x, y), e(x, z)).$$

$$e(p(x, y), z) = p(e(x, z), e(y, z)).$$

$$e(e(x, y), z) = e(x, p(y, z)).$$

$$C = p(a, a).$$

$$P = s(1, a).$$

$$Q = s(P, c).$$

$$R = s(1, p(a, c)).$$

$$S = s(s(1, c), p(c, c)).$$

$$p = (e(s(e(P, a), e(Q, a)), b), e(s(e(R, b), e(S, b)), a)).$$

$$! = p(e(s(e(P, b), e(Q, b)), a), e(s(e(R, a), e(S, a)), b)).$$

Funkcionalni simboli s, p i e označavaju sumiranje, proizvod i stepenovanje, respektivno. Potrebno je naći sve konstante i ove termine: $s(0, 0)$, $s(0, 1)$, $s(0, 3)$, $s(1, 0)$, ..., $p(0, 0)$, $p(0, 1)$, ..., $e(3, 3)$. Svaki od ovih termina uzima vrednost iz domena $D_4 = \{0, 1, 2, 3\}$. Neki od ovih termina moraju dobiti izvesne vrednosti, na primer $e(1, 0) = e(1, 1) =$

1. Ostali termovi, međutim, mogu uzeti proizvoljne vrednosti. Na primer, $s(0, 0)$ može uzimati bilo koju od četiri vrednosti i proveravamo da li imamo kontradikciju. Slično za druge termove i konstante.

Vratimo se ponovo na $W(x, y)$ i pokažimo neka interesantna svojstva ovog identiteta. Neka su $P(x) = 1 + x$, $Q(x) = 1 + x + x^2$, $R(x) = 1 + x^3$, $S(x) = 1 + x^2 + x^4$. Označimo sa $P = P(x)$, $Q = Q(x)$, $R = R(x)$ i $S = S(x)$. Tada $W(x, y)$ glasi

$$(P^x + Q^x)^y \cdot (R^y + S^y)^x \approx (P^y + Q^y)^x \cdot (R^x + S^x)^y,$$

LEMA 3.1.

$$HSI \vdash (\forall x)W(x, y).$$

Dokaz. Očigledno, obzirom da su obe strane $W(x, y)$ iste. \square

LEMA 3.2.

$$HSI \vdash (\forall y)W(x, y).$$

Dokaz. Neka je $m = 1 - n + n^2$, pozitivan ceo broj. Tada je

$$HSI \vdash P(n) \cdot m \approx R(n),$$

$$HSI \vdash Q(n) \cdot m \approx S(n),$$

n i m su numerali. Iz HSI možemo izvesti

$$\begin{aligned} (P(n)^n + Q(n)^n)^y \cdot (R(n)^y + S(n)^y)^n &\approx \\ &\approx m^{ny} \cdot (P(n)^n + Q(n)^n)^y \cdot (P(n)^y + Q(n)^y)^n \\ &\approx (R(n)^n + S(n)^n)^y \cdot (P(n)^y + Q(n)^y)^n \\ &\approx (P(n)^y + Q(n)^y)^n \cdot (R(n)^n + S(n)^n)^y \end{aligned}$$

Sledi, $HSI \vdash (\forall y)W(x, y)$. \square

LEMA 3.3.

$$HSI \vdash P \cdot S \approx Q \cdot R.$$

Dokaz. Ovo sledi iz \overline{HSI} , obe strane su jednake $1 + x + x^2 + x^4 + x^5$. \square

LEMA 3.4. Za fiksno n ceo broj imamo

$$HSI \vdash (\forall x)W(x, n).$$

Dokaz. Koristeći HSI možemo izvesti

$$\begin{aligned} (P^x + Q^x)^n \cdot (R^n + S^n)^x &\approx \left(\sum_{i=0}^n \binom{n}{i} (P^x)^i \cdot (Q^x)^{n-i} \right) \cdot (R^n + S^n)^x \\ &\approx \sum_{i=0}^n \binom{n}{i} (P^i \cdot Q^{n-i} \cdot R^n + P^i \cdot Q^{n-i} \cdot S^n)^x \end{aligned}$$

i

$$\begin{aligned} (P^n + Q^n)^x \cdot (R^x + S^x)^n &\approx (P^n + Q^n)^x \cdot \left(\sum_{i=0}^n \binom{n}{i} (R^x)^i \cdot (S^x)^{n-i} \right) \\ &\approx \sum_{i=0}^n \binom{n}{i} (P^n \cdot R^i \cdot S^{n-i} + Q^n \cdot R^i \cdot S^{n-i})^x \end{aligned}$$

Sad, koristeći lemu 3.3 možemo izvesti sledeće identitete iz *HSI*, za $0 \leq i \leq n$,

$$\begin{aligned} P^i \cdot Q^{n-i} \cdot R^n &\approx P^n \cdot R^i \cdot S^{n-i} \\ P^i \cdot Q^{n-i} \cdot S^n &\approx Q^n \cdot R^i \cdot S^{n-i}. \end{aligned}$$

Prema tome, imamo izvođenje iz *HSI*

$$(P^x + Q^x)^n \cdot (R^n + S^n)^x \approx (P^n + Q^n)^x \cdot (R^x + S^x)^n,$$

što je $W(x, n)$. \square

Sledeću lemu dokazao je S. Lee.

LEMA 3.5.

$$HSI \vdash x|y \Rightarrow W(x, y).$$

Dokaz. $u|v$ znači $(\exists w)(v = u \cdot w)$.

$$\begin{aligned} (P^x + Q^x)^y \cdot (R^y + S^y)^x &\approx (P^x + Q^x)^{n \cdot x} \cdot (R^{n \cdot x} + S^{n \cdot x})^x \\ &\approx [(P^x + Q^x)^n \cdot (R^{n \cdot x} + S^{n \cdot x})]^x \\ &\approx [((PR)^x + (QR)^x)^n + ((PS)^x + (QS)^x)^n]^x \\ &\approx [((PR)^x + (PS)^x)^n + ((QR)^x + (QS)^x)^n]^x \\ &\approx [P^{n \cdot x} (R^x + S^x)^n + Q^{n \cdot x} (R^x + S^x)^n]^x \\ &\approx [(P^{n \cdot x} + Q^{n \cdot x})(R^x + S^x)^n]^x \\ &\approx (P^y + Q^y)^x (R^x + S^x)^{n \cdot x} \\ &\approx (P^y + Q^y)^x (R^x + S^x)^y. \end{aligned}$$

\square

R. Gurevič je 1985. godine u radu [17] dokazao teoremu.

TEOREMA 3.6. *Ako je Σ skup identiteta, (uključujući: $1^x \approx 1$, $x^1 \approx 1 \cdot x \approx x \cdot 1 \approx x$) koji su tačni u \mathbf{N}^+ , onda posledice Σ (jednakosne posledice) čine odlučiv skup identiteta u jednakosnoj logici.*

Posledica ove teoreme je tvrđenje:

TEOREMA 3.7. *Jednakosne posledice *HSI* su odlučive.*

\uparrow	1	2	3	4	a	b	c	d	e	f	g	h
1	1	1	1	1	1	1	1	1	1	1	1	1
2	2	4	4	4	4	4	4	4	f	4	4	4
3	3	4	4	4	e	4	4	4	g	4	e	h
4	4	4	4	4	4	4	4	4	4	4	4	4
a	a	c	c	c	c	c	c	c	c	c	c	c
b	b	4	4	4	4	4	4	4	4	4	4	4
c	c	c	c	c	c	c	c	c	c	c	c	c
d	d	4	4	4	f	4	4	4	4	4	4	4
e	e	4	4	4	4	4	4	4	h	4	4	4
f	f	4	4	4	4	4	4	4	4	4	4	4
g	g	4	4	4	h	4	4	4	4	4	h	4
h	h	4	4	4	4	4	4	4	4	4	4	4

3.3. Varijeteti algebr

Da ponovimo, identitet $s(x) \approx t(x)$ u jeziku $\mathcal{L} = \{+, \cdot, \uparrow, 1\}$ je tačan u algebri \mathbf{N}^+ ako i samo ako

$$\mathbf{N}^+ \models (\forall x)(s(x) \approx t(x)).$$

D. Richardson je 1969. godine u radu [39] dokazao sledeće.

TEOREMA 3.8. *Identiteti sa jednom promenljivom $s(x) \approx t(x)$ od \mathbf{N}^+ su odlučivi.*

Drugim rečima, postoji algoritam koji odlučuje da li bilo koji identitet od jedne promenljive važi u algebri prirodnih brojeva.

Identiteti (zakoni) se u engleskom jeziku nazivaju *equations*, što bi na našem jeziku značilo *jednačine*. Jednačine su ipak nešto drugo. Na primer, jednačina

$$x^3 + 5x^2 + 2x + 1 = 0$$

nema rešenje u \mathbf{N}^+ , što znači da \mathbf{N}^+ nije model identiteta $x^3 + 5x^2 + 2x + 1 \approx 0$. Naprotiv, identitet ne postaje jednakost ni za jedno x u modelu \mathbf{N}^+ . Dakle, možemo reći

$$\mathbf{N}^+ \models \neg(\exists x)(x^3 + 5x^2 + 2x + 1 \approx 0),$$

odnosno

$$\mathbf{N}^+ \models (\forall x)(x^3 + 5x^2 + 2x + 1 \not\approx 0).$$

Identiteti ili zakoni mnogo govore o strukturi algebre (modela). Takav je slučaj sa grupama i prstenima. Međutim, kada su u pitanju polugrupe, sama asocijativnost ne govori mnogo o strukturi polugrupe, o prirodi elemenata. Mi nemamo dovoljno jednostavne algoritme za utvrđivanje da li je Cayleyjeva tablica konačnog grupoida polugrupa.

