Sveučilište u Zagrebu
PMF - Matematički odjel

Filip Nikšić

Nepotpunost aritmetike

Seminarski rad iz Matematičke logike

Voditelj rada:
doc. dr. sc. Mladen Vuković

Zagreb, srpanj 2008.

1 Uvod

Malo povijesti

Još od početka 20. stoljeća njemački matematičar David Hilbert (1862.–1943.) ističe potrebu za formalizacijom matematike u vidu aksiomatskog sustava i potrebu za dokazom konzistentnosti takvog sustava. Svođenjem pitanja konzistentnosti geometrije na pitanje konzistentnosti analize i daljnjim svođenjem na pitanje konzistentnosti aritmetike dolazi do drugog na svojoj listi od 23 problema iznesenoj na Međunarodnom kongresu matematičara 1900.: direktno dokazati konzistentnost aritmetike.

Tokom godina kristaliziraju se pitanja i zahtjevi koje Hilbert smatra bitnima i načini na koje bi se na ta pitanja i zahtjeve trebalo odgovoriti, odnosno ispuniti ih. Početkom 1920-ih Hilbert zaokružuje svoje zahtjeve u prijedlogu utemeljenja matematike poznatom kao Hilbertov program. U svom programu on izražava potrebu i uvjerenje da je matematiku moguće formalizirati na način da se sve matematičke tvrdnje izraze u preciznom formalnom jeziku, da se dokaže potpunost i konzistentnost takvog sustava korištenjem konačnih operacija i dokaza, tj. korištenjem "konačnog rezoniranja", i da se otkrije algoritam koji odlučuje o istinitosti matematičkih tvrdnji.

1930. Kurt Gödel dokazuje da većina Hilbertovih želja ne može biti ostvarena, barem ne u tako općenitoj formulaciji. Naime, na konferenciji u Königsbergu (današnji Kalinjingrad) on iznosi svoj prvi teorem nepotpunosti, kojim se bavimo u ovom seminaru. Taj teorem ugrubo kaže da nijedna formalna teorija prvog reda s "prihvatljivim" skupom aksioma koja sadrži *Peanovu aritmetiku* ne može istovremeno biti potpuna i konzistentna.

Gödelov drugi teorem nepotpunosti kaže da nijedna konzistentna teorija s "prihvatljivim" skupom aksioma koja proširuje *Peanovu aritmetiku* ne može dokazati svoju konzistentnost. Mnogi smatraju da je upravo ovaj teorem zadao konačan udarac Hilbertovom programu jer on je upravo pitanje konzistentnosti smatrao najvažnijim.

Cilj i put do njega

Glavni cilj ovog seminara je dokaz slavnog *Gödelovog prvog teorema nepotpunosti.* Usput će biti dokazana još dva važna rezultata: *Tarskijev teorem o "nedefinabilnosti istine"* i *Churchov teorem o neodlučivosti logike prvog reda.*

Kako bi se došlo do tog cilja, potrebno je razraditi neke tehničke detalje. Naime, u odjeljku 2 vidjet ćemo kako možemo pričati o sintaksi aritmetike u terminima parcijalno rekurzivnih funkcija. To ćemo postići kodiranjem formula, rečenica, izvoda i dokaza.

U odjeljku 3 vidjet ćemo kako parcijalno rekurzivne funkcije možemo reprezentirati formulama i na taj način pričati o njima unutar teorije koju promatramo. Uvest ćemo minimalnu aritmetiku Q.

Kad spojimo odjeljke 2 i 3, dobijemo to da možemo pričati, tj. dokazivati stvari o sintaksi aritmetike unutar same aritmetike. To ćemo iskoristiti da u odjeljku 4 dokažemo *Gödelovu dijagonalnu lemu.* Naš cilj, Gödelov prvi teorem nepotpunosti, a i druga dva spomenuta teorema bit će posljedice te leme.

Pojmovi i oznake

Većina pojmova i oznaka preuzeta je iz [2] i [3].

Ističemo da će nam od značaja biti *logika prvog reda FO* čija je signatura zadana sa

$$\sigma_{FO} = \{A_i^n \mid n, i \in \mathbb{N}\} \cup \{f_j^m \mid m, j \in \mathbb{N}\}$$

pri čemu je A_i^n i-ti relacijski simbol mjesnosti n, a f_j^m j-ti funkcijski simbol mjesnosti m. Konstantskim simbolima smatramo funkcijske simbole mjesnosti 0.

Za potrebe ovog seminara smatramo da je skup logičkih simbola $\{\neg, \vee, \exists\}$. Ostale veznike ($\wedge, \rightarrow, \leftrightarrow$) i univerzalni kvantifikator $\forall$ također ćemo koristiti, ali smatramo da su oni izraženi preko $\neg$, $\vee$ i $\exists$.

Formalni račun nećemo posebno isticati jer nije bitno koji se koristi. Određenosti radi, kažimo da preuzimamo onaj iz [3].

