Nepotpunost i neodlučivost aritmetike

Jelušić, Daniel

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Daniel Jelušić

NEPOTPUNOST I NEODLUČIVOST ARITMETIKE

Diplomski rad

Voditelj rada:
izv. prof. dr. sc. Mladen Vuković

Zagreb, lipanj 2015.

Ovaj diplomski rad obranjen je dana _____ pred ispitnim povjerenstvom u sastavu:

1. _____, predsjednik
2. _____, član
3. _____, član

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

Sadržaj

Uvod

U ovom radu predstavljamo Gödelove fundamentalne rezultate o nepotpunosti formalnih teorija koje su u nekom preciznom smislu dovoljno "bogate", te srodne rezultate Churcha i Tarskog koji govore o neodlučivosti takvih teorija i nedefinabilnosti aritmetičke istine.

Prije nego što krenemo korisno je dati kratki pregled povijesnih zbivanja koja su dovela do tih rezultata. Početkom 20. stoljeća matematičari su pokušavali formalizirati osnove matematike, što je dovodilo do raznih paradoksa poput Russelovog paradoksa u teoriji skupova. Rješenje za tu "krizu" predložio je engleski matematičar David Hilbert. Preciznije, Hilbert je u svom programu predložio da se cijela matematika formalizira kao sustav s konačnim skupom aksioma. Takav sustav bi trebao biti konzistentan (ne može dokazati kontradikcije) i potpun (mora biti u stanju dokazati sve istinite tvrdnje).

1931. godine austrijski matematičar Kurt Gödel dokazao je ([3]) da je Hilbertov program neostvariv već za naizgled vrlo slabe teorije. Neformalno, Gödelov prvi teorem nepotpunosti govori da svaka teorija s odlučivim skupom aksioma u kojoj se može vršiti elementarna aritmetika ne može biti istovremeno konzistentna i potpuna. Sam dokaz se svodi na konstrukciju rečenice γ unutar teorije koja u nekom smislu govori o sebi da nije dokaziva. Tada je γ istinita, ali nije dokaziva u danoj teoriji.

Napomenimo odmah da se ovakva interpretacija bitno razlikuje od stvarne tvrdnje Gödelovog teorema. Naime, Gödelov rezultat je čisto sintaktičke prirode, tj. ne poziva se na nikakav pojam istine. On samo tvrdi da postoji rečenica γ koja nije odlučiva u teoriji, odnosno da nije dokaziva γ niti njena negacija $\neg\gamma$. Prethodnu interpretaciju dobijemo ako rečenicama pridružimo istinosne vrijednosti, jer je tada istinita jedna od rečenica γ i $\neg\gamma$.

Da bismo mogli konstruirati gore opisanu samoreferentnu rečenicu, potrebno je formalizirati neke sintaktičke koncepte poput dokazivosti unutar same teorije. To se možda na prvi pogled čini nemoguće jer smo pretpostavili da naša teorija može samo govoriti o prirodnim brojevima i osnovnim aritmetičkim operacijama na njima. Gödel je imao ključnu ideju da rečenice teorije kodira prirodnim brojevima. Tada prije spomenuta svojstva poput dokazivosti postaju relacije na prirodnim brojevima,

koje se uz malo dosjetljivosti mogu definirati u jeziku teorije. O tome detaljnije govorimo u drugom i trećem poglavlju.

Sama činjenica da se takve relacije mogu definirati u jeziku teorije nije još dovoljna za dokaz prvog teorema nepotpunosti. Naime, potrebno je dokazati da dovoljno jake teorije mogu "govoriti" o tim relacijama, odnosno dokazivati neke tvrdnje o njima. Zato u četvrtom i petom poglavlju uvodimo pojam reprezentabilnosti i dokazujemo da je velika klasa rekurzivnih relacija, kojoj pripadaju i prije spomenute relacije, reprezentabilna već u relativno slabim teorijama poput Robinsonove aritmetike Q.

U šestom poglavlju dokazujemo centralni rezultat, lemu o fiksnoj točki, koja garantira postojanje gore spomenutih samoreferentnih rečenica. Iz te leme slijede Gödelov prvi teorem nepotpunosti, te teoremi Tarskog i Churcha kao jednostavne posljedice.

Konačno, u zadnjem poglavlju se kratko osvrćemo na Gödelov drugi teorem nepotpunosti koji govori da dovoljno jake konzistentne teorije ne mogu dokazati svoju konzistentnost.

Poglavlje 1

Osnovne definicije i rezultati

U ovom poglavlju navest ćemo neke osnovne pojmove i rezultate vezane uz teorije prvog reda. Kroz rad se podrazumijeva predznanje obuhvaćeno kolegijem Matematička logika, čije gradivo prati knjigu [10].

1.1 Jezici, termi i formule

Pojmovi jezika, terma i formule definirani su na standardan način. Jezik obično označavamo s $\mathcal{L}$ i podrazumijevamo da pripadni alfabet L sadrži logičke simbole $\wedge$ (konjunkcija), $\neg$ (negacija), $\forall$ (univerzalni kvantifikator), $\exists$ (egzistencijalni kvantifikator), znak jednakosti $=$, te pomoćne zagrade $(,)$. Ako su φ i ψ oznake za istu formulu tada pišemo $\varphi \equiv \psi$. Znak $\equiv$ nije simbol alfabeta već je pomoćni, tj. metasimbol i svrha mu je izbjegavanje dvoznačnosti. Varijable ćemo označavati s $v_0, v_1, ...$ i $x_0, x_1, ...$, a ostali logički simboli poput $\vee, \rightarrow$, itd. se definiraju na standardan način i uvode kao pokrate.

Konstante i varijable ćemo zvati *atomarni termi*. Skup svih varijabli danog alfabeta označavat ćemo s $\mathcal{V}(= \mathcal{V}_L)$, a skup svih terma s $\mathcal{T}(= \mathcal{T}_L)$. Terme bez varijabli zvat ćemo *zatvoreni termi*. Skup varijabli $var(t)$ terma t definiramo na sljedeći način:

$$var(t) = \{x \in \mathcal{V} \mid \text{ postoje riječi } \xi_0, \xi_1 \in \mathcal{L} \text{ takve da vrijedi } t \equiv \xi_0 x \xi_1\}$$

Na isti način definiramo $var(\alpha)$ za proizvoljnu formulu jezika. Formule oblika $s = t$, gdje su s i t termi, zovemo *atomarne formule*. Formule u kojima se ne javljaju kvantifikatori zvat ćemo *otvorene* formule. Ako formula α sadrži prefiks $\forall x$, tada pišemo $x \in bnd(\alpha)$. Skup $free(\alpha)$ *slobodnih* varijabli formule α definiramo kao

$free(\alpha) = var(\alpha)$ ako je α atomarna formula, a inače

$$free(\alpha \wedge \beta) = free(\alpha) \cup free(\beta), \quad free(\neg\alpha) = free(\alpha),$$
$$free(\forall x\, \alpha) = free(\alpha) \setminus \{x\}.$$

Formule bez slobodnih varijabli nazivamo *zatvorene formule* ili *rečenice*, a skup svih rečenica nekog jezika $\mathcal{L}$ označavamo s $\mathcal{L}^0$. Za formulu φ i term t definiramo *supstituciju* $\varphi\frac{t}{x}$ kao formulu dobivenu zamjenom svih slobodnih nastupa varijable x u φ termom t. Preciznije, prvo za terme definiramo induktivno

$$x\tfrac{t}{x} \equiv t, \quad y\tfrac{t}{x} \equiv y \text{ ako } x \neq y, \quad c\tfrac{t}{x} \equiv c, \quad f(t_1, ..., t_n)\tfrac{t}{x} \equiv f(t_1\tfrac{t}{x}, ..., t_n\tfrac{t}{x}).$$

Sada za atomarne formule definiramo $(t_1 = t_2)\frac{t}{x} \equiv (t_1\frac{t}{x} = t_2\frac{t}{x})$. Ako je r relacijski simbol, tada stavimo $(r\vec{t})\frac{t}{x} \equiv r(t_1\frac{t}{x}, ..., t_n\frac{t}{x})$. Još definiramo $(\alpha \wedge \beta)\frac{t}{x} \equiv \alpha\frac{t}{x} \wedge \beta\frac{t}{x}$, $(\neg\alpha)\frac{t}{x} \equiv \neg(\alpha\frac{t}{x})$. Konačno, $(\forall y\, \alpha)\frac{t}{x} \equiv \forall y\, \alpha$ ako je $x = y$, a $\forall y\, (\alpha\frac{t}{x})$ inače.

Kažemo da je term t slobodan za varijablu x u formuli α ako vrijedi $y \notin bnd(\alpha)$ za sve $y \in var(t) \setminus \{x\}$.

1.2 Teorije

Prije nego što definiramo teoriju opisat ćemo deduktivni sustav, odnosno račun logike prvog reda kojeg ćemo koristiti.

Definicija 1.1. ***Hilbertov račun*** *zadan je skupom* ***logičkih aksioma*** Λ*, koji se sastoji od svih formula oblika* $\forall x_1 \cdots \forall x_n\, \varphi$*, gdje je* φ *instanca jedne od sljedećih shema:*

$\Lambda 1$*:* $(\alpha \to (\beta \to \gamma)) \to ((\alpha \to \beta) \to (\alpha \to \gamma))$,

$\Lambda 2$*:* $(\alpha \to \beta) \to \alpha \wedge \beta$,

$\Lambda 3$*:* $\alpha \wedge \beta \to \alpha, \quad \alpha \wedge \beta \to \beta$,

$\Lambda 4$*:* $(\alpha \to \neg\beta) \to (\beta \to \neg\alpha)$,

$\Lambda 5$*:* $\forall x\, \alpha \to \alpha\frac{t}{x}$ *(t je slobodan za x u* α*),*

$\Lambda 6$*:* $\alpha \to \forall x\, \alpha \quad (x \notin free(\alpha))$,

$\Lambda 7$*:* $\forall x(\alpha \to \beta) \to \forall x\, \alpha \to \forall x\, \beta$,

$\Lambda 8$*:* $\forall y\, \alpha\frac{y}{x} \to \forall x\, \alpha \quad (y \notin var(\alpha))$,

$\Lambda 9$*:* $t = t$,

$\Lambda 10$*:* $x = y \to (\alpha \to \alpha\frac{y}{x})$ *(*α *atomarna).*

Dodatno, Hilbertov račun sadrži jedno pravilo izvoda ***modus ponens****, ili kraće* ***MP****, koje je definirano kao:*

$$MP: \quad \frac{\alpha, \alpha \to \beta}{\beta}$$

Pojmovi ***dokaza*** *i* ***izvoda iz skupa*** *su definirani na standardan način. Dokazivost formule α u Hilbertovom računu označavamo $s \vdash \alpha$, a izvedivost iz skupa S sa $S \vdash \alpha$.*

Ovo je primjer tzv. hilbertovskog deduktivnog sustava. Često se još koriste sustavi *prirodne dedukcije* koji imaju manji skup aksioma i više pravila izvoda. Kao što im ime govori, u takvim sustavima se dokazi provode na puno prirodniji način. Međutim, oni nisu prikladni za dokazivanje činjenica o samim teorijama. Zato smo ovdje izabrali Hilbertov račun, za koji se može pokazati da je ekvivalentan spomenutim sistemima prirodne dedukcije ([6]). Sada možemo definirati teoriju.

Definicija 1.2. *Neka je $\mathcal{L}$ neki jezik i $X \subseteq \mathcal{L}^0$. Kažemo da je skup $T \supseteq X$* ***teorija logike prvog reda*** *ili kratko* ***teorija*** *ako je $T \subseteq \mathcal{L}^0$ i T je deduktivno zatvoren u $\mathcal{L}^0$, odnosno ako vrijedi: $X \vdash \alpha$ ako i samo ako $\alpha \in T$. Ako je $\alpha \in T$ tada kažemo da je α* ***teorem*** *teorije T. To ćemo kraće označavati $s \vdash_T \alpha$. Ako je jasno o kojoj teoriji se radi, pisat ćemo samo $\vdash \alpha$.*

Uz ovakvu definiciju teorija kao skupova formula, možemo na prirodan način definirati pojam proširenja.

Definicija 1.3. *Neka su $\mathcal{L}$ i $\mathcal{L}_1$ jezici takvi da vrijedi $\mathcal{L}_1 \subseteq \mathcal{L}$, te neka su $T \subseteq \mathcal{L}^0$ i $T_1 \subseteq \mathcal{L}_1^0$ teorije. Kažemo da je T* ***proširenje*** *od T_1 ako vrijedi $T \supseteq T_1$. Teoriju T_1 tada zovemo* ***podteorija*** *od T.*

Ako za neku teoriju T i formule $\alpha, \beta \in \mathcal{L}^0$ vrijedi $\vdash_T \alpha \leftrightarrow \beta$, tada pišemo $\alpha \equiv_T \beta$ i kažemo da su α i β *ekvivalentne u T* ili *ekvivalentne modulo T*.

Za jezik $\mathcal{L}$ sa $\texttt{Taut}_{\mathcal{L}}$ označavamo najmanju teoriju u $\mathcal{L}$. Ona sadrži sve valjane rečenice jezika $\mathcal{L}$ i jedan skup aksioma za tu teoriju je prazan skup. Ako je $T \subseteq \mathcal{L}^0$ teorija i $\alpha \in \mathcal{L}^0$ tada ćemo s $T + \alpha$ označavati najmanje proširenje od T u jeziku $\mathcal{L}$ koje sadrži α. Slično ako je $S \subseteq \mathcal{L}^0$ definiramo $T + S$ kao najmanju teoriju koja sadrži $S \cup T$.

Za naša razmatranja posebno su važni pojmovi konzistentnosti i potpunosti teorije.

Definicija 1.4. *Kažemo da je teorija T* ***konzistentna*** *ako ne postoji formula $\alpha \in \mathcal{L}^0$ takva da vrijedi $\vdash_T \alpha$ i $\vdash_T \neg\alpha$. Ako T nije konzistentna tada kažemo da je* ***inkonzistentna****.*

Definicija 1.5. *Kažemo da je teorija T* ***potpuna*** *za svaku formulu $\alpha \in \mathcal{L}^0$ vrijedi $\vdash_T \alpha$ ili $\vdash_T \neg\alpha$. Ako T nije potpuna tada kažemo da je* ***nepotpuna****.*

Slijedi nekoloko rezultata o teorijama. Sljedeći teorem daje karakterizaciju konzistentnosti preko modela.

Teorem 1.6. *Teorija T je konzistentna ako i samo ako postoji model za T.*

Često ćemo bez posebnog naglaska koristiti teorem dedukcije za teorije prvog reda.

Teorem 1.7 (Teorem dedukcije)**.** *Neka je T teorija, $S \subseteq \mathcal{L}^0$ neki skup, te neka su $\alpha, \beta \in \mathcal{L}^0$. Tada vrijedi:*

$$\text{ako } S \cup \{\alpha\} \vdash_T \beta, \text{ onda } S \vdash_T \alpha \to \beta.$$

Na kraju navodimo još Gödelov teorem potpunosti, koji daje vezu između semantičke istine i sintaktičke dokazivosti u teorijama prvog reda.

Teorem 1.8 (Gödelov teorem potpunosti)**.** *Neka je T teorija i $\alpha \in \mathcal{L}^0$. Tada vrijedi:*

$$\vdash_T \alpha \text{ ako i samo ako za svaki model } \mathcal{M} \text{ od } T \text{ vrijedi } \mathcal{M} \models \alpha.$$

1.3 Jezik $\mathcal{L}_{ar}$ i teorija PA

Glavni jezik kojeg ćemo promatrati je jezik aritmetike $\mathcal{L}_{ar}$. On je određen skupom nelogičkih simbola $\{0, S, +, \cdot\}$, pri čemu je 0 konstantski simbol, S jednomjesni funkcijski simbol, a $+$ i $\cdot$ su dvomjesni funkcijski simboli. Uz $\mathcal{L}_{ar}$ vežemo *standardni model* $\mathcal{N}$ čiji je nosač skup $\mathbb{N}$. Pritom se simbolu 0 pridružuje broj 0, simbolu S funkcija sljedbenika $n \mapsto n + 1$, a simbolima $+$ i $\cdot$ odgovaraju funkcije zbrajanja i množenja.

U jeziku $\mathcal{L}_{ar}$ definiramo teoriju PA (Peanova aritmetika) sljedećim nelogičkim aksiomima:

1. $\forall x(Sx \neq 0)$,
2. $\forall x(x + 0 = x)$,
3. $\forall x(x \cdot 0 = 0)$,
4. $\forall x \forall y(Sx = Sy \to x = y)$,
5. $\forall x \forall y(x + Sy = S(x + y))$,

6. $\forall x \forall y (x \cdot Sy = x \cdot y + x)$,

Dodatno, aksiomi teorije PA su i instance *sheme aksioma indukcije*:

$$\text{IS}: \quad \varphi\tfrac{0}{x} \wedge \forall x(\varphi \to \varphi\tfrac{Sx}{x}) \to \forall x \varphi$$

U Peanovoj aritmetici se mogu dokazati sve dobro poznate elementarne istine o zbrajanju i množenju prirodnih brojeva, te mnogu drugi rezultati iz teorije brojeva. Zato je možda razumno očekivati da je PA potpuna teorija aritmetike. Još jedna činjenica koja ide u prilog tomu je potpunost tzv. Presburgerove aritmetike, koja je zapravo PA bez operacije množenja. Cijeli dokaz potpunosti može se naći u [2].

Ipak, PA nije potpuna, o čemu govori Gödelov prvi teorem nepotpunosti. Štoviše, vidjet ćemo da svako konzistentno proširenje od PA čiji su aksiomi u nekom smislu odlučivi nije potpuno.

Poglavlje 2

Rekurzivne funkcije i relacije

U ovom poglavlju definirat ćemo pojam primitivno rekurzivnih, te rekurzivnih funkcija i relacija. Svi pojmovi i tvrdnje koje navodimo detaljnije su definirani, odnosno dokazani u kolegiju Izračunljivost, a ovdje dajemo samo kratki pregled.

Rekurzivne funkcije predstavljaju matematičku formalizaciju klase funkcija koju intuitivno shvaćamo kao izračunljive. Funkcija f je izračunljiva u intuitivnom smislu ako postoji algoritam kojim možemo izračunati $f(\vec{a})$ za neki $\vec{a}$ u konačno mnogo koraka. Također je jasan zahtjev da se takav algoritam mora sastojati od konačno mnogo elementarnih instrukcija. Sada odmah vidimo da ne mogu sve funkcije biti izračunljive. Naime, već je skup unarnih funkcija na $\mathbb{N}$ neprebrojiv, dok algoritama može biti najviše prebrojivo mnogo. Sasvim analogna opažanja vrijede i za relacije, jer svaku relaciju možemo poistovijetiti s njezinom karakterističnom funkcijom.

Rekurzivne funkcije su važne za naša razmatranja jer se može pokazati da već relativno slabe teorije poput Robinsonove aritmetike Q mogu opisati, pa čak i reprezentirati bilo koju rekurzivnu funkciju, što se poklapa s našom intuicijom da se proces računanja takvih funkcija može potpuno opisati konačnim nizom simbola pomoću najosnovnijih aritmetičkih operacija. Više govora o tome biti će u poglavlju o reprezentabilnosti.