Klase algeabri aksiomatizovanih identitetima čine posebnu granu Univerzalne algebre, grane algebre koja se intenzivno razvija. Reč je o tzv. *varijetetima algeabri*. Jedan varijetet algebre može imati tzv. *podvarijetete*. To su klase algeabri koje zadovoljavaju, pored definicionih identiteta i neke specijalne identitete. Na primer, ako je $\mathcal{L} = \{\cdot\}$ i identitet $x \cdot (y \cdot z) \approx (x \cdot y) \cdot z$ imamo varijetet polugrupa. Ako asocijativnosti dodamo $x \cdot y \approx y \cdot x$, onda dobijamo podvarijetet varijeteta polugrupa. To je varijetet komutativnih polugrupa. Ako ovim identitetima dodamo identitet $x \cdot x \approx x$, dobijamo podvarijetet polumreža. Varijetet polumreža nema prave podvarijetete dok podvarijeteta komutativnih polugrupa ima beskonačno mnogo.

Poznata teorema Jacobsona u teoriji prstena kaže da, ako nam je dato $n \geq 2$ i ako je Σ skup aksioma prstena plus identitet $x^n \approx x$, onda je $\Sigma \models x \cdot y \approx y \cdot x$. Dakle, u tom slučaju imamo podvarijetet komutativnih prstena. Međutim, ne postoji neki rutinski način da se izvede formalni dokaz, ako je dato n , da važi $x \cdot y \approx y \cdot x$. Za specijalne $n = 2, 3$ ovo su poznati zadaci iz algebre. Za $n = 2$ dokaz komutativnosti prstena glasi ovako:

$$\begin{aligned} x + y &\approx (x + y)^2 && \text{jer važi identitet } u^2 \approx u \\ \Rightarrow x + y &\approx x + xy + yx + y. \end{aligned}$$

$(R, +)$ je po definiciji komutativna grupa pa važi skraćivanje za $+$, tj.

$$\begin{aligned} xy + yx &\approx 0 \\ \Leftrightarrow xy &\approx -(yx). \end{aligned}$$

Dalje je

$$\begin{aligned} (x + x)^2 &= x^2 + 2x \cdot x + x^2 = x + 2x + x \\ \Leftrightarrow x + x &= x + (x + x) + x \quad (\text{jer je } (x + x)^2 \approx x + x) \\ \Leftrightarrow x + x &\approx 0, \end{aligned}$$

dakle, $yx + yx \approx 0 \Leftrightarrow yx \approx -(yx)$. Kako je $xy \approx -(yx)$, sledi $xy \approx yx$.

DEFINICIJA 3.3. *Varijetet V je trivijalan ako su mu sve algebre jednoelementne (trivijalne). V je minimalan varijetet ako V nije trivijalan i jedini njegov podvarijetet je trivijalan varijetet.*

Poznata teorema Univerzalne algebre, čiji dokaz izostavljamo kaže:

TEOREMA 3.9. *Neka je V netrivialan varijetet. Tada V sadrži minimalan varijetet.*

DEFINICIJA 3.4. *Neka je M neprazan skup, a \wedge i \vee dve binarne operacije skupa M . Za algebru $\mathcal{M} = (M, \wedge, \vee)$ kažemo da je mreža ako za sve $x, y, z \in M$ važi:*

- (M1) $x \wedge x \approx x, x \vee x \approx x$
 (M2) $x \wedge y \approx y \wedge x, x \vee y \approx y \vee x$
 (M3) $x \wedge (y \wedge z) \approx (x \wedge y) \wedge z, x \vee (y \vee z) \approx (x \vee y) \vee z$
 (M4) $x \wedge (y \vee x) \approx x, x \vee (y \wedge x) \approx x.$

Drugim rečima, \mathcal{M} je model zakona (M1) - (M4). Prirodni primer mreže, za dati skup S , je algebra podskupova od S , u oznaci $\mathbf{P}(S) = (P(S), \cap, \cup)$.

Kao što je poznato, mreže se mogu definisati preko parcijalno uređenih skupova, gde svaka dva elementa imaju infimum i supremum. Ako mreža ima najveći i najmanji element, oni se često označavaju sa 1 i 0. Na primer, u mreži podskupova datog skupa S najveći element je S a najmanji \emptyset . Parcijalno uređenje koje induciraju operacije mreže dato je sa

$$a \leq b \quad \text{ako i samo ako} \quad a \vee b = b, a \wedge b = a.$$

Skup podvarijeteta nekog varijeteta V čini mrežu u odnosu na relaciju \subseteq , gde je najveći element te mreže V , a najmanji element trivijalni varijetet. Naime, ako u parcijalno uređenom skupu svaka dva elementa imaju infimum (inf) i supremum (sup), onda se taj skup pretvara u mrežu tako što se operacije definišu na sledeći način:

$$a \wedge b := \inf\{a, b\}, \quad a \vee b := \sup\{a, b\}.$$

Lako se pokazuje da je ova definicija dobra.

Primetimo da je varijetet grupa podvarijetet varijeteta polugrupa. Mreža ne mora imati minimalne elemente, tj. elemente od kojih je manji samo 0. Minimalni elementi mreže se nazivaju i *atomi*. Mreža podvarijeteta polugrupa ima minimalne elemente. To su sledeći varijeteti. $\mathcal{A}_p, \mathcal{LZ}, \mathcal{RZ}, \mathcal{SL}, \mathcal{ZM}$.

\mathcal{A}_p , gde je p prost broj, je varijetet Abelovih grupa (komutativnih) čiji su specijalni aksiomi dati identitetima:

$$x^p y \approx y, \quad xy \approx yx$$

\mathcal{LZ} je varijetet polugrupa levih nula dat sa:

$$xy \approx x.$$

\mathcal{RZ} je varijetet desnih nula dat sa:

$$xy \approx y.$$

\mathcal{ZM} je varijetet sa nultom multiplikacijom:

$$xy \approx 0.$$

\mathcal{SL} je varijetet polumreža:

$$x^2 \approx x, \quad xy \approx yx.$$

Dakle, mreža varijeteta polugrupa ima beskonačno mnogo (prebrojivo mnogo) atoma jer grupa \mathcal{A}_p ima onoliko koliko ima prostih brojeva.

Međutim, u Teoriji polugrupa postoje klase polugrupa koje su nastale uopštenjem grupa. *Inverzne polugrupe* date su sledećim identitetima u jeziku $\{\cdot, {}^{-1}\}$:

$$\begin{aligned}x \cdot x^{-1} \approx x, (x^{-1})^{-1} \approx x, (x \cdot y)^{-1} \approx y^{-1} \cdot x^{-1}, \\(x \cdot x^{-1}) \cdot (y \cdot y^{-1}) \approx (y \cdot y^{-1}) \cdot (x \cdot x^{-1})\end{aligned}$$

Još jedan varijetet polugrupa dat je sledećim identitetima

$$x \approx xx^{-1}x, (x^{-1})^{-1} \approx x, xx^{-1} \approx x^{-1}x.$$

Ovo je varijetet tzv. *kompletno regularnih polugrupa*.

Važna klasa polugrupa je klasa *regularnih polugrupa*, koja ne čini varijetet. Element a polugrupe S je *regularan* ako postoji element $x \in S$ takav da je

$$S \models axa = a.$$

Pojam regularnog elementa u matematiku je uveo 1936. godine znameniti matematičar John von Neumann (1903-1957), za prstene. Neke važne klase algebri ne mogu se definisati identitetima. Takva je poznata klasa algebri *klasa polja*. Klasa polja je u stvari klasa prstena sa jedinicom

$$(P, +, -, \cdot, 0, 1),$$

gde za svaki nenula element važi identitet

$$x \cdot 1 \approx 1 \cdot x \approx x.$$

Ovo *nenula* je neotklonjivo i zbog toga klasa polja ne može biti varijetet.

Interesantno je da neki poznati varijeteti algebri mogu biti određeni samo jednim identitetom. Takvi su, na primer, varijeteti polugrupa, grupa i mreža. Sem asocijativnosti, identiteti koji definišu grupe i mreže su takvi da se iz njih teško zaključuje da se radi o grupama ili mrežama.

Recimo i ovo. Teorija konačnih polugrupa je algebarski ekvivalent Teoriji konačnih automata.

GLAVA 4

Gödelov univerzum

Glavna tema našeg rada je *aritmetika prirodnih brojeva*. U prethodnim poglavljima smo videli da aritmetika nije savršena grana matematike. Preciznije, sintaksa nije savršena, iako su aksiome i pravila izvođenja takvi da je teško zamisliti jednostavnije.

Kraj devetnaestog veka nagovestio je veliko spremanje u matematici. Stvarane su nove matematičke discipline: Matematička logika i Teorija skupova. Centralne figure u razvoju tzv. *osnova matematike* tog doba bili su Gottlob Frege, Georg Cantor, David Hilbert, Bertrand Russell, Giuseppe Peano, Richard Dedekind, Lejeune Dirichlet. Opšte mišljenje je da su najveći logičari u istoriji čovečanstva Aristotel, Frege, Gödel i Tarski.

Ispostavilo se da Euklidovi dokazi nisu tako savršeni kao što se mislilo preko dve hiljade godina. Veliki posao oko sređivanja uradio je Hilbert. Njegova knjiga [18] iz 1899. godine i dan danas se smatra odličnim udžbenikom Geometrije. Hilbertova knjiga je dočekana sa velikim uvažavanjem u matematičkom svetu. Početkom dvadesetog veka Hilbert je smatran za vodećeg matematičara sveta.

David Hilbert je rođen 1862. u Königsbergu u istočnoj Pruskoj. U tom gradu je i studirao, osim što je proveo jedan semestar u Heidelbergu. Doktorsku disertaciju odbranio je 1884. godine. Disertacija je posvećena Teoriji algebarskih invarijanti kojom se bavio sve do 1892. godine. Tokom tih istraživanja došao je do mnogih značajnih otkrića, od kojih neka nose njegovo ime. (Hilbertov Nullstellensatz, Hilbertova teorema o nesvodljivosti polinoma). Metodama koje je koristio u svojim istraživanjima počinje apstraktno tretiranje algebre, koje od onda dominira oblašću klasične algebre.

