SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

DIPLOMSKI RAD br. 206

Gödelovi teoremi nepotpunosti

Tomislav Novak

Zagreb, lipanj 2011.

Sadržaj

1 Uvod

Kada se prezentiraju Gödelovi teoremi nepotpunosti, korisno je spomenuti kontekst u kojem su oni nastali. Početkom dvadesetog stoljeća, osobito nakon otkrića paradoksa u Cantorovoj teoriji skupova[1], njemački je matematičar David Hilbert počeo isticati potrebu za formalizacijom cjelokupne matematike u vidu potpunog i konzistentnog aksiomatskog sustava. Osnovna ideja aksiomatske metode je definirati jezik, niz izraza u tom jeziku koje prihvaćamo kao istinite (aksiomi) te pravila koja nam govore kako iz postojećih izraza dobivamo nove izraze. Uz dobro definirane aksiome i pravila zaključivanja, dokazivanje novih matematičkih rezultata svodi se tako isključivo na postupke temeljene na *sintaksi* (manipulaciju simbolima i izrazima), bez ikakvog prizivanja na intuiciju, druga znanja i sl. Dakako, željeli bismo da aksiomatski sustav koji služi za formalizaciju matematike bude *konzistentan* (ne može dokazati dvije kontradiktorne tvrdnje) te *potpun* (može dokazati sve istinite tvrdnje).

Ideja aksiomatizacije nije nova – još je Euklid u *Elementima* naveo pet aksioma geometrije. Međutim, razvoj aksiomatske metode dobio je novi zamah u dvadesetom stoljeću, otkrićem paradoksa u teoriji skupova.

U svom čuvenom članku iz 1931. godine pod nazivom *O formalno neodlučivim rečenicama* Principia Mathematica *i srodnih sustava*, Kurt Gödel je dokazao kako čak ni za jednostavnu teoriju poput aritmetike, u čijoj se osnovi nalaze operacije zbrajanja i množenja nad prirodnim brojevima, nije moguće definirati skup aksioma iz kojih bi se mogle izvesti sve istinite aritmetičke tvrdnje. Drugim riječima, bez obzira koje aksiome odabrali, uvijek će postojati istinita tvrdnja koja neće biti dokaziva iz tih aksioma. Dodatno, Gödel je dokazao da konzistentnost neke dovoljno jake aritmetičke teorije (poput *Peanove aritmetike* ili *Principia Mathematica*) nije moguće dokazati unutar te teorije same. Ovo odmah povlači da se iz takve teorije ne može dokazati ni konzistentnost jačih teorija (kao što je, primjerice, ZFC). Gödelovi rezultati označili su kraj većeg dijela Hilbertovog programa.

Cilj je ovog rada dokazati Gödelove teoreme nepotpunosti, obraćajući oso-

[1] Teorija skupova kao grana matematike razvila se u drugoj polovici devetnaestog stoljeća. Njezin tvorac, njemački matematičar Georg Cantor, definirao je pojam *skupa* kao kolekciju objekata koji dijele neka zajednička svojstva. Međutim, kasnije se otkrilo kako takva definicija omogućuje pojavu određenih paradoksa (od kojih je vjerojatno najpoznatiji Russelov paradoks). Time je započeo razvoj *aksiomatske* teorije skupova.

bito pozornost na dvije ključne ideje – *aritmetizaciju sintakse* i *reprezentabilnost funkcija*. Razmatraju se dvije aritmetičke teorije – Robinsonova aritmetika Q te Peanova aritmetika, najprihvaćenija aritmetička teorija prvog reda. Teorija Q je slabija teorija od PA te je trivijalno nepotpuna – ona ne sadrži dovoljno aksioma da bi mogla dokazati *generalizacije* mnogih tvrdnji. S druge strane, teorija Q je dovoljno jaka da u njoj budu reprezentabilne primitivno rekurzivne funkcije, što je čini posebno zanimljivom. Peanova aritmetika sadrži sve aksiome Robinsonove aritmetike, uz dodatak *sheme aksioma indukcije*.

U sljedećem poglavlju definiraju se pobliže Robinsonova i Peanova aritmetika. Zatim se opisuje aritmetizacija sintakse, odnosno pridjeljivanje prirodnih brojeva izrazima formalnog aritmetičkog jezika L_A. U 4. poglavlju dokazuje se da je Q primitivno rekurzivno adekvatna teorija, tj. sve primitivno rekurzivne funkcije reprezentabilne su u toj teoriji. Time su izgrađeni potrebni temelji te se do dokaza Gödelovog prvog teorema nepotpunosti brzo dolazi na početku 5. poglavlja. U tom se poglavlju dokazuje još i dijagonalna lema, pomoću koje se tada dobivaju Gödel-Rosserov teorem i Tarskijev teorem o nedefinabilnosti aritmetičke istine. Konačno, u 6. poglavlju razmatra se pitanje dokazivosti konzistentnosti teorija Q i PA te se dokazuje Gödelov drugi teorem nepotpunosti.

2 Teorije Q i PA

Sadržaj

U ovom poglavlju navest ćemo neke osnovne pojmove vezane uz aksiomatske formalne teorije te pobliže opisati aritmetički jezik L_A koji ćemo koristiti u narednim poglavljima. Zatim ćemo iznijeti aksiome teorije Q (tzv. *Robinsonove aritmetike*) te *Peanove aritmetike* (teorije PA).

Kad se govori o nekoj aksiomatskoj teoriji (formalnom sustavu) potrebno je navesti njezin *jezik*, skup *aksioma* te *pravila zaključivanja*. U ovom se radu bavimo **teorijama prvog reda** čiji jezik, osim skupa varijabli i logičkih veznika, sadrži i kvantifikatore. Podrazumijevat ćemo da skup aksioma takvih teorija sadrži i niz valjanih formula – takve formule nazivaju se *logičkim aksiomima*. Dodatno, teorije koje razmatramo koriste *modus ponens* i *generalizaciju* kao pravila zaključivanja. Ovdje se nećemo zadržavati na detaljima – više o teorijama prvog reda i pravilima zaključivanja može se pročitati u [11].

Spomenimo da uz ovakve (tzv. *hilbertovske* sustave), postoje i sustavi *prirodne dedukcije* koji sadrže manji broj aksioma, no puno više pravila zaključivanja. Dokazano je kako su ti sustavi ekvivalentni – skupovi njihovih teorema su jednaki (vidi [11]). Zato ćemo u kasnijim poglavljima, unatoč tome što Robinsonovu i Peanovu aritmetiku promatramo kao hilbertovske sustave, neke dokaze *unutar tih teorija* provoditi koristeći i pravila prirodne dedukcije. Takvi dokazi su kraći i elegantniji, a za svaki od njih postoji i ekvivalentan dokaz koji koristi samo pravila modus ponens i generalizaciju (uz logičke aksiome teorije). Na ovu činjenicu osvrnut ćemo se ponovo u 4. poglavlju.

Navedimo sada definicije nekih pojmova koji će se kasnije često koristiti:

Definicija 2.1. Kažemo da teorija prvog reda T *odlučuje* zatvorenu formulu φ ako T izvodi φ ili njezinu negaciju. Zapisano kraće, $T \vdash \varphi$ ili $T \vdash \neg\varphi$.

Definicija 2.2. Teorija T je *potpuna* ako odlučuje svaku formulu svog jezika.

Pojam potpunosti u logici koristi se često i u nešto drugačijem kontekstu. Teorija T je *semantički* potpuna ako dokazuje svaku formulu φ za koju vrijedi $T \models \varphi$.[1] Gödelov teorem *potpunosti* (vidi [11]) odnosi se upravo na semantičku potpunost teorija prvog reda. U ovom radu, kad se kaže da je teorija T (ne)potpuna, podrazumijeva se da se radi o potpunosti iz definicije 2.2.

Definicija 2.3. Za teoriju prvog reda T kažemo da je *konzistentna* ako ne postoji formula φ u jeziku te teorije takva da $T \vdash \varphi$ i $T \vdash \neg\varphi$.

Konzistentnost je jedna od najvažnijih sintaktičkih karakteristika formalnih teorija. Naime, ako je neka teorija prvog reda *nekonzistentna*, ona može dokazati *svaku formulu* (za dokaz vidi primjerice [11]). Drugim riječima, ako postoji formula koja se ne može dokazati u nekoj teoriji, ta je teorija konzistentna.

2.1. Jezik L_A

Svaka teorija prvog reda određena je nelogičkim simbolima svoga jezika (signaturom) te nelogičkim aksiomima. U ovom odjeljku definiramo jezik aritmetike L_A u kojem su oblikovane teorije Q i PA.

Skup $\{\mathsf{0}, \mathsf{S}, +, \times\}$ čine nelogički simboli jezika L_A. Pritom je $\mathsf{0}$ konstantski simbol, S je jednomjesni funkcijski simbol, dok su $+$ i $\times$ dvomjesni funkcijski simboli. Podrazumijevamo da L_A sadrži i *logički* relacijski simbol $=$.

Standardni model jezika L_A jest upravo skup prirodnih brojeva ω, pri čemu se simbolu $\mathsf{0}$ pridružuje broj 0, funkcijskom simbolu S odgovara funkcija koja svoj argument uvećava za jedan, dok simbolima $+$ i $\times$ odgovaraju funkcije zbrajanja i množenja. Primjerice, ako s φ označimo funkciju koja termima jezika L_A pridružuje elemente nosača (skupa ω), tada vrijedi $\varphi(\mathsf{0}) = 0$, $\varphi(\mathsf{SS0}) = 2$, $\varphi(\tau + \psi) = \varphi(\tau) + \varphi(\psi)$ itd.

U poglavljima koja slijede koristi se pojam numerala kojeg ovdje definiramo.

Definicija 2.4. Zatvoreni term oblika $\mathsf{SS}\ldots\mathsf{S0}$, gdje se simbol S ponavlja n puta, označavamo s $\overline{\mathsf{n}}$ i nazivamo *numeralom* prirodnog broja n.

Istaknimo da numeralu $\overline{\mathsf{n}}$ na standardnom modelu odgovara upravo prirodan broj n.

U ovom radu često će se spominjati pitanje *istinitosti* nekih formula jezika L_A. Pritom ćemo podrazumijevati istinitost *na standardnom modelu.*

2.2. Robinsonova aritmetika

Robinsonova aritmetika (teorija Q), unatoč tome što je *trivijalno nepotpuna* (pokazat ćemo u nastavku zatvorenu formulu koja je istinita, a nije dokaziva u Q),

[1] Podsjetimo se da $T \models \varphi$ označava da je formula φ istinita na svakom modelu teorije T.

veoma je zanimljiva. Naime, teorija Q dovoljno je *jaka* da su u njoj *reprezentabilne sve primitivno rekurzivne funkcije* (što to točno znači opisuje se detaljno u sljedeća dva poglavlja). Kasnije ćemo pokazati kako je upravo to dovoljan uvjet da teorija bude nepotpuna, odnosno da na nju bude primjenjiv Gödelov prvi teorem nepotpunosti.

Teorija Q sadrži sedam nelogičkih aksioma koje ovdje navodimo:

Definicija 2.5. Aksiomatska teorija čiji je jezik L_A, a sadrži nelogičke aksiome navedene u nastavku, naziva se *Robinsonova aritmetika*, a označava s Q.

1. $\forall \mathsf{x}(0 \neq \mathsf{Sx})$
2. $\forall \mathsf{x} \forall \mathsf{y}(\mathsf{Sx} = \mathsf{Sy} \rightarrow \mathsf{x} = \mathsf{y})$
3. $\forall \mathsf{x}(\mathsf{x} \neq 0 \rightarrow \exists \mathsf{y}(\mathsf{x} = \mathsf{Sy}))$
4. $\forall \mathsf{x}(\mathsf{x} + 0 = \mathsf{x})$
5. $\forall \mathsf{x} \forall \mathsf{y}(\mathsf{x} + \mathsf{Sy} = \mathsf{S}(\mathsf{x} + \mathsf{y}))$
6. $\forall \mathsf{x}(\mathsf{x} \times 0 = 0)$
7. $\forall \mathsf{x} \forall \mathsf{y}(\mathsf{x} \times \mathsf{Sy} = (\mathsf{x} \times \mathsf{y}) + \mathsf{x})$

Naglasimo kako su Q i PA *teorije s jednakošću*, što znači da logički aksiomi i pravila zaključivanja ugrađeni u te teorije omogućavaju da se iz $\tau = \rho$ dokaže i $\varphi(\tau) = \varphi(\rho)$ za bilo koju formulu φ. Teorije s jednakošću obrađene su detaljno u [11].

U odjeljku 4.2 pokazat ćemo da Q, između ostaloga, može dokazati $0 + \bar{\mathsf{n}} = \bar{\mathsf{n}}$ za svaki prirodan broj n. Zanimljivo je, međutim, da Q ne može dokazati *generalizaciju* te tvrdnje: $\mathsf{Q} \nvdash \forall \mathsf{x}(0 + \mathsf{x} = \mathsf{x})$. Doista, moguće je izgraditi model za teoriju Q na kojem rečenica $\forall \mathsf{x}(0 + \mathsf{x} = \mathsf{x})$ *nije istinita* (dakle, interpretaciju na kojem su istiniti svi aksiomi teorije, ali ne i gornja rečenica; vidi [8] za detalje oko konstrukcije). Kako je Q *adekvatna* teorija (njezini teoremi istiniti su na svakom modelu te teorije), $\mathsf{Q} \nvdash \forall \mathsf{x}(0 + \mathsf{x} = \mathsf{x})$. U protivnom bi i $\forall \mathsf{x}(0 + \mathsf{x} = \mathsf{x})$ moralo biti istinito na *svakom modelu* od Q – kontradikcija.

Uočimo da je rečenica $\forall \mathsf{x}(0 + \mathsf{x} = \mathsf{x})$ istinita na standardnom modelu (usporedimo je s aksiomom 4). Kako su aksiomi teorije Q svi također istiniti na standardnom modelu, $\mathsf{Q} \nvdash \neg \forall \mathsf{x}(0 + \mathsf{x} = \mathsf{x})$, budući da bi u protivnom Q dokazala neistinitu formulu.

2.3. Peanova aritmetika

Pokazali smo u prethodnom odjeljku kako teorija Q ne može dokazati neke trivijalne generalizacije poput $\forall \mathsf{x}(0 + \mathsf{x} = \mathsf{x})$. Kako bismo tome doskočili, aksiomima teorije Q dodajemo skup aksioma indukcije, čime dobivamo *Peanovu aritmetiku* (kraće: teoriju PA).

Definicija 2.6. Svaku zatvorenu formulu oblika

$$[\varphi(0) \land \forall x(\varphi(x) \to \varphi(Sx))] \to \forall x \varphi(x),$$

gdje je φ proizvoljna formula jezika L_A, nazivamo instancom *sheme aksioma indukcije.*

Definicija 2.7. *Peanova aritmetika* je teorija prvog reda čiji je jezik L_A, a nelogički aksiomi su sljedeći:

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

Dodatno, aksiom teorije PA je i svaka instanca sheme aksioma indukcije:

7. $[\varphi(0) \land \forall x(\varphi(x) \to \varphi(Sx))] \to \forall x \varphi(x)$

Primijetimo kako se među aksiomima teorije PA ne navodi 3. aksiom teorije Q. Rečenica $\forall x(x \neq 0 \to \exists y(x = Sy))$ se, naime, može sada dokazati pomoću aksioma indukcije.

Propozicija 2.1. $\mathsf{PA} \vdash \forall x(0 + x = x)$.

Dokaz. Definirajmo $\varphi(x) =_{\text{def}} 0 + x = x$. Iz aksioma 3 odmah slijedi $\mathsf{PA} \vdash \varphi(0)$. Nastavljajući dokaz *unutar* teorije PA, uzmimo da je a proizvoljan te pretpostavimo da vrijedi $\varphi(a)$, odnosno $0 + a = a$. Iz aksioma 4 dobivamo $0 + Sa = S(0 + a)$. Budući da je PA teorija s jednakošću, sada dobivamo $0 + Sa = Sa$, odnosno $\varphi(Sa)$. Dakle, dokazali smo $\varphi(a) \to \varphi(Sa)$. Kako je a bio proizvoljan, dokazujući unutar PA došli smo do sljedećeg rezultata: $\mathsf{PA} \vdash \forall x(\varphi(x) \to \varphi(Sx))$. Zajedno s $\varphi(0)$ i aksiomom indukcije za φ, dobivamo $\mathsf{PA} \vdash \forall x(0 + x = x)$, što je i trebalo dokazati. $\square$

Iako, za razliku od teorije Q, Peanova aritmetika nije trivijalno nepotpuna, postoji istinita rečenica G takva da ni G, a nije $\neg\mathsf{G}$, nije dokazivo u PA. Tome nam svjedoči Gödelov prvi teorem nepotpunosti kojime se bavimo u narednim poglavljima.

3 Aritmetizacija

Sadržaj

Jedan od temeljnih koraka u Gödelovom dokazu teorema nepotpunosti iz 1931. je konstrukcija rečenice u jeziku aritmetike L_A koja (po uzoru na paradoks lašca te Richardov paradoks) *indirektno* o sebi govori da je nedokaziva. Takva rečenica (označimo je s G), kao što će biti pokazano u kasnijim poglavljima, istinita je ako i samo ako nije dokaziva. Iz toga nadalje slijedi da, ako je teorija Q konzistentna, tada njezina Gödelova rečenica nije dokaziva: $\mathsf{Q} \nvdash \mathsf{G}$. Također, ako je Q ω-konzistentna teorija, tada ni negacija te rečenice nije dokaziva, tj. $\mathsf{Q} \nvdash \neg\mathsf{G}$.

Posebno je fascinantno kako se u jeziku L_A koji ima vrlo ograničeni alfabet – od nelogičkih simbola sadrži samo $\mathsf{0}$, S, $+$ i $\times$ (ti simboli u standardnoj interpretaciji predstavljaju nulu, funkciju sljedbenika te funkcije zbrajanja i množenja) – doista mogu izraziti složene tvrdnje poput onih o dokazivosti formula u nekoj aritmetičkoj teoriji kao što je Q ili PA. Gödel je pokazao da je moguće svakom nizu simbola jezika P_A dodijeliti kôd – prirodan broj – i to na način da sada *tvrdnjama o formulama* jezika L_A ili *teoremima* teorija poput Q izgrađenima nad L_A možemo pridijeliti odgovarajuće *tvrdnje o prirodnim brojevima* (njihovim kodovima). Primjerice, moguće je tako definirati relaciju *Sent* tako da vrijedi $\mathit{Sent}(n)$ samo ako je n kôd neke L_A rečenice.

U prvom dijelu ovog poglavlja definiraju se Gödelovi brojevi i jedan od načina na koji se kodovi mogu dodijeliti simbolima jezika L_A. Zatim se ukratko definiraju klase *primitivno rekurzivnih* funkcija i relacija. Na kraju se demonstrira ideja dijagonalizacije (supstitucije Gödelovog broja formule φ umjesto slobodne varijable same te formule φ) te se pokazuje kako se mogu definirati numeričke relacije poput $\mathit{Sent}(n)$ i $\mathit{Prf}(m, n)$ (koja vrijedi ako je prirodan broj m *köd dokaza* formule koju kodira n; o tome više u nastavku). Posebno, pokazuje se da su te relacije primitivno rekurzivne.

Zašto je to tako važno? Budući da su prirodni brojevi upravo standardna interpretacija ugrađena u L_A, čini se logičnim da sada možemo relacije poput $Sent(n)$ izraziti u jeziku L_A. U 4. poglavlju dokazuje se da to doista vrijedi (štoviše, pokazuje se da se tvrdnje o takvim relacijama mogu i dokazati unutar teorija poput Q). Dakle, moguće je konstruirati rečenice u L_A koje govore (indirektno) o sebi samima. Drugim riječima, čak je i jezik poput L_A dovoljno ekspresivan da omogući samoreferenciranje.

3.1. Gödelovi brojevi

U ovom odjeljku prikazuje se jedan od načina na koji je izrazima jezika L_A moguće pridružiti prirodne brojeve (takve brojeve nazvat ćemo *Gödelovim brojevima* ili *kodovima*). Prvo ćemo definirati kôd za svaku varijablu i simbol jezika L_A, a zatim pokazati kako je moguće kodirati i nizove simbola (odnosno nizove njihovih Gödelovih brojeva). Važno je istaknuti kako nije nužno koristiti upravo ovakav način kodiranja – bitno je samo, što je i apostrofirano kasnije u ovom poglavlju, da su svojstva da je neki prirodan broj n kôd L_A formule ili rečenice, da je n kôd dokaza u nekoj teoriji T oblikovanoj u L_A i sl. primitivno rekurzivna.

U ovom radu koristi se način kodiranja opisan u [8], sličan izvornom Gödelovom. U literaturi (primjerice u [1]) pojavljuje se i način kodiranja gdje se L_A izrazima pridružuje broj koji se dobiva jednostavnim nadovezivanjem kodova pojedinačnih simbola.

Jezik L_A sadrži prebrojivo mnogo varijabli te konačan broj logičkih i nelogičkih simbola. Pridružimo varijablama parne brojeve, a ostalim simbolima neparne brojeve na sljedeći način:

$\neg$	$\wedge$	$\vee$	$\rightarrow$	$\leftrightarrow$	$\forall$	$\exists$	$=$	(	)	0	S	$+$	$\times$	x	y	$\ldots$
1	3	5	7	9	11	13	15	17	19	21	23	25	27	2	4	$\ldots$

Primijetimo kako nije bilo potrebno pridružiti kodove svim logičkim operatorima – naime, $\wedge$, $\rightarrow$ i $\leftrightarrow$ mogu se izraziti pomoću $\neg$ i $\vee$. Ovdje je to napravljeno radi potpunosti te bolje čitljivosti nekih kasnijih definicija relacija vezanih uz te operatore.

Kako bismo dobili Gödelov broj proizvoljnog L_A izraza, kodirat ćemo *niz brojeva* koji predstavljaju kodove pojedinačnih znakova tog izraza. To možemo učiniti na sljedeći način. Označimo s π_i $(i+1)$. po redu prosti broj. Proizvoljnom nizu (c_n) sada pridružujemo kôd c na ovaj način:

$$c = \pi_0^{c_0} \times \pi_1^{c_1} \times \cdots \times \pi_n^{c_n}$$

Primjerice, prvom aksiomu teorije Q pridružujemo broj $2^{11} \times 3^2 \times 5^1 \times 7^{17} \times 11^{21} \times 13^{15} \times 17^{23} \times 19^2 \times 23^{19}$, budući da svakom simbolu tog aksioma pridružujemo kodove na sljedeći način:

$$\begin{array}{ccccccccc} \forall & \mathsf{x} & \neg & (& \mathsf{0} & = & \mathsf{S} & \mathsf{x} &) \\ 11 & 2 & 1 & 17 & 21 & 15 & 23 & 2 & 19 \end{array}$$

Uočimo da, kod kodiranja, sve pokrate (poput $\neq$ ili $\leq$) koristimo u njihovom proširenom obliku.

Prema osnovnom teoremu aritmetike, rastav svakog broja na proste faktore je jedinstven. Iz toga zaključujemo da svaki kôd jedinstveno određuje niz brojeva koji kodira.[1]

Na jednak način sada možemo kodirati i *niz formula* jezika L_A – svaku formulu predstavimo njenim Gödelovim brojem te kodiramo dobiveni niz. Posebno, često ćemo u ovom i sljedećim poglavljima koristiti pojam Gödelovog broja *dokaza* neke formule u teoriji poput Q. To nije ništa drugo nego kôd niza (c_n), gdje je c_n Gödelov broj formule φ koja se dokazuje, a svaki c_i je ili Gödelov broj aksioma teorije Q ili Gödelov broj formule koja se dobiva pomoću generalizacije ili pravila modus ponens iz formula s Gödelovim brojevima c_j i c_k, $j, k < i$ (jedan od razloga što koristimo hilbertovski sustav je upravo jednostavnost definiranja dokaza).