Osim logike prvog reda, teorija koja nam je važna je *Peanova aritmetika PA*. Za detalje o toj teoriji čitatelj se upućuje na [3, str. 221–225]. Naglasimo samo da je njena signatura zadana sa

$$\sigma_{PA} = \{=, <, 0, ', +, \cdot\}$$

pri čemu je $=$ samo druga oznaka za A_0^2, $<$ druga oznaka za A_1^2, 0 je oznaka za f_0^0, $'$ za f_0^1, a $+$ i $\cdot$ za f_0^2 i f_1^2. Dakle, $=$ i $<$ su dvomjesni relacijski simboli, 0 je konstantski simbol, $'$ je jednomjesni funkcijski, a $+$ i $\cdot$ su dvomjesni funkcijski simboli. Vrijedi $\sigma_{PA} \subseteq \sigma_{FO}$.

Terme teorije PA oblika $0''^{\cdots}{}'$ gdje se $'$ pojavljuje n puta označavat ćemo s $\mathbf{n}$ i zvati *numerali*.

Standardni model teorije PA označavamo s ω. Njegov nosač je skup prirodnih brojeva $\mathbb{N}$, a interpretacije nelogičkih simbola su one očekivane (simbol $=$ je interpretiran relacijom jednakosti prirodnih brojeva, $<$ je interpretiran relacijom "manje", 0 označava broj nula, $'$ je interpretiran funkcijom sljedbenika, a interpretacije $+$ i $\cdot$ su zbrajanje i množenje prirodnih brojeva).

2 Aritmetizacija sintakse

Prvi korak k dokazu Gödelovog teorema nepotpunosti je kodiranje simbola, riječi, nizova riječi ili čak kompliciranijih objekata prirodnim brojevima. To je potrebno da bismo mogli govoriti o logici ili, konkretnije, o aritmetici s aspekta izračunljivosti. Primjerice, reći ćemo da je skup nekih objekata (simbola, riječi, nizova riječi, ...) rekurzivan ako je skup kôdova tih objekata rekurzivan. Kôd nekog objekta zovemo *Gödelov broj* tog objekta.

Samom kodiranju se može pristupiti na više načina. Koji način konkretno odaberemo nije osobito bitan. Bitno je samo da kodiranje, dekodiranje i još neke operacije nad kôdovima budu efektivno izvedive.

Jedna mogućnost kodiranja je sljedeća. Počnemo tako da kodiramo simbole alfabeta logike prvog reda na način prikazan u tablici 1. Zatim svaku riječ kodiramo tako da kodiramo konačan niz kôdova njenih simbola primjerice na način opisan u [2, str. 49–54]. Na isti način možemo nastaviti dalje: konačan niz riječi kodiramo tako da kodiramo konačan niz njihovih kôdova. Ako bismo pak htjeli kodirati konačan skup riječi, učinili bismo to tako da njihove kôdove poredamo uzlazno i kodiramo dobiveni konačan niz kôdova.

U [2, str. 49–54] je dokazano da su sljedeće funkcije, odnosno relacije primitivno rekurzivne:

- $\langle . \rangle : \mathbb{N}^k \to \mathbb{N}$, funkcija koja k-torki prirodnih brojeva pridružuje kôd. Primjerice, $\langle 1, 2, 3 \rangle = 2^{1+1} \cdot 3^{2+1} \cdot 5^{3+1} = 67500$.

Simbol	(	)	,	$\neg$	$\vee$	$\exists$	v_i	A_i^n	f_i^n
Kôd	1	3	5	7	9	11	$2\cdot 5^i$	$2^2\cdot 3^n\cdot 5^i$	$2^3\cdot 3^n\cdot 5^i$

Tablica 1: Gödelovi brojevi simbola logike prvog reda

- $\mathrm{lh}\colon \mathbb{N}\to\mathbb{N}$ koja kôdu konačnog niza pridružuje duljinu tog konačnog niza. Primjerice, $\mathrm{lh}(67500)=3$.
- $(.)\colon \mathbb{N}^2\to\mathbb{N}$, funkcija koja kôdu i broju i pridružuje broj na i-tom mjestu u kodiranom konačnom nizu. Primjerice, $(67500)_0=1$, a $(67500)_2=3$.
- Seq, jednomjesna relacija definirana sa

$$Seq(x) \qquad \Longleftrightarrow \qquad x \text{ je kôd nekog konačnog niza brojeva.}$$

- $*\colon \mathbb{N}^2\to\mathbb{N}$, funkcija koja kôdovima nizova $(x_0,\dots,x_{n-1})$ i $(y_0,\dots,y_{m-1})$ pridružuje kôd niza $(x_0,\dots,x_{n-1},y_0,\dots,y_{m-1})$. Ovakvo spajanje nizova zovemo konkatenacija.

Koristeći se navedenim i eventualno još nekim primitivno rekurzivnim funkcijama i relacijama dokazuje se sljedeći niz propozicija i korolara. Dokaze čitatelj može pronaći u [1, str. 187–197].

Propozicija 2.1. *Logičke operacije: negacija, disjunkcija, egzistencijalna kvantifikacija, supstitucija terma za slobodne nastupe varijable, itd. su rekurzivne.*

Dokaz. Ono što ova propozicija zapravo tvrdi je da je primjerice funkcija $\mathrm{neg}(x)=\langle n\rangle * x$ rekurzivna, pri čemu je x kôd formule, a n kôd simbola $\neg$. Drugim riječima, funkcija neg kôdu formule pridružuje kôd njene negacije. Jasno, ona je čak primitivno rekurzivna jer je konkatenacija primitivno rekurzivna funkcija.