2.1 Definicija

U daljnjem tekstu prirodne brojeve označavat ćemo s $i, ..., n$ i $a, ..., e$. Skup svih n-mjesnih funkcija nad $\mathbb{N}$ označavamo sa $\mathbf{F}_n$. Neka je $f \in \mathbf{F}_m$ i $g_1, ..., g_m \in \mathbf{F}_n$. Tada za funkciju $h : \vec{a} \mapsto f(g_1(\vec{a}), ..., g_m(\vec{a}))$ kažemo da je dobivena *kompozicijom* f i funkcija g_i i pišemo $h = f[g_1, ..., g_m]$. Analogno za relacije definiramo $P[g_1, ..., g_m]$ kao $\{\vec{a} \in \mathbb{N}^n \mid P(g_1(\vec{a}), ..., g_m(\vec{a}))\}$.

Od izračunljivih funkcija očekujemo da zadovoljavaju sljedeća tri svojstva:

***Oc*:** Ako su $h \in \mathbf{F}_m$ i $g_1, ..., g_m \in \mathbf{F}_n$ izračunljive, tada je $f = h[g_1, ..., g_m]$ također izračunljiva.

***Op*:** Ako su $g \in \mathbf{F}_n$ i $h \in \mathbf{F}_{n+2}$ izračunljive, tada je izračunljiva funkcija $f \in \mathbf{F}_{n+1}$ definirana kao

$$f(\vec{a}, 0) = g(\vec{a}); \quad f(\vec{a}, Sb) = h(\vec{a}, b, f(\vec{a}, b)).$$

Kažemo da je f dobivena iz g, h *primitivnom rekurzijom.*

***Oμ*:** Ako je $g \in \mathbf{F}_{n+1}$ takva da za svaki $\vec{a}$ postoji b takav da vrijedi $g(\vec{a}, b) = 0$ i g je izračunljiva, tada je izračunljiva funkcija f definirana s $f(\vec{a}) = \mu b[g(\vec{a}, b) = 0]$. Kažemo da je f dobivena iz g *primjenom operatora* μ.

Sada smo spremni definirati primitivno rekurzivne i rekurzivne funkcije.

Definicija 2.1. *Skup* ***primitivno rekurzivnih*** *funkcija je najmanji skup koji je zatvoren na operacije* ***Oc, Op*** *te sadrži* ***inicijalne funkcije****: konstantnu funkciju* 0*, funkciju sljedbenika* S *i projekcije* $I^n_\nu : \vec{a} \mapsto a_\nu \, (1 \leq \nu \leq n)$*. Jednako definiramo skup* ***rekurzivnih*** *funkcija uz dodatnu zatvorenost na* ***Oμ****. Za skup ili relaciju kažemo da su (primitivno) rekurzivni ako im je karakteristična funkcija (primitivno) rekurzivna.*

2.2 Neka svojstva rekurzivnih funkcija i relacija

Lako se vidi da su gotovo sve poznate aritmetičke funkcije (zbrajanje, množenje, modificirano oduzimanje, prethodnik, signum funkcija itd.) primitivno rekurzivne. Nadalje, ako je f primitivno rekurzivna, tada je bilo koja funkcija nastala zamjenom, izjednačavanjem ili dodavanjem argumenata također primitivno rekurzivna. Ako su P, g, h primitivno rekurzivne, onda je također primitivno rekurzivna funkcija f definirana po slučajevima na sljedeći način:

$$f(\vec{a}) = \begin{cases} g(\vec{a}), & \text{ako } P(\vec{a}) \\ h(\vec{a}), & \text{inače} \end{cases}$$

To možemo vidjeti ako zapišemo f kao $f(\vec{a}) = g(\vec{a}) \cdot \chi_P(\vec{a}) + h(\vec{a}) \cdot \overline{sg}(\chi_P(\vec{a}))$.

U nastavku navodimo neke osnovne činjenice o (primitivno) rekurzivnim relacijama koje će nam kasnije biti potrebne.

1. Skup (primitivno) rekurzivnih relacija je zatvoren na konačne unije, presjeke i komplement relacija iste mjesnosti.

2. Neka su P i $Q \subseteq \mathbb{N}^{n+1}$. Ako vrijedi jedno od sljedećeg:

- $Q(\vec{a}, b) \Leftrightarrow (\forall k < b)P(\vec{a}, k)$,
- $Q(\vec{a}, b) \Leftrightarrow (\exists k < b)P(\vec{a}, k)$,
- $Q(\vec{a}, b) \Leftrightarrow (\forall k \leq b)P(\vec{a}, k)$,
- $Q(\vec{a}, b) \Leftrightarrow (\exists k \leq b)P(\vec{a}, k)$,

tada kažemo da je Q dobiven iz P *ograničenom kvantifikacijom.* Ako je P (primitivno) rekurzivna, tada je Q (primitivno) rekurzivna jer npr. za prvi slučaj vrijedi $\chi_Q(\vec{a}, b) = \prod_{k<b} \chi_P(\vec{a}, k)$, a za drugi $\chi_Q(\vec{a}, b) = sg\left(\sum_{k<b} \chi_P(\vec{a}, k)\right)$. Kao primjer, relacija djeljivosti $\mid$ i unarna relacija primarnosti `prim` su primitivno rekurzivne jer vrijedi: $a \mid b$ ako i samo ako postoji $k \leq b$ takav da $a \cdot k = b$ i $\texttt{prim}\, p$ ako i samo ako $p \neq 0, 1$ i za sve $a < p$ vrijedi $a \nmid p$ ili $a = 1$.

3. Neka $P \subseteq \mathbb{N}^{n+1}$ zadovoljava $\forall \vec{a}\, \exists b P(\vec{a}, b)$ i neka je $f(\vec{a}) = \mu k[P(\vec{a}, k)]$ najmanji k takav da vrijedi $P(\vec{a}, k)$. Tada je f rekurzivna ako je P rekurzivna. No f ne mora nužno biti primitivno rekurzivna ako je P primitivno rekurzivna Ipak, vrijedi sljedeće: ako je P primitivno rekurzivna tada je f definirana s $f(\vec{a}, m) = \mu k \leq m[P(\vec{a}, k)]$ primitivno rekurzivna, gdje je desna strana najmanji $k \leq m$ takav da $P(\vec{a}, k)$ ako takav k postoji, a m inače.

   Slično, ako je $h \in \mathbf{F}_n$ primitivno rekurzivna tada je $\vec{a} \mapsto \mu k \leq h(\vec{a})[P(\vec{a}, k)]$ primitivno rekurzivna. Pomoću ovoga možemo dokazati da je bijekcija $\wp(a, b) = \sum_{i \leq a+b}(i + a)$ primitivno rekurzivna.

2.3 Gödelovi brojevi

U nastavku će nam biti potreban način da kodiramo konačne nizove prirodnih brojeva. Jedna mogućnost je da uzastopno koristimo upravo definiranu funkciju $\wp$. Drugi način je da koristimo osnovni teorem algebre i pridružimo nizu produkt prostih brojeva s odgovarajućim potencijama. Mi ćemo koristiti drugi način.

Definicija 2.2. *Neka je $(a_0, ..., a_n)$ konačan niz prirodnih brojeva. Tada broj $\langle a_0, ...a_n\rangle := p_0^{a_0+1} \cdots p_n^{a_n+1}$ zovemo* ***Gödelov broj*** *niza $(a_0, ..., a_n)$. Prazni niz ima Gödelov broj 1 i označava se sa $\langle\rangle$. Skup svih Gödelovih brojeva označavamo s* `GN`*.*

Jasno je da vrijedi $\langle a_0, ...a_n\rangle = \langle b_0, ...b_m\rangle$ ako i samo ako je $m = n$ i $a_i = b_i$ za $i = 1, ..., n$. Nadalje, iz poznate činjenice da je funkcija $n \mapsto p_n$, gdje je p_n n-ti po redu prosti broj, primitivno rekurzivna slijedi da je funkcija $(a_0, ..., a_n) \mapsto \langle a_0, ...a_n\rangle$ primitivno rekurzivna. Skup `GN` je također primitivno rekurzivan jer pripadnost skupu možemo izraziti kao

$$a \in \texttt{GN} \Leftrightarrow a \neq 0\ \&\ (\forall p \leq a)(\forall q \leq p)[\texttt{prim}\, p, q\ \&\ p \mid a \Rightarrow q \mid a].$$

Sada još navodimo neke korisne funkcije vezane uz Gödelove brojeve koje će nam trebati u sljedećem poglavlju kada se budemo bavili aritmetizacijom sintakse. Ponovo koristeći činjenicu da je funkcija $n \mapsto p_n$ primitivno rekurzivna, definiramo primitivno rekurzivnu funkciju ℓ na sljedeći način:

$$\ell(a) = \mu k \leq a[p_k \nmid a].$$

Lako se vidi da je $\ell(a)$ duljina niza kodiranog Gödelovim brojem a. Zaista, $\ell(1) = 0$, a za $a = \langle a_0, ...a_n\rangle = \prod_{i\leq n} p_i^{a_i+1}$ očito imamo $\ell(a) = n + 1$.

Zatim promatramo funkciju $(a, i) \mapsto (a)_i$, koja je definirana sa:

$$(a)_i = \mu k \leq a[p_i^{k+2} \nmid a].$$

Opet je jasno da je funkcija primitivno rekurzivna i vrijedi $(\langle a_0, ..., a_n\rangle)_i = a_i$ za svaki $i \leq n$. Dakle, ova funkcija iz Gödelovog broja "čita" i-tu komponentu početnog niza.

Konačno definiramo *aritmetičku konkatenaciju* $*$ sa:

$$a * b = a \cdot \prod_{i<\ell(b)} p_{\ell(a)+i}^{(b)_i+1} \text{ za } a, b \in \mathtt{GN},\ a * b = 0 \text{ inače.}$$

Vidimo da je $*$ primitivno rekurzivna i da je $\mathtt{GN}$ zatvoren na $*$ jer vrijedi

$$\langle a_1, ..., a_n\rangle * \langle b_1, ..., b_m\rangle = \langle a_1, ..., a_n, b_1, ..., b_m\rangle.$$

Konkatenacija će nam poslužiti pri definiranju generalizirane verzije rekurzije ***Op***. Neka je $f \in \mathbf{F}_{n+1}$. Definiramo funkciju $\bar{f} \in \mathbf{F}_{n+1}$ sa:

$$\bar{f}(\vec{a}, 0) = \langle\rangle; \quad \bar{f}(\vec{a}, b) = \langle f(\vec{a}, 0), ..., f(\vec{a}, b-1)\rangle \text{ za } b > 0.$$

Neka je sada $F \in \mathbf{F}_{n+2}$. Tada postoji jedinstvena funkcija $f \in \mathbf{F}_{n+1}$ koja zadovoljava funkcijsku jednakost:

$$\boldsymbol{Oq}: \quad f(\vec{a}, b) = F(\vec{a}, b, \bar{f}(\vec{a}, b)).$$

Oq ćemo zvati shema *generalizirane rekurzije*.

Teorem 2.3. *Neka funkcija $f \in \mathbf{F}_{n+1}$ zadovoljava svojstvo **Oq**, odnosno neka vrijedi $f(\vec{a}, b) = F(\vec{a}, b, \overline{f}(\vec{a}, b))$. Ako je F primitivno rekurzivna tada je i f primitivno rekurzivna.*

Dokaz. Definiramo funkciju h sa $h(\vec{a}, b, c) = c * \langle F(\vec{a}, b, c)\rangle$. Funkcija h je očito primitivno rekurzivna. Dalje, imamo

$$\bar{f}(\vec{a}, 0) = 1;\ \bar{f}(\vec{a}, \mathrm{S}b) = \bar{f}(\vec{a}, b)) * \langle f(\vec{a}, b)\rangle = \bar{f}(\vec{a}, b) * \langle F(\vec{a}, b, \bar{f}(\vec{a}, b))\rangle = h(\vec{a}, b, \bar{f}(\vec{a}, b)),$$

pa je $\bar{f}$ primitivno rekurzivna po svojstvu ***Op***. No onda je i f primitivno rekurzivna kao kompozicija primitivno rekurzivnih funkcija. □

Za kraj još definiramo pojam rekurzivne prebrojivosti. Kažemo da je skup $M \subseteq \mathbb{N}$ *rekurzivno prebrojiv* ako postoji rekurzivna relacija $R \subseteq \mathbb{N}^2$ takva da vrijedi $M = \{b \in \mathbb{N} \mid (\exists a \in \mathbb{N})R(a, b)\}$.

Intuitivno, skup M je rekurzivno prebrojiv ako postoji algoritam A takav da je skup $\{A(0), A(1), ...\}$ točno jednak M. To se podudara s formalnom definicijom ako uzmemo u obzir sljedeći rezultat: $M \neq \emptyset$ je rekurzivno prebrojiv ako i samo ako je slika neke rekurzivne funkcije.

Općenitije, reći ćemo da je relacija $P \subseteq \mathbb{N}^n$ rekurzivno prebrojiva ako postoji $(n+1)$-mjesna relacija Q takva da vrijedi: $P\vec{a}$ ako i samo ako postoji $x \in \mathbb{N}$ takav da vrijedi $Q(x, \vec{a})$.

Poglavlje 3

Aritmetizacija sintakse

U prethodnom poglavlju definirali smo način kodiranja nizova prirodnih brojeva Gödelovim brojevima. Zatim smo pokazali da je takvo kodiranje efektivno, tj. funkcije koje kodiraju i dekodiraju dane nizove su primitivno rekurzivne. No, takvo kodiranje nije ograničeno samo na nizove prirodnih brojeva. Kao što ćemo sada vidjeti, možemo na isti način kodirati riječi nad proizvoljnim alfabetom tako da svakom simbolu alfabeta pridružimo jedinstven broj.

Posebno, cilj nam je kodirati sintaksu jezika formalne teorije. Nakon što smo svakom simbolu pridružili odgovarajući broj, formule možemo kodirati Gödelovim brojevima. Nadalje, dokaze možemo kodirati kao nizove formula. Na taj način sintaktička svojstva, relacije i operacije dane teorije dobivaju svoje aritmetičke ekvivalente. To dovodi do toga da možemo unutar jezika teorije izraziti neke metateorijske koncepte poput "f je Gödelov broj formule" ili "x je Gödelov broj dokaza formule s Gödelovim brojem y", što je, barem iz naše perspektive, ekvivalentno s "f je formula" ili "x je dokaz za y".

U ovom poglavlju ćemo dakle dokazati da su relacije koje opisuju te koncepte zaista primitivno rekurzivne. Koristit ćemo jezik $\mathcal{L} = \mathcal{L}_{ar}$, čiji su nelogički simboli $0, S, +, \cdot$ definirani u prvom poglavlju. To je jezik Peanove aritmetike PA.

3.1 Kodiranje simbola i riječi

Ako je ζ simbol jezika $\mathcal{L}_{ar}$, tada sa $\sharp\zeta$ označavamo pripadni kod. Simbolima iz $\mathcal{L}_{ar}$ pridružujemo redom neparne brojeve na sljedeći način:

ζ	$=$	$\neg$	$\wedge$	$\forall$	$($	$)$	0	S	$+$	$\cdot$	v_0	v_1	$\dots$
$\sharp\zeta$	1	3	5	7	9	11	13	15	17	19	21	23	

Sada proizvoljnu riječ $\xi = \zeta_0 \cdots \zeta_n$ alfabeta $\mathcal{L}_{ar}$ kodiramo kao

$$\langle \sharp\zeta_0, ..., \sharp\zeta_n \rangle = p_0^{1+\sharp\zeta_0} \cdots p_n^{1+\sharp\zeta_n}.$$

Broj $\langle \sharp\zeta_0, ..., \sharp\zeta_n \rangle$ zovemo Gödelov broj riječi ξ.

Primjer 3.1. *Term* 0 *i formula* $0 = 0$ *imaju još uvijek relativno malene Gödelove brojeve* $2^{1+\sharp 0} = 2^{14}$ *i* $2^{14} \cdot 3^2 \cdot 5^{14}$. *Gödelov broj terma* $\underline{1}$ *jednak je* $2^{16} \cdot 3^{14}$, *gdje s* $\underline{n}$ *označavamo numeral* $SS...0$ *(*S *se pojavljuje* n *puta). Već za malo dulje formule pripadni Gödelovi brojevi postaju jako veliki, pa takvo kodiranje nije ekonomično. No to za naše potrebe nije važno. Puno je važnija činjenica da ovakvo kodiranje bitno olakšava mnoge dokaze i definicije koje slijede. Uočimo još da je kod za simbol* $=$ *jednak Gödelovom broju prazne riječi. To isto ne predstavlja problem, jer ako promatramo* $=$ *kao riječ, ona ima Gödelov broj* $2^2 = 4$.

U daljnjem tekstu s ξ, η, ϑ označavat ćemo riječi nad $\mathcal{L}$, skup svih riječi nad $\mathcal{L}$ sa $\mathcal{S}_\mathcal{L}$, a Gödelov broj riječi ξ sa $\dot{\xi}$. Sa $\xi\eta$ označavat ćemo konkatenaciju riječi ξ i η (uočimo da tada vrijedi $(\xi\eta)^{\cdot} = \dot{\xi} * \dot{\eta}$), a sa $\dot{\mathcal{S}}_\mathcal{L}$ skup $\{\dot{\xi} \mid \xi \in \mathcal{S}_\mathcal{L}\}$. Skup $\dot{\mathcal{S}}_\mathcal{L}$ je primitivno rekurzivan jer vrijedi:

$$n \in \dot{\mathcal{S}}_\mathcal{L} \Leftrightarrow n \in \mathtt{GN} \;\&\; (\forall k < \ell(n))\, 2 \nmid (n)_k.$$

Na isti način za $W \subseteq \mathcal{S}_\mathcal{L}$ definiramo $\dot{W} = \{\dot{\xi} \mid \xi \in W\}$ i za n-mjesne relacije P nad riječima definiramo $\dot{P} = \{(\dot{\xi_0}, ..., \dot{\xi_n}) \mid P(\xi_0, ..., \xi_n)\}$. Kada kažemo da su W ili P (primitivno) rekurzivni podrazumijevamo da su $\dot{W}$, odnosno $\dot{P}$ (primitivno) rekurzivni. Tako kada govorimo o rekurzivnom aksiomatskom sistemu $X \subseteq \mathcal{S}_\mathcal{L}$ zapravo podrazumijevamo da je $\dot{X}$ rekurzivan.

Još preostaje definirati način kodiranja niza riječi. Gödelov broj niza riječi $\Phi = (\xi_0, ..., \xi_n)$ definiramo kao $\dot{\Phi} = \langle \dot{\xi_0}, ..., \dot{\xi_n} \rangle$. Ovakva definicija nam daje jednostavan način da razlikujemo kodove nizova riječi od kodova samih riječi. Naime, za niz riječi Φ vrijedi $2 \mid (\dot{\Phi})_0$, dok za riječ ξ vrijedi $2 \nmid (\dot{\xi})_0$.

Jasno je da se gornja konstrukcija može provesti za bilo koji *aritmetizabilan* jezik, tj. jezik s konačnim ili prebrojivim skupom simbola.