Ovakav način kodiranja, naravno, nije primjenjiv samo na L_A. Pridruživanje brojeva izrazima proizvoljnog jezika L nazivamo *aritmetizacijom*.

Na kraju ovog odjeljka skrenimo samo još pozornost na jednu činjenicu vezanu uz oznake: s $\ulcorner\varphi\urcorner$ označavat ćemo skraćeno Gödelov broj formule φ. Ista oznaka koristit će se i unutar L_A, gdje se pretpostavlja da predstavlja odgovarajući numeral.

3.2. Primitivno rekurzivne funkcije

Klasa *primitivno rekurzivnih funkcija* predstavlja važan (pravi) podskup skupa svih izračunljivih funkcija. Cilj ovog poglavlja je dokazati kako je relacija $Prf(m, n)$, koja vrijedi ako i samo ako m kodira PA dokaz zatvorene formule čiji je Gödelov broj n, upravo primitivno rekurzivna. Kao i reprezentabilnost primitivno rekurzivnih funkcija u teoriji PA, rezultat koji se dokazuje u sljedećem poglavlju, ovo je ključna tvrdnja koja je nužna za dokaz Gödelovih teorema nepotpunosti.

Relacija kao što je $Prf(m, n)$ očito ovisi o samoj teoriji na koju se odnosi, odnosno o njezinim aksiomima. Zato ćemo koristiti oznaku $Prf_T(m, n)$ kad želimo naglasiti da m kodira dokaz u proizvoljnoj teoriji T, umjesto podrazumijevanoj PA.

U ovom odjeljku definiraju se primitivno rekurzivne funkcije te se iznose neke osnovne tvrdnje o toj klasi funkcija. U tekstu se često spominju i primitivno rekurzivne *relacije*. Međutim, pojam izračunljivosti se općenito odnosi na funkcije, pa tako i pojam primitivne rekurzivnosti. Terminologija koju koristimo opravdana je činjenicom da svakoj relaciji možemo pridružiti karakterističnu funkciju.

[1] Naravno, nije svaki prirodan broj kôd nekog niza.

Definicija 3.1. Neka je R proizvoljna n-mjesna relacija nad prirodnim brojevima. Funkciju $\chi_R : \mathbb{N}^n \to \{0,1\}$ definiranu na sljedeći način

$$\chi_R(a_1, a_2, \ldots, a_n) = \begin{cases} 0 & \text{ako } R(a_1, a_2, \ldots, a_n) \\ 1 & \text{inače} \end{cases}$$

nazivamo *karakterističnom funkcijom* relacije R. Kažemo da je relacija R primitivno rekurzivna ako je njezina karakteristična funkcija χ_R primitivno rekurzivna.

Većinom se u literaturi karakteristična funkcija definira tako da poprima vrijednost 1 za argumente za koje relacija vrijedi, no ovakva obrnuta definicija olakšava definiciju nekih relacija (vidi [8]).

Sam pojam izračunljivosti teško je precizno definirani. U intuitivnom smislu, za funkciju $f : \mathbb{N}^n \to \mathbb{N}$ kaže se da je izračunljiva ako postoji algoritam koji ju izračunava – drugim riječima, postoji algoritam koji prilikom izračunavanja funkcije f s vrijednostima $x_1, \ldots, x_n \in \mathbb{N}$ na ulazu stane ako i samo ako su $x_1, \ldots, x_n$ u domeni funkcije f (i tada kao izlaz daje vrijednost funkcije $f(x_1, \ldots, x_n)$). Postoje mnogi modeli izračunljivosti – npr. izračunljivost na Turingovom stroju, RAM-izračunljivost, parcijalno rekurzivne funkcije itd. Dokazano je, međutim, da su svi prethodno navedeni modeli *ekvivalentni* (u [12] može se, primjerice, pronaći dokaz da je skup parcijalno rekurzivnih funkcija jednak skupu RAM-izračunljivih funkcija). Štoviše, prema čuvenoj *Church-Turingovoj tezi*, svaka funkcija koja je izračunljiva u intuitivnom smislu je Turing-izračunljiva (vidi [7]).

Iako ne sadrži sve izračunljive funkcije, klasa primitivno rekurzivnih funkcija veoma je bogata. Tako je i karakteristična funkcija nama važne relacije $Prf(m, n)$ primitivno rekurzivna, što dokazujemo u odjeljku 3.3. Nizom definicija u nastavku opisujemo ovu klasu funkcija.

Definicija 3.2. Nul-funkciju, funkciju sljedbenika i projekciju nazivamo *inicijalnim funkcijama.*

- Nul-funkcija $Z : \mathbb{N} \to \mathbb{N}$ definirana je sa $Z(x) = 0$.
- Funkcija sljedbenika $Sc : \mathbb{N} \to \mathbb{N}$ definirana je kao $Sc(x) = x + 1$.
- Funkcija $I^n_k : \mathbb{N}^n \to \mathbb{N}$ definirana tako da vrijedi $I^n_k(x_1, \ldots, x_n) = x_k$ naziva se projekcija.

Definicija 3.3. Neka je g k-mjesna, a $h_1, \ldots, h_k$ n-mjesne funkcije. Za n-mjesnu funkciju f kažemo da je definirana pomoću *kompozicije* ako je

$$f(\vec{x}) = g(h_1(\vec{x}), \ldots, h_k(\vec{x}))$$

Definicija 3.4. Neka je g totalna n-mjesna, a h totalna $(n+2)$-mjesna funkcija. Za $(n+1)$-mjesnu funkciju f kažemo da je definirana *primitivnom rekurzijom* pomoću g i h ako je definirana na sljedeći način:

$$
\begin{aligned}
f(\vec{x},0) &= g(\vec{x}) \\
f(\vec{x},y+1) &= h(\vec{x},y,f(\vec{x},y))
\end{aligned}
$$

Iz gornjih definicija sada odmah slijedi i definicija klase primitivno rekurzivnih funkcija:

Definicija 3.5. Klasom *primitivno rekurzivnih funkcija* (kraće: p.r. funkcija) nazivamo najmanju klasu totalnih funkcija koja sadrži sve inicijalne funkcije te je zatvorena za kompoziciju i primitivnu rekurziju. Relacija i skup su primitivno rekurzivni ako su primitivno rekurzivne njihove karakteristične funkcije.

Ovdje nećemo zalaziti u detalje, no nije teško dokazati da je svaka primitivno rekurzivna funkcija Turing-izračunljiva (tj. postoji program za Turingov stroj koji ju izračunava). Naime, inicijalne funkcije su trivijalno Turing-izračunljive, a ako su to i funkcije g i h, tada je lako konstruirati program za Turingov stroj koji izračunava funkciju f definiranu pomoću g i h kompozicijom ili primitivnom rekurzijom. Dokaz ove tvrdnje za RAM-stroj može se pronaći u [12]. Nama je posebno zanimljiva činjenica da su primitivno rekurzivne funkcije reprezentabilne u aksiomatskoj Peanovoj aritmetici – teorija PA može dokazati različite tvrdnje o rezultatima primitivno rekurzivnih funkcija, no o tome više u poglavlju 4.

Karakterističnu funkciju relacije $Prf(m,n)$ definirati ćemo pomoću kompozicije i primitivne rekurzije pomoću jednostavnijih p.r. funkcija. Stoga ćemo prvo definirati neke p.r. funkcije te iznijeti neke rezultate koji će nam olakšati takvu definiciju.

Kod izgradnje primitivno rekurzivnih funkcija i relacija često ćemo upotrijebiti logičke operatore i kvantifikatore; istaknimo samo kako oni ovdje nemaju formalnu ulogu simbola jezika neke logičke teorije poput L_A.

Propozicija 3.1. *Za primitivno rekurzivne funkcije i relacije vrijede sljedeće tvrdnje:*

– *Ako je $f : \mathbb{N}^n \to \mathbb{N}$ primitivno rekurzivna funkcija, tada je i $(n+1)$-mjesna relacija R definirana tako da je $(\vec{x},y) \in R$ ako i samo ako $f(\vec{x}) = y$ primitivno rekurzivna.*

– *Ako su P i Q primitivno rekurzivne relacije, tada su i relacije $\neg P$, $P \wedge Q$, $P \vee Q$, $P \to Q$ i $P \leftrightarrow Q$ primitivno rekurzivne. Logičke veznike ovdje koristimo u uobičajenom smislu: primjerice, vrijedi $(P \wedge Q)(\vec{x})$ ako i samo ako $P(\vec{x})$ i $Q(\vec{x})$.*

– *Ako je R primitivno rekurzivna relacija, a f primitivno rekurzivna funkcija, tada su primitivno rekurzivne i relacije $(\forall y \leq f(x))R(y)$ te $(\exists y \leq f(x))R(y)$. Ovdje se u neformalnom smislu koriste ograničeni kvantifikatori: $P(x) \overset{def}{=} (\exists y \leq n)R(y)$ vrijedi za sve one brojeve x za koje postoji neki broj y manji ili jednak od x takav da vrijedi $R(y)$.*

– *Ako je R jednomjesna primitivno rekurzivna relacija, tada je funkcija $f(n) = (\mu x \leq g(n))R(x)$ primitivno rekurzivna. Ovdje μ predstavlja (ograničeni) operator minimizacije – vrijednost funkcije $f(n)$ je najmanji x manji ili jednak od $g(n)$ za koji vrijedi $R(x)$.*

– *Svaka funkcija definirana po slučajevima iz drugih primitivno rekurzivnih funkcija je također primitivno rekurzivna.*[2]

Dokaz gornjih tvrdnji može se pronaći u [8].

U nastavku ovog odjeljka pokazujemo da su neke korisne funkcije primitivno rekurzivne. To će biti funkcije usko vezane uz način kodiranja L_A izraza opisan na početku ovog poglavlja – ovdje posebno želimo pokazati kako je funkcija za dekodiranje Gödelovih brojeva koji kodiraju nizove primitivno rekurzivna.

Lako je pokazati da su funkcija prethodnika $P(n) = \begin{cases} n-1 & \text{ako je } n \geq 1 \\ 0 & \text{inače} \end{cases}$, funkcija $sgn(n)$ koja je jednaka nuli ako je $n = 0$, a 1 inače, te funkcija $\dot{-}$ (gdje je $m \dot{-} n$ jednako $m - n$ ako je $m \geq n$, a 0 inače) primitivno rekurzivne. Doista, funkciju $P(n)$ možemo definirati pomoću primitivne rekurzije na sljedeći način: $P(0) = 0$, $P(n+1) = n$ (primijetimo da ovdje koristimo samo nul-funkciju i projekciju). Na sličan je način $sgn(0) = 0$, a $sgn(n+1) = Sc(Z(n))$ (koristimo kompoziciju nul-funkcije, funkcije sljedbenika i projekcije). Na kraju, $n \dot{-} 0 = n$ te $n \dot{-} (m+1) = P(n \dot{-} m)$.

Iz gornjega odmah slijedi da je i $|n - m| = (n \dot{-} m) + (m \dot{-} n)$ primitivno rekurzivna funkcija, budući da je izgrađena pomoću kompozicije iz p.r. funkcija.[3] Slično, $\overline{sgn}(n) = |sgn(n) - 1|$ je p.r. funkcija. Sada lako dokazujemo da su i relacije $=$, $<$ te $\leq$ primitivno rekurzivne. Primjerice, karakterističnu funkciju za relaciju $\leq$ možemo definirati na sljedeći način: $\chi_{\leq}(m, n) = sgn(m \dot{-} n)$ (prisjetimo se da smo definirali karakterističnu funkciju tako da poprima vrijednost 1 ako relacija *ne* vrijedi), a slično je i za jednakost i strogu nejednakost.

Koristeći dobivene rezultate pokazujemo da su i sljedeće relacije i funkcije primitivno rekurzivne:

a) $m|n$, relacija koja vrijedi kad m dijeli n.

Ovu relaciju možemo definirati iz funkcija i relacija za koje je već pokazano da su primitivno rekurzivne koristeći ograničenu kvantifikaciju i logičke veznike (propozicija 3.1):

$$m|n \leftrightarrow (\exists y \leq n)(y > 0 \land m > 0 \land m \cdot y = n)$$

[2] Preciznije, ako su f_i te R_i primitivno rekurzivne, tada je također primitivno rekurzivna i funkcija $f(x) = \begin{cases} f_1(\vec{x}) & \text{ako vrijedi } R_1(\vec{x}) \\ \vdots & \\ f_n(\vec{x}) & \text{ako vrijedi } R_n(\vec{x}) \end{cases}$

[3] Funkcije zbrajanja i množenja su očito primitivno rekurzivne: $+(n, 0) = I_1^1(n) = n$, $+(n, m+1) = Sc(+(n, m))$; slično se definira i za množenje.

b) $\mathit{Prost}(n)$, relacija koja vrijedi ako i samo ako je n prost broj.

Broj n je prost ako je veći od 1 te nema drugog djelitelja manjeg od n osim jedinice. Dakle, definiramo

$$\mathit{Prost}(n) \leftrightarrow n > 1 \wedge (\forall u \leq n)(\forall v \leq n)(u \cdot v = n \rightarrow (u = 1 \vee v = 1))$$

c) Funkcija $\pi(n)$, čija je vrijednost (n+1). prost broj.

Za definiciju ove funkcije koristimo sljedeću ideju: ako je p prost broj, tada je broj $p!+1$ ili sam prost ili ga dijeli neki prost broj q veći od p (vidi [6]). Dakle, za odrediti $\pi(n+1)$ bit će dovoljno provjeriti sve brojeve $\pi(n) < k \leq \pi(n)!+1$:

$$\begin{aligned} \pi(0) &= 2 \\ \pi(n+1) &= (\mu x \leq \pi(n)! + 1)(x > \pi(n) \wedge \mathit{Prost}(x)) \end{aligned}$$

d) Funkcija $\mathit{exp}(n, i)$, čiji je rezultat eksponent uz $(i + 1)$. prosti broj (π_i) u faktorizaciji broja n.

Primijetimo da, ako je g kôd niza (a_n), tada je $\mathit{exp}(g, i) = a_i$. Pomoću prethodnih funkcija (posebno, $\pi(n)$), $\mathit{exp}(n, i)$ sada možemo definirati ovako:

$$\mathit{exp}(n, i) = (\mu x \leq n)[(\pi_i^x | n) \wedge (\pi_i^{x+1} \nmid n)]$$

e) Funkcija $l(n)$ koja daje broj različitih prostih faktora broja n.

Relacija $\mathit{Prost}(m) \wedge m|n$ je očito primitivno rekurzivna. Označimo s $\chi_{pf}(m, n)$ njezinu karakterističnu funkciju, te neka je $p(m, n) = \overline{sgn}(\chi_{pf}(m, n))$. Vrijednost funkcije $p(m, n)$ je 1 ako je m prosti faktor od n, a 0 u protivnom.

Kako bismo izračunali duljinu faktorizacije broja n, vidimo da je moguće za svaki $2 \leq k < n$ provjeriti je li k prosti faktor od n te u tom slučaju uvećati rezultat za 1. Koristeći $p(m, n)$, za funkciju l sada vrijedi $l(n) = \sum_{k=2}^{n} p(k, n)$. Funkciju $l(n)$ sada je lako definirati pomoću primitivne rekurzije koristeći $p(m, n)$.

Funkcije $\mathit{exp}(n, i)$ te $l(n)$ koristimo za izdvajanje pojedinačnih elemenata kodiranog niza. Ako je g kôd niza (a_n), tada je $l(g) = n$ te je $\mathit{exp}(g, i) = a_i$ za svaki $i < n$. Ove funkcije čine jezgru definicije $\mathit{Prf}(m, n)$.

Na kraju ovog odjeljka definirajmo još jednu važnu funkciju: funkciju *nadovezivanja* (konkatenacije) $* : \mathbb{N}^2 \rightarrow \mathbb{N}$. Tako je $m * n$ Gödelov broj izraza koji se dobiva nadovezivanjem izraza čiji su Gödelovi brojevi m i n. Primjerice, $\ulcorner \mathsf{S} \urcorner * \ulcorner \mathsf{0} \urcorner = \ulcorner \mathsf{S0} \urcorner$, odnosno $2^{23} * 2^{21} = 2^{23} \times 3^{21}$. Slično, $\ulcorner \forall \mathsf{x} \urcorner * \ulcorner \neg(\mathsf{x} = \mathsf{S0}) \urcorner = (2^{11} \times 3^2) * (2^1 \times 3^{17} \times 5^{21} \times 7^{15} \times 11^{23} \times 13^2 \times 17^{19}) = 2^{11} \times 3^2 \times 5^1 \times 7^{17} \times 11^{21} \times 13^{15} \times 17^{23} \times 19^2 \times 23^{19}$.

Primjećujemo da su eksponenti uz prvih $l(m)$ prostih faktora u $m * n$ jednaki onima u m, dok su eksponenti uz π_i u n jednaki onima uz $\pi_{i+l(m)}$ u $m*n$. Koristeći tu činjenicu, definiramo funkciju nadovezivanja na sljedeći način:

$$\begin{aligned} m * n = (\mu x \leq B(m,n))[(\forall k < l(m))(exp(x,k) = exp(m,k)) \land \\ (\forall k < l(n))(exp(x, k + l(m)) = exp(n,k))] \end{aligned}$$

Pritom je $B(m,n)$ gornja granica za vrijednost $m * n$ koja se koristi kako bi operator minimizacije bio ograničen (što je bitno, budući da želimo da funkcija nadovezivanja bude primitivno rekurzivna). Za tu granicu možemo uzeti vrijednost π_{m+n}^{m+n}, a to je primitivno rekurzivna dvomjesna funkcija. Iz primitivne rekurzivnosti funkcija $exp(n,i)$ i $B(m,n)$ te propozicije 3.1 slijedi da je i funkcija nadovezivanja primitivno rekurzivna.

Koristeći funkciju $*$, sada je lako definirati i funkciju $num(n)$ koja daje Gödelov broj numerala za prirodni broj n. Drugim riječima, $num(n)$ je Gödelov broj L_A izraza koji se sastoji od n ponavljanja znaka S, nakon čega slijedi znak $\mathsf{0}$. Funkciju definiramo pomoću primitivne rekurzije na sljedeći način:

$$\begin{aligned} num(0) &= \ulcorner \mathsf{0} \urcorner \\ num(x+1) &= \ulcorner \mathsf{S} \urcorner * num(x) \end{aligned}$$

3.3. Relacija $Prf(m,n)$

Teorem 3.2. *Relacija $Prf(m,n)$, koja vrijedi ako i samo ako je m kôd dokaza (u teoriji* PA*) zatvorene formule čiji je Gödelov broj n, primitivno je rekurzivna.*

U ovom odjeljku iznosi se osnovna ideja iza dokaza gornjeg teorema. Potpuni dokaz može se pronaći u [5]. Valja istaknuti da se na jednak način dokazuje da je $Prf_T(m,n)$ primitivno rekurzivna relacija, sve dok je T tzv. primitivno rekurzivno aksiomatizabilna teorija.

Definicija 3.6. Za aritmetičku teoriju T (s jezikom L_A) kažemo da je *primitivno rekurzivno aksiomatizabilna* (kraće: p.r. aksiomatizabilna) ako je svojstvo da je n Gödelov broj aksioma teorije T primitivno rekurzivno.

Zanimljivo je, međutim, da je dovoljno da T bude *aksiomatizabilna* teorija, što je slabiji uvjet – traži se da je svojstvo da je n Gödelov broj aksioma odlučivo. O tome govori Craigov teorem, čiji se dokaz može vidjeti u [8]:

Teorem 3.3 (Craigov teorem)**.** *Ako je T aksiomatizabilna teorija, tada postoji primitivno rekurzivno aksiomatizabilna teorija T' koja ima iste teoreme kao i T.*

Zašto je uopće važno da je teorija aksiomatizabilna? Uzmimo primjerice teoriju T_A čiji su aksiomi sve formule jezika L_A koje su istinite na standardnoj interpretaciji. Trivijalno, svi teoremi te teorije su aritmetičke istine. Međutim, takva teorija nije aksiomatizabilna – svojstvo da je n Gödelov broj aritmetičke istine nije odlučivo.[4]

Pretpostavimo sada da je m kôd dokaza rečenice s Gödelovim brojem n. Broj m kodira niz čiji je zadnji element upravo n, a za svaki element tog niza vrijedi da je ili jednak Gödelovom broj aksioma (teorije PA ili logičkog aksioma) ili je Gödelov broj formule koja se dobiva upotrebom jednog od pravila dedukcije (modus ponens ili generalizacija) iz formula koje kodiraju prethodni elementi tog niza. Također, formula čiji je Gödelov broj n mora biti zatvorena.

Relaciju $\mathit{Prf}(m,n)$ sada možemo definirati na sljedeći način:

$$\begin{aligned} &\mathit{Prf}(m,n) \leftrightarrow \\ &\qquad \mathit{Sent}(n) \wedge [\mathit{exp}(m, l(m)-1) = n] \wedge [(\forall k < l(m)) R(k,m)] \end{aligned}$$

Pritom je

$$\begin{aligned} R(k,m) \leftrightarrow\ & \mathit{Aksiom}(\mathit{exp}(m,k)) \vee \\ & (\exists i \leq k)(\exists j \leq k) \mathit{MP}(\mathit{exp}(m,i), \mathit{exp}(m,j), \mathit{exp}(m,k)) \vee \\ & (\exists i \leq k) \mathit{Gen}(\mathit{exp}(m,i), \mathit{exp}(m,k)) \end{aligned}$$

Relacija $R(k,m)$ vrijedi ako je k-ta formula u nizu koji kodira broj m aksiom ili pak je dobivena iz prethodnih formula pomoću pravila modus ponens ili generalizacijom.

Za potpuni dokaz da je $\mathit{Prf}(m,n)$ primitivno rekurzivna relacija potrebno je dokazati da su i relacije $\mathit{Sent}(n)$, $\mathit{Aksiom}(n)$, $\mathit{MP}(m,n,o)$ te $\mathit{Gen}(m,n)$ primitivno rekurzivne. Pritom $\mathit{MP}(m,n,o)$ vrijedi ako se formula s Gödelovim brojem o dobiva upotrebom pravila modus ponens nad formulama s kodovima m i n. Analogno vrijedi i za relaciju $\mathit{Gen}(m,n)$.

Rečenica je zatvorena formula, pa se definicija relacije $\mathit{Sent}(n)$ temelji na relaciji $\mathit{Form}(n)$. Za definiciju te relacije može se iskoristiti sličan trik kao i za definiciju $\mathit{Prf}(m,n)$. Naime, definicija formule je rekurzivna – atomarna formula (u L_A to su formule oblika $\tau = \rho$, gdje su τ i ρ termi) je formula, a i svaki izraz dobiven iz formula korištenjem logičkih operatora ili kvantifikatora je također formula. Promotrimo *definicijski niz* neke formule φ – zadnji element tog niza je upravo formula φ, a svaki element niza je ili atomarna formula ili je dobiven iz prethodnih elemenata u nizu korištenjem logičkih operatora ili kvantifikacije. Tako sada možemo definirati relaciju $\mathit{FormNiz}(m,n)$ koja vrijedi ako je m kodira definicijski niz formule s Gödelovim brojem n. Relacija $\mathit{Form}(n)$ je istinita ako

[4] Da je teorija T_A aksiomatizabilna te p.r. adekvatna (poglavlje 4), tada bi postojala Gödelova rečenica $\mathsf{G}_{\mathsf{T_A}}$ takva da ni ona, a ni njezina negacija, nisu dokazive u T_A. Međutim, ili $\mathsf{G}_{\mathsf{T_A}}$ ili $\neg\mathsf{G}_{\mathsf{T_A}}$ istinito je na standardnoj interpretaciji, pa je tako jedna od te dvije rečenice aksiom teorije T_A. Odmah slijedi da je jedna od te dvije rečenice i dokaziva u T_A, što je kontradiktorno Gödelovom prvom teoremu nepotpunosti. Dalje slijedi (vidi [8] za detalje) da navedeno svojstvo nije rekurzivno, pa iz Church-Turingove teze proizlazi da nije odlučivo.

i samo ako postoji neki prirodan broj m tako da vrijedi $\mathit{FormNiz}(m, n)$ (drugim riječima, ako postoji definicijski niz formule s Gödelovim brojem n). Na sličan način definira se i relacija $\mathit{Term}(n)$; detaljnija razrada može se pročitati u [8].