Analogno, funkcije $\mathrm{disj}(x,y)=\langle l\rangle * x * \langle d\rangle * y * \langle r\rangle$ i $\mathrm{exquant}(v,x)=\langle e,v\rangle * x$ su primitivno rekurzivne, pri čemu su l,d,r,e,v redom kôdovi simbola za lijevu zagradu, logički veznik $\vee$, desnu zagradu, egzistencijalni kvantifikator $\exists$ i individualnu varijablu.

Budući da nam je $F\wedge G$ pokrata za $\neg(\neg F\vee\neg G)$, to je i konjunkcija rekurzivna. Tj. preciznije, funkcija $\mathrm{conj}(x,y)=\mathrm{neg}(\mathrm{disj}(\mathrm{neg}(x),\mathrm{neg}(y)))$ je rekurzivna. ■

Propozicija 2.2. *Skupovi formula i rečenica su rekurzivni.*

Propozicija 2.3. *Ako je Γ rekurzivan skup rečenica, onda je relacija 'Σ je izvod rečenice D iz skupa Γ' rekurzivna.*

Korolar 2.4. *Skup rečenica izvodljivih iz danog rekurzivnog skupa rečenica je rekurzivno prebrojiv.*

Korolar 2.5 (Gödelov teorem potpunosti, apstraktna forma)**.** *Skup valjanih rečenica je rekurzivno prebrojiv.*

Korolar 2.6. *Neka je Γ rekurzivan skup rečenica, a $D(x)$ formula u jeziku aritmetike. Tada:*

(a) Skup prirodnih brojeva n takvih da je $D(\mathbf{n})$ izvodljiva iz Γ je rekurzivno prebrojiv.

(b) *Skup prirodnih brojeva n takvih da je $\neg D(\mathbf{n})$ izvodljiva iz Γ je rekurzivno prebrojiv.*

(c) *Ako je za svaki n $D(\mathbf{n})$ ili $\neg D(\mathbf{n})$ izvodljiva iz Γ, onda je skup svih n takvih da je $D(\mathbf{n})$ izvodljiva iz Γ rekurzivan.*

Slijedi korolar koji ćemo kasnije direktno iskoristiti u dokazu Gödelova teorema nepotpunosti. Prije iskaza uvodimo terminologiju po uzoru na [1].

Kažemo da skup Γ *dokazuje* rečenicu D ako se D može izvesti iz Γ. Pišemo $\Gamma \vdash D$ ili $\vdash_\Gamma D$. Rečenice koje dokazuje Γ zovemo *teoremi* od Γ. Riječ *teorija* u ostatku rada koristimo za skup rečenica koji sadrži sve rečenice koje su iz njega dokazive. Dakle, za teoriju T je $\vdash_T D$ ako i samo ako je $D \in T$.

Definicija 2.1. Teorija T je *aksiomatizabilna* ako postoji rekurzivan skup $\Gamma \subseteq T$ takav da je $D \in T$ ako i samo ako je D teorem od Γ. Ako je još k tome Γ konačan, kažemo da je T *konačno aksiomatizabilna.*

Definicija 2.2. Skup rečenica Γ je *potpun* ako za svaku rečenicu D njegovog jezika vrijedi $\vdash_\Gamma D$ ili $\vdash_\Gamma \neg D$.

Dakle, teorija T je potpuna ako i samo ako za svaku rečenicu D njenog jezika vrijedi $D \in T$ ili $\neg D \in T$.

Definicija 2.3. Skup rečenica Γ je *konzistentan* ako ni za jednu rečenicu D njegovog jezika nije istovremeno $\vdash_\Gamma D$ i $\vdash_\Gamma \neg D$.

Ovako definiranoj konzistentnosti skupa Γ ekvivalentno je da postoji rečenica D koja nije teorem od Γ. Prema tome, teorija T je konzistentna ako i samo ako postoji rečenica D njenog jezika takva da $D \notin T$.

Definicija 2.4. Skup rečenica Γ je *odlučiv* ako je skup teorema od Γ rekurzivan.

Iz ovakve definicije odlučivosti slijedi da je teorija T odlučiva ako i samo ako je T rekurzivna.

Spremni smo iskazati najavljeni korolar:

Korolar 2.7. *Neka je T aksiomatizabilna teorija. Ako je T potpuna, onda je T odlučiva.*

Dokaz. Budući da je T aksiomatizabilna teorija, postoji rekurzivan skup rečenica $\Gamma \subseteq T$ takav da su rečenice teorije T one i samo one koje su izvodljive iz Γ. Označimo s T' skup Gödelovih brojeva rečenica iz T. Iz korolara 2.4 slijedi da je T' rekurzivno prebrojiv. Da bismo pokazali da je T odlučiva, moramo pokazati da je T' zapravo rekurzivan.