3.2 Relacija bew_T

Sada ćemo formalno definirati aritmetičku relaciju koja odgovara gore navedenoj rečenici "x je Gödelov broj dokaza formule s Gödelovim brojem y". Sa $\vdash$ označavat ćemo dokazivost u Hilbertovom računu opisanom u uvodnom poglavlju. Neka je T teorija sa skupom aksioma $X \subseteq T$. Neka su zatim $\tilde{\neg}, \tilde{\wedge}, \tilde{\rightarrow}$ primitivno rekurzivne funkcije definirane na sljedeći način: $\tilde{\neg}a := \dot{\neg} * a$, $a\tilde{\wedge}b := (a * \dot{\wedge} * b)^{\cdot}$ i $a\tilde{\rightarrow}b := \tilde{\neg}(a\tilde{\wedge}\tilde{\neg}b)$.

Definiramo relacije $proof_T$, bew_T i bwb_T na sljedeći način:

(1) $proof_T(b) \Leftrightarrow b \in \mathtt{GN}\ \&\ b \neq 1$
$\&\ (\forall k < \ell(b))[(b)_k \in \dot{X} \cup \dot{\Lambda} \vee (\exists i, j < k)(b)_i = (b)_j \tilde{\to} (b)_k]$,

(2) $bew_T(b, a) \Leftrightarrow proof_T(b)\ \&\ a = (b)_{\ell(b) \dot{-} 1}$,

(3) $bwb_T(a) \Leftrightarrow \exists b\ bew_T(b, a)$.

Iz definicije dokaza u teoriji jasno je da vrijedi: $proof_T(b)$ ako i samo ako je b Gödelov broj nekog dokaza u T. Iz toga odmah slijedi: $bew_T(b, a)$ ako i samo ako je b Gödelov broj dokaza formule s Gödelovim brojem a, što smo tražili. Vrijedi još napomenuti da u (1) nije potrebno zahtijevati da je $(b)_k$ formula. Indukcijom se lako pokaže da je taj uvjet uvijek zadovoljen ako je riječ o dokazu.

Propozicija 3.2. *Neka je T teorija čiji je jezik $\mathcal{L}_{ar}$ i neka je $\alpha \in \mathcal{L}^0_{ar}$. Tada vrijedi $\vdash_T \alpha$ ako i samo ako postoji $n \in \mathbb{N}$ takav da vrijedi $bew_T(n, \dot{\alpha})$, odnosno ako vrijedi $bwb_T(\dot{\alpha})$.*

Dokaz. Ako vrijedi $\vdash_T \alpha$, tada postoji dokaz za α u T. Neka je Φ jedan takav dokaz. Ako sada uzmemo $n = \dot{\Phi}$, tada očito vrijedi $bew_T(n, \dot{\alpha})$. Obratno, ako postoji n takav da vrijedi $bew_T(n, \dot{\alpha})$, tada je iz definicije relacije bew_T jasno da postoji dokaz za α u T, pa vrijedi $\vdash_T \alpha$. □

Istaknimo još da vrijede sljedeća svojstva relacija bew_T i bwb_T:

(a) Neka su $a, b, c, d \in \mathbb{N}$. Ako vrijedi $bew_T(c, a)$ i $bew_T(d, a \tilde{\to} b)$, tada vrijedi $bew_T(c * d * \langle b \rangle, b)$,

(b) Neka su $a, b \in \mathbb{N}$. Ako vrijedi $bwb_T(a)$ i $bwb_T(a \tilde{\to} b)$, tada vrijedi $bwb_T(b)$,

(c) Neka su $\alpha, \beta \in \mathcal{L}$. Ako vrijedi $bwb_T(\dot{\alpha})$ i $bwb_T(\alpha \to \beta)^{\cdot}$, tada vrijedi $bwb_T(\dot{\beta})$.

Primijetimo da svojstva (b) i (c) odmah slijede iz (a), a dokaz za (a) je nešto složeniji i može se naći u [6]. Svojstvo (a) je posebno važno jer iz njega slijedi jedan od uvjeta dokazivosti koji se koriste u dokazu Gödelovog drugog teorema nepotpunosti.

Slijedi najvažniji dio ovog poglavlja, gdje dokazujemo da su relacije $proof_T$ i bew_T primitivno rekurzivne. Iz (1) je jasno da samo trebamo dokazati da su skupovi $\dot{X}$ i $\dot{\Lambda}$ primitivno rekurzivni. Uz prethodno definirane funkcije $\tilde{\neg}, \tilde{\wedge}, \tilde{\to}$ dodatno definiramo $n \tilde{=} m := n * \dot{=} * m$ i $\tilde{\forall}(i, n) := \dot{\forall} * i * n$. Slično definiramo $\tilde{\exists}$. Konačno, stavimo $\tilde{S}n := \dot{S} * n$, $n \tilde{+} m := \dot{(} * n * \dot{+} * m * \dot{)}$, i slično za $\cdot$. Označimo još s $\xi \leq \eta$ nejednakost $\dot{\xi} \leq \dot{\eta}$. Jasno je da vrijedi $\xi \leq \eta$ ako je ξ podriječ od η. Napomenimo da dokazi koji slijede nisu sasvim neovisni o jeziku $\mathcal{L}$, pa ćemo radi jednostavnosti uzeti $\mathcal{L} = \mathcal{L}_{ar}$. No biti će jasno da su dokazi sasvim analogni za bilo koji aritmetizabilan jezik teorije.

Lema 3.3. *Skup $\mathcal{T}$ svih terma je primitivno rekurzivan.*

Dokaz. Po definiciji od $\mathcal{T}$ vrijedi $t \in \mathcal{T}$ ako i samo ako

$$t \in \mathcal{T}_{prim} \vee (\exists t_1, t_2 < t)[t_1, t_2 \in \mathcal{T} \;\&\; (t = St_1) \vee t = (t_1 + t_2) \vee t = (t_1 \cdot t_2)],$$

gdje je $\mathcal{T}_{prim}$ skup atomarnih terma. Uočimo da je $\mathcal{T}_{prim}$ primitivno rekurzivan jer vrijedi $n \in \dot{\mathcal{T}}_{prim} \Leftrightarrow n = 2^{14} \vee (\exists k \leq n) n = 2^{22+2k}$. Sada imamo

$$n \in \mathcal{T} \Leftrightarrow n \in \dot{\mathcal{T}}_{prim} \vee (\exists i, k < n)[i, k \in \dot{\mathcal{T}} \;\&\; Q(n, i, k)],$$

gdje je $Q(n, i, k) \Leftrightarrow (n = \tilde{S}i \vee n = i\tilde{+}k \vee n = i\tilde{\cdot}k)$. Relacije koje su dobivene na gore opisan način iz relacija definiranih na riječima jezika ćemo još zvati *aritmetizirane* relacije.

Sada možemo primijeniti prije definiranu generalnu rekurziju. Definiramo relaciju P na sljedeći način:

$$P(a, n) \Leftrightarrow n \in \dot{\mathcal{T}}_{prim} \vee (\exists i, k < n)[(a)_i = (a)_k = 1 \;\&\; Q(n, i, k)].$$

Relacija P je očito primitivno rekurzivna. Dalje, ako definiramo $f := \chi_{\dot{\mathcal{T}}}$ imamo

$$n \in \dot{\mathcal{T}} \Leftrightarrow n \in \dot{\mathcal{T}}_{prim} \vee (\exists i, k < n)[fi = fk = 1 \;\&\; Q(n, i, k)] \Leftrightarrow P(\bar{f}n, n).$$

Dakle, vrijedi $fn = 1$ ako i samo ako $n \in \dot{\mathcal{T}}$, što je ekvivalentno s $P(\bar{f}n, n)$, odnosno

$$\boldsymbol{Oq}: \quad fn = \chi_P(\bar{f}n, n) \text{ za svaki } n \in \mathbb{N},$$

pa je primitivno rekurzivna prema teoremu 2.3. □

Lema 3.4. *Skup $\mathcal{L}$ svih formula je primitivno rekurzivan.*

Dokaz. Skup atomarnih formula $\mathcal{L}_{prim}$ je primitivno rekurzivan jer vrijedi:

$$n \in \dot{\mathcal{L}}_{prim} \Leftrightarrow (\exists i, k < n)[i, k \in \dot{\mathcal{T}} \;\&\; n = (i\tilde{=}k)].$$

Sada je jasno da vrijedi $\varphi \in \mathcal{L}$ ako i samo ako

$$\varphi \in \mathcal{L}_{prim} \vee (\exists \alpha, \beta, x < \varphi)[\alpha, \beta \in \mathcal{L} \;\&\; x \in \mathcal{V} \;\&\; (\varphi = \neg\alpha \vee \varphi = (\alpha \wedge \beta) \vee \varphi = \forall x\alpha)].$$

Slično kao u prethodnoj lemi, pripadna aritmetizirana relacija ima oblik

$$n \in \dot{\mathcal{L}} \Leftrightarrow n \in \dot{\mathcal{L}}_{prim} \vee (\exists a, b, x < n)[fa = fb = 1 \;\&\; x \in \dot{\mathcal{V}} \;\&\; Q(n, a, b)]$$

uz $f = \chi_{\dot{\mathcal{L}}}$ i $Q(n,a,b) \Leftrightarrow (n = \tilde{\neg}a) \vee (n = a\tilde{\wedge}b) \vee (n = \tilde{\forall}(x,a))$. Zatim opet definiramo relaciju P sa:

$$P(a,n) \Leftrightarrow n \in \dot{\mathcal{L}}_{prim} \vee (\exists i,k,j < n)[(a)_i = (a)_k = 1 \;\&\; j \in \dot{\mathcal{V}} \;\&\; Q(i,k,j)],$$

pa opet dobivamo $fn = 1 \Leftrightarrow P(\bar{f}n, n)$ i

$$\boldsymbol{Oq}: \quad fn = \chi_P(\bar{f}n, n) \text{ za svaki } n \in \mathbb{N}.$$

□

Za dokaz sljedeće leme potrebna nam je aritmetizacija supstitucijske funkcije $\xi \mapsto \xi\frac{t}{x}$. Dakle, želimo funkciju *sub* za koju vrijedi $sub(\dot{\xi}, \dot{x}, \dot{t}) = (\xi\frac{t}{x})^{\cdot}$. U daljnjem tekstu ćemo umjesto $sub(\dot{\xi}, \dot{x}, \dot{t})$ često pisati $[\dot{\xi}]^{\dot{t}}_{\dot{x}}$. Po uzoru na rekurzivnu definiciju od $\xi\frac{t}{x}$ želimo definirati *sub* tako da za svaki $m \in \dot{\mathcal{L}} \cup \dot{\mathcal{T}}$, $i \in \dot{\mathcal{V}}$ i $k \in \mathbb{N}$ vrijede sljedeća svojstva:

- $[m]^k_i = k$ ako $i = m \in \dot{\mathcal{T}}_{prim}$, $[m]^k_i = m$ ako $i \neq m \in \dot{\mathcal{T}}_{prim}$,
- $[\tilde{\neg}m]^k_i = \tilde{\neg}[m]^k_i$, $[\tilde{S}m]^k_i = \tilde{S}[m]^k_i$,
- $[m\tilde{+}n]^k_i = [m]^k_i\tilde{+}[n]^k_i$, i slično za $\cdot, \wedge$ i $=$,
- $[\tilde{\forall}jm]^k_i = \tilde{\forall}(j,m)$ ako $j = i$, $[\tilde{\forall}jm]^k_i = \tilde{\forall}(j,[m]^k_i)$ inače.

Sada dajemo ideju za definiciju funkcije *sub*. Definiramo relaciju Q_{neg} sa:

$$Q_{neg}(m,n) \Leftrightarrow m \in \dot{\mathcal{L}} \cup \dot{\mathcal{T}} \;\&\; m = \tilde{\neg}n.$$

Slično definiramo relacije za simbole $S, +, \cdot, \wedge, \vee, \forall, =$. Sada definiramo funkciju $F : \mathbb{N}^4 \to \mathbb{N}$ na sljedeći način:

$$F(m,i,k,a) = \begin{cases} k, & i = m \in \dot{\mathcal{T}}_{prim} \\ m, & i \neq m \in \dot{\mathcal{T}}_{prim} \\ \tilde{\neg}(a)_{\mu n < m[Q_{neg}(m,n)]}, & \text{ako } \exists n < m \; Q_{neg}(m,n) \\ \vdots & \\ 0, & \text{inače} \end{cases}$$

Sasvim analogno definiramo ostale slučajeve za F. Vidimo da je F primitivno rekurzivna. Sada definiramo:

$$sub(m,i,k) := F(m,i,k,\overline{sub}(m,i,k))$$

Lako se provjeri da *sub* zadovoljava gore navedene zahtjeve. Nadalje, *sub* je primitivno rekurzivna jer zadovoljava svojstvo ***Oq***.

Sada možemo dokazati da su relacije $x \in var\,\xi$, $x \in bnd\,\alpha$, $x \in free\,\alpha$ primitivno rekurzivne. Naime, vrijedi

$$x \in var\,\xi \Leftrightarrow x \in \mathcal{V}\ \&\ (\exists \eta, \vartheta \leq \xi)(\xi = \eta x \vartheta),$$

$$x \in bnd\,\xi \Leftrightarrow x \in \mathcal{V}\ \&\ (\exists \eta, \vartheta \leq \xi)(\xi = \eta \forall x \vartheta),$$

$$x \in free\,\alpha \Leftrightarrow x \in \mathcal{V}\ \&\ \alpha\tfrac{0}{x} \neq \alpha\ (\Leftrightarrow \dot{x} \in \dot{\mathcal{V}}\ \&\ [\dot{\alpha}]_{\dot{x}}^{\dot{0}} \neq \dot{\alpha}).$$

Dakle skup svih zatvorenih formula $\mathcal{L}^0$ je primitivno rekurzivan. Nadalje, relacija "term t je slobodan za varijablu x u formuli α", u oznaci Cf, je primitivno rekurzivna jer vrijedi $Cf(t, x, \alpha)$ ako i samo ako

$$(\forall y < \alpha)[y \in bnd\,\alpha\ \&\ y \in var\,t \Rightarrow y = x].$$

Sada smo spremni dokazati najavljenu lemu.

Lema 3.5. *Skup* Λ *svih logičkih aksioma je primitivno rekurzivan.*

Dokaz. Aksiom $\Lambda 1$ je primitivno rekurzivan jer vrijedi $\varphi \in \Lambda 1$ ako i samo ako

$$(\exists \alpha, \beta, \gamma < \varphi)[\alpha, \beta, \gamma \in \mathcal{L}\ \&\ \varphi = (\alpha \to \beta \to \gamma) \to (\alpha \to \beta) \to (\alpha \to \gamma)].$$

Pripadnu aritmetiziranu relaciju dobijemo koristeći prethodno definiranu funkciju $\tilde{\to}$. Sasvim analogno pokazujemo da su aksiomi $\Lambda 2$-$\Lambda 4$ primitvno rekurzivni. Za aksiom $\Lambda 5$ vrijedi $\varphi \in \Lambda 5$ ako i samo ako

$$(\exists \alpha, x, t < \varphi)(\alpha \in \mathcal{L}\ \&\ x \in \mathcal{V}\ \&\ t \in \mathcal{T}\ \&\ \varphi = \forall x \alpha \to \alpha\tfrac{t}{x}\ \&\ Cf(t, x, \alpha)).$$

Slično za aksiome $\Lambda 6$-$\Lambda 10$. Dakle svi aksiomi su primitivno rekurzivni pa je i njihova unija Λ_0 primitivno rekurzivna. Sada svaki $\alpha \in \Lambda$ možemo zapisati kao $\alpha = \forall \vec{x} \alpha_0$, gdje je $\alpha_0 \in \Lambda_0$, a $\forall \vec{x}$ je proizvoljan (možda prazan) prefiks varijabli iz $\mathcal{V}$. Neka je sa Q definirana sljedeća dvomjesna relacija:

$$Q(m, n) \Leftrightarrow (\forall i < \ell m)[2 \mid i\ \&\ (m)_i = \sharp\forall\ \vee\ 2 \nmid i\ \&\ (\exists k \leq n)(m)_i = \sharp v_k].$$

Očito vrijedi $Q(m, n)$ ako i samo ako je m Gödelov broj gore opisanog prefiksa formule s Gödelovim brojem n. Konačno, Λ je primitivno rekurzivan jer vrijedi

$$n \in \dot{\Lambda} \Leftrightarrow n \in \dot{\mathcal{L}}\ \&\ (\exists m, k < n)(n = m * k\ \&\ 2 \mid \ell m\ \&\ k \in \dot{\Lambda}_0\ \&\ Q(m, n)).$$

□

Sada za proizvoljnu teoriju T nad aritmetizabilnim jezikom i s primitivno rekurzivnim skupom nelogičkih aksioma (podrazumijevamo da je skup logičkih aksioma jednak Λ) iz definicija (1) i (2) na stranici 15 slijedi da je bew_T primitivno rekurzivna. Ako uz to još primijetimo da vrijedi $\dot{T} = \{a \in \dot{\mathcal{L}}^0 \mid bwb_T a\}$, dokazali smo sljedeći teorem.

Teorem 3.6. *Neka je T teorija s aritmetizabilnim jezikom i s (primitivno) rekurzivnim skupom nelogičkih aksioma X. Tada je relacija bew_T (primitivno) rekurzivna. Nadalje, teorija T je rekurzivno prebrojiva.*

Kada budemo govorili o odlučivosti teorija, vidjet ćemo da se prethodni teorem može pojačati samo u posebnim slučajevima, npr. kada je T potpuna. Tada će relacija bwb_T biti rekurzivna. S druge strane, vidjet ćemo da to ne vrijedi već za jednostavne teorije poput Robinsonove aritmetike, koju ćemo definirati u sljedećem poglavlju. Time dobivamo prirodan primjer relacija koje su rekurzivno prebrojive, a nisu rekurzivne.

Poglavlje 4

Reprezentabilnost

Ovo poglavlje je priprema za iduću točku, gdje dokazujemo glavni rezultat o reprezentabilnosti rekurzivnih funkcija u teorijama $T \supseteq Q$. Intuitivno, reći ćemo da je relacija P reprezentabilna u T ako T može "govoriti" o P, odnosno ako se pripadnost relaciji P može unutar T opisati nekom formulom $\alpha(\vec{x})$.

Kada to povežemo s razmatranjima prethodnog i idućeg poglavlja dobit ćemo da proizvoljna teorija $T \supseteq Q$ može reprezentirati relaciju bew_T, što je ključni korak u konstrukciji Gödelove rečenice.

4.1 Teorija Q

Ovdje ćemo promatrati konačno aksiomatiziranu teoriju Q, poznatu još pod imenom Robinsonova aritmetika. Ona je zadana sljedećim aksiomima:

$Q1$: $\forall x(Sx \neq 0)$,

$Q2$: $\forall x \forall y(Sx = Sy \to x = y)$,

$Q3$: $(\forall x \neq 0)\exists y(x = Sy)$,

$Q4$: $\forall x(x + 0 = x)$,

$Q5$: $\forall x \forall y(x + Sy = S(x + y))$,

$Q6$: $\forall x(x \cdot 0 = 0)$,

$Q7$: $\forall x \forall y(x \cdot Sy = x \cdot y + x)$.

Lako se vidi da je Q podteorija Peanove aritmetike PA, dok su i jedna i druga podteorije od $Th\mathcal{N} = \{\alpha \in \mathcal{L}^0 \mid \mathcal{N} \models \alpha\}$, gdje je $\mathcal{N}$ standardni model (ℕ,0,S,+,·).