$\mathit{Aksiom}(n) \overset{\text{def}}{=} \mathit{LA}(n) \vee \mathit{Aksiom}_T(n)$, gdje $\mathit{LA}(\ulcorner\varphi\urcorner)$ vrijedi ako je φ logički aksiom, a $\mathit{Aksiom}_T(\ulcorner\varphi\urcorner)$ ako je φ aksiom teorije T. Relaciju $\mathit{LA}(n)$ nije teško definirati. Primjerice, ako je n kôd aksioma $\varphi \to (\psi \to \varphi)$, tada postoje prirodni brojevi m i k manji od n takvi da vrijedi

$$\mathit{Form}(m) \wedge \mathit{Form}(k) \wedge n = m * \ulcorner\to (\urcorner * k * \ulcorner\to\urcorner * m * \ulcorner)\urcorner$$

Nešto je složenija definicija relacije $\mathit{Aksiom}_{\mathsf{PA}}(n)$, budući da je potrebno između ostaloga provjeriti i je li formula s Gödelovim brojem n instanca sheme aksioma indukcije. U [5] ta se relacija definira pomoću funkcije $\mathit{sub}(m, v, n)$, koja daje Gödelov broj izraza koji se dobiva supstitucijom terma s Gödelovim brojem n u formulu s Gödelovim brojem m umjesto varijable čiji je kôd v, a za koju je tamo prethodno dokazano da je primitivno rekurzivna.

Relacije $\mathit{MP}(m, n, o)$ i $\mathit{Gen}(m, n)$ su također primitivno rekurzivne, budući da se mogu definirati na sljedeći način:

$$\begin{aligned}&\mathit{MP}(m, n, o) \leftrightarrow\\ &\qquad\qquad \mathit{Form}(m) \wedge \mathit{Form}(o) \wedge n = m * \ulcorner\to\urcorner * o\end{aligned}$$

$$\begin{aligned}&\mathit{Gen}(m, n) \leftrightarrow\\ &\qquad\qquad \mathit{Form}(m) \wedge (\exists v \leq n)[\mathit{Var}(v) \wedge n = \ulcorner\forall\urcorner * v * m]\end{aligned}$$

Pritom $\mathit{Var}(n)$ vrijedi za Gödelove brojeve jednočlanih nizova čiji je jedini element neka varijabla jezika L_A. Drugim riječima, $\mathit{Var}(n) \leftrightarrow (\exists x \leq n)(n = 2^{2x})$.

Ovime je skiciran dokaz teorema 3.2. Posebno, relacija $\mathit{Prf}_T(m, n)$ je primitivno rekurzivna za primitivno rekurzivno aksiomatizabilnu aritmetičku teoriju T, budući da je za takve teorije relacija $\mathit{Aksiom}_T(n)$ primitivno rekurzivna. Dakle, za svaku p.r. aksiomatizabilnu teoriju T nad jezikom L_A postoji relacija Prf_T takva da za svaki n koji kodira neki teorem teorije T postoji prirodan broj m takav da vrijedi $\mathit{Prf}_T(m, n)$.

3.4. Dijagonalizacija

Nakon što je prikazan način kodiranja te je dokazano da su funkcije poput $\mathit{exp}(n, i)$ te funkcije nadovezivanja primitivno rekurzivne, opišimo jednu jednostavnu, a moćnu ideju koja omogućuje konstrukciju Gödelove rečenice G.

Prisjetimo se da je ključan problem kod paradoksa lašca to što je svakodnevni jezik dovoljno ekspresivan da omogućuje konstrukciju rečenica koje govore o sebi samima ("Ova rečenica je lažna"). Međutim, u ovom poglavlju smo pokazali da je i izrazima jezika L_A moguće pridijeliti kodove, prirodne brojeve, a oni upravo čine standardnu interpretaciju ugrađenu u L_A. Rečenica φ jezika L_A tako može također govoriti sama o sebi (dakako, indirektno) putem numerala za svoj Gödelov broj $\ulcorner\varphi\urcorner$!

Promotrimo sada proizvoljnu formulu jezika L_A $\mathsf{U}(\mathsf{y})$ koja ima jednu slobodnu varijablu y te supstituirajmo *numeral za formulu* U umjesto slobodne varijable u samu tu formulu. Drugim riječima, konstruirajmo formulu $\mathsf{U}(\ulcorner\mathsf{U}\urcorner)$.[5] Ovaj se postupak naziva *dijagonalizacijom*.[6] U poglavlju 5 vidjet ćemo kako se ova ideja, zajedno s relacijom $Prf(m, n)$, koristi za konstrukciju Gödelove rečenice G koja sama o sebi govori da nije dokaziva. Definirajmo još ovdje funkciju $diag(n)$ čiji je rezultat Gödelov broj formule koja se dobiva dijagonalizacijom iz formule s Gödelovim brojem n te pokažimo da je takva formula primitivno rekurzivna.

Funkcija $diag(n)$ lako se može definirati pomoću funkcije $sub(m, v, n)$ spomenute u prethodnom odjeljku. Međutim, korištenje te funkcije može se i izbjeći. Naime, formula $\mathsf{U}(\ulcorner\mathsf{U}\urcorner)$ logički je ekvivalentna formuli $\exists\mathsf{y}(\mathsf{y} = \ulcorner\mathsf{U}\urcorner \wedge \mathsf{U})$. Pritom se podrazumijeva da je y jedina slobodna varijabla u U, pa, kako sada stavljamo formulu U unutar dosega kvantifikatora $\exists\mathsf{y}$, supstitucija nije potrebna. Zato definirajmo dijagonalizaciju na sljedeći način:

Definicija 3.7. Formulu oblika

$$\exists\mathsf{y}(\mathsf{y} = \ulcorner\varphi\urcorner \wedge \varphi)$$

nazivamo *dijagonalizacijom* formule φ.

Uočimo pritom da nije strogo nužno da y bude slobodna u φ da bi dijagonalizacija formule φ bila dobro definirana. Naime, ako φ ne sadrži y kao slobodnu varijablu, tada je dijagonalizacija od φ definirana na gornji način ekvivalentna formuli φ.

Funkciju $diag(n)$ sada možemo definirati pomoću funkcije nadovezivanja i funkcije $num(n)$ (odjeljak 3.2), iz čega odmah proizlazi da je ona primitivno rekurzivna:

$$diag(n) = \ulcorner\exists\mathsf{y}(\mathsf{y} =\urcorner * num(n) * \ulcorner\wedge\urcorner * n * \ulcorner)\urcorner$$

[5]Kao što je ranije u ovom poglavlju bilo naglašeno, $\ulcorner\mathsf{U}\urcorner$ u ovom kontekstu predstavlja numeral Gödelovog broja formule U.

[6]Pojam dijagonalizacije, odnosno dijagonalnog argumenta, potječe iz čuvenog Cantorovog teorema prema kojem skupovi prirodnih i realnih brojeva nisu ekvipotentni. Taj se termin koristi u mnogim dokazima koji upotrebljavaju sličnu ideju.

4 Reprezentabilnost i primitivno rekurzivna adekvatnost

Sadržaj

U prethodnom poglavlju pokazano je kako se formulama jezika L_A mogu dodijeliti kodovi (prirodni brojevi) te definirati numeričke relacije poput $Prf(m, n)$ takve da za $m, n \in \mathbb{N}$ vrijedi $Prf(m, n)$ ako i samo ako m kodira *dokaz* formule s Gödelovim brojem n. Međutim, ono što je ključno za Gödelov dokaz te čemu je posvećeno ovo poglavlje jest činjenica da se takve relacije mogu **preslikati i unutar same teorije**. Tako, primjerice, ako vrijedi $Prf(m, n)$, u Robinsonovoj aritmetici može se dokazati $\mathsf{Q} \vdash \mathsf{Prf}(\overline{\mathsf{m}}, \overline{\mathsf{n}})$.[1] Upravo je to ono što omogućuje konstrukciju samoreferencirajućih rečenica poput čuvene Gödelove rečenice G.

Ovo je poglavlje podijeljeno na sljedeći način:

– na početku se pobliže definira što to znači da je neko aritmetičko svojstvo, relacija ili funkcija *izražena* formulom φ jezika L_A; uvode se pojmovi *reprezentabilnosti* i *primitivno rekurzivne adekvatnosti*

– dokazuju se neka korisna svojstva teorije Q

– definiraju se posebne klase formula u jezika L_A: Δ_0, Σ_1 i Π_1 formule; pokazuje se kako Q *korektno odlučuje* svaku Δ_0 rečenicu

– pokazuje se kako se svaka Σ_1 funkcija može izraziti kao kompozicija dviju Δ_0 funkcija te da Q korektno odlučuje svaku takvu kompoziciju

[1] Ovdje je ispušten indeks uz *Prf*. Ako nije posebno naglašeno, tada se teorija na koju se odnosi relacija $Prf(m, n)$ podrazumijeva iz konteksta. Ovdje se radi o relaciji $Prf_{\mathsf{Q}}(m, n)$.

– konačno, nizom propozicija i teorema zaključuje se da je svaku primitivno rekurzivnu funkciju moguće izraziti Σ_1 formulom; u kombinaciji s prethodnim rezultatom, dolazi se do glavnog rezultata ovog poglavlja – p.r. funkcije reprezentabilne su u Q, tj. Q je p.r. adekvatna teorija

Većina rezultata prikazanih u ovom poglavlju odnose se na Robinsonovu aritmetiku Q, pa tako vrijede i u jačoj teoriji PA.

Prije nego što se krene na detaljna razmatranja prethodnih točaka, valja još skrenuti pozornost na način na koji se provode neki dokazi *unutar teorije*. Kao što je navedeno u početnom poglavlju, dedukcijski sustav za logiku prvog reda koji se razmatra u ovom radu *hilbertovski* je sustav – takvi sustavi sastoje se od puno aksioma (primjerice, Peanova aritmetika ima prebrojivo mnogo aksioma), nasuprot malom broju dedukcijskih pravila (npr. samo modus ponens i generalizacija). Hilbertovski sustavi veoma su pogodni za aritmetizaciju – dokazi u njima nizovi su formula gdje je svaka formula ili aksiom (bilo aksiom teorije koja se razmatra ili logički aksiom) ili se dobiva primjenom nekog od dedukcijskih pravila iz formula koje prethode. Tako se kôd dokaza dobiva kodiranjem niza prirodnih brojeva gdje svaki broj u nizu predstavlja kôd odgovarajuće formule u dokazu.

S druge strane, za provedbu dokaza unutar takve teorije, hilbertovski dedukcijski sustavi vrlo su nezgodni te su dokazi i jednostavnih rezultata nerijetko vrlo dugi. U tu svrhu pogodniji su *sustavi prirodne dedukcije*. Kako su ta dva sustava zapravo ekvivalentna (dokazuju iste teoreme; vidi [11]), opravdano je korištenje prirodne dedukcije u nekim dokazima koji se provode unutar teorije Q u odjeljcima koji slijede. Naime, za svaki takav dokaz postoji i odgovarajući dokaz u izvornom hilbertovskom sustavu.

Ponovimo još na kraju kako teorije Q i PA definiramo u okviru logike prvog reda *s jednakošću*, što znači da je iz $x = y$ moguće izvesti $\varphi(x) = \varphi(y)$ za proizvoljnu formulu φ (Leibnizov zakon).

4.1. Osnovne definicije

Definicija 4.1. Dvomjesna relacija $R(m,n)$ može se **izraziti** pomoću L_A formule $\varphi(\mathsf{x},\mathsf{y})$ ako za sve $m,n \in \mathbb{N}$ vrijedi

$$R(m,n) \text{ ako i samo ako } \varphi(\overline{\mathsf{m}},\overline{\mathsf{n}}) \text{ je istinito}$$

U prethodnom izrazu $\overline{\mathsf{x}}$ predstavlja *numeral* prirodnog broja x (simbol $\mathsf{SSS...S0}$, gdje se S ponavlja x puta), a *istinitost* se odnosi, dakako, na **standardnu interpretaciju**.

Prethodna definicija lako se generalizira na relacije proizvoljne mjesnosti. Analogna definicija vrijedi i za funkcije – naime, funkciju $f(x)$ možemo poistovjetiti s relacijom $F(x,y)$ takvom da za svaki prirodan broj x vrijedi $F(x,y)$ ako i samo ako $f(x) = y$.

Primijetimo kako za izrazivost neke numeričke relacije ili funkcije nije bitna teorija u kojoj radimo, već ona ovisi isključivo o *jeziku* L_A te *standardnoj interpretaciji* koja je u njega ugrađena.

U literaturi se spominje još i analogan pojam *aritmetičke definabilnosti.* L_A formula $\varphi(\mathsf{x})$ aritmetički definira skup $S \subseteq \mathbb{N}$ ako i samo ako za svaki prirodan broj x vrijedi da je $x \in S$ ako i samo ako je $\varphi(\overline{\mathsf{x}})$ istinito. Neki skup S aritmetički je definabilan ako postoji formula $\varphi(\mathsf{x})$ koja ga aritmetički definira.

Definicija 4.2. Dvomjesna relacija $R(x, y)$ **definabilna** je u aritmetičkoj teoriji T (teoriji čiji je jezik L_A) ako i samo ako postoji formula $\varphi(\mathsf{x}, \mathsf{y})$ takva da za sve $m, n \in \mathbb{N}$ vrijedi:

a) ako je m u relaciji R s n, $T \vdash \varphi(\overline{\mathsf{m}}, \overline{\mathsf{n}})$

b) u protivnom, $T \vdash \neg\varphi(\overline{\mathsf{m}}, \overline{\mathsf{n}})$

Pojam definabilnosti sintaktički je analogon semantičkom pojmu izrazivosti. Kao i kod definicije 4.1, generalizacija na višemjesne relacije je jednostavna.

Primijetimo da, ako je T ispravna teorija (postupci zaključivanja čuvaju istinitost, tj. teoremi su istiniti na svakom modelu od T), tada formula $\varphi(\mathsf{x}, \mathsf{y})$ koja definira relaciju $R(x, y)$ nju ujedno i izražava.

Definicija 4.3. Jednomjesna funkcija $f : \mathbb{N} \to \mathbb{N}$ **slabo je reprezentabilna** u teoriji T pomoću formule $\varphi(\mathsf{x}, \mathsf{y})$ ako za sve $m, n \in \mathbb{N}$ vrijedi:

a) ako je $f(m) = n$ tada $T \vdash \varphi(\overline{\mathsf{m}}, \overline{\mathsf{n}})$

b) u protivnom, ako je $f(m) \neq n$, tada $T \vdash \neg\varphi(\overline{\mathsf{m}}, \overline{\mathsf{n}})$

Prethodna definicija potpuno je jednaka definiciji 4.2 ako funkciju f promatramo kao ekvivalentnu relaciju $F(m, n)$. Međutim, funkcije su poseban tip relacija budući da one svaki element domene preslikavaju u samo jedan element kodomene – za relaciju $F(m, n)$ koja odgovara funkciji f vrijedi da za svaki[2] prirodan broj m postoji samo jedan n s kojim je m u relaciji F. Definicija 4.3 ne zahtijeva da teorija T *zna* da formula $\varphi(\mathsf{x}, \mathsf{y})$ reprezentira f upravo kao funkciju. To nas motivira za dodavanje sljedećeg uvjeta:

c) za svaki prirodan broj m, $T \vdash \exists! \mathsf{y}\, \varphi(\overline{\mathsf{m}}, \mathsf{y})$

Gornji uvjet garantira da teorija T *može dokazati* da relacija koju izražava formula $\varphi(\mathsf{x}, \mathsf{y})$ predstavlja upravo funkciju.

U sljedećem odjeljku, nakon što se izgrade potrebni temelji, dokazuje se kako u teoriji Q uvjeti a) i c) u stvari povlače uvjet b) iz definicije 4.3. Štoviše, definicija reprezentabilnosti pomoću tih uvjeta ekvivalentna je sljedećoj:

[2] Ovdje promatramo samo totalne funkcije definirane na skupu prirodnih brojeva.

Definicija 4.4. Jednomjesna funkcija f **reprezentabilna** je u teoriji Q ako za sve $m, n \in \mathbb{N}$ vrijedi da $f(m) = n$ povlači $\mathsf{Q} \vdash \forall \mathsf{z}(\varphi(\overline{\mathsf{m}}, \mathsf{z}) \leftrightarrow \mathsf{z} = \overline{\mathsf{n}})$.

Još jedan važan rezultat dokazan je u sljedećem odjeljku – naime, ako je funkcija f slabo reprezentabilna pomoću formule φ u teoriji T (koja može izvesti barem ono što i Q), tada postoji formula $\tilde{\varphi}$ koja f reprezentira *kao funkciju* (u smislu definicije 4.4). Dakle, u aritmetičkim teorijama koje su jake barem kao Q, slaba reprezentabilnost povlači "potpunu" reprezentabilnost. To znači da je dovoljno pokazati da postoji formula φ koja zadovoljava uvjete a) i b) iz definicije 4.3 kako bismo dokazali da je neka funkcija f reprezentabilna u Q.

Reprezentabilnost neke funkcije u teoriji T omogućuje nam da *unutar* teorije T izvodimo zaključke o ponašanju te funkcije. Cilj je ovog poglavlja dokazati da su sve primitivno rekurzivne funkcije reprezentabilne u teoriji Q (pa tako i u proširenjima poput PA).

Posebno, primitivno je rekurzivna i relacija[3] $Prf(x, y)$, što znači da postoji L_A formula $\mathsf{Prf}(\mathsf{x}, \mathsf{y})$ takva da $\mathsf{Q} \vdash \mathsf{Prf}(\overline{\mathsf{x}}, \overline{\mathsf{y}})$ ako je x kôd dokaza formule kodirane brojem y, dok u protivnom $\mathsf{Q} \vdash \neg\mathsf{Prf}(\overline{\mathsf{x}}, \overline{\mathsf{y}})$. Upravo je ovo ključno svojstvo koje se koristi u dokazu Gödelovog prvog teorema nepotpunosti.

Na kraju ovog odjeljka spomenimo još i koncept primitivno rekurzivne adekvatnosti:

Definicija 4.5. Teorija T je **primitivno rekurzivno adekvatna** ako je svaka primitivno rekurzivna funkcija reprezentabilna u T.

4.2. Neki (meta)teoremi teorije Q

U ovom odjeljku prikazuju se neki korisni rezultati o teoriji Q koji će se koristiti kasnije kod dokaza primitivno rekurzivne adekvatnosti te teorije.

Propozicija 4.1. *Neka su m i n proizvoljni prirodni brojevi. Ako je $m = n$, tada $\mathsf{Q} \vdash \overline{\mathsf{m}} = \overline{\mathsf{n}}$. U slučaju da je $m \neq n$, $\mathsf{Q} \vdash \overline{\mathsf{m}} \neq \overline{\mathsf{n}}$. Drugim riječima, relacija jednakosti definabilna je u Q.*

L_A formula $\mathsf{x} \neq \mathsf{y}$ samo je pokrata za $\neg(\mathsf{x} = \mathsf{y})$. Također, na nekim mjestima se (kratkoće radi) koristi zapis S^n umjesto $\mathsf{SSS...S}$ gdje se simbol S pojavljuje n puta.

Dokaz. Ako je $m = n$, tada su numerali $\overline{m}$ i $\overline{n}$ sintaktički jednaki. Budući da je Q teorija s jednakošću, trivijalno vrijedi $\mathsf{Q} \vdash \overline{\mathsf{m}} = \overline{\mathsf{n}}$.

Pretpostavimo sada da vrijedi $m < n$. Zaključujući *unutar teorije* Q, pretpostavimo $\overline{\mathsf{m}} = \overline{\mathsf{n}}$ te dovodimo do kontradikcije.[4]

[3] Preciznije, njezina *karakteristična funkcija* je primitivno rekurzivna.

[4] Kao što je spomenuto u uvodnom dijelu, ovdje koristimo sustav prirodne dedukcije za provedbu dokaza unutar teorije, pa je moguće ovakvo postavljanje privremene pretpostavke unutar Q.

$$
\begin{array}{lll}
1. & \mathsf{S^m0 = S^n0} & \text{pretpostavka} \\
2. & \mathsf{S^{m-1}0 = S^{n-1}0} & \text{iz 1 i aksioma 2, modus ponens} \\
 & \vdots & \\
(m+1). & \mathsf{0 = S^{n-m}0} & \\
(m+2). & \mathsf{0 = S\overline{k}} & \mathsf{\overline{k} \equiv S^{n-m-1}0} \\
(m+3). & \mathsf{\forall x(0 \neq Sx)} & \text{aksiom 1} \\
(m+4). & \mathsf{0 \neq S\overline{k}} & \text{iz } m+3 \\
 & \text{kontradikcija} &
\end{array}
$$

Dakle, iz pretpostavke da je $\mathsf{\overline{m} = \overline{n}}$, koristeći pravilo modus ponens te aksiom 2 teorije Q koji kaže da vrijedi $\mathsf{\forall x \forall y(Sx = Sy \to x = y)}$ dobiva se $\mathsf{0 = S\overline{k}}$, što je kontradiktorno prvom aksiomu teorije Q. Dakle, koristeći pravilo $(\neg I)$ prirodne dedukcije dobiva se $\mathsf{Q} \vdash \mathsf{\overline{m} \neq \overline{n}}$.

Dokaz za slučaj kad je $m > n$ provodi se na isti način, samo što se u koraku $(m+2)$ dobiva $\mathsf{S\overline{k} = 0}$, no iz simetričnosti jednakosti odmah slijedi $\mathsf{0 = S\overline{k}}$. □

Propozicija 4.2. *Neka su $m, n, k \in \mathbb{N}$ proizvoljni. Vrijede sljedeće tvrdnje:*

– *ako je $m + n = k$, tada* $\mathsf{Q} \vdash \mathsf{\overline{m} + \overline{n} = \overline{k}}$

– *ako je $m + n \neq k$, tada* $\mathsf{Q} \vdash \mathsf{\overline{m} + \overline{n} \neq \overline{k}}$

Dokaz. Za dokaz prve tvrdnje iz propozicije koristimo aksiome 4 i 5 teorije Q. U opisu koraka kratica LL označava Leibnizov zakon koji omogućuje da, uz $\tau = \rho$, iz $\varphi(\tau)$ izvedemo $\varphi(\rho)$.

Neka je $m + n = k$. Pretpostavimo da je $n > 0$. U protivnom, dovoljno je samo preskočiti korake 3 do $(n+3)$.

$$
\begin{array}{lll}
1. & \mathsf{\forall x(x + 0 = x)} & \text{aksiom 4} \\
2. & \mathsf{\forall x \forall y(x + Sy = S(x + y))} & \text{aksiom 5} \\
3. & \mathsf{S^m0 + S^n0 = S(S^m0 + S^{n-1}0)} & \text{instanca aksioma 5} \\
4. & \mathsf{S^m0 + S^{n-1}0 = S(S^m0 + S^{n-2}0)} & \text{instanca aksioma 5} \\
 & \vdots & \\
(n+2). & \mathsf{S^m0 + S0 = S(S^m0 + 0)} & \\
(n+3). & \mathsf{S^m0 + S^n0 = S^n(S^m0 + 0)} & n\text{-terostruka primjena LL} \\
(n+4). & \mathsf{S^m0 + 0 = S^m0} & \text{instanca aksioma 4} \\
(n+5). & \mathsf{S^m0 + S^n0 = S^{n+m}0} & \text{iz } (n+3) \text{ i } (n+4)\text{, LL}
\end{array}
$$

Zadnji red dokaza, zapisan pomoću numerala, glasi upravo $\mathsf{\overline{m} + \overline{n} = \overline{k}}$.