Kad bi teorija T sadržavala sve rečenice svog jezika, iz propozicije 2.2 slijedilo bi da je T' rekurzivan skup. Pretpostavimo stoga da T ne sadrži sve rečenice, tj. da je konzistentna.

Zajedno s potpunosti iz toga slijedi da rečenica D nije teorem od T ako i samo ako $\neg D$ je teorem od T. Stoga je komplement skupa T' unija skupa X brojeva koji uopće nisu kôdovi rečenica, i skupa Y kôdova rečenica čije negacije su teoremi od T.

X je rekurzivan kao komplement rekurzivnog skupa svih rečenica. Y je zapravo skup svih n takvih da je $\mathrm{neg}(n) \in T'$. Dakle, Y se može dobiti supstitucijom rekurzivne funkcije u rekurzivno prebrojiv skup. Iz toga slijedi da je i on rekurzivno prebrojiv.

Imamo: T' je rekurzivno prebrojiv i njegov komplement, $X \cup Y$ je rekurzivno prebrojiv. Slijedi da je T' rekurzivan. (Vidjeti primjerice teorem 1.88 u [2, str. 88].) ∎

3 Reprezentabilnost

Aritmetička definabilnost

Pokažimo sada kako parcijalno rekurzivne funkcije možemo reprezentirati formulama jezika aritmetike. Prvo ćemo pokazati da za svaku parcijalno rekurzivnu funkciju f postoji formula ϕ_f takva da za sve prirodne brojeve a i b vrijedi $f(a) = b$ ako i samo ako je formula $\forall y(\phi_f(\mathbf{a}, y) \leftrightarrow y = \mathbf{b})$ istinita na standardnom modelu ω teorije PA. Zatim ćemo uvesti nešto slabiju teoriju aritmetike Q i pokazati da za svaku parcijalno rekurzivnu funkciju f postoji formula ψ_f takva da za sve a i b vrijedi $f(a) = b$ ako i samo ako je formula $\forall y(\psi_f(\mathbf{a}, y) \leftrightarrow y = \mathbf{b})$ *dokaziva* u Q.

Dokazi svih lema, propozicija i teorema danih u ovom odjeljku mogu se pronaći u literaturi [1, str. 199-212].

U ostatku rada reći ćemo za formulu da je *točna* ako je istinita na standardnom modelu ω. Iskoristimo ovu pokratu kako bismo definirali *aritmetičku definabilnost*:

Definicija 3.1. Formula $F(x_0, \ldots, x_{k-1})$ jezika aritmetike *aritmetički definira* relaciju $R \subseteq \mathbb{N}^k$ ako i samo ako za sve $a_0, \ldots, a_{k-1} \in \mathbb{N}$ vrijedi $R(a_0, \ldots, a_{k-1})$ ako i samo ako je $F(\mathbf{a}_0, \ldots, \mathbf{a}_{k-1})$ točna. Relacija R je *aritmetički definabilna* ili, kraće, *aritmetička* ako i samo ako je neka formula aritmetički definira. k-mjesna funkcija f je aritmetička ako i samo ako neka formula aritmetički definira njen graf, tj. ako i samo ako postoji formula $F(x_0, \ldots, x_{k-1}, y)$ takva da je $f(a_0, \ldots, a_{k-1}) = b$ ako i samo ako je $F(\mathbf{a}_0, \ldots, \mathbf{a}_{k-1}, \mathbf{b})$ točna.

Prvi cilj nam je pokazati da su sve parcijalno rekurzivne funkcije aritmetičke. U tu svrhu dajemo nekoliko primjera koji će kasnije biti iskorišteni.

Primjer 3.1. Inicijalne funkcije su aritmetičke. Naime, projekciju $I^n_j(x_1, \ldots, x_n) = x_j$ aritmetički definira sljedeća formula:

$$x_1 = x_1 \land \ldots \land x_n = x_n \land y = x_j\,.$$

Nul-funkciju $z(x) = 0$ aritmetički definira formula $x = x \land y = \mathbf{0}$, a funkciju sljedbenika $s(x) = x + 1$ aritmetički definira formula $y = x'$.

Primjer 3.2. Zbrajanje i množenje su aritmetičke funkcije. Naime, funkciju zbrajanja aritmetički definira formula $y = x_1 + x_2$, dok funkciju množenja aritmetički definira formula $y = x_1 \cdot x_2$.

Primjer 3.3. Funkcija prethodnika, modificirano oduzimanje, kvocijent i ostatak su aritmetičke funkcije. Naime, prethodnik je aritmetički definiran formulom:

$$F_{\text{pred}}(x_1, y) \equiv (x_1 = \mathbf{0} \land y = \mathbf{0}) \lor x_1 = y'\,.$$

Modificirano oduzimanje je aritmetički definirano formulom:

$$F_{\text{dif}}(x_1, x_2, y) \equiv (x_1 < x_2 \land y = \mathbf{0}) \lor x_1 = x_2 + y\,.$$

Kvocijent i ostatak su aritmetički definirani formulama:

$$\begin{aligned}
&F_{\text{quo}}(x_1, x_2, y) \equiv (x_2 = \mathbf{0} \land y = \mathbf{0}) \lor (\exists u < x_2)(x_1 = y \cdot x_2 + u)\\
&F_{\text{rem}}(x_1, x_2, y) \equiv (x_2 = \mathbf{0} \land y = x_1) \lor (y < x_2 \land (\exists u \leqslant x_1)(x_1 = u \cdot x_2 + y))\,.
\end{aligned}$$

Lema 3.1. *(a) Svaka parcijalno rekurzivna funkcija je aritmetička.*

(b) Svaki rekurzivan skup je aritmetički.