Za Q, PA i druge teorije nad $\mathcal{L}_{ar}$ uvodimo pokratu $x \leq y$ za formulu $\exists z(z+x = y)$ i $x < y$ za $x \leq y \wedge (x \neq y)$.

Propozicija 4.1. *Teorija Q je nepotpuna.*

Dokaz. Dokažimo da formula $\forall x\,(x \neq Sx)$ i njena negacija nisu dokazive u Q. U to se možemo uvjeriti ako promatramo model $\mathcal{N}^{\infty} = (\mathbb{N} \cup \{\infty\}, 0, S, +, \cdot)$, gdje su standardne operacije $S, +, \cdot$ proširene na $\mathbb{N} \cup \{\infty\}$ na sljedeći način:

$$\infty + n = n + \infty = \infty + \infty = n \cdot \infty = \infty \cdot m = \infty, \text{ za sve } n \text{ i sve } m \neq 0.$$

To je zaista model za Q jer zadovoljava sve nelogičke aksiome Q1-Q7. Međutim, vrijedi $\mathcal{N}^{\infty} \models \infty = S\infty$, pa $\mathcal{N}^{\infty} \not\models \forall x(x \neq Sx)$, a iz toga slijedi da formula $\forall x(x \neq Sx)$ nije dokaziva u Q.

S druge strane, metaindukcijom možemo pokazati da za svaki $n \in \mathbb{N}$ vrijedi $\underline{n} \neq S\underline{n}$. Baza indukcije $\vdash 0 \neq S0$ slijedi iz Q1. Pretpostavimo da vrijedi $\vdash \underline{n} \neq S\underline{n}$ za neki n. Sada $\vdash S\underline{n} \neq SS\underline{n}$ slijedi iz $\underline{n} \neq S\underline{n} \vdash S\underline{n} \neq SS\underline{n}$, a to dobivamo primjenom teorema dedukcije i $\Lambda 4$ na $S\underline{n} = SS\underline{n} \vdash \underline{n} = S\underline{n}$, što je jednostavna primjena Q2. Dakle, u Q nije dokazivo $\exists x(x = Sx)$, što je upravo negacija početne formule. □

Tvrdnja upravo dokazane propozicije nije nimalo čudna ako uzmemo u obzir da je Q zapravo PA bez indukcijske sheme. Navedeni primjer nedokazive rečenice upravo predstavlja tvrdnju koju bi unutar PA dokazivali indukcijom.
U dokazima koji slijede često ćemo koristiti činjenicu da vrijedi

$$\text{(L):} \quad \vdash s = t \;\text{ i }\; \vdash \alpha\tfrac{s}{x} \;\text{ povlači }\; \vdash \alpha\tfrac{t}{x}, \text{ gdje je } \alpha \text{ atomarna formula.}$$

Dokaz te tvrdnje za Hilbertov račun može se vidjeti u [6, s. 96]. Posebno, za proizvoljne terme t, t', t'', $\vdash t' = t$ i $\vdash t' = t''$ povlači $\vdash t = t''$ ako u gornjem za α uzmemo formulu $x = t''$.

Propozicija 4.2. *Za svaki $m, n \in \mathbb{N}$ u teoriji* Q *vrijedi:*

(C0): $Sx + \underline{n} = x + S\underline{n}$,

(C1): $\underline{m} + \underline{n} = \underline{m+n}$, $\underline{m} \cdot \underline{n} = \underline{m \cdot n}$,

(C2): $\underline{n} \neq \underline{m}$ *za* $n \neq m$,

(C3): $\underline{m} \leq \underline{n}$ *za* $m \leq n$,

(C4): $\underline{m} \not\leq \underline{n}$ *za* $m \not\leq n$,

(C5): $x \leq \underline{n} \leftrightarrow x = \underline{0} \vee \cdots \vee x = \underline{n}$,

(C6): $x \leq \underline{n} \vee \underline{n} \leq x$.

Dokaz. Tvrdnje (C0)-(C6) dokazujemo metaindukcijom po n.

(C0): Vrijedi za $n = 0$ jer $\vdash Sx + 0 = Sx = S(x + 0) = x + S0$ po Q4 i Q5. Pretpostavka indukcije je $\vdash Sx + \underline{n} = x + S\underline{n}$. Sada je $\vdash Sx + S\underline{n} = S(Sx + \underline{n}) = S(x + S\underline{n}) = x + SS\underline{n}$ po Q5.

(C1): $\vdash \underline{m} + 0 = \underline{m}$ po Q4, pa iz $\underline{m} = \underline{m + 0}$ slijedi baza indukcije. Pretpostavka indukcije daje $\vdash \underline{m} + S\underline{n} = S(\underline{m} + \underline{n}) = S\underline{m + n} = \underline{m + Sn}$ po Q5. Time smo dokazali korak indukcije. Analogno za $\vdash \underline{m} \cdot \underline{n} = \underline{m \cdot n}$.

(C2): Jasno za $n = 0$, jer je tada $m = Sk$ za neki k, pa je $\vdash 0 \neq \underline{m}$ po Q1. Pretpostavimo da $Sn \neq m$. Zbog Q1 tada vrijedi $\vdash \underline{Sn} \neq \underline{m}$ ako je m = 0. Inače $m = Sk$ za neki k, pa $n \neq k$ i $\vdash \underline{n} \neq \underline{k}$ po pretpostavci indukcije. Dakle, $\vdash \underline{Sn} \neq \underline{m}$ po Q2.

(C3): $m \leq n$ povlači $k + m = n$ za neki k, pa $\underline{k + m} = \underline{n}$. Slijedi $\vdash \underline{k} + \underline{m} = \underline{n}$ po (C1). Dakle, $\vdash \exists z\, z + \underline{m} = \underline{n}$, što znači $\vdash \underline{m} \leq \underline{n}$.

(C4): $m \not\leq n \Rightarrow m \neq 0$, pa $m = Sk$ za neki k. Neka vrijedi $m \not\leq 0$. Tada $\vdash \underline{m} \not\leq 0$ jer $\underline{m} \leq 0 \vdash S\underline{k} \leq 0 \vdash \exists v\, v + S\underline{k} = 0 \vdash \exists v\, S(v + \underline{k}) = 0 \vdash \bot$ po Q1. Neka je sada $m \not\leq Sn$. Tada $k \not\leq n$ pa vrijedi $\vdash \underline{k} \not\leq \underline{n}$ po pretpostavci indukcije, što daje $\vdash \underline{m} \not\leq S\underline{n}$ po Q2.

(C5): Indukcijom dokazujemo da vrijedi $x \leq \underline{n} \vdash x = \underline{0} \vee \cdots \vee x = \underline{n}$. Ako je $n = 0$, tada vrijedi $x \neq 0$, $x \leq 0 \vdash \exists v\, Sv = 0 \vdash \bot$ po Q3, Q5, Q1. Korak indukcije je ekvivalentan s $x \neq 0$, $x \leq \underline{Sn} \vdash \bigvee_{i=1}^{n+1} x = \underline{i}$ i dobije se na sljedeći način:

$$\begin{aligned} x \neq 0,\, x \leq \underline{Sn} &\vdash \exists y(x = Sy \wedge y \leq \underline{n}) \quad \text{(Q3, Q5, Q2)} \\ &\vdash \exists y(x = Sy \wedge \bigvee_{i \leq n} y = \underline{i}) \quad \text{(pretpostavka indukcije)} \\ &\vdash \exists y(x = Sy \wedge \bigvee_{i=1}^{n+1} Sy = \underline{i}) \equiv_Q \bigvee_{i=1}^{n+1} x = \underline{i} \end{aligned}$$

Obratno, neka vrijedi $\vdash x = \underline{0} \vee \cdots \vee x = \underline{n}$. Zbog (C3), svaka disjunkcija daje $\vdash x \leq \underline{n}$, pa dobivamo $\vdash x \leq \underline{n}$.

(C6): Jasno za $n = 0$ jer $\vdash 0 \leq x$. Nadalje, $\underline{n} < x \vdash \exists y\, Sy + \underline{n} = x \vdash \exists y\, y + S\underline{n} = x$, po Q3 i Q0 koristeći $\vdash 0 + \underline{n} = \underline{n}$ što se može dokazati indukcijom. Dakle, $\underline{n} < x \vdash S\underline{n} \leq x$. (C5) i (C3) daju $x \leq \underline{n} \vdash x \leq \underline{Sn}$. To nam sad, zajedno s prethodno dokazanim, daje korak indukcije, jer $x \leq \underline{n} \vee \underline{n} \leq x \vdash x \leq \underline{n} \vee \underline{n} < x \vdash x \leq \underline{Sn} \vee \underline{Sn} \leq x$. □

Posebno, iz (C5) slijedi $x \leq \underline{n} \vdash x = \underline{0} \vee \cdots \vee x = \underline{n-1}$, ili kratko $x < n \vdash \bigvee_{i<n} x = \underline{i}$.

4.2 Pojam reprezentabilnosti

Definicija 4.3. *Neka je $P \subseteq \mathbb{N}^n$ relacija. Kažemo da je P* ***reprezentabilna*** *u teoriji $T \supseteq Q$ ako postoji formula $\alpha = \alpha(\vec{x})$ (****reprezentirajuća formula****) takva da vrijedi:*

$$(R^+): \text{ ako } P\vec{a}, \text{ tada } \vdash_T \alpha(\underline{\vec{a}}),$$
$$(R^-): \text{ ako } \neg P\vec{a}, \text{ tada } \vdash_T \neg\alpha(\underline{\vec{a}}).$$

Na primjer, relaciju $\{(a,a) \mid a \in \mathbb{N}\}$ reprezentira formula $x = y$, jer zbog $\Lambda 9$ vrijedi $\vdash \underline{a} = \underline{b}$ ako $a = b$, a inače iz (C2) slijedi $\vdash \underline{a} \neq \underline{b}$, dok po (C3) i (C4) formula $x \leq y$ reprezentira relaciju $\leq$. Prazan skup je reprezentiran bilo kojom formulom α za koju vrijedi $\neg\alpha \in Q$. Jasno je da se reprezentacije dobro ponašaju za presjek i negaciju relacija. Ako su P, Q reprezentirane redom s $\alpha(\vec{x}), \beta(\vec{x})$, tada je $P \cap Q$ reprezentirana formulom $\alpha(\vec{x}) \wedge \beta(\vec{x})$, a $\neg P$ formulom $\neg\alpha(\vec{x})$. Sljedeća propozicija govori da Q korektno "odlučuje" sve aritmetičke jednakosti. Za neku formulu $\varphi(\vec{x})$ kažemo da definira relaciju $R(\vec{x})$ ako vrijedi: $R(\vec{a})$ ako i samo ako je $\varphi(\vec{a})$ istinita.

Propozicija 4.4. *Neka je $\varphi(\vec{x})$ formula oblika $\tau(\vec{x}) = \rho(\vec{x})$, gdje su $\tau(\vec{x})$ i $\rho(\vec{x})$ termi. Tada φ reprezentira u Q relaciju koju definira.*

Dokaz. Pretpostavimo da za neki $\vec{a}$ vrijedi $\mathcal{N} \models \varphi(\underline{\vec{a}})$, odnosno $\mathcal{N} \models \tau(\underline{\vec{a}}) = \rho(\underline{\vec{a}})$. Tada postoji n takav da je $\mathcal{N} \models \tau(\underline{\vec{a}}) = \underline{n}$ i $\mathcal{N} \models \rho(\underline{\vec{a}}) = \underline{n}$. Želimo dokazati da tada vrijedi $\vdash \tau(\underline{\vec{a}}) = \underline{n}$, odnosno $\vdash \rho(\underline{\vec{a}}) = \underline{n}$. Tada će odmah slijediti $\vdash \tau(\underline{\vec{a}}) = \rho(\underline{\vec{a}})$ zbog napomene prije dokaza propozicije 4.2 na prethodnoj stranici.

Dokažimo sada gornju tvrdnju indukcijom po složenosti (zatvorenog) terma σ. Ako je $\mathcal{N} \models \sigma = \underline{0}$, tada očito tvrdnja vrijedi jer $\vdash \underline{0} = \underline{0}$. Pretpostavimo sada da tvrdnja vrijedi za svaki term složenosti manje od n i neka je σ neki zatvoreni term složenosti n. Tada imamo nekoliko slučajeva:

1) Postoji term ϕ takav da vrijedi $\sigma \equiv S\phi$. Iz pretpostavke indukcije slijedi da postoji neki k takav da $\vdash \phi = \underline{k}$. Za formulu $\alpha(x) \equiv S\phi = Sx$ vrijedi $\vdash \alpha\frac{\phi}{x}$, pa zbog (L) dobivamo $\vdash \alpha(\underline{k})$, odnosno $\vdash S\phi = \underline{Sk}$, pa tvrdnja slijedi ponovnom primjenom (L).

2) Postoje termi ϕ i ψ takvi da vrijedi $\sigma \equiv \phi + \psi$. Tada postoje k i l takvi da $\vdash \phi = \underline{k}$ i $\vdash \psi = \underline{l}$, pa slično kao gore dobivamo $\vdash \phi + \psi = \underline{k} + \underline{l}$. Zbog (C1) imamo $\vdash \underline{k} + \underline{l} = \underline{k+l}$, pa jednostavnom primjenom (L) dobivamo $\vdash \sigma = \underline{k+l}$, što smo htjeli dokazati.

3) Postoje termi ϕ i ψ takvi da vrijedi $\sigma \equiv \phi \cdot \psi$. Tada postupamo sasvim analogno kao u prethodnom slučaju.

Na sličan način može se dokazati da ako vrijedi $\mathcal{N} \models \neg\varphi(\underline{\vec{a}})$ za neki $\vec{a}$, tada $\vdash \neg\varphi(\underline{\vec{a}})$. Time smo dokazali tvrdnju propozicije. □

Primijetimo da ako je $T \supseteq Q$ neka konzistentna teorija koja zadovoljava uvjete (R^+) i (R^-) tada vrijede i njihovi obrati. Zaista, neka vrijedi $\vdash_T \alpha(\underline{\vec{a}})$. Tada zbog konzistentnosti vrijedi $\nvdash_T \neg\alpha(\underline{\vec{a}})$, a to po svojstvu (R^-) povlači $P\vec{a}$. Analogno za drugu tvrdnju. Ovdje odmah možemo dati intuitivno opravdanje za tvrdnju da je svaka relacija koja je reprezentabila nekom formulom α u Q ujedno i rekurzivna. Za proizvoljan $\vec{a} \in \mathbb{N}^n$ jednostavno pokrenemo stroj koji nabraja sve teoreme od Q i čekamo dok se na traci pojavi $\alpha(\underline{\vec{a}})$ ili $\neg\alpha(\underline{\vec{a}})$.

Relacije i funkcije koje su definabilne u $\mathcal{N}$ (dakle pomoću $0, S, +, \cdot$) zvat ćemo *aritmetičke*. Da bismo saznali više o tim objektima, promatramo njihove definirajuće formule.

Definicija 4.5. *Atomarne formule u $\mathcal{L}_{ar}$ zovemo **diofantske jednadžbe**. Ako je $\delta(\vec{x}, \vec{y})$ diofantska jednadžba i P relacija, te vrijedi: $P\vec{a}$ ako i samo ako $\mathcal{N} \models \exists\vec{y}\,\delta(\underline{\vec{a}}, \vec{y})$, tada kažemo da je relacija P **diofantska**.*

Jedan primjer je relacija $\leq$ jer vrijedi: $a \leq b$ ako i samo ako $\mathcal{N} \models \exists y\, y + \underline{a} = \underline{b}$. Može se pokazati da su sve relacije koje su definabilne u $\mathcal{N}$ formulama oblika $\exists\vec{y}\,\varphi$, gdje je φ otvorena formula, diofantske [6].

4.3 Klasifikacija formula i Σ_1-potpunost teorije Q

Sljedećom definicijom dajemo općenitiju klasifikaciju aritmetičkih formula.

Definicija 4.6. ***Osnovna Δ_0-formula** zovemo svaku formulu generiranu iz atomarnih formula jezika $\mathcal{L}_{ar}$ upotrebom $\wedge, \neg$ i **ograničene kvantifikacije**, tj. ako su α i β osnovne Δ_0-formule, tada su $\alpha \wedge \beta$, $\neg\alpha$ i $(\forall x \leq t)\alpha$ $(:= \forall x(x \leq t \to \alpha))$ također osnovne Δ_0 formule. Ovdje je t neki $\mathcal{L}_{ar}$-term takav da vrijedi $x \notin var(t)$.*

*Neka je sada φ osnovna Δ_0-formula. Tada svaku formulu oblika $\exists\vec{x}\varphi$ zovemo **osnovna Σ_1-formula**, dok svaku formulu oblika $\forall\vec{x}\varphi$ zovemo **osnovna Π_1-formula**.*

Nadalje, kažemo da je relacija $P \subseteq \mathbb{N}^n$ jedna Δ_0-, Σ_1- ili Π_1-relacija ako je P definabilna u $\mathcal{N}$ nekom osnovnom Δ_0-, Σ_1- ili Π_1-formulom.

Sa Δ_0, Σ_1 i Π_1 označavat ćemo skupove Δ_0-, Σ_1- i Π_1-relacija. Dodatno, definiramo $\Delta_1 := \Sigma_1 \cap \Pi_1$.

Smatrat ćemo da je formula Δ_0-, Σ_1- ili Π_1-formula ako je ekvivalentna nekoj osnovnoj Δ_0-, Σ_1- ili Π_1-formuli. Na primjer, ako je α neka Δ_0-formula tada su formule $(\exists x \leq t)\alpha\,(\equiv_Q \neg(\forall x \leq t)\neg\alpha)$ i $(\forall x \leq t)\alpha\,(\equiv_Q (\forall x \leq t)(x = t \vee \alpha))$ također Δ_0-formule.

Primjer 4.7. *Diofantske jednadžbe su najjednostavnije Δ_0-formule. To su formule $\varphi(\vec{x}, y)$ oblika $y = t(\vec{x})$, gdje je $y \notin var(t)$. One definiraju funkcije $\vec{a} \mapsto t^{\mathcal{N}}(\vec{a})$ jer vrijedi: $t^{\mathcal{N}}(\vec{a}) = y$ ako i samo ako $\mathcal{N} \models \varphi(\vec{a}, y)$.*

Relacije prim $i \mid$ *su Δ_0 jer vrijedi $a \mid b \Leftrightarrow (\exists c \leq b)(a \cdot c = b)$. Nadalje, relacija $\perp$, koja označava da su a i b relativno prosti, je Δ_0 jer vrijedi $a \perp b$ ako i samo ako $(\forall c \leq a + b)(c \mid a, b \Rightarrow c = 1)$.*

Diofantske relacije su očito Σ_1, a obrat također vrijedi i dokaz se može vidjeti u [6].

Lema 4.8. *Neka je $\varphi(x)$ proizvoljna formula, t zatvoren term i $m \in \mathbb{N}$ takav da je $t = \underline{m}$. Tada vrijedi*

$$\vdash (\forall x \leq t)\varphi(x) \leftrightarrow \bigwedge_{i=0}^{m} \varphi(\underline{i}).$$

Dokaz. Pretpostavimo da vrijedi $\vdash \bigwedge_{i=0}^{m} \varphi(\underline{i})$. Tada za svaki $i \leq m$ vrijedi $\vdash \varphi(\underline{i})$, odnosno $\vdash x = \underline{i} \to \varphi(x)$. Sada iz (C5) slijedi $\vdash x \leq \underline{m} \to \varphi(x)$, pa dobivamo $\vdash x \leq t \to \varphi(x)$ jer je $\vdash t = \underline{m}$. No to je upravo $\vdash (\forall x \leq t)\varphi(x)$.