Kako bi se dokazala druga tvrdja propozicije, dovoljno je uočiti da iz $m+n \neq k$ slijedi da postoji $l \neq k$ takav da je $m + n = l$. Sada iz gornjeg razmatranja slijedi $\mathsf{Q} \vdash \mathsf{\overline{m} + \overline{n} = \overline{l}}$. Nadalje, iz propozicije 4.1 dobiva se $\mathsf{Q} \vdash \mathsf{\overline{l} \neq \overline{k}}$. Upotrebom Leibnizovog zakona dolazi se do konačnog rezultata: $\mathsf{Q} \vdash \mathsf{\overline{m} + \overline{n} \neq \overline{k}}$. □

Na sličan način dokazuje se sljedeća propozicija:

Propozicija 4.3. *Neka su $m, n, k \in \mathbb{N}$ proizvoljni. Vrijede sljedeće tvrdnje:*

– *ako je $m \cdot n = k$, tada* $\mathsf{Q} \vdash \overline{\mathsf{m}} \times \overline{\mathsf{n}} = \overline{\mathsf{k}}$

– *ako je $m \cdot n \neq k$, tada* $\mathsf{Q} \vdash \overline{\mathsf{m}} \times \overline{\mathsf{n}} \neq \overline{\mathsf{k}}$

Koristeći prethodne propozicije može se pokazati da vrijedi i nešto jači rezultat. Spomenimo prije samo da, kao što je definirano u poglavlju 2, kažemo da teorija T odlučuje neku rečenicu φ ako $T \vdash \varphi$ ili $T \vdash \neg\varphi$. Aritmetička teorija T korektno odlučuje L_A rečenicu φ ako $T \vdash \varphi$ ako je φ istinita na standardnoj interpretaciji, a $T \vdash \neg\varphi$ inače.

Propozicija 4.4. *Teorija* Q korektno odlučuje *rečenice oblika $\tau = \rho$, gdje su τ i ρ zatvoreni termi jezika L_A.*

Dokaz. Neka su $m, n \in \mathbb{N}$ takvi da su rečenice $\tau = \overline{\mathsf{m}}$ i $\rho = \overline{\mathsf{n}}$ istinite. Ako pokažemo da Q dokazuje te rečenice, dokaz ove propozicije nastavlja se na sljedeći način:

– ako je $\tau = \rho$ istinita rečenica, tada vrijedi $m = n$; iz propozicije 4.1 proizlazi da $\mathsf{Q} \vdash \overline{\mathsf{m}} = \overline{\mathsf{n}}$, a dvostrukom primjenom Leibnizovog zakona dobiva se $\mathsf{Q} \vdash \tau = \rho$

– ako $\tau = \rho$ nije istinita, tada je $m \neq n$; iz propozicije 4.1 i Leibnizovog zakona zaključuje se da vrijedi $\mathsf{Q} \vdash \tau \neq \rho$

Pojam terma definira se rekurzivno. U jeziku L_A $\mathsf{0}$ je zatvoreni term, a ako su τ i ρ zatvoreni termi, tada su to i $\mathsf{S}\tau$, $\tau + \rho$ te $\tau \times \rho$. To nas navodi na ideju induktivnog dokaza gornje tvrdnje.

Neka je sada ψ zatvoreni term jezika L_A, a m prirodan broj takav da je $\psi = \overline{\mathsf{m}}$ istinita rečenica. Indukcijom po složenosti terma ψ dokazujemo da $\mathsf{Q} \vdash \psi = \overline{\mathsf{m}}$.

Za $\psi = \mathsf{0}$ tvrdnja trivijalno vrijedi. Pretpostavimo da ona vrijedi za svaki zatvoreni term složenosti n (izgrađen korištenjem funkcijskih simbola S, $+$ i $\times$ n puta). Neka je sada ψ term složenosti $n + 1$. On je jednog od sljedećih oblika:

a) $\psi = \mathsf{S}\tau$

Po pretpostavci indukcije, $\mathsf{Q} \vdash \tau = \overline{\mathsf{k}}$. Iz Leibnizovog zakona slijedi $\mathsf{Q} \vdash \mathsf{S}\tau = \mathsf{S}\overline{\mathsf{k}}$, odnosno $\mathsf{Q} \vdash \mathsf{S}\tau = \overline{\mathsf{k}+\mathsf{1}}$, pa tvrdnja vrijedi i za ψ.

b) $\psi = \tau + \rho$

Po pretpostavci, $\mathsf{Q} \vdash \tau = \overline{\mathsf{k}}$ i $\mathsf{Q} \vdash \psi = \overline{\mathsf{l}}$. Iz propozicije 4.2 dobiva se $\mathsf{Q} \vdash \overline{\mathsf{k}} + \overline{\mathsf{l}} = \overline{\mathsf{o}}$. Dalje brzo slijedi $\mathsf{Q} \vdash \tau + \rho = \overline{\mathsf{o}}$, pa tvrdnja vrijedi za ψ.

c) $\psi = \tau \times \rho$

Analogno kao i gore, uz upotrebu propozicije 4.3.

Tvrdnja, dakle, vrijedi za svaki zatvoreni term. U kombinaciji s razmatranjem na početku dokaza, zaključujemo da Q korektno odlučuje rečenice oblika $\tau = \psi$ gdje su τ i ψ zatvoreni termi. $\square$

U nastavku se dokazuje još jedan važan rezultat: relacija $\leq$ definabilna je u Q.

Propozicija 4.5. *Formula* $\varphi(\mathsf{x},\mathsf{y}) \stackrel{\text{def}}{=} \exists \mathsf{z}\, (\mathsf{z}+\mathsf{x}=\mathsf{y})$ *definira relaciju* $\leq$ *unutar teorije* Q.

Dokaz. Prema definiciji 4.2, potrebno je demonstrirati da za sve $m, n \in \mathbb{N}$ vrijedi sljedeće: ako je $m \leq n$, tada $\mathsf{Q} \vdash \exists \mathsf{z}\, (\mathsf{z} + \overline{\mathsf{m}} = \overline{\mathsf{n}})$, dok ako je $m > n$, tada $\mathsf{Q} \vdash \neg \exists \mathsf{z}\, (\mathsf{z} + \overline{\mathsf{m}} = \overline{\mathsf{n}})$.

Pretpostavimo prvo da je $m \leq n$. Tada postoji k takav da je $k + m = n$. Prema propoziciji 4.2, $\mathsf{Q} \vdash \overline{\mathsf{k}} + \overline{\mathsf{m}} = \overline{\mathsf{n}}$, iz čega izravno slijedi $\mathsf{Q} \vdash \exists \mathsf{z}\, (\mathsf{z} + \overline{\mathsf{m}} = \overline{\mathsf{n}})$

Pretpostavimo sada da je $m > n$. Dokaz je ovdje nešto duži. Kontradikcije radi, pretpostavimo *unutar teorije* da vrijedi $\exists \mathsf{z}\, (\mathsf{z} + \overline{\mathsf{m}} = \overline{\mathsf{n}})$. Dodatno, pretpostavimo da ta tvrdnja vrijedi za neki a: $\mathsf{a} + \overline{\mathsf{m}} = \overline{\mathsf{n}}$. Nastavljamo dokaz na sljedeći način:

$$
\begin{array}{ll}
\mathsf{a} + \mathsf{S}^{\mathsf{m}}0 = \mathsf{S}^{\mathsf{n}}0 & \text{pretpostavka} \\
\mathsf{a} + \mathsf{S}^{\mathsf{m}}0 = \mathsf{S}(\mathsf{a} + \mathsf{S}^{\mathsf{m}-1}0) & \text{iz aksioma 5} \\
\vdots & \\
\mathsf{a} + \mathsf{S}^{\mathsf{m}}0 = \mathsf{S}^{\mathsf{m}}(\mathsf{a} + 0) & \text{aksiom 5 i LL} \\
\mathsf{a} + 0 = \mathsf{a} & \text{iz aksioma 4} \\
\mathsf{a} + \mathsf{S}^{\mathsf{m}}0 = \mathsf{S}^{\mathsf{m}}\mathsf{a} & \\
\mathsf{S}^{\mathsf{n}}0 = \mathsf{S}^{\mathsf{m}}\mathsf{a} & \text{LL} \\
\mathsf{S}^{\mathsf{n}-1}0 = \mathsf{S}^{\mathsf{m}-1}\mathsf{a} & \text{iz aksioma 2} \\
\vdots & \\
0 = \mathsf{S}^{\mathsf{m}-\mathsf{n}}\mathsf{a} & \\
0 \neq \mathsf{S}^{\mathsf{m}-\mathsf{n}}\mathsf{a} & \text{iz aksioma 1}
\end{array}
$$

Zaključujući i dalje unutar teorije Q, odbacujemo početne pretpostavke budući da dovode do kontradikcije (pravilo $\neg I$), pa izvodimo $\neg \exists \mathsf{z}\, (\mathsf{z} + \overline{\mathsf{m}} = \overline{\mathsf{n}})$. $\square$

Propozicija 4.5 opravdava uvođenje zapisa $\tau \leq \rho$ za $\exists \mathsf{z}\, (\mathsf{z} + \tau = \rho)$. U daljnjem tekstu koristi se i tzv. *ograničena kvantifikacija* za izražavanje činjenice da neko svojstvo vrijedi za sve (ili neke) brojeve manje ili jednake od zadanog. Takve formule su oblika $(\forall x \leq \tau)\varphi(x)$ i $(\exists x \leq \tau)\varphi(x)$, gdje je τ numeral ili varijabla različita od x[5], što su zapravo pokrate za $\forall x(x \leq \tau \to \varphi(x))$ i $\exists x(x \leq \tau \land \varphi(x))$. Za L_A formulu reći ćemo da je da je *ograničena* ako je svako pojavljivanje kvantifikatora u njoj ograničeno (tj. ima jedan od gornja dva oblika).

Teorija Q može izvesti mnoge činjenice vezane uz relaciju $\leq$. U nastavku se navode neke ključne tvrdnje koje se koriste u kasnijim dokazima.

[5] U protivnom bismo dobili $(\forall \mathsf{x} \leq \mathsf{x})\varphi(\mathsf{x})$, što je isto kao i $\forall \mathsf{x}\varphi(\mathsf{x})$.

Propozicija 4.6. *Teorija* Q *korektno odlučuje rečenice oblika* $\tau \leq \rho$*, gdje su* τ *i* ρ *zatvoreni termi jezika* L_A*.*

Dokaz. U dokazu propozicije 4.4 demonstrira se da Q dokazuje istinite rečenice $\tau = \overline{\mathsf{m}}$ i $\rho = \overline{\mathsf{n}}$.

Pretpostavimo sada da je $\tau \leq \rho$ istinita rečenica. Tada je $m \leq n$. Prema propoziciji 4.5, $\mathsf{Q} \vdash \overline{\mathsf{m}} \leq \overline{\mathsf{n}}$. Uz $\mathsf{Q} \vdash \tau = \overline{\mathsf{m}}$ i $\mathsf{Q} \vdash \rho = \overline{\mathsf{n}}$, dvostrukom primjenom Leibnizovog zakona dobiva se $\mathsf{Q} \vdash \tau \leq \rho$.

Neka je sada $\tau \leq \rho$ neistinita. Tada $\mathsf{Q} \vdash \neg(\overline{\mathsf{m}} \leq \overline{\mathsf{n}})$, pa na isti način slijedi $\mathsf{Q} \vdash \neg(\tau \leq \rho)$. □

Propozicija 4.7. Q *je tzv.* uređajno adekvatna *teorija. Neke od tvrdnji koje vrijede za* Q *su sljedeće:*

1. *za svaki* n*,* $\mathsf{Q} \vdash \forall \mathsf{x}((\mathsf{x} = 0 \vee \mathsf{x} = 1 \vee \ldots \vee \mathsf{x} = \overline{\mathsf{n}}) \rightarrow \mathsf{x} \leq \overline{\mathsf{n}})$
2. *za svaki* n*,* $\mathsf{Q} \vdash \forall \mathsf{x}(\mathsf{x} \leq \overline{\mathsf{n}} \rightarrow (\mathsf{x} = 0 \vee \mathsf{x} = 1 \vee \ldots \vee \mathsf{x} = \overline{\mathsf{n}}))$
3. *za svaki* n*, iz* $\mathsf{Q} \vdash \varphi(0)$*,* $\mathsf{Q} \vdash \varphi(1)$*, …,* $\mathsf{Q} \vdash \varphi(\overline{\mathsf{n}})$ *proizlazi* $\mathsf{Q} \vdash (\forall \mathsf{x} \leq \overline{\mathsf{n}})\varphi(\mathsf{x})$
4. *za svaki* n*, ako* $\mathsf{Q} \vdash \varphi(0)$ *ili* $\mathsf{Q} \vdash \varphi(1)$*, …, ili* $\mathsf{Q} \vdash \varphi(\overline{\mathsf{n}})$*, tada* $\mathsf{Q} \vdash (\exists \mathsf{x} \leq \overline{\mathsf{n}})\varphi(\mathsf{x})$
5. *za svaki* n*,* $\mathsf{Q} \vdash \forall \mathsf{x}(\mathsf{x} \leq \overline{\mathsf{n}} \vee \overline{\mathsf{n}} \leq \mathsf{x})$

Neki od gornjih rezultata dokazani su u [8].

Dokažimo sada još dvije tvrdnje vezane uz reprezentabilnost koje su navedene pri kraju odjeljka 4.1.

Propozicija 4.8. *Neka je* f *jednomjesna funkcija, a* $\varphi(\mathsf{x}, \mathsf{y})$ *formula jezika* L_A*. Ako vrijede sljedeće dvije tvrdnje:*

1. *Za sve* $x, y \in \mathbb{N}$ *takve da je* $f(x) = y$*,* $\mathsf{Q} \vdash \varphi(\overline{\mathsf{x}}, \overline{\mathsf{y}})$
2. *Za svaki* $x \in \mathbb{N}$*,* $\mathsf{Q} \vdash \exists! \mathsf{y}\, \varphi(\overline{\mathsf{x}}, \mathsf{y})$

tada vrijedi i:

3. *Za sve* $x, y \in \mathbb{N}$*,* $f(x) \neq y$ *povlači* $\mathsf{Q} \vdash \neg\varphi(\overline{\mathsf{x}}, \overline{\mathsf{y}})$

Drugim riječima, dovoljno je provjeriti tvrdnje 1 i 2 kako bi se dokazalo da $\varphi(\mathsf{x}, \mathsf{y})$ *reprezentira funkciju* f *u teoriji* Q*.*

Dokaz. Pretpostavimo da tvrdnje 1 i 2 vrijede. Neka su $x, y \in \mathbb{N}$ proizvoljni. Pretpostavimo da je $f(x) \neq y$. Tada postoji $z \in \mathbb{N}$, $z \neq y$, takav da je $f(x) = z$. Iz tvrdnje 1 sada slijedi $\mathsf{Q} \vdash \varphi(\overline{\mathsf{x}}, \overline{\mathsf{z}})$. Koristeći taj rezultat i tvrdnju 2 (nakon što se pokrata $\exists!$ zapiše u punom obliku) dobivamo $\mathsf{Q} \vdash \forall \mathsf{u}(\varphi(\overline{\mathsf{x}}, \mathsf{u}) \rightarrow \mathsf{u} = \overline{\mathsf{z}})$. Posebno se tvrdnja može dokazati i za $\overline{\mathsf{y}}$, pa obratom po kontrapoziciji dobivamo $\mathsf{Q} \vdash \overline{\mathsf{y}} \neq \overline{\mathsf{z}} \rightarrow \neg\varphi(\overline{\mathsf{x}}, \overline{\mathsf{y}})$. Iz propozicije 4.1 i $y \neq z$ dobiva se $\mathsf{Q} \vdash \overline{\mathsf{y}} \neq \overline{\mathsf{z}}$, pa upotrebom pravila modus ponens slijedi $\mathsf{Q} \vdash \neg\varphi(\overline{\mathsf{x}}, \overline{\mathsf{y}})$. Time je dokazano da tvrdnje 1 i 2 povlače tvrdnju 3. □

Pokažimo još ovdje da je definicija reprezentabilnosti iz prethodnog odjeljka (definicija 4.4) ekvivalentna definiciji pomoću tvrdnji 1 i 2 iz gornje propozicije.
Definicija 4.4 povlači gornje tvrdnje 1 i 2. Neka je $x \in \mathbb{N}$ proizvoljan. Postoji točno jedan $y \in \mathbb{N}$ takav da je $f(x) = y$. Pretpostavimo da vrijedi $\mathsf{Q} \vdash \forall \mathsf{z}(\varphi(\overline{\mathsf{x}}, \mathsf{z}) \leftrightarrow \mathsf{z} = \overline{\mathsf{y}})$. Jedna strana ove ekvivalencije, $\forall \mathsf{z}(\mathsf{z} = \overline{\mathsf{y}} \to \varphi(\overline{\mathsf{x}}, \mathsf{z}))$, logički je ekvivalentna s $\varphi(\overline{\mathsf{x}}, \overline{\mathsf{y}})$, pa $\mathsf{Q} \vdash \varphi(\overline{\mathsf{x}}, \overline{\mathsf{y}})$. Ovaj rezultat i pretpostavka zajedno daju $\mathsf{Q} \vdash \varphi(\overline{\mathsf{x}}, \overline{\mathsf{y}}) \land \forall \mathsf{z}(\varphi(\overline{\mathsf{x}}, \mathsf{z}) \to \mathsf{z} = \overline{\mathsf{y}})$ iz čega odmah slijedi $\mathsf{Q} \vdash \exists ! \mathsf{y} \varphi(\overline{\mathsf{x}}, \mathsf{y})$, tj. $\mathsf{Q} \vdash \exists \mathsf{y}(\varphi(\overline{\mathsf{x}}, \mathsf{y}) \land \forall \mathsf{z}(\varphi(\overline{\mathsf{x}}, \mathsf{z}) \to \mathsf{z} = \mathsf{y}))$. Dakle, pod pretpostavkom da vrijede tvrdnje 1 i 2, vrijedi i tvrdnja iz definicije 4.4.
Tvrdnje 1 i 2 povlače tvrdnju iz definicije 4.4. Neka su $x, y \in \mathbb{N}$ proizvoljni. Pretpostavimo da vrijedi $f(x) = y$. Sada iz 1 slijedi $\mathsf{Q} \vdash \varphi(\overline{\mathsf{x}}, \overline{\mathsf{y}})$, dok iz 2 zaključujemo $\mathsf{Q} \vdash \forall \mathsf{z}(\varphi(\overline{\mathsf{x}}, \mathsf{z}) \to \mathsf{z} = \overline{\mathsf{y}})$. Koristimo istu logičku ekvivalenciju kao i u gornjem dokazu drugog smjera te u kombinaciji s prethodnom tvrdnjom dobivamo $\mathsf{Q} \vdash \forall \mathsf{z}(\varphi(\overline{\mathsf{x}}, \mathsf{z}) \leftrightarrow \mathsf{z} = \overline{\mathsf{y}})$.

Ovime smo pokazali da su dvije definicije reprezentabilnosti iznesene u odjeljku 4.1 ekvivalentne. Dokažimo sada da je svaka funkcija reprezentabilna u Q ako je slabo reprezentabilna (definicija 4.3).

Propozicija 4.9. *Neka je f jednomjesna funkcija slabo reprezentabilna u teoriji Q pomoću formule $\varphi(\mathsf{x}, \mathsf{y})$. Tada postoji formula $\tilde{\varphi}(\mathsf{x}, \mathsf{y})$ koja reprezentira f kao funkciju u Q.*

Dokaz. Definirajmo formulu $\tilde{\varphi}(\mathsf{x}, \mathsf{y})$ na sljedeći način:

$$\tilde{\varphi}(\mathsf{x}, \mathsf{y}) \stackrel{\text{def}}{=} \varphi(\mathsf{x}, \mathsf{y}) \ \land \ (\forall \mathsf{z} \leq \mathsf{y})(\varphi(\mathsf{x}, \mathsf{z}) \to \mathsf{z} = \mathsf{y})$$

$\tilde{\varphi}(\mathsf{x}, \mathsf{y})$ je definirana tako da je, za svaki $x \in \mathbb{N}$, istinita točno za jedan y – najmanji y takav da je $\varphi(\overline{\mathsf{x}}, \overline{\mathsf{y}})$ istinita.

Potrebno je pokazati da za $\tilde{\varphi}(\mathsf{x}, \mathsf{y})$ vrijede tvrdnje 1 i 2 iz propozicije 4.8. Iz prethodnog razmatranja tada zaključujemo da $\tilde{\varphi}(\mathsf{x}, \mathsf{y})$ reprezentira funkciju f u smislu definicije 4.4.

1) Neka su $m, n \in \mathbb{N}$ takvi da je $f(m) = n$. Iz pretpostavke slijedi $\mathsf{Q} \vdash \varphi(\overline{\mathsf{m}}, \overline{\mathsf{n}})$. Međutim, kako za svaki $k < n$ vrijedi $f(m) \neq k$, tako $\mathsf{Q} \vdash \neg \varphi(\overline{\mathsf{m}}, \overline{\mathsf{k}})$ za svaki takav k. Ova dva rezultata zajedno daju sljedeće: $\mathsf{Q} \vdash \varphi(\overline{\mathsf{m}}, \overline{\mathsf{k}}) \to \overline{\mathsf{k}} = \overline{\mathsf{n}}$ za svaki $k \leq n$. Sada se iz točke 3 propozicije 4.7 zaključuje da Q dokazuje $(\forall \mathsf{x} \leq \overline{\mathsf{n}})(\varphi(\overline{\mathsf{m}}, \mathsf{x}) \to \mathsf{x} = \overline{\mathsf{n}})$. Zajedno s $\varphi(\overline{\mathsf{m}}, \overline{\mathsf{n}})$, to daje konačan rezultat: $\mathsf{Q} \vdash \tilde{\varphi}(\overline{\mathsf{m}}, \overline{\mathsf{n}})$.

2) Neka je $m \in \mathbb{N}$ proizvoljan. Uzmimo opet n takav da je $f(m) = n$. Za dokaz ove tvrdnje trebamo pokazati da $\mathsf{Q} \vdash \forall \mathsf{z}(\tilde{\varphi}(\overline{\mathsf{m}}, \mathsf{z}) \to \mathsf{z} = \overline{\mathsf{n}})$. U kombinaciji s $\mathsf{Q} \vdash \tilde{\varphi}(\overline{\mathsf{m}}, \overline{\mathsf{n}})$ tada se dobiva $\mathsf{Q} \vdash \exists ! \mathsf{y} \tilde{\varphi}(\overline{\mathsf{m}}, \mathsf{y})$.

   Pretpostavimo sada *unutar teorije* Q da za proizvoljni a vrijedi $\tilde{\varphi}(\overline{\mathsf{m}}, \mathsf{a})$. Iz toga slijedi $\varphi(\overline{\mathsf{m}}, \mathsf{a})$ i $(\forall \mathsf{z} \leq \mathsf{a})(\varphi(\overline{\mathsf{m}}, \mathsf{z}) \to \mathsf{z} = \mathsf{a})$. Nadalje, iz točke 5 propozicije 4.7

dobiva se $\mathsf{a} \leq \overline{\mathsf{n}} \vee \overline{\mathsf{n}} \leq \mathsf{a}$. Sada dokazujemo po slučajevima (još uvijek unutar Q):

a) Ako je $\mathsf{a} \leq \overline{\mathsf{n}}$, iz $\tilde{\varphi}(\overline{\mathsf{m}}, \overline{\mathsf{n}})$ dobiva se $\varphi(\overline{\mathsf{m}}, \mathsf{a}) \to \mathsf{a} = \overline{\mathsf{n}}$ te odmah i $\mathsf{a} = \overline{\mathsf{n}}$.

b) Ako je $\overline{\mathsf{n}} \leq \mathsf{a}$, tada iz $(\forall \mathsf{z} \leq \mathsf{a})(\varphi(\overline{\mathsf{m}}, \mathsf{z}) \to \mathsf{z} = \mathsf{a})$ slijedi $\varphi(\overline{\mathsf{m}}, \overline{\mathsf{n}}) \to \overline{\mathsf{n}} = \mathsf{a}$. Odavde opet proizlazi $\mathsf{a} = \overline{\mathsf{n}}$.