Sljedeći cilj nam je analizirati kako izgledaju formule koje aritmetički definiraju parcijalno rekurzivne funkcije. Konkretno, zanimat će nas koliko puta je u njima primijenjena neograničena kvantifikacija. U tu svrhu definiramo različite vrste formula:

Definicija 3.2. Za formulu izgrađenu od atomarnih formula korištenjem negacije, disjunkcije, konjunkcije, kondicionala, bikondicionala i ograničenih kvantifikatora $\forall x < t$ i $\exists x < t$, gdje je t term, kažemo da je *rudimentarna formula.*

Za formulu oblika $\exists xF$, gdje je F rudimentarna formula, kažemo da je $\exists$-*rudimentarna.* Analogno, za formulu oblika $\forall xF$, gdje je F rudimentarna formula, kažemo da je $\forall$-*rudimentarna.*

Za formulu izgrađenu od $\exists$-rudimentarnih formula korištenjem negacije, disjunkcije, konjunkcije, kondicionala, bikondicionala, ograničenih univerzalnih i egzistencijalnih kvantifikatora i neograničenih egzistencijalnih kvantifikatora kažemo da je *generalizirana* $\exists$-rudimentarna formula.

Analizom dokaza leme 3.1 vidi se da su sve formule korištene za aritmetičko definiranje parcijalno rekurzivnih funkcija generalizirane $\exists$-rudimentarne. Stoga slijedi lema:

Lema 3.2. *Svaka parcijalno rekurzivna funkcija je aritmetički definabilna generaliziranom $\exists$-rudimentarnom formulom.*

Međutim, može se pokazati da je u iskazu prethodne leme riječ "generaliziranom" suvišna. Definirajmo prvo jedan novi pojam:

Definicija 3.3. Formule $F(x_0, \ldots, x_n)$ i $G(x_0, \ldots, x_n)$ su *aritmetički ekvivalentne* ako je za sve prirodne brojeve $a_0, \ldots, a_n$ formula $F(\mathbf{a}_0, \ldots, \mathbf{a}_n)$ točna ako i samo ako je $G(\mathbf{a}_0, \ldots, \mathbf{a}_n)$ točna.

Vrijede sljedeća propozicija i lema:

Propozicija 3.3. *Svaka generalizirana $\exists$-rudimentarna formula aritmetički je ekvivalentna nekoj $\exists$-rudimentarnoj formuli.*

Lema 3.4. *Svaka parcijalno rekurzivna funkcija aritmetički je definabilna $\exists$-rudimentarnom formulom.*

Dapače, ako funkciju koja je aritmetički definabilna rudimentarnom formulom nazovemo *rudimentarnom funkcijom*, može se pokazati da vrijedi sljedeća lema:

Lema 3.5. *Svaka parcijalno rekurzivna funkcija može se dobiti kompozicijom rudimentarnih funkcija.*

Definabilnost i reprezentabilnost

Vrijeme je da poopćimo pojam aritmetičke definabilnosti i uvedemo pojam reprezentabilnosti.

Definicija 3.4. Ako je T konzistentna teorija u jeziku aritmetike, kažemo da je relacija $R \subseteq \mathbb{N}^k$ *definirana* u T formulom $F(x_1, \ldots, x_k)$ ako za sve $a_1, \ldots, a_k \in \mathbb{N}$ vrijedi da ako je $R(a_1, \ldots, a_k)$, onda je $\vdash_T F(\mathbf{a}_1, \ldots, \mathbf{a}_k)$, a ako nije $R(a_1, \ldots, a_k)$, onda je $\vdash_T \neg F(\mathbf{a}_1, \ldots, \mathbf{a}_k)$.

Primijetimo da je aritmetička definabilnost specijalan slučaj definabilnosti kad je teorija T upravo prava aritmetika, tj. skup svih točnih rečenica.

Naravno, kao i kod aritmetičke definabilnosti, mogli bismo proširiti pojam definabilnosti na funkcije. Međutim, bit će nam važniji sljedeći pojam:

Definicija 3.5. k-mjesna totalna funkcija f je *reprezentabilna* u teoriji T ako postoji formula $F(x_1, \ldots, x_k, y)$ takva da $f(a_1, \ldots, a_k) = b$ povlači

$$\vdash_T \forall y(F(\mathbf{a}_1, \ldots, \mathbf{a}_k, y) \leftrightarrow y = \mathbf{b})\,.$$

Prethodna definicija je možda na prvi pogled čudna. Naime, odjednom govorimo samo o totalnim funkcijama. Demonstrirajmo na sljedećem primjeru čemu to služi i naglasimo da do kraja ovog odjeljka, kad spomenemo funkciju, mislimo na totalnu funkciju.