Obratno, ako vrijedi $\vdash (\forall x \leq t)\varphi(x)$ tada isto kao prije dobivamo $\vdash x \leq \underline{m} \to \varphi(x)$. Ako je $i \leq m$ tada zbog (C3) vrijedi $\vdash \underline{i} \leq \underline{m}$, pa odmah slijedi $\vdash \varphi(\underline{i})$. Ako to ponovimo za svaki $i \leq m$ dobivamo $\vdash \bigwedge_{i=0}^{m} \varphi(\underline{i})$. □

Teorem 4.9 (Σ_1-potpunost teorije Q)**.**
Svaka Σ_1-rečenica istinita na standardnom modelu $\mathcal{N}$ je dokaziva u Q.

Dokaz. Prvo ćemo dokazati tvrdnju za osnovne Σ_1-rečenice. Iz prethodne leme slijedi da ograničenu kvantifikaciju možemo zamijeniti konjunkcijama, pa tvrdnju trebamo samo dokazati za osnovne Σ_1-rečenice bez ograničene kvantifikacije.

Ako je φ istinita atomarna formula ili istinita negacija neke atomarne formule, tada tvrdnja slijedi iz propozicije 4.4. Pretpostavimo da tvrdnja vrijedi za sve formule složenosti manje od k, za neki $k \in \mathbb{N}$. Neka je φ osnovna Σ_1-rečenica istinita u $\mathcal{N}$ složenosti točno k. Tada imamo nekoliko slučajeva:

1) $\varphi \equiv \psi \wedge \phi$. Tada su ψ i ϕ osnovne Σ_1-rečenice istinite na $\mathcal{N}$ složenosti strogo manje od k pa vrijedi $\vdash \psi$ i $\vdash \phi$. No tada odmah slijedi $\vdash \psi \wedge \phi$.

2) $\varphi \equiv \neg\psi$. Ako je ψ atomarna formula, tada je φ istinita negacija atomarne formule, pa po propoziciji 4.4 slijedi tvrdnja. Ako je $\psi \equiv \neg\sigma$, tada $\mathcal{N} \models \neg\neg\sigma$, odnosno $\mathcal{N} \models \sigma$, pa tvrdnja odmah slijedi iz pretpostavke indukcije i činjenice da vrijedi $\vdash \sigma \leftrightarrow \neg\neg\sigma$. Ako je ψ oblika $\sigma \wedge \phi$, tada vrijedi $\mathcal{N} \models \neg(\sigma \wedge \phi)$, pa bez smanjenja općenitosti možemo pretpostaviti $\mathcal{N} \models \neg\sigma$. Formula $\neg\sigma$ je složenosti manje od k pa dobivamo $\vdash \neg\sigma$, pa iz $\vdash (\neg\sigma \vee \neg\phi) \leftrightarrow \neg(\sigma \wedge \phi)$ slijedi $\vdash \neg(\sigma \wedge \phi)$.

3) $\varphi \equiv \exists x\, \psi(x)$. Tada postoji $i \in \mathbb{N}$ takav da vrijedi $\mathcal{N} \models \psi(\underline{i})$. Očito je $\psi(\underline{i})$ jedna Σ_1-rečenica složenosti $k-1$, pa vrijedi $\vdash \psi(\underline{i})$, a onda i $\vdash \exists x\, \psi(x)$.

Neka je sada φ proizvoljna Σ_1-rečenica takva da vrijedi $\mathcal{N} \models \varphi$. Tada postoji osnovna Σ_1-rečenica ψ takava da je $\vdash \varphi \leftrightarrow \psi$, pa je $\mathcal{N} \models \psi$. Sada iz prethodno dokazane tvrdnje slijedi $\vdash \psi$, a onda i $\vdash \varphi$. □

Ako je $\varphi(\vec{x})$ Δ_0 onda $\mathcal{N} \models \varphi(\vec{a})$ povlači $\vdash_Q \varphi(\vec{a})$, i $\mathcal{N} \models \neg\varphi(\vec{a})$ povlači $\vdash_Q \neg\varphi(\vec{a})$ jer su $\varphi(\underline{\vec{a}})$ i $\neg\varphi(\underline{\vec{a}})$ obje Σ_1. Slijedi korolar

Korolar 4.10. *Neka je P relacija definirana u $\mathcal{N}$ Δ_0-formulom φ. Tada φ reprezentira relaciju P u Q.*

Lema 4.11. *Neka je $P \subseteq \mathbb{N}^{n+1}$ reprezentirana sa $\alpha(\vec{a}, y)$. Tada formule $(\exists z < y)\alpha(\vec{x}, z)$ i $(\forall z < y)\alpha(\vec{x}, z)$ reprezentiraju relacije Q i R, gdje*

$$Q(\vec{a}, b) \Leftrightarrow (\exists c < b)P(\vec{a}, c) \text{ i } R(\vec{a}, b) \Leftrightarrow (\forall c < b)(P(\vec{a}, c)).$$

Dokaz. Uočimo da je dovoljno dokazati tvrdnju za relaciju Q jer vrijedi:

$$R(\vec{a}, b) \Leftrightarrow \neg(\exists c < b)\neg P(\vec{a}, c).$$

Dokažimo sada da formula $(\exists z < y)\alpha(\vec{x}, z)$ zadovoljava svojstva (R^+) i (R^-).

(R^+): Neka vrijedi $Q(\vec{a}, b)$, dakle $P(\vec{a}, c)$ za neki $c < b$. Tada očito $\vdash \underline{c} < \underline{b} \wedge \alpha(\underline{\vec{a}}, \underline{c})$, pa stoga vrijedi $\vdash (\exists z < \underline{b})\alpha(\underline{\vec{a}}, z)$.

(R^-): Neka vrijedi $\neg Q(\vec{a}, b)$, odnosno $\neg P(\vec{a}, i)$ za sve $i < b$. Sada vrijedi $\bigvee_{i<b} z = \underline{i} \vdash \neg\alpha(\underline{\vec{a}}, z)$. Po (C5) imamo $z < \underline{b} \vdash \bigvee_{i<b} z = \underline{i}$, pa $z < \underline{b} \vdash \neg\alpha(\underline{a}, z)$. Konačno, $\vdash (\forall z < \underline{b})\neg\alpha(\vec{a}, z) \equiv_Q \neg(\exists z < \underline{b})\alpha(\vec{a}, z)$, čime smo dokazali (R^-). □

Primijetimo još da vrijedi $(\exists z \leq y)\alpha \equiv_Q (\exists z < y)\alpha \vee \alpha^z_y$, pa su relacije $(\exists c \leq b)P(\vec{a}, c)$ i $(\forall c \leq b)P(\vec{a}, c)$ također reprezentabilne za proizvoljnu reprezentabilnu relaciju P.

4.4 Reprezentabilnost funkcija i neki rezultati

Sada definiramo pojam reprezentabilnosti funkcije u proizvoljnoj aritmetičkoj teoriji T. Neka je f neka n-mjesna totalna funkcija. Jedna ideja za reprezentaciju funkcije f je da reprezentiramo njen graf, odnosno relaciju G_f za koju vrijedi $G_f(\vec{a}, m) \Leftrightarrow f\vec{a} = m$. Međutim takva definicija, iako je prirodna, nije zadovoljavajuća. Naime, ona nigdje ne zahtijeva da φ reprezentira funkciju kao funkciju, tj. da T može dokazati da za dani $\vec{a}$ postoji jedinstvena vrijednost funkcije, upravo $f\vec{a}$. To je motivacija za sljedeću definiciju.

Definicija 4.12. *Funkcija $f \in \mathbf{F}_n$ je **reprezentabilna** u teoriji T (ako izostavimo "u T" podrazumijeva se $T = Q$) ako postoji formula $\varphi(\vec{x}, y)$ takva da za sve $\vec{a} \in \mathbb{N}^n$ vrijedi*

$$(\mathrm{R}^+) : \vdash_T \varphi(\underline{\vec{a}}, \underline{f\vec{a}}) \quad i \quad (\mathrm{R}^=) : \ \varphi(\underline{a}, y) \vdash_T y = \underline{f\vec{a}}.$$

Ako je Δ_0- (odnosno Σ_1-, Π_1-) formula, onda kažemo da je funkcija f Δ_0- (odnosno Σ_1-, Π_1-) reprezentabilna. Sličnu terminologiju koristimo za relacije. Posebno, kažemo da je $P \subseteq \mathbb{N}^n$ Δ_1-reprezentabilna ako je Σ_1- i Π_1-reprezentabilna.

Ovdje smo zbog sličnosti s uvjetom (R^+) kod reprezentabilnosti relacija ostavili istu oznaku. Iz konteksta će uvijek biti jasno na što se oznaka odnosi. Uočimo da smo izostavili uvjet (R^-). Taj uvjet slijedi iz $(\mathrm{R}^=)$ jer za $b \neq f\vec{a}$ vrijedi $\vdash \underline{b} \neq \underline{f\vec{a}}$ zbog (C2), pa iz $(R^=)$ slijedi $\vdash \varphi(\underline{a}, b) \to b = \underline{f\vec{a}}$. Zatim primjenom $\Lambda 4$ dobivamo $\vdash b \neq \underline{f\vec{a}} \to \neg\varphi(\underline{a}, y)$, odnosno $\vdash \neg\varphi(\underline{a}, y)$, što je upravo uvjet (R^-). Dakle, ako je f reprezentabilna, tada je i njen graf reprezentabilan istom formulom. Sljedeća lema pokazuje da vrijedi i obrat.

Lema 4.13. *(a) Neka je relacija $P \subseteq \mathbb{N}^{n+1}$ reprezentirana formulom $\alpha(\vec{x}, y)$ i pretpostavimo da za svaki $\vec{a}$ postoji b takav da vrijedi $P(\vec{a}, b)$. Tada formula $\varphi(\vec{x}, y) := \alpha(\vec{x}, y) \wedge (\forall z < y)\neg\alpha(\vec{x}, z)$ reprezentira funkciju $f : \vec{a} \mapsto \mu b[P(\vec{a}, b)]$. Ako je relacija P Δ_0-reprezentabilna, tada je funkcija f također Δ_0-reprezentabilna. Ako je relacija P Δ_1-reprezentabilna, tada je funkcija f Σ_1-reprezentabilna.*
(b) Ako je graf funkcije f reprezentabilan tada je f također reprezentabilna.
(c) Ako je funkcija f Σ_1-reprezentabilna tada je f također Π_1-reprezentabilna.
(d) Ako je funkcija χ_p Σ_1-reprezentabilna, tada je relacija P Δ_1-reprezentabilna.

Dokaz. (a) Jasno je da je relacija koju definira $\varphi(\vec{x}, y)$ upravo graf funkcije f. Sada iz prethodne leme slijedi da $\varphi(\vec{x}, y)$ reprezentira graf funkcije f. Time smo dokazali (R^+). Za $(\mathrm{R}^=)$ treba dokazati:

$$(*) \quad \alpha(\underline{\vec{a}}, y) \wedge (\forall z < y)\neg\alpha(\vec{a}, z) \vdash y = \underline{f\vec{a}}.$$

Stavimo $b := f\vec{a}$. Tada zbog $\vdash \alpha(\underline{\vec{a}}, \underline{b})$ vrijedi $\underline{b} < y \vdash (\exists z < y)\alpha(\underline{\vec{a}}, z)$. Kontrapozicijom dobivamo $(\forall z < y)\neg\alpha(\underline{\vec{a}}, z) \vdash \underline{b} \not< y$. Po (C5) i (R^-) imamo $y < \underline{b} \vdash \bigvee_{i<b} y = \underline{i} \vdash \neg\alpha(\underline{\vec{a}}, y)$. Ponovno kontrapozicijom dobivamo $\alpha(\underline{\vec{a}}, y) \vdash y \not< \underline{b}$. Konačno, $\alpha(\underline{\vec{a}}, y) \wedge (\forall z < y)\neg\alpha(\underline{\vec{a}}, z) \vdash y \not< \underline{b} \wedge \underline{b} \not< y \vdash y = \underline{b}$ po (C6). Time smo dokazali $(*)$. Ako je α Δ_0-formula tada je očito i φ Δ_0-formula. Za zadnju tvrdnju, pretpostavimo da je relacija P istovremeno reprezentabilna nekom Π_1 formulom β. Tada možemo ponoviti isti postupak kao gore ako zamijenimo φ formulom $\varphi(\vec{x}, y) := \alpha(\vec{x}, y) \wedge (\forall z < y)\neg\beta(\vec{x}, z)$.

(b)Vrijedi $f\vec{a} = \mu b[P(\vec{a}, b)]$, gdje je $P = \mathrm{graf} f$, pa primjenom (a) slijedi tvrdnja.

(c)Neka Σ_1-formula $\varphi(\vec{a}, y)$ reprezentira f i neka je $z \notin var(\varphi)$. Tada je $\varphi'(\vec{x}, y) := \forall z(\varphi(\vec{x}, z) \to z = y)$ jedna Π_1-formula koja također reprezentira f. Zaista, primjena uvjeta ($R^=$) daje $\vdash \varphi'(\underline{\vec{a}}, \underline{f\vec{a}})$, pa vrijedi uvjet ($R^+$) za φ', a zbog $\vdash \varphi(\underline{\vec{a}}, \underline{f\vec{a}})$ dobivamo da vrijedi uvjet ($R^=$) za φ' iz

$$\varphi'(\underline{\vec{a}}, y) = \forall z(\varphi(\underline{\vec{a}}, z) \to y = z) \vdash \varphi(\underline{\vec{a}}, \underline{f\vec{a}}) \to y = \underline{f\vec{a}} \vdash y = \underline{f\vec{a}}.$$

(d) Neka je funkcija χ_P Σ_1-reprezentirana formulom $\varphi(\vec{x}, y)$. Tada je relacija P očito Σ_1-reprezentirana formulom $\varphi(\vec{x}, \underline{1})$ i Π_1-reprezentirana formulom $\neg\varphi(\vec{x}, 0)$. □

U prvom poglavlju spomenuli smo bijekciju $\wp : \mathbb{N}^2 \to \mathbb{N}$ definiranu s $\wp(a, b) = \sum_{i \le a+b}(i+a)$. Lako se vidi da vrijedi $\wp(a, b) = \frac{1}{2}(a+b)(a+b+1)+a$, pa je po propoziciji 4.4 graf$\wp$ reprezentiran Δ_0-formulom $\alpha(x, y, z) = (z \cdot \underline{2} = (x + y) \cdot S(x + y) + x \cdot \underline{2})$. Iz prethodne leme slijedi da je $\wp$ reprezentabilna Δ_0-formulom.

Lema 4.14. *(a) Neka je relacija $P \subseteq \mathbb{N}^k$ reprezentirana formulom $\alpha(\vec{y})$, te $g_i \in \mathbf{F}_n$ sa γ_i za $i = 1, ..., k$. Tada $\beta(\vec{x}) := \exists\vec{y}[\bigwedge_i \gamma_i(\vec{x}, y_i) \wedge \alpha(\vec{y})]$ reprezentira relaciju $Q := P[g_1, ..., g_k]$. Ako su funkcije g_i Σ_1-reprezentabilne i relacija P Δ_1-reprezentabilna, tada je relacija Q Δ_1-reprezentabilna.*

(b) Ako su funkcije $h \in \mathbf{F}_m$ i $g_1, ..., g_m \in \mathbf{F}_n$ reprezentabilne onda je i funkcija $f := h[g_1, ..., g_m]$ reprezentabilna.

Dokaz. Neka je $b_i := g_i\vec{a}$ i $\vec{b} = (b_1, ..., b_k)$. Tada imamo $\vdash \gamma_i(\underline{\vec{a}}, \underline{b_i})$ za $i = 1, ..., k$. Ako uz to vrijedi $Q\vec{a}$, odnosno $P\vec{b}$, tada imamo $\vdash \alpha(\underline{\vec{b}})$, pa slijedi $\vdash \bigwedge_i \gamma_i(\underline{\vec{a}}, \underline{b_i}) \wedge \alpha(\underline{\vec{b}})$, odnosno $\vdash \beta(\underline{\vec{a}})$

S druge strane, ako vrijedi $\neg Q\vec{a}$, odnosno $\neg P\vec{b}$, tada $\vdash \neg\alpha(\underline{\vec{b}})$. Koristeći uvjet ($R^=$) za formule γ_i dobivamo $\bigwedge_i \gamma_i(\underline{\vec{a}}, y_i) \vdash \bigwedge_i y_i = \underline{b_i} \vdash \neg\alpha(\vec{y})$, pa konačno vrijedi $\vdash \forall\vec{y}[\bigwedge_i \gamma_i(\underline{\vec{a}}, y_i) \to \neg\alpha(\vec{y})] \equiv \neg\beta(\underline{\vec{a}})$. Ako su γ_i i α Σ_1-formule, tada je β također Σ_1-formula. Ako je relacija P dodatno reprezentirana Π_1-formulom $\alpha'(\vec{x})$, tada je Q reprezentirana Π_1-formulom $\forall\vec{y}[\bigwedge_i \gamma_i(\vec{x}, y_i) \to \alpha'(\vec{y})]$. Tvrdnja (b) slijedi iz (a) i prethodne leme ako primijetimo da vrijedi graf$f$ = graf$h[g_1, ...g_m]$. □

Poglavlje 5

Teorem reprezentabilnosti

Da bismo dokazali reprezentabilnost svih rekurzivnih funkcija, potrebna nam je reprezentabilna dekodirajuća funkcija $g \in \mathbf{F}_2$, odnosno funkcija koja zadovoljava sljedeće svojstvo: za svaki n i svaki niz $c_0, ..., c_n$ postoji broj c takav da vrijedi

$$(*): \ g(c,i) = c_i, \text{ za svaki } i \leq n.$$

Takve funkcije se standardno zovu β-funkcije, po K. Gödelu. Kasnije ćemo vidjeti da je $(c,i) \mapsto (c)_i$ jedna takva funkcija, no trenutno ne znamo kako ju reprezentirati u Q jer je definirana pomoću eksponencijalne funkcije.

Zato želimo definirati β-funkciju koristeći samo funkcije koje su "ugrađene" u Q, odnosno $\mathrm{S}, +, \cdot$. Danas je poznato više takvih funkcija, a mi ćemo slijediti izvornu Gödelovu konstrukciju.