Godine 1886. Hilbert postaje *Privatdozent*, a 1892. godine vanredni profesor na Univerzitetu u Königsbergu. Sledeće godine nasleđuje svog učitelja Ferdinanda Lindemanna (1852-1939) kao redovni profesor u Königsbergu. Podsetimo se, Lindemann je čovek koji je pokazao da je π transcendentan broj. 1895. godine Hilbert prihvata poziv Felixa Kleina (1849-1925) da pređe na Univerzitet u Göttingenu, gde će ostati do kraja života, iako su ga pozivali na mnoge druge univerzitete. Uspeo

je da u Göttingen prebaci svog druga iz studentskih dana, Hermanna Minkowskog (1864-1909), takođe velikog matematičara.

U leto 1900. godine održao 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 Hilbert piše kako ne zna tačno o čemu bi govorio. Razmišlja da, kako 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 drugo više sviđa i napisao je:

Sa takvom temom, može se desiti da ljudi decenijama govore o tom predavanju.

Predavanje pod naslovom *Matematički problemi* Hilbert je osmislio na sledeći način. U prvom delu govori se o važnosti problema za određivanje pravca razvoja u nauci. Razmatraju se neki veliki plodni problemi u matematici i govori se o zahtevima koje rešenja moraju da zadovolje. Hilbert je insistirao na rigoroznosti. Zatim slede 23 problema sa komentarima. O svemu ovome videti [30]. Prvih nekoliko problema tiču se osnova matematike i sugerisani su onim što je Hilbert smatrao velikim dostignućem veka koji se završio.

Minkowski je umro 1909. godine i to je bio veliki udarac za Hilberta. Posle smrti Minkowskog, Hilbert se uglavnom bavio teorijskom fizikom. Neposredno posle pojave opšte teorije relativnosti Alberta Einsteina (1879-1955), objavio je prvi pokušaj da se objedine gravitaciona teorija i elektrodinamika.

Od 1922. do 1930. godine Hilbert se opet bavi osnovama matematike. Iz ovih istraživanja nastala je knjiga [19] i enciklopedijska rasprava *Osnove matematike* [20].

Mi ćemo se u ovom radu osvrnuti na drugi Hilbertov problem koji je rešio, istina negativno, austrijski matematičar Kurt Gödel.

Drugi problem koji je postavio na svetskom matematičkom kongresu 1900. godine Hilbert je fomulisao 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.

Aksiome koje je Hilbert imao u vidu na kongresu odnose se na aritmetiku realnih brojeva. Kasnije, a naročito počevši od dvadesetih godina

prošlog veka, problem je shvaćen kao da se odnosi, pre svega, na aritmetiku u pravom smislu reči, tj. na teoriju prirodnih brojeva i Peanove aksiome.

Pitanje neprotivrečnosti je za Hilberta bilo važno zato što je on, početkom dvadesetog veka, verovao da je u matematici tvrditi da je neka teorija istinita isto što i tvrditi da je neprotivrečna. Odmah dobijamo da je dovoljno da utvrdimo neprotivrečnost neke matematičke teorije da bismo mogli da tvrdimo da objekti o kojima govori ta teorija postoje. Slično gledište imao je čuveni matematičar onog vremena Poencaré.

Problem neprotivrečnosti aritmetike bio je posebno težak i zato ga je Hilbert izdvojio na kongresu. Nije bilo jasno kako prići tom problemu. Hilbert nije očekivo za aritmetiku dokaz neprotivrečnosti dobijen pomoću interpretacije aritmetike u nekoj drugoj teoriji za koju verujemo da je neprotivrečna. Kao što smo Geometriju interpretirali u Teoriji realnih brojeva, tj. pokazali da je Geometrija neprotivrečna ako je Teorija realnih brojeva neprotivrečna. Za aritmetiku, koja je osnovna matematička teorija, traži se direktan dokaz. Naravno, Hilbert pretpostavlja da je aritmetika data kao formalni sistem. Formalizaciju aritmetike, koja se zasniva na formalizaciji logike koju je započeo Frege, Hilbert je detaljno izveo tek dvadesetih godina dvadesetog veka.

Od 5. do 7. septembra 1930. godine u nemačkom gradu Königsbergu održana je konferencija o epistemologiji egzaktnih nauka. Konferenciju je organizovalo Društvo za empirijsku filozofiju iz Berlina, koje je održavalo veze sa Bečkim krugom. Sastanak je održan uoči konferencije Društva nemačkih naučnika i lekara i Šeste skupštine nemačkih fizičara i matematičara.

Prvi dan su bila jednočasovna preliminarna izlaganja tri rivalska filozofska pravca: logicizam, intuicionizam i formalizam. Govornici su bili Rudolf Carnap (1891-1970), Arend Heyting (1898-1980) i John van Neumann. Dan kasnije Hilbert, na skupštini matematičara drži svoje čuveno predavanje. Tada je rekao:

Za matematičara nema Ignorabimus i po mom mišljenju, ni uopšte za bilo koju prirodnu nauku. Pravi razlog zašto niko nije pronašao nerešiv problem je, prema mom mišljenju, taj da ne postoji nerešiv problem. Nasuprot luckastom Ignorabimus, naš credo glasi:

Mi moramo znati - mi ćemo znati.

(Wir müssen wissen. Wir werden wissen.)

Hilbert aludira na "Ignoramus et ignorabimus", reči koje je 1818. godine izgovorio slavni fiziolog Emil du Bois-Reymond (1818-1896) u govoru o tajnama prirode.

Sutradan, u nedelju, za okruglim stolom, Gödel je jednostavno rekao:

Možemo navesti primere rečenica koje su jasno tačne, ali nedokazive u formalnom sistemu klasične matematike.

Ovo je jedva bilo registrovano. Ali, u publici je bio još jedan genije - John von Neumann. Ostalo je istorija.

Gödelov rezultat je dokrajčio skoro stogodišnji trud da se pronađu aksiome matematike iz kojih bi pomoću logičkih pravila mogla biti dokazana sva tačna matematička tvrđenja. Priča kaže da se skoro sve što je do tada dokazano u matematici moglo formalizovati, tj. formalno dokazati iz skupa jednostavnih aksioma.

Grubo rečeno, Gödelova teorema o nepotpunosti formalne aritmetike glasi:

Unutar formalne aritmetike, pod uslovom da je neprotivrečna, postoje istinita tvrđenja za koja ne postoji formalni dokaz unutar te teorije.

Komentar čuvenog matematičara André Weila (1906-1998) je bio:

Bog postoji jer je aritmetika nesumnjivo neprotivrečna, a đavo postoji jer to ne možemo dokazati.

Jasno, Gödelova teorema je uzdrmala svet dotadašnje matematike. Mi ćemo u ovom radu prikazati, naravno neformalno, ove rezultate jer je to kruna priče o jednakosnoj logici i njenoj primeni u Formalnoj aritmetici. Glavni junak naše priče je jedan od najvećih *antiheroja* u nauci uopšte. U novije doba Gödelov značaj sve više i više raste. Pojavom knjige Douglasa Hofstadtera (1945-2012) [21], nastaje prava lavina radova, knjiga, filozofskih rasprava pa i zloupotreba Gödelovih rezultata u drugim naukama. Hofstadter je za svoju knjigu dobio najveće američko priznanje u domenu publicistike, Pulitzerovu nagradu. Praveći duhovita poređenja Gödelovih rezultata sa načinom rada holandskog umetnika Morica Eschera (1898-1972) i muzikom Johana Sebastijana Bacha (1685-1750), Hofstadter je veoma uspešno pokazao da se i vrhunska matematika može približiti širokom krugu čitalaca.

Kurt Fridrih Gödel (28.04.1906. - 14.01.1978.) se rodio u Brnu, današnja Češka, kao drugo dete dobrostojećih roditelja nemačkog porekla. Školu je završio u Brnu i 1924. godine prešao na studije u Beč. U početku je Gödel hteo da studira fiziku. Tokom studija matematike, Gödel je pokazivao interesovanje i za fiziku. Otuda njegovo veliko poznavanje fizike, a kasnije, posebno poznavanje Teorije relativnosti. Narednih petnaest godina Gödel živi u Beču. Opis matematičke scene tih godina u Beču dala je Gödelova koleginica Olga Taussky-Todd (1906-1995) u knjizi [13] tvrdeći da je Gödel bio izuzetan student. Poznao je sve oblasti matematike. Vrlo brzo je Gödel došao u kontakt

sa Bečkim krugom, skupom vrhunskih intelektualaca tog vremena. Na sastanke Bečkog kruga dolazilo se po preporuci. Gödel je verovatno preporučio njegov mentor Hans Hahn (1879-1934). Radilo se o grupi filozofa koji su ostavili dubok trag u svetskoj nauci i pripadali filozofskom pravcu tog vremena, *empirista*. Empiristi su govorili da sva saznanja u nauci dolaze na osnovu iskustva. Gödel nije delio njihove filozofske stavove. Bečki krug je formalno nastao kad je filozof Moritz Schlick (1882-1936) odlučio da neformalno druženje po bečkim kafanama proglasi za seminar i pronađe odgovarajući prostor. Gödel je posećivao sastanke od 1926. do 1928. godine. Po svemu sudeći je sedeo i samo slušao. Učesnici Bečkog kruga su bili Herbert Feigl (1902-1988) (filozof), Rudolf Carnap (filozof), Hans Hahn, (matematičar), Otto Neurath (1882-1845) (sociolog i ekonomista), čija je sestra Olga Neurath bila udata za Hahna i učestvovala na sastancima, Karl Menger (1902-1985) (matematičar) i guru logičkog pozitivizma, Ludvig Wittgenstein (1889-1951). Prebogati Wittgenstein je bio *spiritus movens* Bečkog kruga. Nikad pozvan, i tajni obožavalac, siromašnog porekla, koji se celog života suprotstavljao Wittgensteinu, bio je niko drugi do Karl Popper (1902-1994). Po svemu sudeći, bar u početku, Wittgenstein nije dobro razumeo Gödelove rezultate i Gödel se prilično prezrivo izražavao o njemu.