Primjer 3.4 (Reprezentabilnost povlači definabilnost)**.** Pretpostavimo da je f jednomjesna funkcija koja je u teoriji T reprezentirana formulom $F(x, y)$ i pokažimo da je njen graf G u T definiran upravo formulom $F(x, y)$.

Pretpostavimo prvo da za neke $a, b \in \mathbb{N}$ vrijedi $G(a, b)$. Tada je $f(a) = b$ pa imamo

$$\vdash_T \forall y(F(\mathbf{a}, y) \leftrightarrow y = \mathbf{b})\,.$$

Prethodna formula je logički ekvivalentna sljedećoj formuli:

$$F(\mathbf{a}, \mathbf{b}) \land \forall y(y \neq \mathbf{b} \to \neg F(\mathbf{a}, y))\,.$$

Stoga, ako je jedna teorem teorije T, onda je to i druga. Međutim, iz činjenice da je druga teorem slijedi

$$\vdash_T F(\mathbf{a}, \mathbf{b})\,.$$

Pretpostavimo sad da za neke $a, c \in \mathbb{N}$ ne vrijedi $G(a, c)$. Tad nije ni $f(a) = c$, ali zbog totalnosti funkcije f postoji $b \in \mathbb{N}$, očito različit od c, takav da je $f(a) = b$. Zbog reprezentabilnosti f opet slijedi

$$\vdash_T F(\mathbf{a}, \mathbf{b}) \land \forall y(y \neq \mathbf{b} \to \neg F(\mathbf{a}, y))$$

pa specijalno supstitucijom terma $\mathbf{c}$ slijedi

$$\vdash_T \mathbf{c} \neq \mathbf{b} \to \neg F(\mathbf{a}, \mathbf{c})\,.$$

Tu u igru ulazi detalj koji će vrijediti u teorijama koje mi promatramo. Naime, mora biti

$$\vdash_T \mathbf{c} \neq \mathbf{b}\,.$$

Ako to vrijedi, slijedi

$$\vdash_T \neg F(\mathbf{a}, \mathbf{c})\,.$$

Minimalna aritmetika Q

Sljedeći cilj nam je uvesti *minimalnu aritmetiku* Q, teoriju koja postavlja minimalne zahtjeve na to kako su interpretirani simboli iz skupa σ_{PA}, a da sve točne $\exists$-rudimentarne rečenice u njoj budu dokazive. Pokazat ćemo da su sve rekurzivne funkcije reprezentabilne u Q.

Reprezentabilnost rekurzivnih funkcija u Q povlači reprezentabilnost rekurzivnih funkcija i u svim teorijama koje sadrže Q. Budući da je Q relativno slaba teorija, dobiveni rezultat će biti jak.

Slijedi lista aksioma teorije Q, s tim da dajemo listu otvorenih formula čija su univerzalna zatvorenja stvarni aksiomi:

(Q1) $\mathbf{0} \neq x'$

(Q2) $x' = y' \rightarrow x = y$

(Q3) $x + \mathbf{0} = x$

(Q4) $x + y' = (x + y)'$

(Q5) $x \cdot \mathbf{0} = \mathbf{0}$

(Q6) $x \cdot y' = (x \cdot y) + x$

(Q7) $\neg(x < \mathbf{0})$

(Q8) $x < y' \leftrightarrow (x < y \vee x = y)$

(Q9) $x < y \vee x = y \vee y < x$

Teorija Q je teorija koja sadrži sve rečenice dokazive iz navedenih aksioma.

Teorem 3.6. *$\exists$-rudimentarna rečenica je točna ako i samo ako je teorem teorije Q.*

Lema 3.7. *Svaka rudimentarna funkcija reprezentabilna je u Q (i to rudimentarnom formulom).*

Lema 3.8. *Svaka kompozicija rudimentarnih funkcija reprezentabilna je u Q (i to $\exists$-rudimentarnom formulom).*

Iz prethodne leme i leme 3.5 slijedi glavni rezultat ovog odjeljka:

Teorem 3.9. *(a) Svaka rekurzivna funkcija je reprezentabilna u Q (i to $\exists$-rudimentarnom formulom).*

(b) Svaka rekurzivna relacija je definabilna u Q (i to $\exists$-rudimentarnom formulom).

4 Nepotpunost

Konačno imamo sve potrebno da zaokružimo priču i dokažemo poznati Gödelov teorem. Kao što je već spomenuto, to ćemo napraviti tako da prvo dokažemo Gödelovu dijagonalnu lemu.

U odjeljku 2 uveli smo pojam Gödelovog broja nekog objekta. Neka je A riječ u jeziku aritmetike i neka je a njen Gödelov broj. Numeral $\mathbf{a}$ zovemo *Gödelov numeral* riječi A. Označavamo ga s $\ulcorner A \urcorner$.

Definicija 4.1. Neka je A riječ u jeziku aritmetike. Definiramo njenu *dijagonalizaciju* kao riječ $\exists x(x = \ulcorner A \urcorner \land A)$.