Time smo unutar teorije dokazali $\tilde{\varphi}(\overline{\mathsf{m}}, \mathsf{a}) \to \mathsf{a} = \overline{\mathsf{n}}$. Kako je a bio proizvoljan, $\mathsf{Q} \vdash \forall \mathsf{z}(\tilde{\varphi}(\overline{\mathsf{m}}, \mathsf{z}) \to \mathsf{z} = \overline{\mathsf{n}})$.

□

4.3. Δ_0, Σ_1 i Π_1 formule

Cilj ovog cijelog poglavlja je dokazati kako je jezik L_A dovoljan da se u njemu izraze primitivno rekurzivne funkcije te, štoviše, da su takve funkcije reprezentabilne u teorijama koje sadrže Q (tj. mogu izvesti iste teoreme kao i Q). Međutim, za izražavanje p.r. funkcija dovoljan je samo podskup svih formula jezika L_A – skup tzv. Σ_1 formula.

U ovom odjeljku definiraju se Δ_0, Σ_1 i Π_1 klase L_A formula. Nakon toga dokazuje se, koristeći rezultate iz prethodnog odjeljka, da teorija Q korektno odlučuje sve Δ_0 rečenice. Posljedica toga je reprezentabilnost Δ_0 funkcija (funkcija koje su izrazive Δ_0 formulama) u Q. Ta se činjenica koristi kasnije za dokaz jednog od glavnih rezultata ovog poglavlja – teorema o reprezentabilnosti Σ_1 funkcija u Q.

Prilikom definicije ovih formula koristimo i simbol $\leq$ i ograničenu kvantifikaciju poput $(\forall \mathsf{x} \leq \tau)\varphi(\mathsf{x})$. Pritom je važno napomenuti kako ne proširujemo jezik L_A (koji od nelogičkih simbola sadrži samo $\mathsf{0}$, $+$, $\times$ i S), već ih uvodimo definicijski.

Δ_0 formulama nazivamo one formule koje ili ne sadrže kvantifikatore uopće ili je svako pojavljivanje kvantifikatora ograničeno. Preciznije:

Definicija 4.6. Pojam Δ_0 formule definira se rekurzivno. *Atomarna* Δ_0 formula je svaka formula oblika $\tau = \rho$ ili $\tau \leq \rho$, gdje su τ i ρ termi. Svaka Δ_0 formula dobivena je na jedan od sljedećih načina:

– svaka atomarna Δ_0 formula je Δ_0 formula

– ako su φ i ψ Δ_0 formule, tada su to i $\neg\varphi$, $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$, $(\varphi \to \psi)$ i $(\varphi \leftrightarrow \psi)$

– ako je φ Δ_0 formula, ξ varijabla slobodna u φ, a κ numeral ili varijabla različita od ξ, tada su Δ_0 formule i $(\forall \xi \leq \kappa)\varphi$ i $(\exists \xi \leq \kappa)\varphi$

Sada pomoću Δ_0 formula definiramo Σ_1 i Π_1 formule.

Definicija 4.7. Formule oblika $\exists\xi\exists\zeta\ldots\exists\eta\varphi$, gdje je φ Δ_0 formula u kojoj su ξ, ζ, ..., η slobodne varijable, nazivamo *strogo* Σ_1 formulama. Formule oblika $\forall\xi\forall\zeta\ldots\forall\eta\varphi$, gdje je φ Δ_0 formula u kojoj su ξ, ζ, ..., η slobodne varijable, nazivamo *strogo* Π_1 formulama. Formula je Σ_1 ako je logički ekvivalentna nekoj strogo Σ_1 formuli. Na isti način, formula je Π_1 ako je logički ekvivalentna nekoj strogo Π_1 formuli.

Strogo Σ_1 formule, dakle, čini Δ_0 jezgra i grupa od jednog ili više egzistencijalnog kvantifikatora. Teorije koje proširuju Q, a sadrže barem tračak indukcije (npr. dovoljna je teorija $\mathsf{I\Delta_0}$ koja dopušta indukciju po Δ_0 formulama), mogu *dokazati* da je svaka Σ_1 formula ekvivalentna[6] nekoj formuli koja sadrži samo jedan egzistencijalni kvantifikator ispred Δ_0 jezgre. Npr. formula $\exists\mathsf{x}\exists\mathsf{y}\varphi(\mathsf{x},\mathsf{y})$ istinita je ako i samo ako je i $\exists\mathsf{w}(\exists\mathsf{x}\leq\mathsf{w})(\exists\mathsf{y}\leq\mathsf{w})\varphi(\mathsf{x},\mathsf{y})$ istinita. U [8] daje se dokaz da $\mathsf{I\Delta_0}$ dokazuje ekvivalenciju gornje dvije formule.

Lako se uvjeriti da je negacija strogo Σ_1 formule Π_1 formula (takva formula logički je ekvivalentna strogo Π_1 formuli) ili da je Δ_0 formula ujedno i Σ_1 te Π_1 formula.

Iznesimo ovdje još jednu definiciju prije dokaza važnog teorema o Δ_0 rečenicama.

Definicija 4.8. Kažemo da je f Δ_0 *funkcija* ako i samo ako se može izraziti pomoću Δ_0 formule. Isto tako, Σ_1 *funkcija* je ona koja se može izraziti pomoću Σ_1 formule, a Π_1 *funkcije* izrazive su Π_1 formulama.

Teorem 4.10. Q *korektno odlučuje svaku zatvorenu* Δ_0 *formulu.*

Dokaz. Teorem dokazujemo indukcijom po složenosti formule.

Bazu indukcije čine atomarne Δ_0 *rečenice.* One su oblika $\tau=\rho$ ili $\tau\leq\rho$, gdje su τ i ρ zatvoreni termi. Tvrdnja teorema slijedi iz propozicija 4.4 i 4.6.

Pretpostavimo sada da tvrdnja vrijedi za sve Δ_0 rečenice složenosti do n (rečenice dobivene iz atomarnih upotrebom logičkih veznika i ograničenih kvantifikatora najviše n puta). Dokažimo da vrijedi i za rečenice složenosti $n+1$.

Neka je χ proizvoljna Δ_0 rečenica složenosti $n+1$. Dokazujemo po slučajevima:

1. χ je jednog od sljedećih oblika: $\neg\varphi$, $(\varphi\wedge\psi)$, $(\varphi\vee\psi)$, $(\varphi\rightarrow\psi)$, $(\varphi\leftrightarrow\psi)$, gdje su φ i ψ složenosti najviše n. Prema pretpostavci indukcije, Q korektno odlučuje rečenice φ i ψ. Sada lako slijedi da Q korektno odlučuje i rečenicu χ. Neka je χ oblika $(\varphi\wedge\psi)$. Pretpostavimo da je χ istinita. Tada su istinite i φ i ψ, pa $\mathsf{Q}\vdash\varphi$ i $\mathsf{Q}\vdash\psi$. Iz toga odmah slijedi $\mathsf{Q}\vdash\varphi\wedge\psi$. Ako je χ neistinita, tada je neistinita barem jedna od rečenica φ i ψ. Pretpostavimo bez

[6] Važno je naglasiti kako se ovdje radi o ekvivalenciji *na standardnom modelu.*

gubitka općenitosti da je neistinita φ. Po pretpostavci indukcije, $\mathsf{Q} \vdash \neg\varphi$. Dodavanjem disjunkcije dobiva se $\mathsf{Q} \vdash \neg\varphi \vee \neg\psi$, odnosno $\mathsf{Q} \vdash \neg(\varphi \wedge \psi)$. Na sličan način pokazuje se i za ostale oblike rečenice χ.

2. χ je oblika $(\forall \xi \leq \overline{\mathsf{n}})\varphi(\xi)$. Pretpostavimo da je istinita. Tada je za svaki $k \leq n$ rečenica $\varphi(\overline{\mathsf{k}})$ istinita. Kako je $\varphi(\overline{\mathsf{k}})$ složenosti najviše n, tako $\mathsf{Q} \vdash \varphi(\overline{\mathsf{k}})$ za svaki $k \leq n$. Iz tvrdnje 3 propozicije 4.7 dobiva se $\mathsf{Q} \vdash (\forall \xi \leq \overline{\mathsf{n}})\varphi(\xi)$. Pretpostavimo sada da je χ neistinita. Tada postoji $k \leq n$ za koji je $\varphi(\overline{\mathsf{k}})$ neistinita, pa tako i $\mathsf{Q} \vdash \neg\varphi(\overline{\mathsf{k}})$ po pretpostavci indukcije. Iz tvrdnje 4 propozicije 4.7 dobiva se $\mathsf{Q} \vdash (\exists \xi \leq \overline{\mathsf{n}})\neg\varphi(\xi)$ iz čega slijedi $\mathsf{Q} \vdash \neg(\forall \xi \leq \overline{\mathsf{n}})\varphi(\xi)$.

3. χ je oblika $(\exists \xi \leq \overline{\mathsf{n}})\varphi(\xi)$. Dokaz je simetričan onome za rečenice oblika $(\forall \xi \leq \overline{\mathsf{n}})\varphi(\xi)$. Ako je rečenica istinita, postoji $k \leq n$ za koji je $\varphi(\overline{\mathsf{k}})$ istinita, što Q i dokazuje, pa iz propozicije 4.7, točke 4, slijedi tvrdnja. Ako je χ neistinita, tada je $\varphi(\overline{\mathsf{k}})$ neistinita za svaki $k \leq n$, pa tvrdnja slijedi iz propozicije 4.7, točke 3.

Pokazali smo da u sva tri slučaja, ako Q korektno odlučuje Δ_0 rečenice složenosti do n, tada korektno odlučuje i proizvoljnu rečenicu χ složenosti $n+1$. Time je indukcijom dokazana tvrdnja teorema. $\square$

Na kraju ovog odjeljka dokažimo još dvije jednostavne posljedice teorema 4.10.

Korolar 4.11. *Svaka Δ_0 funkcija reprezentabilna je u Q.*

Dokaz. Neka je f proizvoljna jednomjesna Δ_0 funkcija (dokaz se provodi na jednak način i za funkcije proizvoljne mjesnosti), izražena Δ_0 formulom $\varphi(\mathsf{x}, \mathsf{y})$. Neka su sada $m, n \in \mathbb{N}$ proizvoljni. Prema teoremu 4.10, Q korektno odlučuje rečenicu $\varphi(\overline{\mathsf{m}}, \overline{\mathsf{n}})$. Dakle, ako je $f(m) = n$, $\mathsf{Q} \vdash \varphi(\overline{\mathsf{m}}, \overline{\mathsf{n}})$, a u suprotnom $\mathsf{Q} \vdash \neg\varphi(\overline{\mathsf{m}}, \overline{\mathsf{n}})$. Zaključujemo da $\varphi(\mathsf{x}, \mathsf{y})$ slabo reprezentira funkciju f. Međutim, prema propoziciji 4.9, sada postoji funkcija $\tilde{\varphi}(\mathsf{x}, \mathsf{y})$ koja reprezentira f kao funkciju. $\square$

Korolar 4.12. *Svaka istinita Σ_1 rečenica dokaziva je u Q.*

Dokaz. Neka je $\exists \mathsf{x}_1 \exists \mathsf{x}_2 \ldots \exists \mathsf{x}_\mathsf{k} \varphi(\mathsf{x}_1, \mathsf{x}_2, \ldots, \mathsf{x}_\mathsf{k})$ proizvoljna istinita strogo Σ_1 rečenica. $\varphi(\mathsf{x}_1, \mathsf{x}_2, \ldots, \mathsf{x}_\mathsf{k})$ je pritom Δ_0 formula. Iz istinitosti početne formule zaključujemo da postoje prirodni brojevi $n_1, n_2, \ldots, n_k$ takvi da je $\varphi(\overline{\mathsf{n}_1}, \overline{\mathsf{n}_2}, \ldots, \overline{\mathsf{n}_\mathsf{k}})$ istinita. Prema teoremu 4.10, $\mathsf{Q} \vdash \varphi(\overline{\mathsf{n}_1}, \overline{\mathsf{n}_2}, \ldots, \overline{\mathsf{n}_\mathsf{k}})$. Dodavanjem egzistencijalnih kvantifikatora dolazi se do rezultata: $\mathsf{Q} \vdash \exists \mathsf{x}_1 \exists \mathsf{x}_2 \ldots \exists \mathsf{x}_\mathsf{k} \varphi(\mathsf{x}_1, \mathsf{x}_2, \ldots, \mathsf{x}_\mathsf{k})$. Dakle, Q dokazuje svaku istinitu strogo Σ_1 rečenicu. Konačno, tvrdnja teorema slijedi iz činjenice da je svaka Σ_1 rečenica logički ekvivalentna nekoj strogo Σ_1 rečenici. $\square$

U sljedećem odjeljku dokazuje se jači rezultat – svaka Σ_1 funkcija također je reprezentabilna u Q.

4.4. Reprezentabilnost Σ_1 funkcija

Reprezentabilnosti Σ_1 funkcija dokazujemo u dva koraka: prvo se pokazuje da je svaka Σ_1 funkcija f ekvivalentna kompoziciji dviju Δ_0 funkcija g i h, a zatim se demonstrira da je u Q reprezentabilna takva kompozicija Δ_0 funkcija.

Lema 4.13. *Svaka Σ_1 funkcija ekvivalentna je kompoziciji dviju Δ_0 funkcija.*

Dokaz. Neka je $f : \mathbb{N} \to \mathbb{N}$ proizvoljna jednomjesna Σ_1 funkcija, a $\varphi(\mathsf{x}, \mathsf{y})$ strogo Σ_1 formula koja ju izražava. Prepostavimo da $\varphi(\mathsf{x}, \mathsf{y})$ ima samo jedan egzistencijalni kvantifikator, tj. oblika je $\exists \mathsf{z} \mathsf{R}(\mathsf{x}, \mathsf{y}, \mathsf{z})$, gdje je $\mathsf{R}(\mathsf{x}, \mathsf{y}, \mathsf{z})$ Δ_0 formula. Slučajevi u kojima $\varphi(\mathsf{x}, \mathsf{y})$ ima više od jednog kvantifikatora ili je f višemjesna funkcija dokazuju se na isti način.

Formula $\mathsf{R}(\mathsf{x}, \mathsf{y}, \mathsf{z})$ pod standardnom interpretacijom izražava neku relaciju $R(x, y, z)$ nad prirodnim brojevima. Dakle, $f(x) = y$, odnosno $\exists \mathsf{z} \mathsf{R}(\bar{\mathsf{x}}, \bar{\mathsf{y}}, \mathsf{z})$ je istinita, ako i samo ako postoji prirodan broj z tako su x, y, z u relaciji R. Pomoću relacije R sada možemo definirati dvije nove funkcije:

1. Neka je $g(x)$ najmanji prirodan broj y takav da postoje $u \leq y$ i $v \leq y$ za koje vrijedi $Rxuv$. Kako ovdje razmatramo samo totalne funkcije, za svaki x postoje u i v takvi da vrijedi $Rxuv$, pa je ova funkcija dobro definirana. Funkcija $g(x)$ određuje gornju granicu za vrijednosti u i v.

2. Funkciju $h(x, y)$ definiramo na način da je jednaka najmanjem broju $u \leq y$ takvom da postoji $v \leq y$ i da vrijedi $Rxuv$. Ako takav u ne postoji, definiramo $h(x, y) = 0$ (ovo koristimo kako bi funkcija h bila totalna). Primijetimo da, ako koristimo $y = g(x)$, tada je $h(x, y)$ zapravo jednaka $f(x)$.

Funkcije g i h definirane su tako da f bude ekvivalentna njihovoj kompoziciji. Doista, $f(x) = h(x, g(x))$. Međutim, one su definirane i tako da se mogu izraziti pomoću L_A formula koje koriste samo ograničenu kvantifikaciju – g i h su Δ_0 funkcije! Funkciju g možemo izraziti Δ_0 formulom $\mathsf{G}(\mathsf{x}, \mathsf{y})$ definiranu na sljedeći način:

$$
\begin{aligned}
\mathsf{G}(\mathsf{x}, \mathsf{y}) \stackrel{\text{def}}{=} & (\exists \mathsf{u} \leq \mathsf{y})(\exists \mathsf{v} \leq \mathsf{y}) \mathsf{R}(\mathsf{x}, \mathsf{u}, \mathsf{v}) \wedge \\
& (\forall \mathsf{w} \leq \mathsf{y})(\mathsf{w} \neq \mathsf{y} \to (\forall \mathsf{u} \leq \mathsf{y})(\forall \mathsf{v} \leq \mathsf{y}) \neg \mathsf{R}(\mathsf{x}, \mathsf{u}, \mathsf{v}))
\end{aligned}
$$

$\mathsf{H}(\mathsf{x}, \mathsf{y}, \mathsf{z})$ definirana na sljedeći način izražava funkciju h:

$$
\begin{aligned}
\mathsf{H}(\mathsf{x}, \mathsf{y}, \mathsf{z}) \stackrel{\text{def}}{=} & [(\exists \mathsf{v} \leq \mathsf{y}) \mathsf{R}(\mathsf{x}, \mathsf{z}, \mathsf{v}) \wedge (\forall \mathsf{u} \leq \mathsf{z})(\forall \mathsf{v} \leq \mathsf{y})(\mathsf{u} \neq \mathsf{z} \to \neg \mathsf{R}(\mathsf{x}, \mathsf{u}, \mathsf{v}))] \vee \\
& [\neg (\exists \mathsf{v} \leq \mathsf{y}) \mathsf{R}(\mathsf{x}, \mathsf{z}, \mathsf{v}) \wedge \mathsf{z} = 0]
\end{aligned}
$$

Ovime je dokazano da je f ekvivalentna kompoziciji dviju Δ_0 funkcija. $\square$

Teorem 4.14. *Svaka Σ_1 funkcija reprezentabilna je u* Q.

Dokaz. Pretpostavimo, kao i u dokazu gornje leme, da je f proizvoljna jednomjesna funkcija. Za višemjesne funkcije dokaz se provodi na isti način. Prema lemi 4.13, postoje Δ_0 funkcije g i h takve da vrijedi $f(x) = h(x, g(x))$ za svaki $x \in \mathbb{N}$. Iz korolara 4.11 slijedi da postoje Δ_0 formule $\tilde{\mathsf{G}}(\mathsf{x}, \mathsf{y})$ i $\tilde{\mathsf{H}}(\mathsf{x}, \mathsf{y}, \mathsf{z})$ koje reprezentiraju funkcije g i h unutar teorije Q. Definirajmo sada formulu $\mathsf{F}(\mathsf{x}, \mathsf{y})$ na sljedeći način i dokažimo da ona reprezentira funkciju f u Q:

$$\mathsf{F}(\mathsf{x}, \mathsf{y}) \stackrel{\text{def}}{=} \exists \mathsf{u}(\tilde{\mathsf{G}}(\mathsf{x}, \mathsf{u}) \land \tilde{\mathsf{H}}(\mathsf{x}, \mathsf{u}, \mathsf{y}))$$

Neka su sada m, n proizvoljni prirodni brojevi takvi da $f(m) = n$. Potrebno je pokazati da vrijedi $\mathsf{Q} \vdash \forall \mathsf{y}(\mathsf{F}(\overline{\mathsf{m}}, \mathsf{y}) \leftrightarrow \mathsf{y} = \overline{\mathsf{n}})$. Budući da je $f(x) = h(x, g(x))$, zaključujemo da postoji neki $o \in \mathbb{N}$ takav da je $g(m) = o$ te $h(m, o) = n$. Iz reprezentabilnosti funkcija g i h sada slijedi $\mathsf{Q} \vdash \forall \mathsf{u}(\tilde{\mathsf{G}}(\overline{\mathsf{m}}, \mathsf{u}) \leftrightarrow \mathsf{u} = \overline{\mathsf{o}})$ te $\mathsf{Q} \vdash \forall \mathsf{y}(\tilde{\mathsf{H}}(\overline{\mathsf{m}}, \overline{\mathsf{o}}, \mathsf{y}) \leftrightarrow \mathsf{y} = \overline{\mathsf{n}})$. Formule $\tilde{\mathsf{H}}(\overline{\mathsf{m}}, \overline{\mathsf{o}}, \mathsf{y})$ i $\exists \mathsf{u}(\mathsf{u} = \overline{\mathsf{o}} \land \tilde{\mathsf{H}}(\overline{\mathsf{m}}, \mathsf{u}, \mathsf{y}))$ logički su ekvivalentne, pa koristeći tu i gornje dvije dokazane ekvivalencije, zaključujući unutar Q, dobivamo:

1. $\forall \mathsf{y}(\exists \mathsf{u}(\mathsf{u} = \overline{\mathsf{o}} \land \tilde{\mathsf{H}}(\overline{\mathsf{m}}, \mathsf{u}, \mathsf{y})) \leftrightarrow \mathsf{y} = \overline{\mathsf{n}})$
2. $\forall \mathsf{y}(\exists \mathsf{u}(\tilde{\mathsf{G}}(\overline{\mathsf{m}}, \mathsf{u}) \land \tilde{\mathsf{H}}(\overline{\mathsf{m}}, \mathsf{u}, \mathsf{y})) \leftrightarrow \mathsf{y} = \overline{\mathsf{n}})$
3. $\forall \mathsf{y}(\mathsf{F}(\overline{\mathsf{m}}, \mathsf{y}) \leftrightarrow \mathsf{y} = \overline{\mathsf{n}})$

što je i trebalo dokazati. □

4.5. P.r. adekvatnost teorije Q

U ovom odjeljku, koristeći dosad dokazane rezultate, dolazimo do centralnog rezultata ovog poglavlja – sve primitivno rekurzivne funkcije reprezentabilne su u Q. Ponovimo definiciju te klase funkcija:

Definicija 4.9. Klasom *primitivno rekurzivnih funkcija* nazivamo najmanju klasu (totalnih) funkcija koja sadrži sve inicijalne funkcije te je zatvorena za *kompoziciju* i *primitivnu rekurziju.*

Pritom su inicijalne funkcije nul-funkcija $Z(x) = 0$, funkcija sljedbenika $Sc(x) = x + 1$ te projekcija $I_k^n(x_1, \ldots, x_n) = x_k$, a funkcija f definirana je primitivnom rekurzijom pomoću funkcija g i h ako je definirana na sljedeći način:

$$\begin{aligned} f(\vec{x}, 0) &= g(\vec{x}) \\ f(\vec{x}, y + 1) &= h(\vec{x}, y, f(\vec{x}, y)) \end{aligned}$$

U nastavku dokazujemo da se primitivno rekurzivne funkcije mogu *izraziti* u L_A – štoviše, mogu se izraziti pomoću Σ_1 formula. Iz teorema 4.14 zatim slijedi da su primitivno rekurzivne funkcije reprezentabilne u Q, tj. Q je p.r. adekvatna teorija. Ovo je ključan rezultat, kao što je i naglašeno u uvodu, jer nam govori da Q može donositi zaključke o relacijama poput $Prf(m,n)$ (čija karakteristična funkcija je primitivno rekurzivna), tj. teorija Q može dokazati tvrdnje o dokazima unutar same sebe.[7]

Na početku je potrebno pokazati da su inicijalne funkcije Σ_1 funkcije. Nakon toga dokazujemo da, ako su g i h Σ_1 funkcije, tada je i funkcija f dobivena iz g i h kompozicijom ili primitivnom rekurzijom također Σ_1 funkcija. Iz definicije klase primitivno rekurzivnih funkcija tada slijedi da su sve funkcije iz te klase Σ_1 funkcije.