Pozitivisti su odbacivali netrivialne iskaze koji se nisu mogli verifikovati kroz naše iskustvo. Gödel je odbacio ideje pozitivizma koji se pozivao na ljudsko iskustvo i kontakt sa stvarnim svetom. On se čuvao zaključaka na osnovu *zdravog razuma*.

Sam Gödel je bio prilično rezervisan kada su u pitanju zaključci izvedeni iz njegove teoreme, a tiču se zaključivanja na osnovu ljudskog razuma. Ovo je naglasio u čuvenom *Gibbs Lecture* iz 1951. (26. februar), po pozivu American Mathematical Society (AMS), na Univerzitetu Brown, Providence, Rhode Island.

Doktorsku disertaciju na Univerzitetu u Beču Gödel je završio 1929. godine kad je imao 23 godine. Zvanje doktora nauka Gödelu je odobreno februara 1930. godine i teza je štampana u radu [8]. U svojoj doktorskoj disertaciji Gödel je dokazao, danas čuvenu, Teoremu kompletnosti za Kvantifikatorski račun prvog reda. U našem radu je to teorema 2.3. Ova teorema se danas dokazuje u svim udžbenicima Matematičke logike. Značaj ovog rezultata rastao je vremenom ali se već tada videlo da se rađa nova zvezda Matematičke logike.

Tridesete godine prošlog veka u Nemačkoj i Austriji bile su godine rađanja nacizma. Bečki krug se ugasio 1936. godine kada je poludeli student ubio Schlicka. U ovom periodu, tri puta, Gödel je gostovao na Institute for Advanced Studies (IAS) u Princetonu SAD, gde je izlagao

svoje rezultate. Period od 1937. do 1939. godine donosi velike promene u Gödelovom životu. Adele Nimbursky (1899-1981) i Kurt Gödel venčavaju se 1938. godine. Samo dve nedelje posle venčanja Gödel je ostavio Adele u Beču i otišao na Princeton. Proveo je letnji semestar na univerzitetu Notre Dame gde je već stigo njegov kolega Menger. Vraća se u Beč i biva regrutovan za rad u *vojnim garnizonima*. Očajan šalje pismo Oswaldu Veblenu (1880-1960), novembra 1939. godine da mu pošalje pozivno pismo za Princeton. Nekako je uspeo da dobije imigrantsku vizu za Ameriku i u januaru 1940. zajedno sa Adele odlazi na Princeton. Više se nije vraćao u Austriju.

Nažalost, Gödelovi su vodili prilično usamljen život u Princetonu. Bečka gospoda sa Princetona nisu podnosila Adele. Neobrazovana, pomalo gruba, sa reputacijom barske igraciće, nije bila rado viđena u visokom društvu.

U to vreme na Princetonu su već bila velika imena evropske nauke, većinom jevrejskog porekla. Pomenimo samo neke: Johannes Alexander, Marston Morse (1882-1977), Albert Einstein (1879-1955), Hermann Weyl (1885-1955), Oswald Veblen, John von Neumann.

U to vreme, u Beču, branio se *viši doktorat*, tzv. *Habilitationsschrift*. Gödel nije odmah podneo svoj rad o nepotpunosti aritmetike. To je uradio tek 25. juna 1932. godine. Imao je u međuvremenu niz izlaganja na seminarima. Habilitationsschrift se branio na fakultetskom seminaru i svaki korak u procesu do odbrane morao je ići na glasanje celog filozofskog kolegijuma. Interesantno je da je Gödelova teza dobila ocenu *da* od pedeset jednog člana, a jedan je glasao *ne*, misleći da je teza suviše liči na prethodnu temu doktorata.

7. aprila 1933. godine donet je u Austriji *Zakon o preuređenju profesionalne civilne službe*, što je značilo otpuštanje osoba *nearijevskog porekla*. Univerziteti u Berlinu i Frankfurtu izgubili su 32% osoblja, Getingen 25% itd. U februaru 1939. godine Univerzitet u Beču je zatvoren, a Martin Heidegger (1889-1976) je postavljen za rektora slaveći *novi zaokret u nemačkoj sudbini*.

Gödel je štampao rezultate iz Habilitationsschrift 1931. godine u radu [9]. Shvativši ideju o čemu se zapravo radi, u Gödelovom komentaru za okruglim stolom u Königsbergu John von Neumann je relativno brzo, posle kongresa, uspeo da dokaže nešto kao neprotivrečnost aritmetike, ali Gödelov rad je već izašao iz štampe.

Kurt Gödel se smatra najvećim logičarem od vremena Aristotela. Napisao je samo nekoliko radova i oko hiljadu stranica rukopisa sadržanih u sveskama koje je zvao *Nachlass*. Sve ovo je nađeno u njegovoj zavostavštini. Među pismima koje nikad nije poslao, nalaze se i čuveni

odgovor engleskom logičaru i filozofu Bertrandu Russellu, na Russellovu priču u drugom tomu autobiografije iz 1968. godine.

I used to go to [Einstein] house once a week to discuss with him and Gödel and Pauli. These discussions were in some way disappointing, for although all three of them were Jews and exiles and, in intention, cosmopolitans, I found they all had a German bias towards meta-physics [and that] Gödel turned out to be an unadulterated Platonist.

Gödelu je skrenuta pažnja na ovo 1971. godine i on je napravio skicu odgovora koji nikad nije poslao. U odgovoru Gödel kaže:

As far as the passage about me [by Russell] is concerned, I have to say first (for the sake of truth) that I am not a Jew (even though I don't think this question is of any importance) that the passage gives the wrong impression that I had many discussions with Russell, which was by no means the case (I remember only one). Concerning my "unadulterated" Platonism, it is no more "unadulterated" than Russell's own in 1921.

Duboko privatn i rezervisan, Gödel je imao neverovatnu moć sveobuhvatne racionalnosti i do ludila posvećenu pažnju detaljima svakodnevnog života. Oprezno prima hranu i u strahu od bolesti bio je stalno preokupiran svojim zdravljem. Primaio je sa nepoverenjem savete lekara kada su mu bili najpotrebniji. Praktično posle svakog velikog rezultata koji je dobio doživljavao je nervne slomove. Brzo se oporavljao posle boravka u odgovarajućim ustanovama. Nije se radilo o ludilu. Krhko telo nije moglo da izdrži velike napore. Pred starost je padao u depresije praćene paranojom. Umišljao je da hoće da ga otruju i uzimao je samo hranu od Adele. Bio je apolitičan i potpuno nesvestan onoga što se događalo oko njega. Posle rata odbio je austrijsko državljanstvo i članstvo u akademiji nauka.

Američki magazin *Time* je u znak sećanja na protekli milenijum posvetio nekoliko specijalnih brojeva najvećim misliocima prošlog veka. Kurt Gödel je naveden kao najveći matematičar prošlog veka. Tu je i Alan Turing i Ludvig Wittgenstein, a Albert Einstein je proglašen najvećim umom dvadesetog veka.

Među bliske prijatelje Gödel je ubrajao i Oskara Morgensterna (1902-1977) koji je sa von Neumannom bio tvorac čuvene *Teorije igara*. Morgenstern je bio ekonomista koji je iz Beča došao u Ameriku. U literaturi se citira izjava Morgensterna:

Einstein mi je često govorio da je u poznim godinama svog života neprekidno tražio Gödelovo društvo u nameri da sa njim diskutuje.

Jednom mi je rekao da mu njegov sopstveni rad više ne znači mnogo i da je na Institut došao da bi imao privilegiju da šeta sa Gödelom.

Gödelova reakcija na ovu izjavu je bila je da on (Gödel) misli da je Einstein voleo da šeta s njim jer mu je Gödel često protivrečio i nije hteo da se povuče u diskusiji.

Evo svedočenja Ernsta Strausa (1922-1983) koji je bio Einsteinov asistent od 1944. do 1948. godine.

The one man who was, during the last years, certainly by far Einstein's best friend, and in same ways strongly resembled him most was Kurt Gödel, the great logician. They were very different, in almost every personal way. Einstein gregarious, happy, full of laughter, and common sense, and Gödel extremely solemn, very serious, quite solitary, and distrustful of common sense as a means of arriving at the truth. But they shared a fundamental quality: both went directly and wholeheartedly to the questions at the very center of things.

Gödel je izabran za redovnog člana IAS-a 1947. godine. Interesantno je da je izvestan broj ljudi na IAS-u smatrao da je on jednostavno lud. Predavanje po pozivu na International Congress of Mathematics (ICM) Gödel je održao 31. avgusta 1950. godine. Iste godine dobija Einsteinovu nagradu. Umesto da na ICM-u drži predavanje iz Teorije skupova, Gödel se opredelio da prikaže svoj *rotirajući univerzum* iz radova [10], [11].

Gödelov univerzum je beskonačan i oblika cilindra. Ugaona brzina na nekim eliptičnim putanjama bliska je brzini svetlosti. Interesantno je da se Gödel u svojim radovima pozivao na Immanuela Kanta i Teoriju relativnosti, jer, po njima, vreme nije apsolutno kao kod Isaaca Newtona (1643-1727). Gödel svoj model naziva *Rotirajuće kosmološko rešenje*. Gödel je otišao dalje od činjenice da vreme ne postoji u njegovim teorijskim univerzumima. On je pokazao, koristeći Teoriju relativnosti, da vreme ne postoji u našem svetu.

Einstein je smatrao da je Gödelov rad *važan doprinos Opštoj teoriji relativnosti*. Fizičari od tog vremena pokušavaju bezuspešno da pronađu grešku u Gödelovoj fizici ili *nedostajući element* u samoj relativnosti koji bi odbacio modele univerzuma kao Gödelove. Stephen Hawking (1942-2018) je išao tako daleko da je predlagao ad hoc modifikaciju zakona prirode, nekakvu *hipotezu zaštite hronologije* u nameri da negira Gödelov doprinos relativnosti.