Dijagonalizacija će nam biti najzanimljivija u slučaju formula $A(x)$ u kojoj je x jedina slobodna varijabla. Naime, u tom slučaju je dijagonalizacija od $A(x)$ formula $\exists x(x = \ulcorner A \urcorner \land A(x))$ koja je logički ekvivalentna s $A(\ulcorner A \urcorner)$.

Lema 4.1 (Dijagonalna lema)**.** *Neka je T teorija koja sadrži Q. Tad za svaku formulu $B(y)$ postoji rečenica G takva da je $\vdash_T G \leftrightarrow B(\ulcorner G \urcorner)$.*

Dokaz. Postoji (primitivno) rekurzivna funkcija diag koja Gödelovom broju a riječi A pridružuje Gödelov broj dijagonalizacije od A. Naime, ta funkcija je

$$\mathrm{diag}(a) = \mathrm{exquant}(\langle x \rangle, \mathrm{conj}(\langle i, l, x, c \rangle * \mathrm{num}(a) * \langle r \rangle, a)) .$$

Pritom su x, i, l, c, r redom kôdovi simbola za varijablu, znak jednakosti, lijevu zagradu, zarez i desnu zagradu, a funkcije exquant i conj su kao u propoziciji 2.1. Funkcija num je funkcija koja broju y pridruži kôd numerala $\mathbf{y}$. Možemo je dobiti primitivnom rekurzijom na sljedeći način:

$$\begin{aligned} \mathrm{num}(0) &= \langle \mathbf{0} \rangle \\ \mathrm{num}(y+1) &= \langle s, l \rangle * \mathrm{num}(y) * \langle r \rangle \end{aligned}$$

Pritom je s kôd za simbol $'$, a l i r su kôdovi za lijevu i desnu zagradu. Iz toga slijedi da je num (primitivno) rekurzivna funkcija.

Budući da T sadrži Q, iz teorema 3.9 slijedi da je diag reprezentabilna u T; označimo s $\mathrm{Diag}(x, y)$ formulu koja je reprezentira. Dakle, ako vrijedi $\mathrm{diag}(m) = n$, onda je $\vdash_T \forall y(\mathrm{Diag}(\mathbf{m}, y) \leftrightarrow y = \mathbf{n})$.

Neka je $A(x)$ formula $\exists y(\mathrm{Diag}(x, y) \land B(y))$ i neka su a njen Gödelov broj i $\mathbf{a}$ njen Gödelov numeral. Označimo s G dijagonalizaciju od $A(x)$:

$$G \equiv \exists x(x = \mathbf{a} \land \exists y(\mathrm{Diag}(x, y) \land B(y))) .$$

G je logički ekvivalentna formuli $A(\mathbf{a})$, tj. formuli $\exists y(\mathrm{Diag}(\mathbf{a}, y) \land B(y))$. Stoga je formula $G \leftrightarrow \exists y(\mathrm{Diag}(\mathbf{a}, y) \land B(y))$ valjana i kao takva dokaziva u svakoj teoriji:

$$\vdash_T G \leftrightarrow \exists y(\mathrm{Diag}(\mathbf{a}, y) \land B(y)) .$$

Označimo s g Gödelov broj rečenice G, a s $\mathbf{g}$ njen Gödelov numeral. Budući da je G dijagonalizacija formule $A(x)$, to je $\mathrm{diag}(a) = g$ pa slijedi

$$\vdash_T \forall y(\mathrm{Diag}(\mathbf{a}, y) \leftrightarrow y = \mathbf{g}) .$$

Koristeći teorem 2.55 i korolar 2.59 (teorem o zamjeni) iz [3, str. 179 i 181], zaključujemo da je

$$\vdash_T G \leftrightarrow \exists y(y = \mathbf{g} \land B(y)) ,$$

a kako je $\exists y(y = \mathbf{g} \land B(y))$ logički ekvivalentna formuli $B(\mathbf{g})$, slijedi

$$\vdash_T G \leftrightarrow B(\mathbf{g}) ,$$

što je i trebalo dokazati. ∎

Lema 4.2. *Neka je T konzistentna teorija koja proširuje Q. Tada skup Gödelovih brojeva teorema od T nije definabilan u T.*

Dokaz. Pretpostavimo da T proširuje Q i da je skup Θ Gödelovih brojeva rečenica iz T definiran u T formulom $\theta(y)$. Iz dijagonalne leme slijedi da postoji rečenica G takva da je

$$\vdash_T G \leftrightarrow \neg\theta(\ulcorner G \urcorner)\,. \qquad (\spadesuit)$$

Označimo s g Gödelov broj, a s $\mathbf{g}$ Gödelov numeral rečenice G.

Kad G ne bi bio teorem teorije T, imali bi $g \notin \Theta$, a zbog činjenice da $\theta(y)$ definira Θ to bi impliciralo $\vdash_T \neg\theta(\mathbf{g})$. No to nam, zajedno s ($\spadesuit$), daje $\vdash_T G$ pa je G ipak teorem od T.

Budući da je G teorem, g je u Θ pa vrijedi $\vdash_T \theta(\mathbf{g})$. No, zajedno s ($\spadesuit$), to nam daje $\vdash_T \neg G$. Zaključujemo da je teorija T inkonzistentna. ∎

Jednostavna posljedica prethodne leme je najavljeni Tarskijev teorem o "nedefinabilnosti istine".