5.1 Gödelova β-funkcija

Neka je $\alpha(a,b,i) := \mathrm{rem}(a : (1 + (1 + i)b))$, gdje $\mathrm{rem}(c : d)$ označava ostatak pri dijeljenju c sa $d \neq 0$, i $\mathrm{rem}(c : 0) := 0$. Graf funkcije α, tj. graf$\alpha(a,b,i,k)$ je definiran Δ_0-formulom

$$(\exists c \leq a)[a = c(1 + (1 + i)b) + k \ \wedge \ k < 1 + (1 + i)b],$$

pa iz propozicije 4.4 i leme 4.11 slijedi da je grafα reprezentiran tom istom formulom. Sada iz leme 4.13 zaključujemo da je α također Δ_0-reprezentabilna. Isto vrijedi i za funkciju $\wp$. Funkcija $\wp$ je bijekcija, pa postoje unarne funkcije $\varkappa_1, \varkappa_2$ takve da vrijedi $\wp(\varkappa_1 k, \varkappa_2 k) = k$ za svaki k, i $\varkappa_1 k, \varkappa_2 k \leq k$. Sada β-funkciju definiramo sa $\beta(c,i) = \alpha(\varkappa_1 c, \varkappa_2 c, i)$. Graf funkcije β, tj. graf$\beta(c,i,k)$ definiran je Δ_0-formulom

$$(\exists a \leq c)(\exists b \leq c)[\wp(a,b) = c \ \wedge \ \alpha(a,b,i) = k],$$

pa je po lemi 4.13 β funkcija reprezentirana Δ_0-formulom `beta`, odnosno

$$(1) \quad \vdash_Q \texttt{beta}(\underline{c}, \underline{i}, y) \leftrightarrow y = \underline{\beta(c,i)}, \text{ za sve } c, i \in \mathbb{N}$$

Prije dokaza sljedeće leme iskazat ćemo dobro poznati rezultat iz teorije brojeva, kineski teorem o ostacima. Dokaz i diskusija o dokazivosti tog rezultata unutar teorije PA može se naći u [6].

Teorem 5.1 (Kineski teorem o ostacima)**.**
Neka su $c_0, ..., c_n$ i $d_0, ..., d_n$ takvi da vrijedi $c_i < d_i$ za sve $i \leq n$. Nadalje, neka su $d_0, ..., d_n$ u parovima relativno prosti. Tada postoji $a \in \mathbb{N}$ takav da vrijedi

$$\text{rem}(a : d_i) = c_i \text{ za svaki } i \leq n.$$

Lema 5.2 (O β-funkciji)**.** *Za svaki n i svaki niz $c_0, ..., c_n$ postoji c takav da vrijedi $\beta(c, i) = c_i$, za $i = 0, ..., n$.*

Dokaz. Dovoljno je dokazati da postoje brojevi a, b takvi da vrijedi $\alpha(a, b, i) = c_i$, $i \leq n$. Tada tvrdnja slijedi ako uzmemo $c = \wp(a, b)$ jer vrijedi $\beta(c, i) = \alpha(a, b, i)$.

Neka je $m = max\{n, c_0, ..., c_n\}$ i $b = \text{lcm}\{i + 1 \mid i \leq m\}$. Tvrdimo da su brojevi $d_i := 1 + (1 + i) \cdot b > c_i \, (i \leq n)$ u parovima relativno prosti. Zaista, neka je p prosti faktor od d_i. Tada je $p > m+1$ jer bi inače vrijedilo $p \mid b \mid d_i - 1$, što je kontradikcija. Ako $p \mid d_i, d_j$ za $i < j \leq n$, tada $p \mid d_j - d_i = (j - i)b$. No zbog $p \nmid b$ vrijedi $p \mid j - i \leq n \leq m < p$, pa $j - i = 0$. Dakle, brojevi d_i su u parovima relativno prosti. Po kineskom teoremu o ostacima tada postoji a takav da je $\text{rem}(a : d_i) = c_i$, odnosno $\alpha(a, b, i) = c_i$ za $i = 0, ..., n$. □

Sada smo spremni dokazati glavni rezultat ovog poglavlja.

Teorem 5.3 (O reprezentabilnosti)**.** *Svaka rekurzivna funkcija f (pa i svaka rekurzivna relacija) je reprezentabilna u proizvoljnom konzistentnom proširenju teorije Q. Nadalje, funkcija f je Σ_1-reprezentabilna.*

Dokaz. Očito je dovoljno konstruirati Σ_1-formulu koja reprezentira f u Q. Za inicijalne funkcije 0,S,I^n_ν možemo uzeti formule $v_0 = 0$, $v_1 = Sv_0$ i $v_n = v_\nu$.

(i) Neka je $f = h[g_1, ..., g_m]$ i neka su $\beta(\vec{y}, z)$ i $\gamma_i(\vec{x}, y_i)$ Σ_1 formule koje reprezentiraju funkcije h i g_i. Tada iz leme 4.14 slijedi da Σ_1-formula $\varphi(\vec{x}, z) := \exists \vec{y}[\bigwedge_i \gamma_i(\vec{x}, y_i) \wedge \beta(\vec{y}, z)]$ reprezentira f.

(ii) Neka je $f = \boldsymbol{Op}(g, h)$ te neka su f i g Σ_1-reprezentabilne. Definiramo relaciju P na sljedeći način:

$$P(\vec{a}, b, c) \Leftrightarrow \beta(c, 0) = g\vec{a} \wedge (\forall v < b)\beta(c, Sv) = h(\vec{a}, v, \beta(c, v))$$

Ovo je očito kompozicija Δ_0-, odnosno Δ_1-relacije sa Σ_1-reprezentabilnim funkcijama, pa iz leme 4.14 slijedi da je P Δ_1-reprezentabilna. Relacija $P(\vec{a}, b, c)$ je ekvivalentna s

$$(*) \quad \beta(c, i) = f(\vec{a}, i), \text{ za sve } i \leq b$$

Sada za proizvoljne $\vec{a}, b$ po prethodnoj lemi slijedi da postoji c koji zadovoljava $(*)$, odnosno za sve $\vec{a}, b$ postoji c takav da vrijedi $P(\vec{a}, b, c)$, pa iz leme 4.13 slijedi da je funkcija $\tilde{f} : \vec{a} \mapsto \mu c[P(\vec{a}, b, c)]$ Σ_1-reprezentabilna. Sada za $c = \tilde{f}(\vec{a}, b)$ vrijedi $(*)$, pa uz $i = b$ imamo $f(\vec{a}, b) = \beta(\tilde{f}(\vec{a}, b), b)$. Dakle, f je Σ_1-reprezentabilna kao kompozicija Σ_1-reprezentabilnih funkcija.

(iii) Neka je f dobivena iz g pravilom $\boldsymbol{O\mu}$, odnosno $f\vec{a} = \mu b[P(\vec{a}, b)]$, gdje je: $P(\vec{a}, b)$ ako i samo ako $g(\vec{a}, b) = 0$, i g je Σ_1-reprezentabilna. Po lemi 4.13, funkcija g je Π_1-reprezentabilna, pa je relacija P Δ_1-reprezentabilna. Konačno, po lemi 4.13, funkcija f je Σ_1-reprezentabilna. □

Neka je $T \supseteq Q$ teorija čiji je jezik $\mathcal{L}_{ar}$. Kažemo da riječi $\varphi \in \mathcal{L}_{ar}$ odgovara *unutar* T term $\underline{n}$, gdje je $n = \dot{\varphi}$. Taj term još zovemo *Gödelov term* riječi φ i označavamo ga s $\ulcorner\varphi\urcorner$. Analogno definiramo $\ulcorner t\urcorner$ za terme. Ako je T aksiomatizabilna, za dokaze je dobro definiran term $\ulcorner\Phi\urcorner = \dot{\underline{\Phi}}$.

U poglavlju o aritmetizaciji dokazali smo da je relacija bew_T primitivno rekurzivna, pa je po prethodnom teoremu reprezentirana nekom Σ_1-formulom koju označavamo s $\mathtt{bew}_T(y, x)$. Ako definiramo $\mathtt{bwb}_T(x) \equiv \exists y \mathtt{bew}_T(y, x)$ iz propozicije 3.2 slijedi sljedeći korolar.

Korolar 5.4. *Neka je $T \supseteq Q$ aksiomatizabilna. Tada iz $\vdash_T \varphi$ slijedi $\vdash_T \mathtt{bew}_T(\underline{n}, \ulcorner\varphi\urcorner)$ za neki n. Iz toga odmah slijedi da $\vdash_T \varphi$ povlači $\vdash_T \mathtt{bwb}_T(\ulcorner\varphi\urcorner)$, te da $\nvdash_T \varphi$ povlači $\vdash_T \neg\mathtt{bew}_T(\underline{n}, \ulcorner\varphi\urcorner)$ za svaki n.*

5.2 Reprezentabilnost i odlučivost

Sljedeći teorem bi se mogao dokazati jednostavnom primjenom Churchove teze. Neka je T konzistentna, potpuna i aksiomatizabilna teorija. Za danu riječ α najprije provjerimo je li $\alpha \in \mathcal{L}^0$. Ako nije, vraćamo $\alpha \notin T$. Inače pokrenemo stroj koji nabraja teoreme od T (takav stroj sigurno možemo konstruirati ako je T rekurzivno aksiomatizabilna) i ako u nekom trenutku naiđemo na α vratimo $\alpha \in T$, a ako naiđemo na $\neg\alpha$ vraćamo $\alpha \notin T$ (jer je T konzistentna pa odmah znamo da tada ne postoji dokaz za α). Ovaj proces će uvijek stati jer je T potpuna. Dakle, T je odlučiva pa je i rekurzivna po Churchovoj tezi.

Sada dajemo dokaz za taj rezultat bez korištenja Churchove teze. Imajući to u vidu, kasnije ćemo liberalnije koristiti Churchovu tezu u nekim dokazima jer se na sasvim analogan način može eliminirati iz tih dokaza.

Teorem 5.5. *Svaka konzistentna, potpuna i aksiomatizabilna teorija T je rekurzivna.*

Dokaz. Zbog potpunosti, funkcija $f : a \mapsto \mu b[a \notin \dot{\mathcal{L}}^0 \vee bew_T(b,a) \vee bew_T(b, \tilde{\neg} a)]$ je dobro definirana totalna funkcija. Da bismo se u to uvjerili, označimo relaciju u uglatim zagradama s $P(a,b)$. Tada za svaki a postoji b takav da vrijedi $P(a,b)$. Naime, ako $a \notin \dot{\mathcal{L}}^0$ tada je trivijalno zadovoljeno $P(a,0)$. Inače, zbog potpunosti znamo da postoji b takav da $bew_T(b,a)$ ili $bew_T(b, \tilde{\neg} a)$. Relacija P je očito primitivno rekurzivna pa je f rekurzivna zbog uvjeta $\boldsymbol{O\mu}$. Sada imamo

$$a \in \dot{T} \Leftrightarrow a \in \dot{\mathcal{L}}^0 \;\&\; bew_T(fa, a).$$

Zaista, neka je $a \in \dot{T}$. Tada je $a \in \dot{\mathcal{L}}^0$ i postoji b takav da vrijedi $bew_T(b,a)$. Tada je fa nužno jedan takav b jer zbog konzistentnosti od T ne postoji c takav da vrijedi $bew_T(c, \tilde{\neg} a)$. Dakle, vrijedi $bew_T(fa, a)$. Obratno, ako je $a \in \dot{\mathcal{L}}^0$ i $bew_T(fa,a)$ tada je očito $a \in \dot{T}$. □

Ovdje postaje jasnija razlika između primitivno rekurzivne i rekurzivne procedure odlučivanja. Funkcija f ne mora biti primitivno rekurzivna čak i ako je P primitivno rekurzivna jer za općenitu potpunu teoriju T nemamo načina da odredimo gornju ogradu za duljinu dokaza neke rečenice. Više o tome može se vidjeti u [7].

Teorem 5.6. *Neka je $P \subseteq \mathbb{N}^n$ relacija i $T \supseteq Q$ konzistentna aksiomatizabilna teorija. Tada su sljedeće tvrdnje ekvivalentne:*

(i) *P je reprezentabilna u T,* (ii) *P je rekurzivna,* (iii) *P je Δ_1.*

Dokaz. (i) $\Rightarrow$ (ii): Neka je P reprezentirana s $\alpha(\vec{x})$. Za dani $\vec{a}$ pokrenemo stroj koji nabraja teoreme od T i čekamo dok se ne pojavi $\alpha(\vec{a})$ ili $\neg\alpha(\vec{a})$. Zbog definicije reprezentabilnosti ovaj proces će uvijek stati. Dakle, P je odlučiva, pa je rekurzivna po Churchovoj tezi.

(ii) $\Rightarrow$ (i),(iii): Po teoremu 5.3, χ_P je Σ_1-reprezentabilna u T, pa je relacija P Δ_1-reprezentabilna u T po lemi 4.13, te je definirana odgovarajućim formulama u $\mathcal{N}$. Dakle, $P \in \Delta_1$.

(iii) $\Rightarrow$ (ii): Neka je P definirana Σ_1-formulom $\alpha(\vec{x})$ i Π_1-formulom $\beta(\vec{x})$. Za dani $\vec{a}$ pokrenemo enumeracijski stroj za T i čekamo dok se pojavi jedna od Σ_1-rečenica $\alpha(\underline{\vec{a}})$ ili $\neg\beta(\underline{\vec{a}})$. Ovaj proces uvijek staje jer je Q Σ_1-potpuna po teoremu 4.9. □

Kao što smo već spomenuli, uporaba Churchove teze u dokazu prethodnog teorema može se eliminirati na isti način kao u teoremu 5.5.

U idućem poglavlju trebat će nam općenitija verzija supstitucijske funkcije definirane u drugom poglavlju. Neka je $cf\, n = (\underline{n})^{\cdot}$. Funkcija $n \mapsto cf\, n$ je primitivno rekurzivna jer vrijedi $cf\, 0 = \dot{0}$ i $cf\, Sn = \dot{S} * cf\, n$. Neka je zatim $\mathrm{sb}_x(m,n) = [m]_{\dot{x}}^{cf\, n}$. Definiramo funkciju $\mathrm{sb}_{\vec{x}} \in \mathbf{F}_{n+1}$ sa $\mathrm{sb}_{\vec{x}}(m,\vec{a}) = sb_{x_n}(sb_{x_1,\ldots,x_{n-1}}(m,a_1,\ldots,a_{n-1}),a_n)$ gdje je $n > 1$ i $\mathrm{sb}_{\emptyset}(m) = m$. Ovdje x_i označavaju različite varijable. Neka je sada $\dot{\alpha}_{\vec{x}}(\underline{\vec{a}})$ Gödelov broj formule $\alpha_{\vec{x}}(\underline{\vec{a}})$ koja nastaje iz α zamjenom svih slobodnih nastupa varijable x_i sa $\underline{a_i}$.

Teorem 5.7. *Vrijedi* $\mathrm{sb}_{\vec{x}}(\dot{\alpha},\vec{a}) = \dot{\alpha}_{\vec{x}}(\underline{\vec{a}})$*, za* $\alpha \in \mathcal{L}$ *i sve* $\vec{a} \in \mathbb{N}^n$*.*

Dokaz. Formulu $\alpha_{\vec{x}}(\underline{\vec{a}})$ dobivamo uzastopnim jednostavnim supstitucijama, a to je upravo naša definicija funkcije sb. Dakle, treba samo provjeriti da sb korektno radi pojedinačne supstitucije, odnosno da vrijedi $\mathrm{sb}_x(\dot{\alpha},a) = \dot{\alpha}_x(\underline{a})$ za sve $\alpha \in \mathcal{L}$, $x \in Var$ i $a \in \mathbb{N}$.

No to odmah slijedi iz činjenice da vrijedi $[\xi]_{\dot{x}}^{\dot{t}} = (\xi\frac{t}{x})^{\cdot}$ jer je tada (uz oznaku $s = \underline{a}$) $sb_x(\dot{\alpha},a) = [\dot{\alpha}]_{\dot{x}}^{\dot{s}} = (\alpha\frac{s}{x})^{\cdot} = (\alpha_x(\underline{a}))^{\cdot} = \dot{\alpha}_x(\underline{a})$. □

Poglavlje 6

Prvi teorem nepotpunosti, Tarskijev i Churchov teorem

Reći ćemo da je teorija T *aritmetizabilna* ako je pripadni jezik $\mathcal{L}$ aritmetizabilan i postoji niz $(\underline{n})_{n\in\mathbb{N}}$ konstantnih terma takvih da $\vdash_T \underline{n} \neq \underline{m}$ za $n \neq m$ i funkcija cf: $n \mapsto (\underline{n})^{\cdot}$ je primitivno rekurzivna. To su minimalni uvjeti da bi reprezentabilnost aritmetičkih relacija u T imala smisla. U našim razmatranjima, ti uvjeti su trivijalno zadovoljeni jer pretpostavljamo $T \supseteq Q$, a može se vidjeti da su zadovoljeni i za teorije poput ZFC.

Reći ćemo da je rečenica γ *fiksna točka* formule $\alpha = \alpha(x)$ u T ako vrijedi $\gamma \equiv_T \alpha(\ulcorner\gamma\urcorner)$, odnosno $\vdash_T \gamma \leftrightarrow \alpha(\ulcorner\gamma\urcorner)$. Intuitivno, γ govori o sebi da ima svojstvo izraženo formulom α.

6.1 Lema o fiksnoj točki i prvi teorem nepotpunosti

Sljedeća važna lema govori da već za relativno skromne teorije svaka formula sa slobodnom varijablom ima fiksnu točku. U literaturi se taj rezultat još često naziva Dijagonalna lema.

Lema 6.1 (O fiksnoj točki)**.** *Neka je T aritmetizabilna teorija takva da je sb_x reprezentabilna u T. Tada za svaku formulu $\alpha = \alpha(x) \in \mathcal{L}$ postoji $\gamma \in \mathcal{L}^0$ takva da vrijedi*

$$(1) \quad \gamma \equiv_T \alpha(\ulcorner\gamma\urcorner)$$

Dokaz. Neka su $x_1, x_2, y \neq x$ i neka formula $\mathrm{sb}(x_1, x_2, y)$ reprezentira sb_x u T. Tada imamo $\mathrm{sb}(\ulcorner\varphi\urcorner, \underline{n}, y) \equiv_T y = \underline{sb_x(\dot{\varphi}, n)}$, odnosno $\mathrm{sb}(\ulcorner\varphi\urcorner, \underline{n}, y) \equiv_T y = \ulcorner\varphi(\underline{n})\urcorner$, pa za

$\underline{n} = \ulcorner\varphi\urcorner$ imamo

$$(2) \quad \mathrm{sb}(\ulcorner\varphi\urcorner, \ulcorner\varphi\urcorner, y) \equiv_T y = \ulcorner\varphi(\ulcorner\varphi\urcorner)\urcorner$$

Neka je sada $\beta(x) \equiv \forall y(\mathrm{sb}(x, x, y) \to \alpha\frac{y}{x})$. Tada tvrdnju dobivamo ako stavimo $\gamma \equiv \beta(\ulcorner\beta\urcorner)$. Zaista,

$$\begin{aligned}
\gamma \equiv\ & \forall y(sb(\ulcorner\beta\urcorner, \ulcorner\beta\urcorner, y) \to \alpha\tfrac{y}{x}) \\
\equiv_T\ & \forall y(y = \ulcorner\beta(\ulcorner\beta\urcorner)\urcorner \to \alpha\tfrac{y}{x}) \quad \text{(zbog (2))} \\
\equiv\ & \forall y(y = \ulcorner\gamma\urcorner \to \alpha\tfrac{y}{x}) \quad \text{(jer je } \gamma \equiv \beta(\ulcorner\beta\urcorner)\text{)} \\
\equiv\ & \alpha(\ulcorner\gamma\urcorner)
\end{aligned}$$

□

Lema 6.2 (O nereprezentabilnosti)**.** *Neka je T teorija kao u prethodnoj lemi. Tada T (odnosno $\dot{T}$) nije reprezentabilna u T.*

Dokaz. Pretpostavimo da je T reprezentirana nekom formulom $\tau(x)$. Pošto je T konzistentna vrijedi uvjet (R^-) i obrat (v. komentar na str.24), odnosno

$$\text{(a): } \alpha \notin T \text{ ako i samo ako } \vdash_T \neg\tau(\ulcorner\alpha\urcorner), \text{ za svaki } \alpha \in \mathcal{L}^0.$$

Neka je γ fiksna točka od $\neg\tau(x)$. Tada vrijedi $\vdash_T \gamma$ ako i samo ako $\vdash_T \neg\tau(\ulcorner\gamma\urcorner)$. No to je kontradikcija jer iz (a) slijedi $\nvdash_T \gamma$, što je ekvivalentno s $\gamma \notin T$, a to je ekvivalentno s $\vdash_T \neg\tau(\ulcorner\gamma\urcorner)$, pa vrijedi $\vdash_T \gamma$ ako i samo ako $\nvdash_T \gamma$. □

Sada možemo dokazati prvu verziju prvog Gödelovog teorema nepotpunosti kao jednostavnu posljedicu prethodno dokazanih tvrdnji.