Ponovimo još jednom. Formalni sistem je:

Neprotivrečan (konzistentan) ako ne postoji tvrđenje (rečenica) A takva da se u sistemu može dobiti formalni dokaz da je $\vdash A$ i $\vdash \neg A$.

Kompletan ako je za svako tvrđenje $\vdash A$ ili $\vdash \neg A$.

Rešiti problem odlučivosti znači dati algoritam (program) koji omogućava da u konačno mnogo koraka odlučimo u Formalnom aksiomatskom sistemu da li je bilo koje smisleno tvrđenje teorema. To će reći, za svako tvrđenje A možemo naći dokaz u Formalnom aksiomatskom sistemu da je A ili njena negacija teorema. Ovo se zove

Entscheidungsproblem

Koristeći ideje Gödelovog dokaza nepotpunosti aritmetike Alan Turing dokazuje 1936. godine sledeću teoremu.

TEOREMA 4.1. *Entscheidungsproblem je nerešiv za logiku prvog reda.*

Ovaj rezultat je štampan u radu [43].

Neka je \mathcal{T} bilo koja teorija istih simbola kao \mathcal{N} . Tada za \mathcal{T} kažemo da je ω -neprotivrečna ako i samo ako, za svaku formulu $A(x)$ od \mathcal{T} , ako je $\vdash_{\mathcal{T}} A(\bar{n})$ za svaki prirodan broj n , onda nije $\vdash_{\mathcal{T}} (\exists x)\neg A(x)$.

Lako se vidi da ako je \mathcal{T} ω -neprotivrečna, onda je \mathcal{T} neprotivrečna. Naime, ako je \mathcal{T} ω -neprotivrečna, posmatrajmo bilo koju formulu $A(x)$ koja je dokaziva u \mathcal{T} , na primer $x \approx x \Rightarrow x \approx x$. Posebno, $\vdash \bar{n} \approx \bar{n} \Rightarrow \bar{n} \approx \bar{n}$, za sve prirodne brojeve n . Prema tome, $(\exists x)\neg(x \approx x \Rightarrow x \approx x)$ nije dokaziva u \mathcal{T} . Ako bi \mathcal{T} bila protivrečna, iz tautologije $\neg A \Rightarrow (A \Rightarrow B)$ mogla bi se izvesti bilo koja formula B pa i $(\exists x)\neg(x \approx x \Rightarrow x \approx x)$. Kontradikcija.

Gödelov dokaz teoreme nekompletnosti počiva na samo nekoliko jednostavnih ideja.

- kodiranje formule (u aritmetici);
- kodiranje dokaza;
- Cantorova dijagonala;
- samoreferentna rečenica.

(2) *Pravila za dobijanje novih funkcija iz skupa datih funkcija:*

IV $f(x_1, \dots, x_n) = g(h_1(x_1, \dots, x_n), \dots, h_m(x_1, \dots, x_n))$
za f kažemo da je dobijena iz funkcija $g(y_1, \dots, y_m)$, $h_1(x_1, \dots, x_n)$,
 \dots , $h_m(x_1, \dots, x_n)$ supstitucijom.

V *Rekurzija:*

$$f(x_1, \dots, x_n, 0) = g(x_1, \dots, x_n)$$

$$f(x_1, \dots, x_n, y + 1) = h(x_1, \dots, x_n, y, f(x_1, \dots, x_n, y)).$$

Ovde dozvoljavamo da je $n = 0$, i u tom slučaju imamo

$$f(0) = k, \text{ gde je } k \text{ fiksni prirodni broj}$$

$$f(y + 1) = h(y, f(y)).$$

Kažemo da je f dobijena od g i h rekurzijom.

VI μ - operator:

Pretpostavimo da je $g(x_1, \dots, x_n, y)$ takva funkcija na \mathbf{N} da za svako x_1, \dots, x_n postoji y takvo da je $g(x_1, \dots, x_n, y) = 0$.

Označavamo sa

$$\mu_y(g(x_1, \dots, x_n, y) = 0)$$

najmanje y za koje je $g(x_1, \dots, x_n, y) = 0$. Uopšte, za bilo koju relaciju $R(x_1, \dots, x_n, y)$ označavamo sa

$$\mu_y(R(x_1, \dots, x_n, y))$$

najmanje y za koje je $R(x_1, \dots, x_n, y)$ tačno. Neka je

$$f(x_1, \dots, x_n) = \mu_y(g(x_1, \dots, x_n, y) = 0).$$

Kažemo da je f dobijena iz g μ -operatorom.

(3) *Funkcija f je prosto rekurzivna ako i samo ako je f dobijena iz osnovnih funkcija konačnom primenom supstitucija IV i rekurzije V. Drugim rečima, ako postoji konačan niz funkcija $f_1, \dots, f_n = f$ i za $0 \leq n$ ili je f_i osnovna funkcija ili f_i je dobijena iz prethodnih funkcija u nizu primenom IV ili V.*

(4) *Funkcija f je rekurzivna ako i samo ako se može dobiti iz osnovnih funkcija konačnom primenom IV, V i VI.*

Sledi da je svaka prosto rekurzivna funkcija rekurzivna. Obrat ne važi.

Rekurzivne funkcije je u matematiku uveo Gödel. Ispostaviće se da su funkcije skupa \mathbf{N} čije vrednosti mogu da se izračunaju u konačno mnogo koraka upravo rekurzivne funkcije. Čuvena *Church-Turing teza* kaže da je svaka (konačno) izračunljiva funkcija rekurzivna. Funkcija $f(x_1, \dots, x_n)$ je *predstavljiva* u \mathcal{N} ako i samo ako postoji formula

$F(x_1, \dots, x_n, x_{n+1})$ u \mathcal{N} gde su x_1, \dots, x_{n+1} slobodne promenljive tako da za bilo koje brojeve k_1, \dots, k_{n+1} važi:

- (1) ako je $f(k_1, \dots, k_n) = k_{n+1}$, onda je $\vdash_{\mathcal{N}} F(\bar{k}_1, \dots, \bar{k}_{n+1})$
- (2) postoji tačno jedno x_{n+1} takva da je $\vdash_{\mathcal{N}} F(\bar{k}_1, \dots, \bar{k}_n, x_{n+1})$

DEFINICIJA 4.2. *Relacija $R(x_1, \dots, x_n) \subseteq \mathbf{N}^n$ se može predstaviti u \mathcal{N} ako postoji formula $\mathcal{R}(x_1, \dots, x_n)$ u \mathcal{N} , sa n slobodnih promenljivih, takva da za bilo koje prirodne brojeve k_1, \dots, k_n*

- (1) *ako je $R(k_1, \dots, k_n)$ tačno, onda $\vdash_{\mathcal{N}} \mathcal{R}(\bar{k}_1, \dots, \bar{k}_n)$*
- (2) *ako je $R(k_1, \dots, k_n)$ netačno, onda $\vdash_{\mathcal{N}} \neg \mathcal{R}(\bar{k}_1, \dots, \bar{k}_n)$*

DEFINICIJA 4.3. *Neka je $R(x_1, \dots, x_n) \subseteq \mathbf{N}^n$. Tada se karakteristična funkcija $C_R(x_1, \dots, x_n)$ definiše na sledeći način*

$$C_R(x_1, \dots, x_n) = \begin{cases} 0 & \text{ako je } R(x_1, \dots, x_n) \text{ tačno} \\ 1 & \text{ako je } R(x_1, \dots, x_n) \text{ netačno} \end{cases}$$

Relacija $R(x_1, \dots, x_n)$ je prosto rekurzivna (rekurzivna) ako je $C_R(x_1, \dots, x_n)$ prosto rekurzivna funkcija.

TEOREMA 4.2. *Svaka rekurzivna relacija je predstavljiva u \mathcal{N} .*

Dokaz ove teoreme koristi činjenicu da je svaka rekurzivna funkcija predstavljiva u \mathcal{N} . Obzirom da je karakteristična funkcija rekurzivne relacije rekurzivna, dokaz direktno sledi.

Na osnovu prethodnih činjenica pokušaćemo da prikažemo dokaz Gödelove teoreme.

Dakle, ako je relacija $R(x, y)$ prosto rekurzivna, onda je ona predstavljiva nekom formulom $\mathcal{R}(x, y)$ od dve slobodne promenljive u \mathcal{N} i važi:

$$\begin{aligned} (k_1, k_2) \in R, \text{ tj. } R(k_1, k_2) \text{ onda je } \vdash_{\mathcal{N}} \mathcal{R}(\bar{k}_1, \bar{k}_2) \\ (k_1, k_2) \notin R, \text{ tj. nije } R(k_1, k_2) \text{ onda je } \vdash_{\mathcal{N}} \neg \mathcal{R}(\bar{k}_1, \bar{k}_2). \end{aligned}$$

Neka je $\mathcal{R} = \text{Proof} \in \mathbf{N} \times \mathbf{N}$. Pogledajmo formulu

$$(4.1) \quad (\forall x_2) \neg \text{Proof}(x_1, x_2),$$

gde je $\text{Proof}(x_1, x_2)$ formula koja u \mathcal{N} predstavlja relaciju $\text{Proof}(x_1, x_2)$ koja je rekurzivna.

Neka je m Gödelov broj formule (4.1). Uvrstimo m umesto x_1 u formulu (4.1). Dobijamo:

$$(4.2) \quad (\forall x_2) \neg \text{Proof}(\bar{m}, x_2),$$

što je rečenica ili tvrđenje u \mathcal{N} .