Lema 4.15. *Inicijalne funkcije mogu se izraziti pomoću Σ_1 formula.*

Dokaz. Lako se provjerava da nul-funkciju $Z(x) = 0$ izražava sljedeća L_A formula: $\mathsf{Z}(\mathsf{x},\mathsf{y}) \stackrel{\text{def}}{=} (\mathsf{x}=\mathsf{x} \land \mathsf{y}=\mathsf{0})$.[8] Isto vrijedi i za funkciju sljedbenika koja se može izraziti formulom $\mathsf{Sc}(\mathsf{x},\mathsf{y}) \stackrel{\text{def}}{=} (\mathsf{Sx}=\mathsf{y})$ te projekciju, izraženu pomoću $\mathsf{I}^{\mathsf{n}}_{\mathsf{k}}(\mathsf{x}_1,\ldots,\mathsf{x}_\mathsf{n},\mathsf{y}) \stackrel{\text{def}}{=} (\mathsf{x}_1=\mathsf{x}_1 \land \ldots \land \mathsf{x}_\mathsf{k}=\mathsf{y} \land \ldots \land \mathsf{x}_\mathsf{n}=\mathsf{x}_\mathsf{n})$. Sve navedene su Δ_0 formule, a $\Delta_0 \subset \Sigma_1$, što dokazuje tvrdnju ove leme. □

Lema 4.16. *Svaka funkcija dobivena pomoću kompozicije iz Σ_1 funkcija je također Σ_1 funkcija.*

Dokaz. Neka je f proizvoljna funkcija dobivena kompozicijom Σ_1 funkcija g i h. Pretpostavimo da su sve funkcije jednomjesne. Općenita tvrdnja dobiva se na sličan način. Sada je $f(x) = h(g(x))$ za svaki x. Funkcije g i h izražene su formulama $\mathsf{G}(\mathsf{x},\mathsf{y})$ te $\mathsf{H}(\mathsf{x},\mathsf{y})$. Funkciju f sada možemo izraziti pomoću formule $\mathsf{F}(\mathsf{x},\mathsf{y}) \stackrel{\text{def}}{=} \exists \mathsf{z}(\mathsf{G}(\mathsf{x},\mathsf{z}) \land \mathsf{H}(\mathsf{z},\mathsf{y}))$.

Doista, ako je $f(x) = y$, tada postoji prirodan broj o takav da je $g(x) = o$ i $h(o) = y$. Dakle, formule $\mathsf{G}(\overline{\mathsf{x}},\overline{\mathsf{o}})$ i $\mathsf{H}(\overline{\mathsf{o}},\overline{\mathsf{y}})$ istinite su, pa je istinita i formula $\mathsf{F}(\overline{\mathsf{x}},\overline{\mathsf{y}})$. Na sličan način pokazuje se i da je $\mathsf{F}(\overline{\mathsf{x}},\overline{\mathsf{y}})$ neistinita ako je $f(x) \neq y$.

Potrebno je još pokazati da tako definirana $\mathsf{F}(\mathsf{x},\mathsf{y})$ jedna Σ_1 formula. Prema pretpostavci, $\mathsf{G}(\mathsf{x},\mathsf{y})$ i $\mathsf{H}(\mathsf{x},\mathsf{y})$ su Σ_1 formule, pa koristeći pravila prijelaza za kvantifikatore, niz egzistencijalnih kvantifikatora ispred Δ_0 jezgri tih formula možemo staviti ispred zagrade, čime se dobiva logički ekvivalentna formula. Primjerice, ako $\mathsf{G}(\mathsf{x},\mathsf{y})$ i $\mathsf{H}(\mathsf{x},\mathsf{y})$ imaju samo jedan egzistencijalni kvantifikator, tj. oblika su $\exists \mathsf{u}\mathsf{G}'(\mathsf{x},\mathsf{u},\mathsf{y})$ i $\exists \mathsf{v}\mathsf{H}'(\mathsf{x},\mathsf{v},\mathsf{y})$, tada se iz $\exists \mathsf{z}(\exists \mathsf{u}\mathsf{G}'(\mathsf{x},\mathsf{u},\mathsf{z}) \land \exists \mathsf{v}\mathsf{H}'(\mathsf{u},\mathsf{v},\mathsf{y}))$ pomakom kvantifikatora dobije ekvivalentna formula $\exists \mathsf{z}\exists \mathsf{u}\exists \mathsf{v}(\mathsf{G}'(\mathsf{x},\mathsf{u},\mathsf{z}) \land \mathsf{H}'(\mathsf{u},\mathsf{v},\mathsf{y}))$, što je evidentno Σ_1 formula.[9] □

[7] S druge strane, važno je naglasiti, sama relacija dokazivosti nije definabilna u Q. O tome ima više riječi u poglavljima koja slijede.

[8] Izraze poput $\mathsf{x}=\mathsf{x}$ koji su trivijalno istiniti ovdje koristimo kako bi formula sadržavala sve slobodne varijable.

[9] Pritom su korištene ekvivalencije $\exists \mathsf{x}(\mathsf{A} \land \mathsf{B}) \Leftrightarrow (\exists \mathsf{x}\mathsf{A} \land \mathsf{B})$ i $\exists \mathsf{x}(\mathsf{B} \land \mathsf{A}) \Leftrightarrow (\mathsf{B} \land \exists \mathsf{x}\mathsf{A})$ (vidi [11]).

Izražavanje funkcija definiranih pomoću primitivne rekurzije nešto je ipak složenije. Primijetimo kako se vrijednost funkcije $f(\vec{x}, y)$ izračunava pomoću vrijednosti za manje y, sve dok se ne dođe do $f(\vec{x}, 0)$. To nas navodi na ideju definiranja niza brojeva $k_0, k_1, \ldots, k_y$ takvog da je $k_i = f(\vec{x}, i)$ za svaki $0 \leq i \leq y$. Ako je funkcija f definirana primitivnom rekurzijom pomoću funkcija g i h, tada je $f(\vec{x}, y) = z$ ako i samo ako postoji niz $k_0, k_1, \ldots, k_y$ takav da je $k_0 = g(\vec{x})$, $k_y = z$, a $k_{i+1} = h(\vec{x}, i, k_i)$ za svaki $0 \leq i < y$ (tvrdnja slijedi izravno iz definicije primitivne rekurzije). Formula koja izražava funkciju f unutar L_A koristit će upravo gornju činjenicu.

Kako bi se u jeziku L_A moglo govoriti o nizu brojeva proizvoljne duljine, potrebno je koristiti kodiranje. U prethodnom poglavlju korišten je već jedan način kodiranja niza (gdje su elementi niza bili kodovi simbola jezika L_A):

$$c = 2^{k_0} \times 3^{k_1} \times \cdots \times \pi_y^{k_y}$$

Međutim, takav način kodiranja koristi potenciranje, a ta operacija nije ugrađena u L_A – jezik L_A ne sadrži funkcijski simbol koji bi pod standardnom interpretacijom predstavljao operaciju potenciranja.

Gödel je ovaj problem riješio na način da se svakom nizu pridijele *dva* broja c i d, a za dekodiranje koristi tzv. *β-funkcija* definirana na sljedeći način:

$$\beta(c, d, i) = \mathrm{rem}(c, d(i+1) + 1)$$

Pritom $\mathrm{rem}(m, n)$ predstavlja ostatak dijeljenja broja m sa n. Za izražavanje ove funkcije dovoljni su resursi koje jezik L_A ima ugrađene – funkcija sljedbenika, zbrajanje i množenje:

$$\mathsf{B}(\mathsf{c}, \mathsf{d}, \mathsf{i}, \mathsf{y}) \stackrel{\text{def}}{=} (\mathsf{y} \leq (\mathsf{d} \times \mathsf{Si})) \land (\exists \mathsf{u} \leq \mathsf{c})[(\mathsf{u} \times \mathsf{S}(\mathsf{d} \times \mathsf{Si})) + \mathsf{y} = \mathsf{c}]$$

Primijetimo kako je $\mathsf{B}(\mathsf{c}, \mathsf{d}, \mathsf{i}, \mathsf{y})$ Δ_0 formula.

Lema 4.18 potvrđuje ispravnost ovakvog načina kodiranja. Za njen dokaz koristimo poznati Kineski teorem o ostacima:

Teorem 4.17 (Kineski teorem o ostacima)**.** *Neka su $n_1, \ldots, n_k$ međusobno relativno prosti prirodni brojevi. Za svaki niz brojeva $a_1, \ldots, a_k$ postoji prirodan broj x takav da je $x \equiv a_i \pmod{n_i}$ za svaki $1 \leq i \leq k$.*

Dokaz teorema 4.17 može se pronaći, primjerice, u [6].

Lema 4.18. *Za svaki niz $k_0, k_1, \ldots, k_n$ moguće je odrediti brojeve c i d takve da vrijedi $\beta(c, d, i) = k_i$ za svaki $0 \leq i \leq n$.*

Dokaz. Prvo ćemo pokazati da je moguće odrediti d takav da svi $d_i \stackrel{\text{def}}{=} d(i+1)+1$, za $i \leq n$, budu međusobno relativno prosti. Nakon toga, postojanje broja c koji zadovoljava traženi uvjet proizlazi iz Kineskog teorema o ostacima.

Uzmimo s kao najveći od brojeva n i $k_0, k_1, \ldots, k_n$ te postavimo $d = s!$. Pretpostavimo, kontradikcije radi, da postoje indeksi j i k, $j < k \leq n$, takvi da je $\text{nzd}(d_j, d_k) > 1$. Označimo $j' = j+1$ i $k' = k+1$. Drugim riječima, postoji prosti faktor p takav da $p \mid (dj'+1)$ i $p \mid (dk'+1)$. Iz ovoga odmah slijedi i $p \mid d(k'-j')$.

Budući da je $d = s!$, svaki broj manji ili jednak od s dijeli broj dk bez ostatka, pa ovdje mora vrijediti $p > s$. Međutim, kako $p \not| \, d$ (u protivnom p ne bi dijelio $dj'+1$ i $dk'+1$), mora vrijediti $p \mid (k'-j')$. Kako je $k'-j' \leq n$, mora vrijediti $p < n$, odnosno $p < s$ (zbog načina na koji je s definiran). Time smo došli do kontradikcije s prethodno utvrđenim rezultatom $p > s$, pa zaključujemo da su svi d_i međusobno relativno prosti.

Tvrdnja leme sada odmah slijedi iz Kineskog teorema o ostacima – postoji broj c takav da je $c \equiv k_i \pmod{d_i}$ za svaki $i \leq n$ (štoviše, postoji beskonačno mnogo takvih brojeva; svi su međusobno kongruentni modulo $\prod_{i=0}^{n} d_i$). Dakle, postoje brojevi c i d takvi da je $k_i = \text{rem}(c, d_i)$ za svaki $i \leq n$, što je i trebalo dokazati. $\square$

Koristeći rezultat prethodne leme sada napokon možemo dokazati sljedeće:

Lema 4.19. *Svaka funkcija definirana pomoću primitivne rekurzije iz Σ_1 funkcija je također Σ_1 funkcija.*

Dokaz. Neka je f funkcija definirana pomoću primitivne rekurzije iz Σ_1 funkcija g i h. Kao i u ranijim dokazima, pretpostavimo da je g jedno-, f dvo-, a h tromjesna funkcija (opet, općenitiji rezultati dokazuju se na jednak način).

Iz ranijih razmatranja znamo da vrijedi $f(x,y) = z$ ako i samo ako postoji niz $k_0, \ldots, k_y$ takav da je $k_0 = g(x)$, $k_y = z$ te $k_{i+1} = h(x, i, k_i)$ za svaki $i < y$. Koristeći β-funkciju i lemu 4.18, prethodna je tvrdnja ekvivalentna ovoj: $f(x,y) = z$ ako i samo ako postoje $c, d \in \mathbb{N}$ takvi da je $\beta(c,d,0) = g(x)$, $\beta(c,d,y) = z$ te $\beta(c,d,i+1) = h(x,i,\beta(c,d,i))$ za svaki $i < y$. Pomoću formule $\mathsf{B(c,d,i,y)}$ koja izražava β-funkciju te formula $\mathsf{G(x,y)}$ i $\mathsf{H(x,y,z,u)}$ koje po pretpostavci izražavaju funkcije g i h sada možemo definirati funkciju $\mathsf{F(x,y,z)}$ koja izražava funkciju f definiranu pomoću primitivne rekurzije:

$$\begin{aligned} \mathsf{F(x,y,z)} \overset{\text{def}}{=} \exists \mathsf{c} \exists \mathsf{d} \{ \exists \mathsf{k} [\mathsf{G(x,k)} \land \mathsf{B(c,d,0,k)}] \land \mathsf{B(c,d,y,z)} \land (\forall \mathsf{u} \leq \mathsf{y})[\mathsf{u} \neq \mathsf{y} \rightarrow \\ \exists \mathsf{v} \exists \mathsf{w} \{ \mathsf{B(c,d,u,v)} \land \mathsf{B(c,d,Su,w)} \land \mathsf{H(x,u,v,w)} \}]\} \end{aligned}$$

Valja još pokazati da je $\mathsf{F(x,y,z)}$ Σ_1 formula, što nije baš odmah očito. Međutim, B je Δ_0 formula, a kvantifikatore ispred G i H, koristeći pravila za prijelaz kvantifikatora, možemo prebaciti izvan odgovarajućih zagrada. Jedinu poteškoću još predstavljaju egzistencijalni kvantifikatori koji su u dosegu ograničenog kvantifikatora $(\forall \mathsf{u} \leq \mathsf{y})$. No, uočimo da, ako je neka formula oblika $(\forall \mathsf{u} \leq \mathsf{y}) \exists \mathsf{v} \mathsf{F(u,v)}$ istinita, tada za svaki $u \leq y$ postoji neki v za koji vrijedi $F(u,v)$. Uzmimo v' kao najveći od svih tih brojeva v. Sada je istinita i formula $(\forall \mathsf{u} \leq \mathsf{y})(\exists \mathsf{v} \leq \overline{\mathsf{v}'}) \mathsf{F(u,v)}$, ili općenitije $\exists \mathsf{w} (\forall \mathsf{u} \leq \mathsf{y})(\exists \mathsf{v} \leq \mathsf{w}) \mathsf{F(u,v)}$. Dakle, formula

$(\forall \mathsf{u} \leq \mathsf{y})\exists \mathsf{v}\mathsf{F}(\mathsf{u},\mathsf{v})$ istinita je pod standardnom interpretacijom ako i samo ako je i formula $\exists \mathsf{w}(\forall \mathsf{u} \leq \mathsf{y})(\exists \mathsf{v} \leq \mathsf{w})\mathsf{F}(\mathsf{u},\mathsf{v})$ istinita. Ta nas činjenica upućuje na to da je moguće prebaciti egzistencijalne kvantifikatore ispred ograničenog univerzalnog kvantifikatora $(\forall \mathsf{u} \leq \mathsf{y})$, iz čega zaključujemo da postoji strogo Σ_1 formula ekvivalentna s $\mathsf{F}(\mathsf{x},\mathsf{y},\mathsf{z})$ koja izražava funkciju f definiranu pomoću primitivne rekurzije. To odmah povlači da je f Σ_1 funkcija, što smo i htjeli dokazati. □

Sljedeći teorem sada jednostavno slijedi iz lema 4.15, 4.16 i 4.19.

Teorem 4.20. *Svaka primitivno rekurzivna funkcija je* Σ_1 *funkcija.*

Konačno, teoremi 4.14 i 4.20 zajedno daju:

Teorem 4.21. *Svaka primitivno rekurzivna funkcija reprezentabilna je u* Q*. Drugim riječima,* Q *je p.r. adekvatna teorija.*

5 Prvi teorem nepotpunosti

Sadržaj

Dosad su pokazana dva ključna rezultata – definiran je način kodiranja izraza jezika L_A takav da, posebno, tvrdnji o dokazivosti rečenice u nekoj L_A teoriji odgovara primitivno rekurzivna numerička relacija $Prf_T(m, n)$ te je pokazano da je Q (pa tako i jače teorije poput PA) primitivno rekurzivno adekvatna teorija, što znači da su primitivno rekurzivne funkcije reprezentabilne u Q (posebno, karakteristične funkcije p.r. relacija poput $Prf_T(m, n)$ su reprezentabilne, pa su takve relacije definabilne u Q). Vidjet ćemo da Gödelov prvi teorem nepotpunosti, a i mnogi vezani rezultati, sada (kad su izgrađeni potrebni temelji) brzo slijedi.

Teorem 5.1 (Gödelov prvi teorem nepotpunosti)**.** *Ako je T aksiomatizabilna aritmetička teorija koja proširuje Q, tada postoji rečenica $\mathsf{G_T}$ u jeziku teorije T takva da, ako je T konzistentna teorija, $T \nvdash \mathsf{G_T}$ te, ako je T ω-konzistentna, $T \nvdash \neg\mathsf{G_T}$.*

U odjeljku 5.1 teorem se dokazuje konstruktivno za Peanovu aritmetiku (definira se rečenica G koja je istinita ako i samo ako nije dokaziva u PA), nalik izvornom Gödelovom dokazu. Kasnije se definira i dokazuje još jedan veoma važan rezultat – dijagonalna lema (katkad nazvana i teoremom o fiksnoj točki). Pokazuje se kako je prvi teorem nepotpunosti jednostavna posljedica dijagonalne leme, a ta se lema koristi poslije i za pojačanje rezultata teorema 5.1. Naime, uvjet da T mora biti ω-konzistentna da bi vrijedilo $T \nvdash \neg\varphi$ može se oslabiti – dovoljna je obična konzistentnost (Gödel-Rosserov teorem). Na kraju poglavlja dokazuje se još i Tarskijev teorem o nedefinabilnosti aritmetičke istine.

Kao što je već više puta natuknuto, ključni sastojci za dokaz Gödelovih teorema nepotpunosti su primitivna rekurzivnost relacije $\mathit{Prf}_T(m,n)$ te primitivno rekurzivna adekvatnost teorije T. Pogledajmo sada pozornije iskaz teorema 5.1. Traži se da T bude aksiomatizabilna aritmetička teorija, što znači da je jezik te teorije L_A (ili neko proširenje) te je svojstvo da je n Gödelov broj aksioma te teorije odlučivo. Iz Craigovog teorema (odjeljak 3.3) slijedi da postoji teorija T' koja ima iste teoreme kao i T (dakle, ako $T' \nvdash \varphi$, tada i $T \nvdash \varphi$), a koja je p.r. aksiomatizabilna. Dakle, relacija $\mathit{Aksiom}_{T'}(n)$ koja vrijedi ako n kodira aksiom teorije T' je primitivno rekurzivna, pa je tako i relacija $\mathit{Prf}_{T'}(m,n)$ primitivno rekurzivna (odjeljak 3.3). Istaknimo samo da jezik teorije T ne mora biti L_A, već može biti i neko proširenje. Također, nije nužno da se koristi hilbertovski sustav s poznatim logičkim aksiomima (vidi npr. [11]) te generalizacijom i pravilom modus ponens kao jedinim pravilima izvoda. U tom slučaju je, doduše, potrebno uvesti dodatne uvjete na primitivno rekurzivnu aksiomatizabilnost teorije T – osim svojstva da je n Gödelov broj aksioma, potrebno je i da svojstvo da je n kôd rečenice jezika teorije T te svojstvo da je n ispravan dokaz rečenice koju kodira m budu primitivno rekurzivna svojstva.

U iskazu teorema 5.1 traži se još i da teorija T proširuje Robinsonovu aritmetiku Q. Drugim riječima, teorija T mora biti primitivno rekurzivno adekvatna (odjeljak 4.5). To posebno znači da je relacija $\mathit{Prf}_T(m,n)$ definabilna u T. Kasnije će postati jasno kako upravo iz činjenice da prvi teorem nepotpunosti vrijedi za svaku konzistentnu, p.r. aksiomatizabilnu te p.r. adekvatnu teoriju T slijedi ne samo da je svaka takva teorija T nepotpuna, već se T nikako ni ne može učiniti potpunom (dodavanjem rečenica koje nisu dokazive u T).

5.1. Gödelova rečenica G

U ovom odjeljku konstruiramo L_A rečenicu G koja indirektno za sebe govori da nije dokaziva u PA. Drugim riječima, definira se rečenica G čiji je Gödelov broj g, a koja kazuje da u PA ne postoji dokaz rečenice s Gödelovim brojem g. Zatim pokazujemo kako je rečenica G istinita ako i samo ako nije dokaziva te da postojanje te rečenice dokazuje teorem 5.1 za teoriju PA.

Za konstrukciju takve samoreferencirajuće rečenice evidentno ćemo koristiti dijagonalizaciju (odjeljak 3.4). Prisjetimo se – funkcija $\mathit{diag}(n)$ daje Gödelov broj formule koja se dobiva dijagonalizacijom iz formule s Gödelovim brojem n. Definirajmo sada relaciju

$$\mathit{Gdl}(m,n) \overset{\text{def}}{=} \mathit{Prf}(m, \mathit{diag}(n))$$

koja vrijedi ako i samo ako je m dokaz (u PA) *dijagonalizacije* formule čiji je Gödelov broj n. Ova relacija očito je primitivno rekurzivna (njezina karakteristična funkcija definirana je pomoću kompozicije iz karakteristične funkcije relacije

Prf i funkcije *diag*, koje su primitivno rekurzivne). Budući da je PA p.r. adekvatna teorija, postoji Σ_1 formula $\mathsf{Gdl}(\mathsf{x},\mathsf{y})$ koja definira (odjeljak 4.1), a ujedno i izražava, relaciju $Gdl(m,n)$ u PA.

Sada definirajmo L_A formulu $\mathsf{U}(\mathsf{y})$ na sljedeći način:

$$\mathsf{U}(\mathsf{y}) \overset{\mathrm{def}}{=} \neg\exists \mathsf{x}\mathsf{Gdl}(\mathsf{x},\mathsf{y})$$

Formula $\mathsf{U}(\overline{\mathsf{n}})$ istinita je ako u PA ne postoji dokaz dijagonalizacije formule čiji je Gödelov broj n. Ovaj je korak sada ključan: promotrimo rečenicu koja se dobiva ako u $\mathsf{U}(\mathsf{y})$ uvrstimo Gödelov broj same formule U umjesto varijable y! Ovom dijagonalizacijom formule $\mathsf{U}(\mathsf{y})$ dobivamo čuvenu Gödelovu rečenicu G. Definiramo:

$$\mathsf{G} \overset{\mathrm{def}}{=} \exists \mathsf{y}(\mathsf{y} = \ulcorner \mathsf{U} \urcorner \wedge \mathsf{U})$$

Formula G logički je ekvivalentna s $\mathsf{U}(\ulcorner \mathsf{U} \urcorner)$, odnosno $\neg\exists \mathsf{x}\mathsf{Gdl}(\mathsf{x},\ulcorner \mathsf{U} \urcorner)$. Pokažimo sada da je formula G istinita (na standardnom modelu) ako i samo ako nije dokaziva u PA. Ako je G istinita formula, tada za nijedan prirodan broj m nije istinita formula $\mathsf{Gdl}(\overline{\mathsf{m}},\ulcorner \mathsf{U} \urcorner)$. Budući da formula $\mathsf{Gdl}(\mathsf{x},\mathsf{y})$ izražava relaciju $Gdl(m,n)$, zaključujemo da za nijedan prirodan broj m ne vrijedi $Gdl(m,\ulcorner \mathsf{U} \urcorner)$. Drugim riječima, ne postoji kôd dokaza dijagonalizacije formule U, tj. dijagonalizacija od U nije dokaziva u PA. Kako je po definiciji upravo G dijagonalizacija formule U (vrijedi $diag(\ulcorner \mathsf{U} \urcorner) = \ulcorner \mathsf{G} \urcorner$), zaključujemo da formula G nije dokaziva ako je istinita. Druga strana dobiva se na sličan način – ako G nije istinita, tada postoji broj m takav da je $\mathsf{Gdl}(\overline{\mathsf{m}},\ulcorner \mathsf{U} \urcorner)$ istinita, iz čega slijedi da je G dokaziva rečenica.