Teorem 6.3 (Gödelov prvi teorem nepotpunosti, prva verzija)**.** *Svaka konzistentna (rekurzivno) aksiomatizablina teorija $T \supseteq Q$ je nepotpuna.*

Dokaz. Ako je T potpuna tada je i rekurzivna po teoremu 5.5, pa je $\dot{T}$ reprezentabilan u T po teoremu 5.3. No to je nemoguće zbog prethodno dokazane leme 6.2. □

Ovakav dokaz nije konstruktivan jer se nigdje eksplicitno ne konstruira rečenica za koju vrijedi $\nvdash_T \alpha$ i $\nvdash_T \neg\alpha$. Da bismo dokazali izvornu konstruktivnu verziju teorema, prvo uvodimo pojam ω-konzistentnosti.

Definicija 6.4. *Kažemo da je teorija $T \subseteq \mathcal{L}_{ar}$ ω-konzistentna ako za svaku formulu $\varphi = \varphi(x)$ takvu da $\vdash_T \exists x\varphi(x)$ postoji n takav da vrijedi $\nvdash_T \neg\varphi(\underline{n})$. Ekvivalentno, ako vrijedi $\vdash_T \neg\varphi(\underline{n})$ za sve n, tada $\nvdash_T \exists x\varphi(x)$.*

Uočimo da je svaka ω-konzistentna teorija konzistentna, jer inkonzistentne teorije dokazuju sve formule. Obrat ne vrijedi nužno, što ćemo vidjeti kada budemo govorili o drugom teoremu nepotpunosti.

Pojam ω-konzistentnosti je sintaktičko svojstvo teorije, no ono ima i semantički značaj. Naime, pretpostavimo da je $\mathcal{N}$ model za teoriju T. Nadalje, neka je $\varphi(x)$ neka formula takva da vrijedi $\vdash_T \neg\varphi(\underline{n})$, za svaki $n \in \mathbb{N}$. Tada je $\mathcal{N} \models \neg\varphi(n)$ za svaki n, pa $\mathcal{N} \not\models \exists x\varphi(x)$, jer smo već iscrpili sve objekte u domeni. Zato ne može vrijediti $\vdash_T \exists x\varphi(x)$. Dakle, ako T nije ω-konzistentna, onda $\mathcal{N} \not\models T$.

Sada smo spremni dokazati drugu verziju prvog teorema nepotpunosti.

Teorem 6.5 (Gödelov prvi teorem nepotpunosti, druga verzija)**.** *Neka je $T \supseteq Q$ ω-konzistentna teorija s primitivno rekurzivnim skupom aksioma X. Tada postoji Π_1-rečenica α takva da $\nvdash_T \alpha$ i $\nvdash_T \neg\alpha$. Drugim riječima, α je nezavisna u T.*

Dokaz. Neka je bew_T reprezentirana u T Σ_1-formulom $\mathtt{bew}(y, x)$. Za $\mathtt{bwb}(x) = \exists y\, \mathtt{bew}(y, x)$ iz korolara 5.4 dobivamo:

$$(a): \text{ ako } \vdash_T \varphi, \text{ tada } \vdash_T \mathtt{bwb}(\ulcorner\varphi\urcorner), \text{ za sve } \varphi.$$

Neka je γ fiksna točka formule $\neg\mathtt{bwb}(x)$, odnosno neka vrijedi:

$$\text{(b): } \gamma \equiv_T \neg\mathtt{bwb}(\ulcorner\gamma\urcorner).$$

Pretpostavimo sada da vrijedi $\vdash_T \gamma$. Tada je $\vdash_T \mathtt{bwb}(\ulcorner\gamma\urcorner)$ po (a), i $\vdash_T \neg\mathtt{bwb}(\ulcorner\gamma\urcorner)$ po (b), što je nemoguće jer je T konzistentna. Dakle, $\nvdash_T \gamma$.

S druge strane, pretpostavimo da vrijedi $\vdash_T \neg\gamma$, odnosno $\vdash_T \mathtt{bwb}(\ulcorner\gamma\urcorner)$ po (b). Slijedi $\vdash_T \exists y\, \mathtt{bew}(y, \ulcorner\gamma\urcorner)$. Pošto je T konzistentna, tada vrijedi $\nvdash_T \gamma$. Sada iz korolara 5.4 slijedi $\vdash_T \neg\mathtt{bew}(\underline{n}, \ulcorner\gamma\urcorner)$ za sve n, što je skupa sa (c) kontradikcija sa ω-potpunošću od T. Dakle, $\nvdash_T \neg\gamma$, pa je γ nezavisna T. No tada je Π_1-rečenica $\alpha \equiv \neg\mathtt{bwb}(\ulcorner\gamma\urcorner)$ također nezavisna u T jer je ekvivalentna rečenici γ. □

Rosser je 1936. godine dokazao da se pretpostavka ω-konzistentnosti može oslabiti na običnu konzistentnost.

Teorem 6.6 (Rosserova verzija prvog teorema nepotpunosti)**.** *Neka je $T \supseteq Q$ konzistentna teorija s primitivno rekurzivnim skupom aksioma X. Tada postoji Π_1-rečenica α takva da $\nvdash_T \alpha$ i $\nvdash_T \neg\alpha$.*

Dokaz. Definiramo formulu

$$\mathtt{prov}(x) \equiv \exists y\, [\mathtt{bew}(y, x) \wedge (\forall z < y)\neg\mathtt{bew}(z, \tilde{\neg}x)].$$

Ovdje smatramo da smo eliminirali funkciju $\tilde{\neg}$ zamjenom s odgovarajućom formulom. Dokažimo da formula $\mathtt{prov}(x)$ ima sljedeća svojstva:

$$\text{(a) ako } \vdash_T \alpha, \text{ tada } \vdash_T \mathtt{prov}(\ulcorner \alpha \urcorner),$$
$$\text{(b) ako } \vdash_T \neg\alpha, \text{ tada } \vdash_T \neg\mathtt{prov}(\ulcorner \alpha \urcorner).$$

Zaista, pretpostavimo da vrijedi $\vdash_T \alpha$. Tada po korolaru 5.4 postoji n takav da $\vdash_T \mathtt{bew}(\underline{n}, \ulcorner \alpha \urcorner)$. Pošto je T konzistentna, tada vrijedi $\nvdash_T \neg\alpha$, odnosno $\vdash_T \neg\mathtt{bew}(\underline{k}, \ulcorner \neg\alpha \urcorner)$ za sve k jer je bew reprezentabilna u T. Sada (C5) (str. 12) daje $\vdash_T (\forall z < \underline{n})\neg\mathtt{bew}(z, \ulcorner \neg\alpha \urcorner)$, pa zajedno imamo $\vdash_T \mathtt{bew}(\underline{n}, \ulcorner \alpha \urcorner) \wedge (\forall z < \underline{n})\neg\mathtt{bew}(z, \ulcorner \neg\alpha \urcorner)$. Sada uvođenjem kvantifikatora dobivamo $\vdash_T \mathtt{prov}(\ulcorner \alpha \urcorner)$.

Neka sada vrijedi $\vdash_T \neg\alpha$ i neka je m takav da vrijedi $\vdash_T \mathtt{bew}(\underline{m}, \ulcorner \neg\alpha \urcorner)$. Sada je $\nvdash_T \alpha$ jer je T konzistentna, pa opet po (C5) imamo $\vdash_T (\forall y \leq \underline{m})\neg\mathtt{bew}(y, \ulcorner \alpha \urcorner)$. To i (C6) daju $\mathtt{bew}(y, \ulcorner \alpha \urcorner) \vdash_T y > \underline{m}$. Sada uz $z = \underline{m}$ vrijedi $y > \underline{m} \vdash_T (\exists z < y)\mathtt{bew}(z, \ulcorner \neg\alpha \urcorner)$, pa konačno dobivamo

$$\vdash_T \forall y[\mathtt{bew}(y, \ulcorner \alpha \urcorner) \to (\exists z < y)\mathtt{bew}(z, \ulcorner \neg\alpha \urcorner)] \equiv_T \neg\mathtt{prov}(\ulcorner \alpha \urcorner).$$

Neka je sada γ fiksna točka formule $\neg\mathtt{prov}$. Tada iz $\vdash_T \neg\gamma$ slijedi $\vdash_T \mathtt{prov}(\ulcorner \gamma \urcorner)$, što je kontradikcija s (b), a iz pretpostavke $\vdash_T \gamma$ slijedi kontradikcija isto kao u prethodnom teoremu. Dakle, vrijedi $\nvdash_T \gamma$ i $\nvdash_T \neg\gamma$. □

Slično kao za konzistentnost, za potpunost možemo definirati pojam ω-potpunosti na sljedeći način:

Definicija 6.7. *Za teoriju $T \subseteq \mathcal{L}_{ar}$ kažemo da je ω-potpuna ako za svaku formulu $\varphi(x)$, za koju vrijedi $\vdash_T \varphi(\underline{n})$, za sve n, također vrijedi $\vdash_T \forall x\varphi$.*

Već smo ranije vidjeli da je Q ω-nepotpuna jer vrijedi $\vdash_Q \underline{n} \neq S\underline{n}$ za svaki n, no $\nvdash_Q \forall x\,(x \neq Sx)$. Dokažimo sada da je PA također ω-nepotpuna.

Neka je $\gamma \equiv_{PA} \neg\mathtt{bwb}_{PA}(\ulcorner \gamma \urcorner)$ i definiramo $\varphi(x) \equiv \neg\mathrm{bew}_{PA}(x, \ulcorner \gamma \urcorner)$. Sada na isti način kao u teoremu 6.5 zaključujemo $\nvdash_{PA} \gamma \equiv_{PA} \neg\mathtt{bwb}_{PA}(\ulcorner \gamma \urcorner) \equiv_{PA} \forall x\,\varphi$, odnosno $\nvdash_{PA} \forall x\,\varphi$. S druge strane, zbog $\nvdash_{PA} \gamma$ iz korolara 5.4 slijedi $\vdash_{PA} \varphi(\underline{n})$ za sve n. Dakle, PA je ω-nepotpuna.

6.2 Tarskijev teorem i neodlučivost

Sada dokazujemo Tarskijev teorem o nedefinabilnosti aritmetičke istine. Neka je $\mathcal{A}$ neka struktura. Reći ćemo da je $\alpha \in \mathcal{L}^0$ *istinita na* $\mathcal{A}$ ako vrijedi $\mathcal{A} \models \alpha$. Posebno, ako $\mathcal{N} \models \alpha$ reći ćemo da je α *istinita*. Ako postoji $\tau = \tau(x) \in \mathcal{L}$ takva da vrijedi: $\mathcal{A} \models \alpha$ ako i samo ako $\mathcal{A} \models \tau(\ulcorner \alpha \urcorner)$, za sve $\alpha \in \mathcal{L}^0$, kažemo da je *istina na* $\mathcal{A}$ *definabilna u* $\mathcal{A}$.

Teorem 6.8 (Tarski)**.** *Istina na $\mathcal{N}$ nije definabilna u $\mathcal{N}$.*

Dokaz. Pretpostavimo suprotno, tj. da postoji formula $\tau = \tau(x) \in \mathcal{L}$ takva da vrijedi: $\mathcal{N} \models \alpha$ ako i samo ako $\mathcal{N} \models \tau(\ulcorner \alpha \urcorner)$, za sve $\alpha \in \mathcal{L}^0$. Tvrdimo da je tada $Th\mathcal{N}$ reprezentabilna u $Th\mathcal{N}$. Zaista, ako $\vdash_{Th\mathcal{N}} \alpha$ onda po definiciji imamo $\mathcal{N} \models \alpha$, pa slijedi $\mathcal{N} \models \tau(\ulcorner \alpha \urcorner)$, odnosno $\vdash_{Th\mathcal{N}} \tau(\ulcorner \alpha \urcorner)$. S druge strane, ako $\nvdash_{Th\mathcal{N}} \alpha$, tada $\mathcal{N} \not\models \alpha$, pa $\mathcal{N} \not\models \tau(\ulcorner \alpha \urcorner)$, odnosno $\mathcal{N} \models \neg\tau(\ulcorner \alpha \urcorner)$. No to je nemoguće po lemi 6.2. □

U sljedećem dijelu poglavlja iznosimo neke rezultate o neodlučivosti teorije Q i proširenja. Reći ćemo da je teorija T *odlučiva* ako je skup teorema od T rekurzivan.

Lema 6.9. *Svako konačno proširenje T' odlučive teorije T nad istim jezikom $\mathcal{L}$ je odlučivo.*

Dokaz. Neka je $T' = T + \alpha$, gdje je $\alpha \equiv \bigwedge_{i \leq n} \alpha_i$ za neke formule $\alpha_0, ..., \alpha_n$. Vrijedi $\beta \in T'$ ako i samo ako $\alpha \to \beta \in T$. Iz toga slijedi

$$n \in \dot{T}' \Leftrightarrow n \in \dot{\mathcal{L}}^0 \ \& \ \dot{\alpha}_0 \tilde{\to} n \in \dot{T}.$$

Sada je $\dot{T}'$ rekurzivan jer su $\dot{T}, \dot{\mathcal{L}}^0$ i $\tilde{\to}$ rekurzivni, pa slijedi tvrdnja. □

Ovdje je važna pretpostavka da T' i T imaju isti jezik. Naime, odlučiva teorija T aksiomatizirana s $X \subseteq \mathcal{L}^0$ može biti neodlučiva ako se promatra kao teorija nad jezikom $\mathcal{L}' \supset \mathcal{L}$, na primjer zbog dodatnih tautologija jezika $\mathcal{L}'$.

Reći ćemo da je teorija T' *kompatibilna* s teorijom T ako je $T + T'$ konzistentna teorija. Nadalje, kažemo da je $T_0 \subseteq \mathcal{L}_0$ *jako neodlučiva* ako je T_0 konzistentna i svaka teorija nad jezikom $\mathcal{L}$ kompatibilna s T_0 je neodlučiva. Tada je svaka teorija T nad $\mathcal{L} \supseteq \mathcal{L}_0$, koja je kompatibilna s T_0, također neodlučiva, jer bi inače $T \cap \mathcal{L}_0$ bila odlučiva. Ako je T_0 jako neodlučiva, tada je svaka konzistentna teorija $T_1 \supseteq T_0$ također jako neodlučiva, jer ako je T kompatibilna sa T_1, tada je očito kompatibilna i s T_0. Nadalje, svaka podteorija od T_0 u $\mathcal{L}_0$ je tada isto neodlučiva.

Iz svega ovoga vidimo da što je teorija slabija, to je jače svojstvo jake neodlučivosti. Zato je važan sljedeći teorem.

Teorem 6.10. *Teorija Q je jako neodlučiva.*

Dokaz. Neka je $T \subseteq \mathcal{L}_0$ kompatibilna s Q. Pretpostavimo da je T odlučiva. Tada je po prethodnoj lemi odlučivo proširenje $T_1 = T + Q$. No tada je po teoremu o reprezentabilnosti $\dot{T}_1$ reprezentabilan u T_1, što je nemoguće zbog leme o nereprezentabilnosti. □

Teorem 6.11 (Churchov teorem neodlučivosti)**.** *Skup $\mathtt{Taut}_{\mathcal{L}}$ svih valjanih rečenica logike prvog reda je neodlučiv za $\mathcal{L} \supseteq \mathcal{L}_{ar}$.*

Dokaz. $\texttt{Taut}_{\mathcal{L}}$ je očito kompatibilan s Q, pa je neodlučiv po prethodnom teoremu. □

Ovaj rezultat se može poopćiti na jezike s jednom binarnom relacijom, pa tako i na sva proširenja takvih jezika [6]. Štoviše, može se pokazati da vrijedi za sve jezike osim onih koji sadrže samo unarne relacijske simbole i najviše jedan unarni funkcijski simbol. Za takve jezike postoje razne procedure odlučivanja za valjanost.

Iz prethodnog teorema posebno slijedi da je $Th\mathcal{N}$ neodlučiva, kao i svaka podteorija od $Th\mathcal{N}$, uključujući PA i sva konzistentna proširenja od PA jer su sve one kompatibilne s Q. Štoviše, $Th\mathcal{N}$ nije ni aksiomatizabilna jer je svaka potpuna aksiomatizabilna teorija odlučiva.

6.3 Hilbertov deseti problem

Na kraju ovog poglavlja osvrnut ćemo se još na neodlučivost Hilbertovog desetog problema kao posljedicu teorema 6.10. Hilbertov deseti problem je pitanje postoji li algoritam koji za svaki polinom $p(\vec{x})$ sa cjelobrojnim koeficijentima odlučuje je li pripadna diofantska jednadžba $p(\vec{x}) = 0$ ima rješenje u $\mathbb{Z}$. Odgovor je ne, a ovdje ćemo dati kratku skicu dokaza.

Prvo primijetimo da je dovoljno dokazati da takav algoritam ne postoji za diofantske jednadžbe u $\mathbb{N}$. Naime, Lagrangeov teorem o četiri kvadrata kaže da se svaki prirodan broj može zapisati kao zbroj četiri kvadrata cijelih brojeva. Iz toga odmah slijedi da $p(\vec{x}) = 0$ ima rješenje u $\mathbb{N}$ ako i samo ako $p(u_1^2+v_1^2+w_1^2+z_1^2, ..., u_n^2+v_n^2+w_n^2+z_n^2) = 0$ ima rješenje u $\mathbb{Z}$. Dakle, ako bi postojao algoritam za odlučivanje rješivosti diofantske jednadžbe u $\mathbb{Z}$, tada tada bi također postojao algoritam za $\mathbb{N}$.

Dalje uočimo da je rješivost diofantske jednadžbe u $\mathbb{N}$ ekvivalentna rješivosti diofantske jednadžbe u $\mathcal{L}_{ar}$ (prisjetimo se, diofantske jednadžbe u $\mathcal{L}_{ar}$ smo definirali kao atomarne formule). Dakle, Hilbertov deseti problem je zapravo pitanje postojanja algoritma za pitanje vrijedi li $\mathcal{N} \models \exists\vec{x}\,\delta(\vec{x})$, gdje je $\delta(\vec{x})$ proizvoljna diofantska jednadžba u $\mathcal{L}_{ar}$. Negativan odgovor na to pitanje će slijediti iz sljedećeg teorema, kojeg ćemo ovdje samo iskazati. Dokaz se može vidjeti u [4].