TEOREMA 4.3. (1) *Ako je \mathcal{N} neprotivrečan, onda je*

$$(\forall x_2)\neg \mathcal{P}roof(\bar{m}, x_2) \text{ nedokaziva u } \mathcal{N}.$$

(2) *Neka je \mathcal{N} ω -neprotivrečan, onda je*

$$\neg(\forall x_2)\neg \mathcal{P}roof(\bar{m}, x_2) \text{ nedokaziva u } \mathcal{N}.$$

Dokaz. (1) Pretpostavimo da je \mathcal{N} neprotivrečan i neka je (4.2) dokaziva u \mathcal{N} , tj.

$$\vdash_{\mathcal{N}} (\forall x_2)\neg \mathcal{P}roof(\bar{m}, x_2).$$

Neka je k Gödelov broj dokaza ove formule. Sledi da je $(m, k) \in \text{Proof}$. Kako formula $\mathcal{P}roof$ predstavlja Proof u \mathcal{N} , imamo $\vdash \mathcal{P}roof(\bar{m}, \bar{k})$. Iz pretpostavke imamo $\vdash (\forall x)\neg \mathcal{P}roof(\bar{m}, x)$, pa je na osnovu Ax4 kvantifikatorskog računa prvog reda $\vdash \neg \mathcal{P}roof(\bar{m}, \bar{k})$. Kontradikcija sa pretpostavkom da je \mathcal{N} neprotivrečan.

(2) Neka je \mathcal{N} ω -neprotivrečan i neka je (postoji dokaz)

$$\vdash \neg(\forall x_2)\neg \mathcal{P}roof(\bar{m}, x_2) \text{ u } \mathcal{N}.$$

Ovo je ekvivalentno sa

$$\vdash (\exists x_2)\mathcal{P}roof(\bar{m}, x_2).$$

Videli smo da je \mathcal{N} neprotivrečan ako je ω -neprotivrečan. Sledi da nije

$$\vdash (\forall x_2)\neg \mathcal{P}roof(\bar{m}, x_2).$$

Prema tome, za svaki prirodan broj n , n nije Gödelov broj dokaza formule (4.2). Dakle, za svako n , (m, n) nije u relaciji Proof . Sledi da je za svako n

$$\vdash \neg \mathcal{P}roof(\bar{m}, \bar{n})$$

Označimo

$$A(x_2) \equiv \neg \mathcal{P}roof(\bar{m}, x_2).$$

Vidimo da je za svako n , $\vdash A(\bar{n})$. \mathcal{N} je ω -neprotivrečan pa

$$\text{nije } \vdash (\exists x_2)\neg \neg \mathcal{P}roof(\bar{m}, x_2),$$

to jest

$$\text{nije } \vdash (\exists x_2)\mathcal{P}roof(\bar{m}, x_2).$$

Kontradikcija sa pretpostavkom. \square

Ovo praktično znači da postoji istinito tvrđenje u \mathcal{N} koje je nedokazivo u \mathcal{N} , pod uslovom da je \mathcal{N} neprotivrečan.

Druga Gödelova teorema direktno sledi iz prve:

TEOREMA 4.4. *Ako je \mathcal{N} neprotivrečan, onda se to ne može dokazati u \mathcal{N} .*

Iako su Gödel i von Neumann bili dobri prijatelji, nisu uspjeli da naprave neki zajednički rad, što je velika šteta. John von Neumann je primljen u bolnicu krajem 1955. godine, gde je ostao sve do svoje smrti februara 1957. godine. Nije bilo većeg druženja sa Gödelom jer je von Neumann radio na dizajniranju kompjutera EDVAC i bio je savetnik u nekim vojnim agencijama, uključujući i Manhattan Project. Po svemu sudeći, von Neumann je umro od prevelikog zračenja u laboartorijama Los Alamosa. Marta 1956. godine Gödel šalje von Neumannu pismo u kome prvi put praktično postavlja pitanje da li je $P = NP$.

Već u to vreme počele su rasprave da li će mašine nadmašiti čoveka u znanju i možda postati *svesne*. Takva pitanja se i danas postavljaju. Alan Turing nije odbacivao mogućnost da će mašine jednog dana nadmašiti ljude. U tome je bio preteča onoga što se danas naziva *Veštačka inteligencija*.

Turing je nametao argument da *mentalne procedure* ne mogu prevazilaziti mehaničke jer je ljudska memorija ograničena. Gödel je jednom napisao da:

Turingovi rezultati ne predstavljaju granice ljudskom mišljenju, već samo moćima formalnih sistema.

Gödel je smatrao da je 1969. godine otkrio grešku u Turingovom rezonovanju. Naime,

mozak u svom radu, nije statičan, već se stalno razvija.

Dakle, moguće je pretpostaviti da je u svakom trenutku broj svih stanja mozga (kao mašine) konačan, ali nema razloga zašto taj broj ne bi težio beskonačnosti u svom razvoju.

Za razliku od Posta i Turinga, on nije video svoje rezultate nepotpunosti kao ograničenje moći ljudskog rezonovanja, nego

da jedna vrsta ljudskog rezonovanja ne može biti potpuno mehanizovana.

Gödel je obožavao Leibnitza i tvrdio da su zli ljudi sakrili deo Leibnitsovih istraživanja.

Krajem 1977. godine Adele odlazi u bolnicu gde ostaje nekoliko nedelja. Gödel ostaje sam i odbija da jede bilo šta što Adele nije spremila. Iscrpljen od gladi dočekuje Adele koja ga ubeđuje da ide u bolnicu. Primljen je 29. decembra u prinstonsku bolnicu. Umire 14. januara 1978. godine od *neuhranjenosti i iscrpljenosti* uzrokovanih *personalnim poremećajem*, kako je glasilo bolnički nalaz.

Danas smo svedoci čestih zloupotreba Gödelove teoreme nekompletnosti. Ono što je sigurno, Gödelova popularnost sve više i više raste.

Od 1952. godine Gödel je uglavnom prerađivao svoje stare radove. Biran je za počasnog doktora na više univerziteta. Ogorčen na austrijske vlasti, odbija da bude član Austrijske akademije nauka.

Postavlja se pitanje da li postoje *apsolutno nedokaziva* tvrđenja, odnosno matematička tvrđenja koja su nedokaziva u bilo kom formalnom sistemu. Ovo je trivijalno netačno, jer ako je tvrđenje A nedokazivo u nekom formalnom sistemu, \mathcal{S} , onda se napravi sistem $\mathcal{S} + A$, gde je A nova aksioma, i kao takava teorema sistema $\mathcal{S} + A$. Naravno, ne misli se na takvu dokazivost.

Jedan pogled na teoremu nekompletnosti, koje su zagovarali Roger Penrose u knjigama [33], [34] i J.R. Lucas u radu [27], je da ova teorema navodi, čak dokazuje, da ljudski um prevazilazi bilo koju mašinu. Gödel nije bio tog mišljenja, već više nekakvog *dualnog stanovišta*, koje je poznato kao *Gödelova disjunkcija* koju je izneo u radu [12]

Ili se ljudsko mišljenje ne može obuhvatiti algoritmom ili ne postoje apsolutni nedokazivi problemi.

Postoji široko prihvaćeno mišljenje da bilo koje od ova dva stanovišta nije ubedljivo kako su formulisana. Kad kažemo *algoritam* mislimo na kompjuterski program, mašinu. Primetimo da sve do danas pojam bilo koje mašine ima ekvivalent koji je Turingova mašina. Kompjuteri su *otelotvorenje* Turingove mašine i upravo je Alan Turing čovek koji je konstruisao prvi kompjuter.

Gödelov argument, prema tumačenju Solomona Fefermana (1928-2016) u radu [7] sadrži neke pretpostavke, koje nisu navedene eksplicitno. One znatno olakšavaju objašnjenje Gödelove disjunkcije:

- (I) Ljudski um, u dokazu matematičkih istina, koristi samo evidentno tačne aksiome i evidentna pravila koja očuvavaju istinu u svakom koraku.
- (II) Aksiome i pravila zaključivanja koji su prihvatljivi za čovekov razum uključuju aksiome formalne aritmetike \mathcal{N} .
- (III) Pod konačnom mašinom podrazumevamo Turingovu mašinu koja obeležava (numerise) sve teoreme koje su dokazive ljudskim umom.

Pokazuje se da je ljudski um, kao proizvođač matematičke istine, ekvivalentan nekoj mašini (Turingovoj) isto je što i reći da je skup ljudski dokazivih teorema aksiomatizabilan u efektivno datom formalnom sistemu \mathcal{S} . Pretpostavimo da je to slučaj. Prema (I) ljudski um proizvodi samo istine, pa \mathcal{S} mora biti neprotivrečan. Prema (II) \mathcal{S} sadrži \mathcal{N} . Prema drugoj Gödelovoj teoremi neprotivrečnost je tačna ali nedokaziva, pa prema tome ljudski um je ne može dokazati, tako i negacija neprotivrečnosti ne može biti dokazana u \mathcal{S} . Kako je Gödel,

svojom numeracijom, pokazao da se neprotivrečnost \mathcal{S} može prikazati kao problem rešavanja Diofantove jednačine, dobijamo primer apsolutno nerešivog tvrđenja.

S druge strane, ako ljudski um nije ekvivalentan mašini, onda za svaku mašinu možemo naći tvrđenje koje ne može mašina izlistati kao teoremu. Ovo znači da ljudski um beskonačno prevazilazi bilo koju konačnu mašinu.

Kritička razmišljanja ovog argumenta kažu da ako Gödelovo tvrđenje shvatimo kao matematičku činjenicu, onda moramo dati matematičko značenje svim pojmovima koje koristimo u pretpostavkama. Jasno, teško da će bilo koji matematičar prihvatiti kao matematički pojam ljudski um.

U knjizi [44] Hao Wang navodi Gödelove reči:

Pod umom podrazumevam individualni um beskonačnog raspona (mogućnosti).

Pitanje da li je um mehanički, privlači danas pažnju istraživača u filozofiji, psihologiji, veštačkoj inteligenciji. Matematičari retko spominju aksiome u nameri da podrže svoja tvrđenja.

U svom čuvenom predavanju *Gödel and the end of Physics*, Hawking kaže:

Sve do sad, većina ljudi implicitno pretpostavlja da postoji Konačna teorija (Teorija svega), koju ćemo mi otkriti. Naravno, i ja sam sugerisao da možemo naći neku uskoro.

.....

Možda nije moguće formulisati teoriju univerzuma u konačno mnogo koraka. Ovo jako podseća na Gödelovu teoremu.