Primijetimo kako nijednom dosad u ovom radu nije korišteno semantičko svojstvo *adekvatnosti* teorija Q i PA u odnosu na standardni model (za aritmetičku teoriju ćemo reći da je adekvatna u odnosu na standardni model ako su njezini teoremi istiniti na tom modelu).[1] Primjerice, kod dokaza da je Q p.r. adekvatna teorija, nigdje nismo pretpostavili da su aksiomi te teorije istiniti pod standardnom interpretacijom – sve tvrdnje mogle su se izvesti samo iz aksioma teorije Q koristeći pravila modus ponens i generalizaciju[2], bez ikakvih dodatnih pretpostavki, dakle isključivo *sintaktičkim* postupcima (manipulacijama simbola).

Ako pretpostavimo da je PA adekvatna teorija u odnosu na standardni model, nepotpunost te teorije jako se lako dokazuje. Doista, ako PA dokazuje G, tada G nije istinita rečenica, što je kontradiktorno pretpostavci da su teoremi teorije

[1] Općenito kažemo da je teorija T adekvatna (engl. *sound*) ako su njezini teoremi istiniti na svakom modelu teorije T. Teorija je adekvatna ako njezina pravila zaključivanja čuvaju istinitost. Lako se može provjeriti da to vrijedi za pravila modus ponens i generalizaciju (vidi npr. [11]). Ovdje, međutim, posebno zahtjevamo da su teoremi istiniti *na standardnom modelu.* Uz pravila koja čuvaju istinitost, dovoljan dodatan semantički zahtjev za takve teorije je istinitost njezinih aksioma na standardnom modelu.

[2] U poglavlju 4 korišten je sustav prirodne dedukcije, no već je tamo bilo istaknuto kako su ti dedukcijski sustavi ekvivalentni.

PA istinite formule. Zato zaključujemo da je $\mathsf{PA} \nvdash \mathsf{G}$, iz čega slijedi da je G istinita rečenica. Međutim, sada se odmah dobiva i $\mathsf{PA} \nvdash \neg\mathsf{G}$, budući da bi inače PA dokazala neistinitu rečenicu, što se također protivi pretpostavci da je PA adekvatna teorija.

Primijetimo kako za dokaz da je G istinita ako i samo ako nije dokaziva nismo koristili jače svojstvo da formula $\mathsf{Gdl}(\mathsf{x}, \mathsf{y})$ *definira* relaciju $Gdl(m, n)$, već samo da je *izražava*. Dakle, za gornji dokaz nepotpunosti Peanove aritmetike dovoljan nam je slabiji uvjet na dokazivost teorije (dovoljno je da primitivno rekurzivne funkcije budu izrazive u L_A), ali potrebna je jača pretpostavka da je PA adekvatna na standardnom modelu!

Gödel je izvorno dokaz svog prvog teorema proveo koristeći samo sintaktičku pretpostavku o konzistentnosti teorije, bez ikakvih dodatnih pretpostavki o istinitosti aksioma teorije na standardnom modelu. Slabiji uvjet (konzistentnost umjesto adekvatnosti), međutim, ne dolazi bez cijene. Kao što ćemo vidjeti u nastavku, postavlja se jači zahtjev za moći dokazivanja teorije – potrebno je da ona bude primitivno rekurzivno adekvatna.

Počevši sa sljedećom propozicijom, u ovom se radu fokusiramo na sintaktički dokaz Gödelovih teorema.

Propozicija 5.2. *Ako je* PA *konzistentna teorija, tada* $\mathsf{PA} \nvdash \mathsf{G}$.

Dokaz. Pretpostavimo suprotno: $\mathsf{PA} \vdash \mathsf{G}$, odnosno $\mathsf{PA} \vdash \neg\exists \mathsf{x}\mathsf{Gdl}(\mathsf{x}, \ulcorner \mathsf{U} \urcorner)$. Budući da je G dijagonalizacija formule U, a G je dokaziva, zaključujemo da postoji neki prirodan broj m za koji vrijedi $Gdl(m, \ulcorner \mathsf{U} \urcorner)$. Budući da je relacija $Gdl(m, n)$ definabilna (PA je primitivno rekurzivno adekvatna teorija) pomoću formule $\mathsf{Gdl}(\mathsf{x}, \mathsf{y})$, vrijedi $\mathsf{PA} \vdash \mathsf{Gdl}(\overline{\mathsf{m}}, \ulcorner \mathsf{U} \urcorner)$. Međutim, iz $\neg\exists \mathsf{x}\mathsf{Gdl}(\mathsf{x}, \ulcorner \mathsf{U} \urcorner)$ dobiva se (zamjenom egzistencijalnog kvantifikatora univerzalnim te upotrebom univerzalne instancijacije) i $\mathsf{PA} \vdash \neg\mathsf{Gdl}(\overline{\mathsf{m}}, \ulcorner \mathsf{U} \urcorner)$. Ovime smo dobili da je PA nekonzistentna teorija, što je protivno početnoj pretpostavci. Stoga zaključujemo da $\mathsf{PA} \nvdash \mathsf{G}$. □

Ovime je dokazan jedan dio teorema 5.1 za Peanovu aritmetiku. Kako bi se dokazalo da $\mathsf{PA} \nvdash \neg\mathsf{G}$, potreban je nešto stroži uvjet ω-konzistentnosti (u odjeljku 5.4 pokazuje se da postoji rečenica R takva da je dovoljno da PA bude konzistentna kako bi vrijedilo $\mathsf{PA} \nvdash \mathsf{R}$ i $\mathsf{PA} \nvdash \neg\mathsf{R}$).

Definicija 5.1. Za aritmetičku teoriju T kažemo da je ω-nekonzistentna ako postoji formula $\varphi(\mathsf{x})$ takva da $T \vdash \varphi(\overline{\mathsf{m}})$ za svaki prirodan broj m, ali i $T \vdash \neg\forall \mathsf{x}\varphi(\mathsf{x})$.

Teorije T je ω-konzistentna ako nije ω-nekonzistentna. Budući da se, ako je teorija T nekonzistentna, može dokazati svaka formula, nekonzistentnost povlači ω-nekonzistentnost. Obratom po kontrapoziciji dobiva se da ω-konzistentnost povlači konzistentnost teorije. ω-konzistentnost je, dakle, jači uvjet od obične konzistentnosti. Doista, promotrimo teoriju koja se dobiva iz PA dodavanjem rečenice $\neg\mathsf{G}$ kao novog aksioma, tj. teoriju $\mathsf{PA}' \stackrel{\text{def}}{=} \mathsf{PA} + \neg\mathsf{G}$. Pretpostavimo da je PA konzistentna teorija. Budući da je $\mathsf{PA} \nvdash \mathsf{G}$, PA' je konzistentna teorija. Nadalje, trivijalno vrijedi $\mathsf{PA}' \vdash \neg\mathsf{G}$, odnosno $\mathsf{PA}' \vdash \neg\forall\mathsf{x}\neg\mathsf{Gdl}(\mathsf{x}, \ulcorner\mathsf{U}\urcorner)$. Međutim, kako PA' proširuje PA, a $\mathsf{PA} \nvdash \mathsf{G}$, dobivamo da i PA' dokazuje $\neg\mathsf{Gdl}(\overline{\mathsf{m}}, \ulcorner\mathsf{U}\urcorner)$ za svaki prirodni broj m (razmišljanje je slično kao i kod dokaza propozicije 5.2 – ne postoji prirodan broj m tako da vrijedi $Gdl(m, \ulcorner\mathsf{U}\urcorner)$, pa navedena tvrdnja proizlazi iz definabilnosti te relacije u PA). Zadnje dvije tvrdnje čine PA' ω-nekonzistentnom teorijom. Zaključujemo da, ako je teorija PA konzistentna, tada postoji teorija $\mathsf{PA} + \neg\mathsf{G}$ koja je konzistentna, ali nije i ω-konzistentna.

Propozicija 5.3. *Ako je* PA *ω-konzistentna teorija, tada* $\mathsf{PA} \nvdash \neg\mathsf{G}$.

Dokaz. Opet pretpostavimo suprotno: neka vrijedi $\mathsf{PA} \vdash \neg\mathsf{G}$. PA je prema pretpostavci ω-konzistentna, pa je i konzistentna, što znači da $\mathsf{PA} \nvdash \mathsf{G}$ (u protivnom PA ne bi bila konzistentna). Dokaz sada slijedi na jednak način kao i u prethodnom razmatranju teorije $\mathsf{PA} + \neg\mathsf{G}$: kako rečenica G nije dokaziva u PA, $\mathsf{PA} \vdash \neg\mathsf{Gdl}(\overline{\mathsf{m}}, \ulcorner\mathsf{U}\urcorner)$ za svaki m. Rečenica $\neg\mathsf{G}$ i $\neg\forall\mathsf{x}\neg\mathsf{Gdl}(\mathsf{x}, \ulcorner\mathsf{U}\urcorner)$ logički su ekvivalentne, pa dobivamo da je PA ω-nekonzistentna, što je kontradiktorno pretpostavci iz iskaza propozicije. Dakle, zaključujemo $\mathsf{PA} \nvdash \neg\mathsf{G}$. $\square$

Kako je samo jedna od zatvorenih formula G i $\neg\mathsf{G}$ istinita (pod standardnom interpretacijom), možemo reći da postoji *istinita* rečenica koja *nije dokaziva* u PA (pod uvjetom da je ona ω-konzistentna).

Propozicijama 5.2 i 5.3 dokazan je prvi teorem nepotpunosti za Peanovu aritmetiku. Na jednak način teorem se dokazuje i za proizvoljnu konzistentnu, primitivno rekurzivno adekvatnu te primitivno rekurzivno aksiomatizabilnu teoriju T. Za svaku takvu teoriju postoji primitivno rekurzivna relacija $Prf_T(m, n)$, pa tako i $Gdl_T(m, n)$. Isto tako postoji i L_A formula $\mathsf{Gdl}_\mathsf{T}(\mathsf{x}, \mathsf{y})$ koja definira relaciju $Gdl_T(m, n)$ u teoriji T. Sada na isti način možemo definirati Gödelovu rečenicu za teoriju T, G_T, a nepotpunost te teorije dokazuje se na jednak način kao i za PA (propozicije 5.2 i 5.3).

Gornji rezultat odražava se i u činjenici da je svaka (ω-)konzistentna, p.r. aksiomatizabilna i p.r. adekvatna teorija T ne samo nepotpuna, već se ne može ni proširiti do potpune teorije! Uzmimo primjerice teoriju PA', definiranu ranije kao teoriju koja se dobiva iz PA dodavanjem $\neg\mathsf{G}$ kao aksioma. Ako je PA konzistentna, i PA' je konzistentna teorija. PA' je i p.r. adekvatna teorija (budući da je proširenje od PA). Konačno, PA' je i p.r. aksiomatizabilna – relacija $Aksiom_{\mathsf{PA}'}(n) \stackrel{\text{def}}{=} Aksiom_{\mathsf{PA}}(n) \vee n = \ulcorner\neg\mathsf{G}\urcorner$ je očito primitivno rekurzivna. Budući da PA' zadovoljava potrebne uvjete, moguće je konstruirati rečenicu $\mathsf{G}_{\mathsf{PA}'}$ takvu da $\mathsf{PA}' \nvdash \mathsf{G}_{\mathsf{PA}'}$ ako je PA' konzistentna, a $\mathsf{PA}' \nvdash \neg\mathsf{G}_{\mathsf{PA}'}$ ako je i ω-konzistentna.

Zanimljivo je vidjeti kako aritmetička teorija T može izbjeći utjecaj Gödelovih teorema samo ako prestane biti p.r. adekvatna, aksiomatizabilna ili jednostavno postane nekonzistentna. Teorija koja nije p.r. adekvatna vrlo je slaba – čak je i teorija Q koja ne može dokazati jednostavne generalizacije poput $\forall \mathsf{x}(0+\mathsf{x}=\mathsf{x})$ p.r. adekvatna. Ako teorija nije aksiomatizabilna, ona postaje praktično neupotrebljivom – za niz formula nije moguće reći predstavlja li uopće valjan dokaz. Konačno, nije ni potrebno isticati kako je nekonzistentnost najgore svojstvo koje se može pripisati nekoj aksiomatskoj teoriji općenito. Zaključujemo da se kod svakog ozbiljnijeg pokušaja aksiomatizacije aritmetike nailazi na istu prepreku – bez obzira na odabir aksioma, uvijek će postojati rečenica koja je istinita (na standardnom modelu), a nije dokaziva u teoriji.

5.2. Dijagonalna lema

U prethodnom odjeljku pokazano je kako je za proizvoljnu konzistentnu, p.r. aksiomatizabilnu i p.r. adekvatnu teoriju T moguće definirati Gödelovu rečenicu G_T takvu da $T \nvdash \mathsf{G}_T$, a ako je T ω-konzistentna teorija, tada i $T \nvdash \neg\mathsf{G}_T$. Ovdje se dokazuje još jedan iznimno važan rezultat – tzv. *dijagonalna lema* – pomoću kojeg se također može dokazati Gödelov prvi teorem nepotpunosti, a i mnogi vezani rezultati:

Teorem 5.4 (Dijagonalna lema)**.** *Neka je T konzistentna, p.r. adekvatna teorija, a $\varphi(\mathsf{x})$ proizvoljna formula jezika teorije T s jednom slobodnom varijablom. Postoji rečenica γ takva da vrijedi $T \vdash \gamma \leftrightarrow \varphi(\ulcorner\gamma\urcorner)$.*

Kasnije ćemo vidjeti kako postojanje Gödelove rečenice G_T slijedi iz teorema 5.4 koristeći negaciju predikata dokazivosti. Međutim, prvo dokazujemo teorem:

Dokaz. Budući da je funkcija $diag(n)$ koja daje Gödelov broj dijagonalizacije formule jezika teorije T čiji je Gödelov broj n primitivno rekurzivna (vidi odjeljak 3.4), ona je reprezentabilna u teoriji T pomoću formule $\mathsf{Diag}(\mathsf{x},\mathsf{y})$. Koristeći tu formulu definiramo

$$\psi(\mathsf{y}) \overset{\text{def}}{=} \forall \mathsf{z}[\mathsf{Diag}(\mathsf{y},\mathsf{z}) \to \varphi(\mathsf{z})]$$

Primijetimo da je formula $\psi(\mathsf{y})$ istinita ako je istinita $\varphi(\mathsf{z})$, gdje je z numeral Gödelovog broja dijagonalizacije formule kodiranog s y. Slično kao i kod konstrukcije rečenice G u prethodnom odjeljku, sljedeći korak u dokazu je dijagonalizacija formule $\psi(\mathsf{y})$.

$$\gamma \overset{\text{def}}{=} \exists \mathsf{y}(\mathsf{y} = \ulcorner\psi\urcorner \wedge \psi)$$

Tako definirana rečenica γ logički je ekvivalentna rečenici $\psi(\ulcorner\psi\urcorner)$, pa T i dokazuje tu ekvivalenciju: $T \vdash \gamma \leftrightarrow \forall \mathsf{z}[\mathsf{Diag}(\ulcorner\psi\urcorner,\mathsf{z}) \to \varphi(\mathsf{z})]$. Nadalje, iz same definicije rečenice γ i funkcije $diag(n)$ proizlazi $diag(\ulcorner\psi\urcorner) = \ulcorner\gamma\urcorner$. Budući da $\mathsf{Diag}(\mathsf{x},\mathsf{y})$ reprezentira funkciju $diag(n)$, dobiva se $T \vdash \forall \mathsf{z}(\mathsf{Diag}(\ulcorner\psi\urcorner,\mathsf{z}) \leftrightarrow \mathsf{z} = \ulcorner\gamma\urcorner)$. Zaključujući unutar teorije T, brzo dolazimo do traženog rezultata:

1.	$\forall \mathsf{z}(\mathsf{Diag}(\ulcorner\psi\urcorner, \mathsf{z}) \leftrightarrow \mathsf{z} = \ulcorner\gamma\urcorner)$	(reprezentabilnost)
2.	$\gamma \leftrightarrow \forall \mathsf{z}(\mathsf{Diag}(\ulcorner\psi\urcorner, \mathsf{z}) \to \varphi(\mathsf{z}))$	(iz definicije od γ)
3.	$\gamma \leftrightarrow \forall \mathsf{z}(\mathsf{z} = \ulcorner\gamma\urcorner \to \varphi(\mathsf{z}))$	(iz 1 i 2)
4.	$\gamma \leftrightarrow \varphi(\ulcorner\gamma\urcorner)$	(iz 3, logička ekvivalencija)

Ovime je dokazano da je, za proizvoljnu $\varphi(\mathsf{x})$, moguće definirati rečenicu γ tako da $T \vdash \gamma \leftrightarrow \varphi(\ulcorner\gamma\urcorner)$. $\square$

Katkad se za gornji teorem koristi i naziv *teorem o fiksnoj točki*, budući da se rečenica γ čije postojanje teorem garantira može smatrati fiksnom točkom za formulu $\varphi(\mathsf{x})$.

Dijagonalna lema veoma je koristan alat. U nastavku ovog poglavlja koristimo je za dokaz mnogih tvrdnji.

5.3. Predikat dokazivosti

Formulu $\mathsf{U}(\mathsf{y})$ u odjeljku 5.1 definirali smo indirektno preko formule $\mathsf{Prf}(\mathsf{x}, \mathsf{y})$ (koja izražava numeričku relaciju $Prf(m, n)$) na način da je $\mathsf{U}(\mathsf{y})$ istinita ako i samo ako ne postoji dokaz u PA dijagonalizacije formule s Gödelovim brojem y. Ovdje na sličan način definiramo numerički predikat $Prov_T(n)$:

$$Prov_T(n) \stackrel{\text{def}}{=} \exists x Prf_T(x, n)$$

Vidimo da $Prov_T(n)$ vrijedi onda kada je rečenica jezika teorije T s Gödelovim brojem n *dokaziva* u teoriji T. Ovakav predikat nazivamo *predikatom dokazivosti.*

Budući da je relacija $Prf_T(m, n)$ primitivno rekurzivna (ako je T p.r. aksiomatizabilna), a pod pretpostavkom da je T i konzistentna, p.r. adekvatna teorija, ta je relacija definabilna u teoriji T pomoću formule $\mathsf{Prf_T}(\mathsf{x}, \mathsf{y})$. Posebno, formula $\mathsf{Prf_T}(\mathsf{x}, \mathsf{y})$ izražava relaciju $Prf_T(m, n)$, iz čega odmah slijedi da formula $\mathsf{Prov_T}(\mathsf{x}) \stackrel{\text{def}}{=} \exists \mathsf{y}\, \mathsf{Prf_T}(\mathsf{y}, \mathsf{x})$ izražava relaciju $Prov_T(n)$. Važno je naglasiti kako to ne znači da $\mathsf{Prov_T}(\mathsf{x})$ ujedno i definira relaciju $Prov_T(n)$ – dapače, kasnije pokazujemo kako ova relacija uopće nije definabilna u T.

Koristeći formulu $\mathsf{Prov_T}(\mathsf{x})$ i dijagonalnu lemu pokazat ćemo još jedan dokaz Gödelovog prvog teorema nepotpunosti, no dokažimo još prije toga dva korisna rezultata. U ovom poglavlju ćemo dalje pretpostavljati da radimo s proizvoljnom konzistentnom, p.r. aksiomatizabilnom i p.r. adekvatnom aritmetičkom teorijom T, pa se to neće više posebno naglašavati (osim svojstva ω-potpunosti kada će biti potrebno).

Lema 5.5. *Neka je φ proizvoljna rečenica jezika teorije T. Ako $T \vdash \varphi$, tada $T \vdash \mathsf{Prov_T}(\ulcorner\varphi\urcorner)$.*

Dokaz. Budući da je rečenica φ dokaziva u T, postoji prirodan broj m takav da vrijedi $Prf_T(m, \ulcorner\varphi\urcorner)$. Kako je T p.r. adekvatna teorija, znamo da vrijedi i $T \vdash \mathsf{Prf_T}(\overline{\mathsf{m}}, \ulcorner\varphi\urcorner)$. Sada se odmah dobiva $T \vdash \exists \mathsf{x} \mathsf{Prf_T}(\mathsf{x}, \ulcorner\varphi\urcorner)$, odnosno $T \vdash \mathsf{Prov_T}(\ulcorner\varphi\urcorner)$. □

Uočimo kako je $\mathsf{Prov_T}(\mathsf{x})$ Σ_1 formula. Ako $T \vdash \varphi$, tada vrijedi $Prov_T(\ulcorner\varphi\urcorner)$, pa tvrdnja gornje leme odmah slijedi iz korolara 4.12!

Lema 5.6. *Neka je φ proizvoljna rečenica jezika teorije T. Ako je T ω-konzistentna i $T \vdash \mathsf{Prov_T}(\ulcorner\varphi\urcorner)$, tada $T \vdash \varphi$.*

Dokaz. Kontradikcije radi, pretpostavimo da $T \nvdash \varphi$. U tom slučaju ne postoji prirodan broj m takav da vrijedi $Prf_T(m, \ulcorner\varphi\urcorner)$, pa $T \vdash \neg\mathsf{Prf_T}(\overline{\mathsf{m}}, \ulcorner\varphi\urcorner)$ za svaki m. Međutim, prema pretpostavci $T \vdash \exists \mathsf{x} \mathsf{Prf_T}(\mathsf{x}, \ulcorner\varphi\urcorner)$, pa je T ω-nekonzistentna. To je proturječno drugoj pretpostavci, iz čega zaključujemo da $T \vdash \varphi$. □

Promotrimo *negaciju* formule $\mathsf{Prov_T}(\mathsf{x})$ i njezinu fiksnu točku – to je rečenica za koju T *dokazuje* da je istinita ako i samo ako nije dokaziva u T. Gödelov prvi teorem nepotpunosti (teorem 5.1) sada možemo dokazati i na sljedeći način:

Dokaz. Dijagonalna lema (5.4) dokazuje egzistenciju rečenice $\mathsf{G_T}$ jezika teorije T za koju vrijedi

$$T \vdash \mathsf{G_T} \leftrightarrow \neg\mathsf{Prov_T}(\ulcorner\mathsf{G_T}\urcorner). \tag{5.1}$$

a) Pretpostavimo da $T \vdash \mathsf{G_T}$. Iz gornje ekvivalencije slijedi $T \vdash \neg\mathsf{Prov_T}(\ulcorner\mathsf{G_T}\urcorner)$. Međutim, iz leme 5.5 dobiva se i $T \vdash \mathsf{Prov_T}(\ulcorner\mathsf{G_T}\urcorner)$, pa je T nekonzistentna teorija, što se protivi pretpostavci. Zaključujemo, dakle, da $T \nvdash \mathsf{G_T}$.

b) Neka je T ω-konzistentna teorija. Pretpostavimo da $T \vdash \neg\mathsf{G_T}$. Slično kao i gore, sada se dobiva $T \vdash \mathsf{Prov_T}(\ulcorner\mathsf{G_T}\urcorner)$. Iz leme 5.6 slijedi $T \vdash \mathsf{G_T}$, što je proturječno pretpostavci o konzistentnosti teorije T. Zaključujemo: $T \nvdash \neg\mathsf{G_T}$.