Teorem 6.12. *Aritmetička relacija P proizvoljne mjesnosti je diofantska ako i samo ako je rekurzivno prebrojiva.*

Korolar 6.13. (a) *Hilbertov deseti problem ima negativan odgovor.* (b) *Za svaku aritmetizabilnu teoriju $T \supseteq Q$, posebno za $T = PA$, postoji diofantska jednadžba čija je nerješivost dokaziva u T.*

Dokaz. (a) bwb_Q je rekurzivno prebrojiva po teoremu 3.6, pa iz prethodnog teorema slijedi da postoji diofantska jednadžba $\delta(x, \vec{y})$ takva da vrijedi

$$(*): \quad bwb_q(n) \Leftrightarrow \mathcal{N} \models \exists y\, \delta(\underline{n}, \vec{y}).$$

No sada vidimo da već skup $\{\exists \vec{y}\, \delta(\underline{n}, \vec{y}) \mid \mathcal{N} \models \exists \vec{y}\, \delta(\underline{n}, \vec{y})\}$ nije rekurzivan, jer po teoremu 6.10 bwb_Q nije rekurzivna.
(b) Ako bi nerješivost svake nerješive diofantske jednadžbe $\delta(\vec{x})$ bila dokaziva u T, tada bi vrijedilo $\vdash_T \neg\exists \vec{x}\, \delta(\vec{x})$ (ako je $\delta(\vec{x})$ nerješiva) ili $\vdash_T \exists \vec{x}\, \delta(\vec{x})$ inače (zbog teorema 4.9). No tada bi mogli odlučiti je li proizvoljna diofantska jednadžba rješiva jer je $\dot{T}$ rekurzivno prebrojiv, što je kontradikcija s (a). □

Poglavlje 7

Drugi teorem nepotpunosti i Löbov teorem

Neformalno rečeno, Gödelov drugi teorem nepotpunosti kaže da dovoljno jaka konzistentna teorija T ne može dokazati svoju konzistentnost. Štoviše, ta činjenica je dokaziva unutar T.

U ovom poglavlju uvodimo oznaku $\Box(x)$ za $\mathrm{bwb}_T(x)$, dok s $\Box\alpha$ označavamo $\mathrm{bwb}_T(\ulcorner\alpha\urcorner)$ i čitamo "α je dokaziva u T". Ako nije jasno iz konteksta na koju teoriju se $\Box$ odnosi, tada pišemo odgovarajući indeks $\Box_T$.

Da bismo mogli govoriti o konzistentnosti, trebamo prvo definirati konzistentnost unutar teorije. Ako je $T \supseteq Q$, možemo na prirodan način definirati rečenicu

$$\mathtt{Con}_T \equiv \neg\Box\bot \ (\equiv \neg\mathrm{bwb}_T(\ulcorner\bot\urcorner)).$$

Ovdje za $\bot$ uzimamo rečenicu $0 \neq 0$. Očito je T konzistentna ako i samo ako $\nvdash_T \bot$ jer zbog $T \supseteq Q$ vrijedi $\vdash_T \neg\bot$. Uskoro ćemo vidjeti da je $\mathtt{Con}_T$ neovisna o izboru $\bot$ ako vrijedi $\bot \equiv_T (0 \neq 0)$.

7.1 Uvjeti dokazivosti

Prije dokaza drugog teorema nepotpunosti potrebno je dokazati tri rezultata zvana Löbovi uvjeti dokazivosti:

$$\begin{aligned}
&\text{(D1)}: \quad \vdash_T \alpha \ \Rightarrow\ \vdash_T \Box\alpha,\\
&\text{(D2)}: \quad \vdash_T \Box\alpha \wedge \Box(\alpha \to \beta) \to \Box\beta,\\
&\text{(D3)}: \quad \vdash_T \Box\alpha \to \Box\Box\alpha.
\end{aligned}$$

Ovdje su $\alpha, \beta \in \mathcal{L}^0$. Uvjet (D2) se često još piše u ekvivalentnom obliku $\Box(\alpha \to \beta) \vdash_T \Box\alpha \to \Box\beta$. Dodatno, iz $\alpha \vdash_T \beta$ slijedi $\vdash_T \alpha \to \beta$, što zbog (D1) povlači $\vdash_T \Box(\alpha \to \beta)$. Sada iz toga i (D2) dobivamo $\vdash_T \Box\alpha \to \Box\beta$. Dakle, dobili smo

$$(\text{D0}): \quad \alpha \vdash_T \beta \;\Rightarrow\; \Box\alpha \vdash_T \Box\beta.$$

Sada iz (D0) dobivamo da $\alpha \equiv_T \beta$ povlači $\Box\alpha \equiv_T \Box\beta$. Posebno, izbor $\bot$ u $\mathtt{Con}_T$ je proizvoljan ako $\bot \equiv_T (0 \neq 0)$.

Uvjet (D1) odmah slijedi iz reprezentabilnosti relacije bew_T u T, pa vrijedi i za slabe teorije poput $T = Q$. S druge strane, obrat od (D1),

$$(\text{D1}^*): \quad \vdash_T \Box\alpha \;\Rightarrow \vdash_T \alpha, \text{ za sve } \alpha \in \mathcal{L}^0$$

ne mora vrijediti. Ipak, ako je T ω-konzistentno proširenje od Q (kao npr. PA), tada (D1*) vrijedi. Zaista, $\nvdash_T \alpha$ povlači $\vdash_T \neg\mathrm{bew}_T(\underline{n}, \ulcorner\alpha\urcorner)$ za sve n zbog korolara 5.4. Sada zbog ω-konzistentnosti od T slijedi $\nvdash_T \Box\alpha$.

Postavlja se pitanje za kakve teorije vrijede uvjeti (D2) i (D3). Može se dokazati da ti uvjeti vrijede u aksiomatizabilnim proširenjima od $\mathrm{I}\Sigma_1$, gdje je $\mathrm{I}\Sigma_1$ teorija dobivena dodavanjem indukcijske sheme za Σ_1-rečenice teoriji Q. Dokaz je nešto složeniji i ovdje ćemo ga izostaviti, a može se naći u [7]. Jasno je da je PA jedno takvo proširenje, pa posebno uvjeti dokazivosti vrijede u PA.

Lema 7.1. *Neka je $T \supseteq Q$ teorija za koju vrijede Löbovi uvjeti dokazivosti i neka su $\alpha, \gamma \in \mathcal{L}^0$ takve da vrijedi $\gamma \equiv_T \Box\gamma \to \alpha$. Tada vrijedi:*
(a) $\Box\gamma \equiv_T \Box\alpha$
(b) $\gamma \equiv_T \Box\alpha \to \alpha$.

Dokaz. Ako vrijedi (a), tada (b) odmah slijedi ako u $\gamma \equiv_T \Box\gamma \to \alpha$ zamijenimo $\Box\gamma$ formulom $\Box\alpha$. Dokažimo sada (a). Iz pretpostavke $\gamma \equiv_T \Box\gamma \to \alpha$ zbog (D0) i (D2) slijedi $\Box\gamma \vdash_T \Box(\Box\gamma \to \alpha) \vdash_T \Box\Box\gamma \to \Box\alpha$. Iz (D3) dobivamo $\Box\gamma \vdash_T \Box\Box\gamma$ pa iz prethodnog slijedi $\Box\gamma \vdash_T \Box\alpha$.

S druge strane, očito vrijedi $\alpha \vdash_T \Box\gamma \to \alpha \equiv_T \gamma$, pa $\alpha \vdash_T \gamma$. No sada iz (D0) dobivamo $\Box\alpha \vdash_T \Box\gamma$. Time je tvrdnja (a) dokazana. □

7.2 Drugi teorem nepotpunosti i posljedice

Sada smo spremni preciznije izreći i dokazati drugi teorem nepotpunosti.

Teorem 7.2 (Gödelov drugi teorem nepotpunosti)**.** *Neka je T teorija kao u prethodnoj lemi. Tada vrijedi sljedeće:*
(1) $\nvdash_T \mathtt{Con}_T$, *ako je T konzistentna,*
(2) $\vdash_T \mathtt{Con}_T \to \neg\Box\mathtt{Con}_T$.

Dokaz. Uočimo da (1) slijedi odmah iz (2). Zaista, neka vrijedi $\vdash_T \mathtt{Con}_T$. Tada zbog (D1) imamo $\vdash_T \mathtt{Con}_T$, a iz (2) slijedi $\vdash_T \neg\Box\mathtt{Con}_T$. Dakle, T nije konzistentna, što je kontradikcija. Dokažimo sada (2). Neka je γ fiksna točka od $\neg\Box(x)$. Tada vrijedi

$$(*) \quad \gamma \equiv_T \neg\Box\gamma \equiv_T \Box\gamma \to \bot.$$

Sada iz (b) dijela prethodne leme uz $\alpha \equiv \bot$ dobivamo $\gamma \equiv_T \Box\bot \to \bot \equiv_T \neg\Box\bot \equiv \mathtt{Con}_T$, pa možemo u $(*)$ zamijeniti γ s $\mathtt{Con}_T$. Time dobivamo $\mathtt{Con}_T \equiv_T \neg\Box\mathtt{Con}_T$, iz čega odmah slijedi (2). □

Jasno je da je tvrdnja (2) upravo drugi teorem nepotpunosti formaliziran unutar T. Dokaz prethodnog teorema pokazuje da je $\mathtt{Con}_T$ jedina fiksna točka od $\neg\mathrm{bwb}_T$ do na ekvivalenciju u T. Zato se tvrdnja (2) može interpretirati i kao formalizirana verzija prvog teorema nepotpunosti, odnosno jednog njegovog smjera.

Jedna posljedica drugog teorema nepotpunosti je postojanje konzistentnih teorija $T \supseteq \mathrm{PA}$ u kojima su, osim tvrdnji istinitih u $\mathcal{N}$, dokazive i neistinite tvrdnje. Takve teorije su vrlo bogate jer sadrže standardnu teoriju brojeva. Jedan primjer je teorija $\mathrm{PA}^\bot := \mathrm{PA} + \neg\mathtt{Con}_{\mathrm{PA}}$. Može se dokazati([6]) da za $\mathrm{PA}^\bot$ vrijedi

$$(3) \quad \mathtt{Con}_{\mathrm{PA}} \equiv_{\mathrm{PA}} \mathtt{Con}_{\mathrm{PA}^\bot} \quad (\text{iz čega slijedi } \mathtt{Con}_{\mathrm{PA}} \equiv_{\mathrm{PA}^\bot} \mathtt{Con}_{\mathrm{PA}^\bot}).$$

Primijetimo da vrijedi $\neg\mathtt{Con}_{\mathrm{PA}} \equiv \mathrm{bwb}_{\mathrm{PA}}(\ulcorner 0 \neq 0 \urcorner)$. Dakle, $\mathrm{PA}^\bot$ dokazuje neke očito neistinite tvrdnje. Nadalje, zbog $\vdash_{\mathrm{PA}^\bot} \neg\mathtt{Con}_{\mathrm{PA}}$ i (3) dobivamo $\vdash_{\mathrm{PA}^\bot} \neg\mathtt{Con}_{\mathrm{PA}^\bot}$, pa $\mathrm{PA}^\bot$ dokazuje svoju inkonzistentnost, iako je zapravo konzistentna. To znači da $\mathrm{PA}^\bot$ tvrdi da ima nekakav dokaz za $\bot$, što na prvi pogled izgleda kao paradoks. No slično kao kod Skolemovog "paradoksa", to samo znači da pojam konzistentnosti unutar teorije ima drugo značenje nego izvan teorije.

Sada ćemo se osvrnuti na još jedan poznati primjer samoreferentne rečenice, tj. rečenice koja "govori o sebi". Već smo spomenuli da lema o fiksnoj točki (6.1) omogućava konstrukciju takvih rečenica iz bilo koje formule s jednom slobodnom varijablom. Ako je α fiksna točka od $\Box(x)$, tada vrijedi $\alpha \equiv_T \Box\alpha$, tj. α tvrdi o sebi da je dokaziva.

Trivijalan primjer takve rečenice je bilo koji teorem od T. Naime, ako vrijedi $\vdash_T \alpha$ tada imamo $\vdash_T \Box\alpha$ i $\vdash_T \Box\alpha \to \alpha$, pa vrijedi $\alpha \equiv_T \Box\alpha$. Iznenađujuća činjenica je da ne postoje druge fiksne točke za $\Box(x)$. Preciznije, zbog tvrdnje (D4°) iz teorema koji slijedi $\vdash_T \Box\alpha \to \alpha$ povlači da je α teorem od T. Intuitivno bismo očekivali da $\vdash_T \Box\alpha \to \alpha$ vrijedi za svaku rečenicu.

Teorem 7.3 (Löbov teorem)**.** *Neka T zadovoljava Löbove uvjete dokazivosti i lemu o fiksnoj točki i neka je $\alpha \in \mathcal{L}^0$. Tada vrijedi:*

(D4) $\vdash_T \Box(\Box\alpha \to \alpha) \to \Box\alpha$,

(D4°) *Ako vrijedi* $\vdash_T \Box\alpha \to \alpha$, *tada* $\vdash_T \alpha$.

Dokaz. Neka je γ fiksna točka formule $\Box(x) \to \alpha$, tj. neka vrijedi $\gamma \equiv_T \Box\gamma \to \alpha$. Tada zbog leme 7.1 vrijedi $\gamma \equiv_T \Box\alpha \to \alpha$. Iz toga i (D0) slijedi $\Box\gamma \equiv_T \Box(\Box\alpha \to \alpha)$. Iz leme 7.1 dobivamo $\Box\gamma \equiv_T \Box\alpha$, pa zajedno dobivamo $\Box\alpha \equiv_T \Box(\Box\alpha \to \alpha)$. Iz toga odmah slijedi (D4).

Neka sada vrijedi $\vdash_T \Box\alpha \to \alpha$. Tada zbog (D1) vrijedi $\vdash_T \Box(\Box\alpha \to \alpha)$. Koristeći (D4) dobivamo $\vdash_T \Box\alpha$, pa $\vdash_T \Box\alpha \to \alpha$ daje $\vdash_T \alpha$. □

Jedna jednostavna posljedica Löbovog teorema je drugi teorem nepotpunosti. Zaista, tvrdnja (1) odmah slijedi jer iz $\vdash_{\mathrm{PA}} \mathtt{Con}_{\mathrm{PA}} (\equiv \Box\bot \to \bot)$ zbog (D4°) slijedi $\vdash_{\mathrm{PA}} \bot$, što je kontradikcija jer je PA konzistentna. Slično, kontrapozicijom dobivamo da (D4) povlači (2) za $\alpha \equiv \bot$.

Zaključak

Kao što smo na početku već najavili, dokazali smo da je Hilbertov program formaliziranja cijele matematike "razumnim" skupom aksioma neostvariv. Štoviše, bilo koja teorija s rekurzivnim skupom aksioma iz kojeg se mogu dokazati aksiomi jednostavne teorije Q nije potpun.

Možda se na prvi pogled čini da je ovdje bitna pretpostavka da vrijedi $T \supseteq Q$. Na primjer, to ne vrijedi za Zermelo-Fraenkelovu teoriju skupova `ZFC`, barem ne direktno. Naime, `ZFC` ne sadrži simbole jezika $\mathcal{L}_{ar}$ pomoću kojih definiramo prirodne brojeve i operacije na njima. Ipak, u teoriji `ZFC` i još mnogim drugim teorijama ti simboli i definicije se mogu *interpretirati* na način da se rezultati poput Gödelovog teorema nepotpunosti i pripadnih rezultata o neodlučivosti mogu prenijeti iz jedne teorije u drugu. Više o tome može se naći primjerice u [6].

To ipak ne znači da ne postoje primjeri netrivijalnih teorija koje su potpune. U takvim teorijama se ne mogu definirati prirodni brojevi pa prethodno spomenute interpretacijske tehnike nisu primjenjive. Prije smo već spomenuli Presburgerovu aritmetiku, odnosno PA bez operacije množenja. Još jedan primjer je teorija zatvorenih realnih polja (polja koja imaju ista svojstva kao polje $\mathbb{R}$). Ta teorija nije nimalo trivijalna jer može dokazati mnoge standardne tvrdnje o realnim brojevima.

Za kraj još naglasimo da smo se u ovom radu bavili samo matematičkim posljedicama Gödelovih teorema. Zanimljiv pregled filozofskih posljedica i diskusija o raznim krivim zaključcima može se naći primjerice u [9].

Bibliografija

[1] G. Boolos, J. P. Burgess i R. C. Jeffrey, *Computability and logic*, Cambridge university press, 2002.

[2] H. Enderton i H. B. Enderton, *A mathematical introduction to logic*, Academic press, 2001.

[3] K. Gödel, *Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I*, Monatshefte für mathematik und physik **38** (1931), br. 1, 173–198.

[4] Y. Matiyasevich, *Hilbert's 10th Problem*, MIT Press, 1994.

[5] P. Raatikainen, *Gödel's Incompleteness Theorems*, http://plato.stanford.edu/entries/goedel-incompleteness/.

[6] W. Rautenberg, *A concise introduction to mathematical logic*, Springer Science & Business Media, 2006.

[7] P. Smith, *An introduction to Gödel's theorems*, Cambridge University Press, 2013.

[8] R. M. Smullyan, *Gödel's incompleteness theorems*, Oxford University Press, 1992.

[9] F. Torkel, *Gödel's Theorem: An Incomplete Guide to its Use and Abuse*, Wellesley, MA: AK Peters, 2005.

[10] M. Vuković, *Matematička logika*, Element, 2009.

Sažetak

U ovom radu dokazuju se Gödelovi teoremi nepotpunosti koji ukazuju na fundamentalna ograničenja dokazivosti unutar teorija prvog reda. Nadalje, dokazuje se Tarskijev teorem o nedefinabilnosti aritmetičke istine, te Churchov teorem o neodlučivosti logike prvog reda.

U prvom dijelu obrađuje se postupak aritmetizacije sintakse i definiraju se aritmetičke relacije dokazivosti u teorijama. Zatim se dokazuje da se takve relacije mogu reprezentirati u dovoljno jakim teorijama, iz čega lako slijede gore spomenuti rezultati. Na kraju se razmatra pitanje dokazivosti konzistentnosti u teorijama te se dokazuje Gödelov drugi teorem nepotpunosti.

Summary

The main goal of this thesis is proving Gödel's incompleteness theorems, which establish fundamental limitations of provability in first-order theories. Additionally, we prove Tarski's nondefinability theorem and Church's undecidability theorem.

In the first part, we describe the process of arithmetization and define arithmetical provability predicates. Next, we show that such predicates can be represented in all sufficiently strong theories, from which the results mentioned above immediately follow. Finally, we explore the provability of consistency and prove Gödel's second incompleteness theorem.

Životopis

Rođen sam 8.7.1991. u Solothurnu, Švicarska, gdje sam živio sve do 2000. godine kada sam se preselio u Zadar. Tamo sam pohađao Osnovnu školu Smiljevac, te potom opću gimnaziju Vladimira Nazora. Kroz cijelu osnovnu i srednju školu sudjelovao sam u raznim natjecanjima iz matematike i fizike. Godine 2010. upisao sam Preddiplomski sveučilišni studij Matematike na Matematičkom odsjeku Prirodoslovno-matematičkog fakulteta u Zagrebu. Nakon završenog preddiplomskog studija upisao sam Diplomski sveučilišni studij Računarstvo i matematika.