.....

Prema tome neka teorija u fizici je samoreferentna, kao Gödelova teorema. Prema tome, čovek može očekivati da bude ili protivrečna ili nekompletna. Teorije koje imamo do sada su oboje protivrečne i nekompletne. Neki ljudi će biti vrlo razočarani ako ne postoji konačna teorija, koja može biti formulisana kao konačan broj principa. I ja sam bio deo te grupe, ali sam se predomislio. Sad mi je drago da se naše traganje za razumevanjem neće nikad završiti, i da ćemo uvek imati izazov ka novom otkriću. Bez toga bismo stagnirali. Gödelove teoreme osiguravaju da će uvek biti posla za matematičare.

Pitanje *Da li je moguća Konačna teorija?* je sasvim nezavisno od svega prethodno razmatranog o aritmetici. Neodlučivost ne implicira da se Teorija svega ne može konstruisati. Gödel ne sprečava fizičare da to urade. Tvrđenje da Gödelovi ili Turingovi rezultati impliciraju logičku nemogućnost Teorije svega (konačne teorije) je isto kao tvrđenje

da se zbog teoreme nepotpunosti ne može konstruisati aksiomska logika.

U suštini, Entscheidungsproblem je negativan rezultat: *Nemoguće je algoritamski odlučiti da li su bilo koja aritmetička tvrđenja tačna ili lažna.*

Kao što je ranije rečeno, ovo je dokazao Alan Turing 1936. godine. Treba reći i da je veliki logičar Alonzo Church u isto vreme dobio taj rezultat nezavisno od Turinga. Za svoj dokaz Church je koristio svoju originalnu tvorevimu λ - račun.

Negativno rešenje Entscheidungsproblema nije obeshrabilo Turinga da na principima svoje *mašine* konstruiše prvi kompjuter. Naravno, sadašnji i budući računari neće moći dokazivati Gödelove samoreferentne formule ali će zato raditi mnoge druge značajne stvari.

Takđe, treba reći da se neprotivrečnost aritmetike može dokazati u složenijim sistemima, kao što je to uradio Gerhard Gentzen, [15]. Međutim, ovi složeniji sistemi imaju svoje probleme nepotpunosti i odlučivosti.

Naravno, u ovom radu izostavili smo mnoge teme osnova matematike kojima se Gödel bavio. Ne ulazeći u definicije i najnovije rezultate u vezi složenosti algoritama, pomenućemo ovde jedan od najpoznatijih otvorenih problema danas, $P = NP$. Kao što je rečeno, Gödel je poslao pismo von Neumannu, koji je ležao u bolnici marta 1956. godine iz koga se vidi da je Gödel bio na tragu ovog značajnog problema Teorije algoritama:

... Pošto se sada, koliko čujem, osećate bolje, dozvoliću sebi da vam pišem o matematičkom problemu, o kome me vaše mišljenje veoma interesuje: Možemo očigledno lako konstruisati Turingovu mašinu, koja za svaku formulu F logike prvog reda i svaki prirodan broj n , omogućava da odluči da li postoji dokaz formule F dužine n (dužina = broj simbola). Neka je $\Psi(F, n)$ broj koraka koji je za to potreban mašini i neka je $\varphi(n) = \max \Psi(F, n)$. Pitanje je koliko brzo raste $\varphi(n)$ za optimalnu mašinu. Može se pokazati da je $\varphi(n) \geq k \cdot n$. Ako bi stvarno postojala mašina sa $\varphi(n) \sim k \cdot n$ (ili čak $\sim k \cdot n^2$), ovo bi imalo posledice od velike važnosti. Naime, ovo bi očigledno značilo da uprkos neodlučivosti Entscheidungsproblema, mentalni rad matematičara po pitanju DA - ili - NE pitanja bi morao biti potpuno zamenjen mašinom. Posle svega, mogli bismo da izaberemo prigodan broj n dovoljno velik da ako mašina ne isporuči rezultat, više nema smisla razmišljati o problemu.

Na žalost, legenda kaže, da je već u to vreme von Neumann bio potpuno nesvestan događaja oko sebe.

Vratimo se sada na HSI i problem Tarskog. Pitanje kakav je odnos Gödelovih rezultata i problema Tarskog. Jasno, HSI se mogu izvesti iz aksioma \mathcal{N} , tj.

$$\mathcal{N} \vdash HSI.$$

$W(x, y)$ je identitet i \mathcal{N} je moćniji sistem od HSI . Naime, \mathcal{N} ima aksiomu indukcije, pa je moguć dokaz $W(x, y)$.

Priča o formalnoj aritmetici je, kao što smo videli, puna logičkih rezultata. Ono što do sada nismo videli u radovima je dokaz da je neki poznati problem Teorije brojeva nedokaziv. Na primer, Goldbachova hipoteza

Svaki paran broj veći od dva je zbir dva prosta broja.

Ako bismo dokazali da je Goldbachov problem nedokaziv, to bi značilo da je nedokaziv u Teoriji brojeva kao formalnoj teoriji. Možda možemo metodima Analize, Verovatnoće, jednog dana dokazati Goldbachovu hipotezu, kao što je to bio slučaj sa Velikom Fermatovom teoremom.

Ovaj naš rad je malo priznanje veličini genijalnih logičara Kurtu Gödelu i Alfredu Tarskom.

Jean Cocteau (1889-1963), pisac i režiser, je 1926. godine napisao

The worst tragedy for a poet is to be admired through being misunderstood.

Za logičara, specijalno onakvog kao Gödel, sa delikatnom psihologijom, tragedija je možda i veća.



SLIKA 4.1. Kurt Gödel u mladim danima



SLIKA 4.2. Kurt Gödel



SLIKA 4.3. Kurt Gödel i Alfred Tarski



SLIKA 4.4. Kurt Gödel i Alfred Tarski



SLIKA 4.5. Kurt Gödel i Albert Einstein

GLAVA 5

Zaključak

Centralna tema rada je Problem Tarskog. Šezdesetih godina prošlog veka Alfred Tarski je primetio da postoji samo jedanaest osnovnih identiteta koji važe u algebri pozitivnih celih brojeva \mathbf{N}^+ i čija posledica bi bili svi zakoni koji važe u \mathbf{N}^+ . Ove zakone učimo u osnovnoj i srednjoj školi. Velikan matematičke logike, Tarski, odmah je postavio problem

Da li su svi identiteti koji važe u algebri \mathbf{N}^+ sintaksna posledica jedanaest osnovnih identiteta?

Odgovor je negativan. U radu smo naveli identit koji nije posledica osnovnih identiteta aritmetike. Njega je pronašao engleski matematičar Wilkie osamdesetih godina prošlog veka. Mi smo u radu pokazali tačnost Wilkijevog identiteta. Postavilo se pitanje da li možda postoje neki drugi konačni skupovi identiteta u \mathbf{N}^+ čija posledica su svi zakoni aritmetike. Kao što smo naveli, odgovor je negativan. Ovo je pokazao Ruben Gurevič 1990. godine.

Rezultat i nije tako iznenađujući obzirom na Teoremu nekompaktnosti aritmetike koja je uzdrmla svet nauke uopšte. Ovo je 1931. godine dokazao austrijski matematičar Kurt Gödel. U radu se pominju Gödelovi rezultati iz Teorije relativnosti kojima je Gödel pokazao da iz jednačina Einsteinove teorije možemo pokazati da u našem univerzumu vreme ne postoji.

U radu je data skica dokaza Teoreme nekompaktnosti. Namera nam je bila da ovim radom pokažemo da se i najozbiljnije teoreme matematičke logike mogu predavati na akademskim studijama.

U decenijama koje su dolazile, posle Gödelovih rezultata, primećeno je da oni ne utiču mnogo na razvoj matematike kojom se svakodnevno bave istraživači. Naime, retko se dolazilo do nečeg što liči na *nedokazivost*.

Circulus viciosus nastaje kad se u praktičnim istraživanima pojavi mogućnost primene *samoreferentnih tvrdjenja*. Onda u Russellovom stilu ubacimo pojam dokaza kao promenljivu. Tako dobijamo da je nešto dokaz da to isto ne može biti dokaz.

Kao što smo naveli u radu, Gödelova teorema je direktno dovela do pojave računara, što se teško može reći za druge matematičke rezultate.

Na prvi pogled navedeni rezultati u radu ne ukazuju na neku praktičnu primenu. Ovo je samo delimično tačno. Pomenimo Coq softver koji zajedno sa Isabelle generičkim pomoćnim dokazivačem spada u interaktivne dokazivače. Između ostalog, navedeni softveri se razvijaju u centru za matematiku i statistiku Fakulteta tehničkih nauka u Novom Sadu.

Kad je u pitanju problem Tarskog, istaknimo da aktuelnost i primenljivost ovih rezultata potvrđuje njihova implementacija i verifikacija u interaktivnom dokazivaču, koji je u Coq uradio Joseph Tassarotti 2015. godine, [41].