Teorem 4.3 (Tarskijev teorem)**.** *Skup Gödelovih brojeva rečenica u jeziku aritmetike koje su točne (istinite na standardnom modelu ω) nije aritmetički definabilan.*

Dokaz. Direktno iz leme 4.2. Naime, ovdje se radi o pravoj aritmetici (skupu svih točnih rečenica) koja je konzistentno proširenje teorije Q. Aritmetička definabilnost je definabilnost u toj teoriji. ∎

Teorem 4.4 (Neodlučivost aritmetike)**.** *Skup Gödelovih brojeva rečenica u jeziku aritmetike koje su točne (istinite na standardnom modelu ω) nije rekurzivan.*

Dokaz. Direktno iz teorema 4.3 i 3.9. ∎

Teorem 4.5 (Teorem esencijalne neodlučivosti)**.** *Svako konzistentno proširenje teorije Q je neodlučivo. (Specijalno, Q je neodlučiva.)*

Dokaz. Neka je T konzistentno proširenje teorije Q. Iz leme 4.2 slijedi da skup Θ Gödelovih brojeva teorema od T nije definabilan u T. Budući da je svaki rekurzivan skup definabilan u Q (teorem 3.9), a time i u T, slijedi da Θ nije rekurzivan. No tad T nije odlučiva. ∎

Teorem 4.6 (Churchov teorem)**.** *Skup valjanih rečenica nije odlučiv.*

Dokaz. Označimo sa C konjunkciju svih aksioma teorije Q. Po teoremu potpunosti za teorije prvog reda A je teorem teorije Q ako i samo ako A logički slijedi iz C, a to je ako i samo ako je rečenica $(\neg C \vee A)$ valjana.

Funkcija f koja Gödelovom broju rečenice A pridružuje Gödelov broj rečenice $(\neg C \vee A)$ je rekurzivna jer je ona naprosto dana s $f(a) = \mathrm{disj}(\mathrm{neg}(c), a)$. Označimo li s Λ skup Gödelovih brojeva svih valjanih rečenica, vidimo da skup K Gödelovih brojeva teorema od Q možemo dobiti supstitucijom funkcije f u Λ. ($a \in K$ ako i samo ako je $f(a) \in \Lambda$.)

Stoga, kad bi Λ bio rekurzivan, to bi bio i K, što je u kontradikciji s teoremom 4.5. ∎

Konačno dolazimo i do glavnog cilja ovog seminara.

Teorem 4.7 (Gödelov prvi teorem nepotpunosti)**.** *Ne postoji konzistentno, potpuno, aksiomatizabilno proširenje teorije Q.*

Dokaz. Prema korolaru 2.7 svaka potpuna aksiomatizabilna teorija je odlučiva, a prema teoremu 4.5 svako konzistentno proširenje teorije Q je neodlučivo. ■

5 Zaključak

Gödelov prvi teorem nepotpunosti u obliku u kojem je u ovom radu iskazan i dokazan govori o teorijama koje proširuju Q. Jedna od tih teorija je Peanova aritmetika PA koja je zasigurno aksiomatizabilna. Prema tome, ako je konzistentna, mora biti nepotpuna.

Kako je Q relativno slaba teorija, budući da dokazuje samo osnovne stvari o aritmetici koje su nam bile potrebne za reprezentaciju rekurzivnih funkcija, to je dokazana verzija Gödelovog teorema odgovarajuće jaka.

Međutim, formalni sustavi mogu biti i takvi da im je nosač namijenjene strukture općenitiji od skupa prirodnih brojeva, ili u svom alfabetu nemaju aritmetičke simbole i stoga ne mogu direktno izraziti rečenice kao što su aksiomi teorije Q. Svejedno, ako je moguće da na nekakav indirektni način izraze i dokažu te aksiome, jasno je da će se ograničenja Gödelovog prvog teorema nepotpunosti i na njih odnositi.

Primjerice, unutar ZFC teorije skupova možemo definirati prirodne brojeve i izraziti i dokazati sve aksiome od Q. Jasno je da bismo onda mogli i reprezentirati rekurzivne funkcije i dokazati rezultate slične onima iznesenim u ovom radu. Prema tome, i za teoriju ZFC vrijedi da, ako je konzistentna, mora biti nepotpuna.

Na kraju, vratimo se Hilbertovom programu i želji za formalizacijom matematike. Osnovna želja tog programa bila je da se matematika svede na listu aksioma iz kojih se dokaznim postupkom može dokazati svaka istinita tvrdnja (i, naravno, samo istinite tvrdnje). Vjerojatno najvažnija stvar koju je Gödel rasvijetlio svojim teoremom je da *dokazivost* i *istinitost* nikako nisu jedno te isto.

Literatura

[1] George S. Boolos, John P. Burgess, and Richard C. Jeffrey. *Computability and Logic.* Cambridge University Press, 4th edition, 2002.

[2] Mladen Vuković. Izračunljivost. 2007.

[3] Mladen Vuković. *Matematička logika 1.* PMF-Matematički odjel, 2007.