Bibliografija

- [1] S. Burris, S. Lee, Small models of the high school identities, *International Journal of Algebra and Computation*, Vol. 2., No. 2. 139-178, 1992.
- [2] S. Burris, S. Lee, Tarski's high school identities, *American Mathematical Monthly*, 100, No. 3, 231-236, 1993.
- [3] S. Burris, K. Yeats, The Saga of the High School Identities, *Algebra Universalis*, Vol. 52, 325-342, 2008.
- [4] R. Dedekind, Was sind und was sollen die Zahlen, Vierweg, 1898.
- [5] R. Dedekind, Šta su i čemu služe brojevi? Matematički institut, Beograd, 1976.
- [6] J. Doneđ, A. Tarski, An extended arithmetic of ordinal numbers, *Fundamenta Mathematicae*, 65, 95-127, 1969.
- [7] S. Feferman, Are There Absolutely Unsolvable Problems? Gödel's Dichotomy, *Philosophia Mathematica (III)* 14 (2006), 134-152
- [8] K. Gödel, Die Vollständigkeit der Axiome des logischen Funktionen-kalküls, *Monatshefte für Mathematik und Physik*, 37, 349-360, 1930.
- [9] K. Gödel, Üformal unentscheidbare Sätze der Principia Mathematica und verwandeter Systeme I. Monatshefte für Mathematik und Physik, 39, 173-198, 1931.
- [10] K. Gödel, An example of a new type of cosmological solutions of Einstein field equations, *Reviews of modern physics* 21, 1949, 447-450.
- [11] K. Gödel, Rotating universes in general relativity theory, *Proceedings of the International Congress of Mathematics*, Cambridge, Massachusetts, USA, August 30 - September 6, 1950. Providence R.I.: American Mathematical Society, 1952.
- [12] K. Gödel, Some basic theorems on the foundations of mathematics and their implications, In: S. Feferman et al. (eds.) Kurt Gödel. *Collected Works*, Volume III: Unpublished Essays and Lectures. Oxford University Press, (1995) 304-323
- [13] R. Gödel, O. Taussky-Todd, S. Kleene, G. Kreisel, *Gödel Remembered*, Bibliopolis, 1983.
- [14] H. Grassmann, *Lehrbuch der Arithmetik*, Berlin, 1861.
- [15] G. Gentzen, *The Collected papers of Gerhard Gentzen*, ed.M.E. Szabo, North-Holland, 1969.
- [16] R. Gurevič, Equational theory of positive numbers with exponentiation is not finitely axiomatizable, *Annals of Pure and Applied Logic* 49, 1-30, 1990.
- [17] R. Gurevič, Equational theory of positive numbers with exponentiation, *Proc. Amer. math. Soc.* 94 : 135-146, 1985.
- [18] D. Hilbert, *Grundlagen der Geometrie*, Festschrift 1899.

- [19] D. Hilbert, W. Ackermann, Grundzüge der theoretischen Logik, Springer, Berlin, 1928.
- [20] D. Hilbert, P. Bernays, Grundlagen der Mathematik, Springer, Berlin, 1934.
- [21] D. Hofstadter, Gödel, Escher, Bach, Vintage Books Edition, 1980.
- [22] P. Janičić, Matematička logika u računarstvu, Matematički fakultet, Beograd 2009.
- [23] J. Ježek, Nonfinitely based three-element idempotent groupoids, Algebra Universalis, 20 (1985) 292-301.
- [24] P.E.B. Jourdain, The development of mathematical logic and the principles of mathematics, Quart. Jour. pure appl maths 43, 219-314, 1912.
- [25] R.L. Kruse, Identities satisfied by a finite rings, J. algebra 26, 298-318, 1973.
- [26] G. Lolli, Peano and the Foundations of Arithmetics, Fulvia Skaf (ed), Giuseppe Peano between Mathematics and Logics, 47-66
- [27] J.R. Lucas, Minds, Machines, and Gödel, Philosophy, July 1961 p. 112
- [28] I.V. Lvov, Varieties of associative rings I, II, algebra and Logic, 12150-167, 381-393, 1973.
- [29] R. Lyndon, Identities in two-valued calculi, Trans. Amer. Math. Soc. 71, 457-465, 1951
- [30] Ž., Mijačlović, Z. Marković, K. Došen, Hilbertovi problemi i logika, Mat. biblioteka 48, Zavod za udžbenike, Beograd, 1986.
- [31] R. McKenzie, Tarski's finite basis problem is undecidable, International Journal of Algebra and Computation Vol. 6, No.1 (1996) 49-104.
- [32] Sheila Oates and M.B. powell, Identical Relations in Finite Groups, Journal of Algebras 1, 11-39
- [33] R. Penrose, The Emperor's New Mind, Oxford University Press, 1989.
- [34] R. Penrose, Shadows of the Mind, Oxford University Press, 1994.
- [35] P. Marković, Problemi konačne baze identiteta u univerzalnoj algebri, prvi deo, Univerzitet u Novom Sadu, Prirodno matematički fakultet, Departman za matematiku, Novi Sad, 2005
- [36] P. Perkins, Bases for equationed theories of semigroups, J. Algebra 11 298-314, 1969.
- [37] E. Post, The two-valued iterative systems of mathematical logic, Anals of mathematical Studies, No 5, Princeton University Press N.J. 1941.
- [38] S. B. Prešić, Elementi matematičke logike, Matematička biblioteka, Zavod za udžbenike i nastana sredstva, Beograd, 1974.
- [39] D. Richardson, Solution of the identity problem for integral exponential functions, Zeitschr. f. math. Logik und Grundlagen d. Math. 15 (1969), 333-340
- [40] A. Tarski, Logic, Semantics, Mathematics. Hackett, Indianapolis, 1983. 1st edition edited and translated by J.H. Woodger, Oxford 1956.
- [41] Tassarotti, Formalization of Tarski's High School Algebra Problem in Coq. GitHub <https://github.com/jtassarotti/tarski-hsap>, 2015
- [42] A.N. Trahtman, the finite basis question for semigroups of order less than six, Semigroup Forum, Vol. 27 (1983) 387-389
- [43] A.M. Turing, On ccomputable numbers, with application to the Entscheidungsproblem, Proceedings of the London Mathematical Society, 42, 230-265, 1936.
- [44] H. Wang, A Logical Journey. From Gödel to Philosophy, Cambridge Mass, MIT Press, 2016.

- [45] A. I. Wilkie, On exponentiation - a solution to Tarski's high school problem, Oxford University 1980.
- [46] J. Zhang, Coputer Search for Counterexamples to Eilkie's Identity. R. Nieuwehuis (ed): CADE 2005, LNAI, 3632, 441-451, 2005
- [47] J.Zhang, H. Zhang, SEM: a System for Enumerating Models. Proc. of the 14th International conf. on Artif. Intel. (IJCAI-95), 268-303, 1995.



УНИВЕРЗИТЕТ У НОВОМ САДУ • ФАКУЛТЕТ ТЕХНИЧКИХ НАУКА
21000 НОВИ САД, Трг Доситеја Обрадовића 6

КЉУЧНА ДОКУМЕНТАЦИЈСКА ИНФОРМАЦИЈА

Редни број, РБР:	
Идентификациони број, ИБР:	
Тип документације, ТД:	Монографска документација
Тип записа, ТЗ:	Текстуални штампани материјал
Врста рада, ВР:	Дипломски – мастер рад
Аутор, АУ:	Марко-Георгије Црвенковић
Ментор, МН:	проф. др Силвиа Гилезан
Наслов рада, НР:	Ј еднакосна логика
Језик публикације, ЈП:	Српски / латиница
Језик извода, ЈИ:	Српски
Земља публиковања, ЗП:	Република Србија
Уже географско подручје, УГП:	Војводина
Година, ГО:	2021
Издавач, ИЗ:	Ауторски репринт
Место и адреса, МА:	Нови Сад; трг Доситеја Обрадовића 6
Физички опис рада, ФО: <small>(поглавља/страна/цифата/табела/слика/графика/прилога)</small>	5/69/46/0/5/10/0
Научна област, НО:	Математика
Научна дисциплина, НД:	Математичка логика
Предметна одредница/Кључне речи, ПО:	Релација једнакости, једнакосне класе алгебри, проблем Тарског, теорема некомплетности
УДК	
Чува се, ЧУ:	У библиотеци Факултета техничких наука, Нови Сад
Важна напомена, ВН:	
Извод, ИЗ:	Дати су основни појмови и теореме логике првог реда, као и једнакосне логике. Наводе се примери једнакосних класа алгебри. Основни модел је Формална теорија бројева, дата Пеановим аксиомама. Посебан део рада је посвећен Средњошколском проблему Тарског и приказан је елементаран део доказа. Такође, дата је скица доказа чувене теореме некомплетности К. Гедела.
Датум прихватања теме, ДП:	
Датум одбране, ДО:	
Чланови комисије, КО:	Председник: проф. Љубо Недовић
	Члан: проф. Петар Ђапић
	Члан, ментор: проф. др Силвиа Гилезан
	Потпис ментора



УНИВЕРЗИТЕТ У НОВОМ САДУ • ФАКУЛТЕТ ТЕХНИЧКИХ НАУКА
21000 НОВИ САД, Трг Доситеја Обрадовића 6

КЉУЧНА ДОКУМЕНТАЦИЈСКА ИНФОРМАЦИЈА

Accession number, ANO :	
Identification number, INO :	
Document type, DT :	Monographic publication
Type of record, TR :	Textual printed material
Contents code, CC :	Master Thesis
Author, AU :	Marko-Georgije Crvenković
Mentor, MN :	Professor Silvia Ghilezan
Title, TI :	Equational logic
Language of text, LT :	Serbian
Language of abstract, LA :	Serbian
Country of publication, CP :	Republic of Serbia
Locality of publication, LP :	Vojvodina
Publication year, PY :	2021
Publisher, PB :	Author's reprint
Publication place, PP :	Novi Sad, Dostiteja Obradovica sq. 6
Physical description, PD : <small>(chapters/pages/ref./tables/pictures/graphs/appendixes)</small>	5/69/46/0/5/10/0
Scientific field, SF :	Mathematics
Scientific discipline, SD :	Mathematical logic
Subject/Key words, S/KW :	Equational relation, equational classes of algebras, Tarski's problem, incompleteness theorem.
UC	
Holding data, HD :	The Library of Faculty of Technical Sciences, Novi Sad, Serbia
Note, N :	
Abstract, AB :	Basic notions and theorems of first order logic and equational logic are given. Some examples of equational classes of algebras are presented. The main model is Formal number theory, given by Peano axioms. The special part is devoted to Tarski's High School problem, and elementary part of the proof is presented. Also, the short proof of incompleteness theorem of K. Gödel is given.
Accepted by the Scientific Board on, ASB :	
Defended on, DE :	
Defended Board, DB :	President: Prof. Ljubo Nedović
	Member: Prof. Perat Đapić
	Member, Mentor: Prof. Silvia Ghilezan
	Mentor's sign