Ovime je dokazano da postoji rečenica $\mathsf{G_T}$ takva da $T \nvdash \mathsf{G_T}$ te, ako je T ω-konzistentna teorija, $T \nvdash \neg\mathsf{G_T}$. □

Za razliku od dokaza u odjeljku 5.1, gornji dokaz nije konstruktivan – dijagonalna lema nam samo garantira postojanje fiksne točke za $\neg\mathsf{Prov_T}(\mathsf{x})$, a ne daje i njezin oblik. Za teoriju PA, ta fiksna točka jest upravo rečenica G definirana u odjeljku 5.1 (doista, može se pokazati kako vrijedi $\mathsf{PA} \vdash \mathsf{G} \leftrightarrow \neg\mathsf{Prov}(\ulcorner\mathsf{G}\urcorner)$; vidi [8], odjeljak 20.4).

Koristeći dijagonalnu lemu možemo dokazati i sljedeći veoma važan i zanimljiv teorem:

Teorem 5.7. *Neka je T proizvoljna konzistentna, p.r. aksiomatizabilna i p.r. adekvatna teorija. Predikat dokazivosti za teoriju T, $Prov_T(n)$, nije definabilan u T.*

Dokaz. Pretpostavimo suprotno – neka formula $\mathsf{P_T}(\mathsf{x})$ definira relaciju $Prov_T(n)$. Iz dijagonalne leme upotrijebljene nad negacijom formule $\mathsf{P_T}(\mathsf{x})$ zaključujemo da postoji rečenica φ takva da

$$T \vdash \varphi \leftrightarrow \neg \mathsf{P_T}(\ulcorner \varphi \urcorner). \tag{5.2}$$

Koristeći pretpostavku da $\mathsf{P_T}(\mathsf{x})$ definira $Prov_T(n)$, dokazujemo po slučajevima:

a) $T \vdash \varphi$.

   Sada vrijedi $Prov_T(\ulcorner \varphi \urcorner)$, pa $T \vdash \mathsf{P_T}(\ulcorner \varphi \urcorner)$. Iz (5.2) se dalje dobiva $T \vdash \neg\varphi$. Međutim, to znači da je T nekonzistentna, što je protivno pretpostavci.

b) $T \nvdash \varphi$.

   Budući da sada $Prov_T(\ulcorner \varphi \urcorner)$ ne vrijedi, a $\mathsf{P_T}(\mathsf{x})$ definira $Prov_T(n)$, dobivamo $T \vdash \neg\mathsf{P_T}(\ulcorner \varphi \urcorner)$. Slično kao i gore, iz (5.2) se sada dobiva $T \vdash \varphi$, tj. T je nekonzistentna – kontradikcija.

U oba smo slučaja dobili kontradikciju pa zaključujemo da ne postoji formula u jeziku teorije T koja definira relaciju $Prov_T(n)$. □

Iz gornjeg teorema vidimo da, iako postoji Σ_1 formula $\mathsf{Prov_T}(\mathsf{x})$ koja *izražava* relaciju $Prov_T(n)$, ta formula ju ne definira! Ako pomnije promotrimo rezultate 4. poglavlja (osobito odjeljka 4.4), primijetit ćemo da se tamo nigdje ne implicira da teorija kao što je Q ispravno *odlučuje* svaku Σ_1 rečenicu.[3]

Ako je T konzistentna, p.r. aksiomatizabilna i p.r. adekvatna teorija, tada je po definiciji svaka primitivno rekurzivna relacija definabilna u T. Međutim, upravo smo pokazali da relacija $Prov_T(n)$ nije definabilna u takvoj teoriji T. Sada odmah dobivamo sljedeći rezultat:

Korolar 5.8. *Za svaku konzistentnu, p.r. aksiomatizabilnu i p.r. adekvatnu teoriju T, relacija $Prov_T(n)$ nije primitivno rekurzivna.*

5.4. Gödel-Rosserov teorem

Rečenica G (odjeljak 5.1) konstruirana je tako da bude nedokaziva u PA ako je PA konzistentna teorija, a da njena negacija također bude nedokaziva ako je PA ω-konzistentna. J. B. Rosser pokazao je 1936. godine kako je moguće konstruirati rečenicu $\mathsf{R_T}$ tako da je dovoljan slabiji uvjet konzistentnosti teorije T da bi se dokazalo da $\mathsf{R_T}$ nije odlučiva u T.

Za razliku od Gödelove rečenice G koja indirektno za sebe tvrdi da nije dokaziva, Rosserova rečenica R govori da, u slučaju da je R dokaziva, tada već postoji dokaz njezine negacije. Preciznije, R tvrdi da, ako postoji n koji je Gödelov broj

[3] U odjeljku 4.4 dokazali smo da je svaka Σ_1 *funkcija* reprezentabilna u Q, što je nužno, ali ne i dovoljno da Q ispravno odlučuje svaku Σ_1 rečenicu!

dokaza rečenice R, tada postoji $m < n$ koji je Gödelov broj dokaza negacije te rečenice.

U ovom odjeljku dokazujemo da ni $\mathsf{R_T}$, a ni $\neg\mathsf{R_T}$ nisu dokazive u T. Slično kao i kod dokaza Gödelovog prvog teorema nepotpunosti u prethodnom odjeljku, rečenicu $\mathsf{R_T}$ ovdje ne definiramo izravno, već njezino postojanje slijedi iz dijagonalne leme (5.4).

Teorem 5.9 (Gödel-Rosserov teorem)**.** *Ako je T konzistentna, p.r. aksiomatizabilna i p.r. adekvatna teorija, onda postoji rečenica $\mathsf{R_T}$ jezika teorije T takva da $T \nvdash \mathsf{R_T}$ i $T \nvdash \neg\mathsf{R_T}$.*

Dokaz. Definirajmo prvo $\overline{Prf}_T(m,n) \overset{\mathrm{def}}{=} Prf_T(m, \ulcorner\neg\urcorner * n)$. Ova relacija vrijedi ako je m kôd dokaza *negacije* formule s Gödelovim brojem n. Relacija $\overline{Prf}_T(m,n)$ je primitivno rekurzivna, pa postoji formula $\overline{\mathsf{Prf}}_\mathsf{T}(\mathsf{x},\mathsf{y})$ koja je definira u T.

Definirajmo sada formulu $\mathsf{RProv_T(x)}$:

$$\mathsf{RProv_T(x)} \overset{\mathrm{def}}{=} \exists \mathsf{z}[\mathsf{Prf_T(z,x)} \wedge \neg(\exists \mathsf{y} \le \mathsf{z})\overline{\mathsf{Prf}}_\mathsf{T}(\mathsf{y},\mathsf{x})]$$

Za formulu $\mathsf{RProv_T(x)}$ kažemo da izražava *Rosserov predikat dokazivosti*: $\mathsf{RProv_T}(\overline{\mathsf{n}})$ istinito je ako i samo ako postoji prirodan broj m, Gödelov broj dokaza rečenice kodirane brojem n, te nijedan broj manji od m ne kodira dokaz negacije te rečenice.

Označimo sada s $\mathsf{R_T}$ fiksnu točku za *negaciju* Rosserovog predikata dokazivosti (njezinu egzistenciju garantira dijagonalna lema). Vrijedi

$$T \vdash \mathsf{R_T} \leftrightarrow \neg\mathsf{RProv_T}(\ulcorner \mathsf{R_T} \urcorner). \tag{5.3}$$

Primijetimo da su $\forall \mathsf{z}[\mathsf{Prf_T(z,x)} \to (\exists \mathsf{y} \le \mathsf{z})\overline{\mathsf{Prf}}_\mathsf{T}(\mathsf{y},\mathsf{x})]$ i $\neg\mathsf{RProv_T(x)}$ logički ekvivalentne formule. Dakle, vidimo da teorija T *dokazuje* da je $\mathsf{R_T}$ istinita ako i samo ako vrijedi da, ako je $\mathsf{R_T}$ dokaziva, tada postoji "manji" dokaz negacije te formule.

Sada je još potrebno dokazati da $T \nvdash \mathsf{R_T}$ i $T \nvdash \neg\mathsf{R_T}$:

a) Pretpostavimo suprotno: $T \vdash \mathsf{R_T}$. Iz ovoga odmah slijedi da postoji prirodan broj n takav da vrijedi $Prf_T(n, \ulcorner \mathsf{R_T} \urcorner)$, pa $T \vdash \mathsf{Prf_T}(\overline{\mathsf{n}}, \ulcorner \mathsf{R_T} \urcorner)$. Iz (5.3) se pak dobiva $T \vdash \neg\mathsf{RProv_T}(\ulcorner \mathsf{R_T} \urcorner)$.

   Kako je T konzistentna teorija, ona sada ne može dokazati i negaciju rečenice $\mathsf{R_T}$. Na sličan način kao i ranije sada dobivamo da, posebno, za svaki $m \le n$ vrijedi $T \vdash \neg\overline{\mathsf{Prf}}_\mathsf{T}(\overline{\mathsf{m}}, \ulcorner \mathsf{R_T} \urcorner)$. Budući da je T p.r. adekvatna teorija, ona je i uređajno adekvatna (vidi [8]), pa za nju vrijede svojstva iz propozicije 4.7. Iz točke 3 te propozicije dobivamo $T \vdash (\forall \mathsf{y} \le \overline{\mathsf{n}})\neg\overline{\mathsf{Prf}}_\mathsf{T}(\mathsf{y}, \ulcorner \mathsf{R_T} \urcorner)$, odnosno $T \vdash \neg(\exists \mathsf{y} \le \overline{\mathsf{n}})\overline{\mathsf{Prf}}_\mathsf{T}(\mathsf{y}, \ulcorner \mathsf{R_T} \urcorner)$. Kombinacijom ovog rezultata s $T \vdash \mathsf{Prf_T}(\overline{\mathsf{n}}, \ulcorner \mathsf{R_T} \urcorner)$ i dodavanjem egzistencijalne kvantifikacije dobiva se, međutim, $T \vdash \mathsf{RProv_T}(\ulcorner \mathsf{R_T} \urcorner)$. Dakle, slijedi da je, protivno pretpostavci, teorija T nekonzistentna. Zaključujemo da mora vrijediti $T \nvdash \mathsf{R_T}$.

b) Pretpostavimo da $T \vdash \neg \mathsf{R_T}$. Kao i gore, iz (5.3) se u ovom slučaju dobiva $T \vdash \mathsf{RProv_T}(\ulcorner \mathsf{R_T} \urcorner)$, a iz definabilnosti relacije $\overline{Prf}_T(m,n)$ u T slijedi $T \vdash \overline{\mathsf{Prf}}_\mathsf{T}(\overline{\mathsf{n}}, \ulcorner \mathsf{R_T} \urcorner)$.

   Pretpostavka o konzistentnosti teorije T dalje povlači $T \nvdash \mathsf{R_T}$ pa, slično kao i prije, $T \vdash (\forall \mathsf{z} \leq \overline{\mathsf{n}}) \neg \mathsf{Prf_T}(\mathsf{z}, \ulcorner \mathsf{R_T} \urcorner)$. Sada dokazujemo unutar teorije T:

1.	$\forall \mathsf{z}(\mathsf{z} \leq \overline{\mathsf{n}} \to \neg \mathsf{Prf_T}(\mathsf{z}, \ulcorner \mathsf{R_T} \urcorner))$	(definicija)
2.	$\forall \mathsf{z}(\mathsf{Prf_T}(\mathsf{z}, \ulcorner \mathsf{R_T} \urcorner) \to \neg(\mathsf{z} \leq \overline{\mathsf{n}}))$	(obrat)
3.	$\forall \mathsf{z}(\mathsf{z} \leq \overline{\mathsf{n}} \vee \overline{\mathsf{n}} \leq \mathsf{z})$	(propozicija 4.7)
4.	$\forall \mathsf{z}(\neg(\mathsf{z} \leq \overline{\mathsf{n}}) \to \overline{\mathsf{n}} \leq \mathsf{z})$	(iz 3)
5.	$\forall \mathsf{z}(\mathsf{Prf_T}(\mathsf{z}, \ulcorner \mathsf{R_T} \urcorner) \to \overline{\mathsf{n}} \leq \mathsf{z})$	(iz 2 i 4)
6.	$\overline{\mathsf{Prf}}_\mathsf{T}(\overline{\mathsf{n}}, \ulcorner \mathsf{R_T} \urcorner)$	(dokazano gore)
7.	$\forall \mathsf{z}(\mathsf{Prf_T}(\mathsf{z}, \ulcorner \mathsf{R_T} \urcorner) \to \exists \mathsf{y}(\mathsf{y} \leq \mathsf{z} \wedge \overline{\mathsf{Prf}}_\mathsf{T}(\mathsf{y}, \ulcorner \mathsf{R_T} \urcorner)))$	(iz 5 i 6)
8.	$\neg \mathsf{RProv_T}(\ulcorner \mathsf{R_T} \urcorner)$	(iz 7)

   Ovime je pokazano da i $T \vdash \neg \mathsf{RProv_T}(\ulcorner \mathsf{R_T} \urcorner)$, pa je T nekonzistentna, što je kontradiktorno pretpostavci. Dakle, $T \nvdash \neg \mathsf{R_T}$.

□

5.5. Tarskijev teorem o nedefinabilnosti aritmetičke istine

Koristeći dijagonalnu lemu, na kraju ovog poglavlja dokazujemo jedan zanimljiv rezultat vezan uz pojam aritmetičke istine.

Neka je $True_L(n)$ relacija koja vrijedi ako i samo ako je n Gödelov broj rečenice jezika L koja je istinita pod standardnom interpretacijom ugrađenom u taj jezik. Pretpostavimo da postoji formula $\mathsf{True_L}(\mathsf{x})$ jezika L koja *izražava* tu relaciju. Svaka formula φ jezika L istinita je, dakle, ako i samo ako je $\mathsf{True_L}(\ulcorner \varphi \urcorner)$ istinita. Drugim riječima, za svaku rečenicu φ, $\mathsf{True_L}(\ulcorner \varphi \urcorner) \leftrightarrow \varphi$ je istinita formula.

Definicija 5.2. Kažemo da teorija T *definira istinu* za svoj jezik L ako i samo ako postoji L-formula $\mathsf{True_L}(\mathsf{x})$ takva da $T \vdash \mathsf{True_L}(\ulcorner \varphi \urcorner) \leftrightarrow \varphi$ za svaku rečenicu φ jezika L.

Primijetimo kako je ovo svojstvo posve sintaktičko – odnosi se na *viđenje istinitosti teorije* T.

Teorem 5.10 (Tarskijev teorem)**.** *Nijedna konzistentna, p.r. aksiomatizabilna i p.r. adekvatna aritmetička teorija T ne definira istinu za svoj jezik.*

Dokaz. Neka je T proizvoljna teorija koja zadovoljava zadane uvjete. Pretpostavimo suprotno. Neka je $\mathsf{True_L}(\mathsf{x})$ formula jezika teorije T takva da $T \vdash$

$\mathsf{True_L}(\ulcorner\varphi\urcorner) \leftrightarrow \varphi$ za svaku rečenicu φ. Prema dijagonalnoj lemi, postoji rečenica γ takva da $T \vdash \gamma \leftrightarrow \neg\mathsf{True_L}(\ulcorner\gamma\urcorner)$, no kako po pretpostavci T definira istinu za svoj jezik, vrijedi i $T \vdash \gamma \leftrightarrow \mathsf{True_L}(\ulcorner\gamma\urcorner)$. Dakle, T je nekonzistentna, protivno pretpostavci. Iz toga zaključujemo da T ne može definirati istinu za svoj jezik. $\square$

Uvedimo sada dodatnu (semantičku) pretpostavku da je aritmetička teorija T adekvatna u odnosu na standardni model (dakle, aksiomi te teorije istiniti su pod standardnom interpretacijom, pa su istiniti i njezini teoremi). Uvjerimo se kako se sada relacija $True_L(n)$ *ne može ni izraziti* u jeziku L te teorije. Doista, ako postoji formula $\mathsf{True_L}(\mathsf{x})$ koja izražava relaciju $True_L(n)$, tada je $\varphi \leftrightarrow \mathsf{True_L}(\ulcorner\varphi\urcorner)$ istinita formula za svaku rečenicu φ. Međutim, $T \vdash \gamma \leftrightarrow \neg\mathsf{True_L}(\ulcorner\gamma\urcorner)$, a teoremi teorije T su istinite formule, pa je tako istinita i rečenica $\gamma \leftrightarrow \neg\mathsf{True_L}(\ulcorner\gamma\urcorner)$. Ovo je, nažalost, proturječno pretpostavci da $\mathsf{True_L}(\mathsf{x})$ izražava relaciju $True_L(n)$.

6 Drugi teorem nepotpunosti

Sadržaj

U prethodnom poglavlju definirali smo L_A rečenicu G te dokazali da, ako je Peanova aritmetika konzistentna, tada $\mathsf{PA} \nvdash \mathsf{G}$, a ako je PA k tome i ω-konzistentna, onda $\mathsf{PA} \nvdash \neg\mathsf{G}$. Kasnije smo tu tvrdnju poopćili i pokazali da je svaka konzistentna, primitivno rekurzivno aksiomatizabilna te primitivno rekurzivno adekvatna teorija nužno nepotpuna.

U ovom poglavlju osvrćemo se na pitanje konzistentnosti Peanove aritmetike i srodnih teorija. Posebno, dokazat ćemo da se konzistentnost teorije PA *ne može dokazati unutar te teorije same*! Generalizirana verzija ove tvrdnje poznata je kao Gödelov drugi teorem nepotpunosti:

Teorem 6.1 (Gödelov drugi teorem nepotpunosti)**.** *Neka je T konzistentna, p.r. aksiomatizabilna i p.r. adekvatna aritmetička teorija koja dopušta indukciju po Σ_1 formulama. Teorija T ne može dokazati svoju konzistentnost, tj. $T \nvdash \mathsf{Con_T}$.*

U iskazu teorema koristimo rečenicu $\mathsf{Con_T}$ koja izražava svojstvo da je T konzistentna teorija. Postavimo prvo $\perp =_{\text{def}} \mathsf{0} = \mathsf{1}$ i definirajmo ovu rečenicu na sljedeći način:

$$\mathsf{Con_T} \stackrel{\text{def}}{=} \neg\mathsf{Prov_T}(\ulcorner \perp \urcorner)$$

Prisjetimo se iz odjeljka 5.3 da je $\mathsf{Prov_T}(\mathsf{x}) =_{\text{def}} \exists \mathsf{y}\, \mathsf{Prf_T}(\mathsf{y}, \mathsf{x})$. Rečenica $\mathsf{Con_T}$ istinita je ako i samo ako $\mathsf{0} = \mathsf{1}$ nije dokazivo u teoriji T. Da ta rečenica izražava svojstvo konzistentnosti teorije T proizlazi iz sljedeće jednostavne leme:

Lema 6.2. *Aritmetička teorija T koja proširuje Robinsonovu aritmetiku Q konzistentna je ako i samo ako $T \nvdash \perp$.*

Dokaz. Ako T nije konzistentna teorija, ona dokazuje svaku formulu, pa tako posebno i $T \vdash \perp$. S druge strane, ako $T \vdash \perp$, tada je T nužno nekonzistentna. Naime, teorija T, budući da dokazuje sve teoreme kao i Q, trivijalno dokazuje i $\forall \mathsf{x}(\mathsf{0} \neq \mathsf{Sx})$, pa tako i $\mathsf{0} \neq \mathsf{1}$. $\square$

U iskazu teorema 6.1 koristimo dodatan uvjet koji nije bio prisutan u teoremima iz 5. poglavlja: traži se da teorija T dopušta barem indukciju po Σ_1 formulama (drugim riječima, T proširuje teoriju $\mathsf{I\Sigma_1}$). Zašto je to potrebno? U sljedećem odjeljku navest ćemo tri *uvjeta dokazivosti* koje zadovoljava svaka p.r. aksiomatizabilna teorija koja proširuje Q i dopušta indukciju po Σ_1 formulama. Ono što je sada ključno je da se Gödelov prvi teorem može dokazati *unutar* takve teorije: $T \vdash \mathsf{Con_T} \to \neg\mathsf{Prov_T}(\ulcorner \mathsf{G_T} \urcorner)$. Iz ove činjenice i dijagonalne leme Gödelov drugi teorem nepotpunosti trivijalno slijedi.

6.1. Löbovi uvjeti dokazivosti

Definicija 6.1. Neka je T konzistentna, p.r. aksiomatizabilna i p.r. adekvatna teorija. Kažemo da teorija T zadovoljava *Löbove uvjete dokazivosti* ako za sve rečenice φ i ψ jezika te teorije vrijede sljedeće tvrdnje:

L1. Ako $T \vdash \varphi$, onda $T \vdash \mathsf{Prov_T}(\ulcorner \varphi \urcorner)$,

L2. $T \vdash \mathsf{Prov_T}(\ulcorner \varphi \to \psi \urcorner) \to (\mathsf{Prov_T}(\ulcorner \varphi \urcorner) \to \mathsf{Prov_T}(\ulcorner \psi \urcorner))$

L3. $T \vdash \mathsf{Prov_T}(\ulcorner \varphi \urcorner) \to \mathsf{Prov_T}(\ulcorner \mathsf{Prov_T}(\ulcorner \varphi \urcorner) \urcorner)$

U odjeljku 5.3 već smo dokazali da prvi Löbov uvjet vrijedi za svaku teoriju T iz gornje definicije (lema 5.5). Preostale dvije tvrdnje zahtjevaju ipak da teorija T bude malo jača. Može se pokazati da je dovoljan dodatni zahtjev da T dopušta indukciju po Σ_1 formulama. Dokaz ove činjenice nešto je složeniji i može se pronaći, primjerice, u [8].

Teorem 6.3. *Löbovi uvjeti dokazivosti vrijede za svaku p.r. aksiomatizabilnu teoriju koja proširuje* Q *i dopušta indukciju po* Σ_1 *formulama.*

Budući da PA sadrži neograničenu indukciju, Löbovi uvjeti dokazivosti vrijede za tu teoriju. Važno je ovdje naglasiti kako je Σ_1-indukcija dovoljan, ali nije i nužan uvjet – može se pokazati da uvjeti dokazivosti vrijede i za neke teorije slabije od $\mathsf{I\Sigma_1}$ (vidi [8], odjeljak 26.5).

Pod pretpostavkom da teorija T zadovoljava uvjete dokazivosti, sada nam je cilj dokazati da je Gödelov prvi teorem nepotpunosti (preciznije, samo jedan njegov smjer) dokaziv unutar te teorije.

Teorem 6.4. *Ako je T konzistentna, p.r. aksiomatizabilna teorija koja proširuje* Q *i zadovoljava Löbove uvjete dokazivosti, onda* $T \vdash \mathsf{Con_T} \to \neg\mathsf{Prov_T}(\ulcorner \mathsf{G_T} \urcorner)$.

Dokaz. Iz dijagonalne leme (5.4) dobiva se $T \vdash \mathsf{G_T} \leftrightarrow \neg\mathsf{Prov_T}(\ulcorner \mathsf{G_T} \urcorner)$. Nadalje, $T \vdash \neg\bot$ (instanca prvog aksioma teorije Q). Također, lako se dobiva da za svaku formulu φ vrijedi $T \vdash \neg\varphi \to (\varphi \to \bot)$, budući da je to valjana formula. Iz uvjeta L1 i L2 te prethodnog izraza slijedi

$$T \vdash \mathsf{Prov_T}(\ulcorner \neg\varphi \urcorner) \to \mathsf{Prov_T}(\ulcorner \varphi \to \bot \urcorner) \tag{6.1}$$

Kratkoće radi, uvedimo oznaku $\Box\varphi$ za $\mathsf{Prov_T}(\ulcorner \varphi \urcorner)$. Primjerice, uvjet L3 možemo zapisati na sljedeći način: $T \vdash \Box\varphi \to \Box\Box\varphi$. Koristeći dijagonalnu lemu i (6.1) sada dokazujemo *unutar* T:

1.	$\mathsf{G_T} \to \neg\Box\mathsf{G_T}$	(iz dijagonalne leme)
2.	$\Box\mathsf{G_T} \to \Box\neg\Box\mathsf{G_T}$	(iz 1, pomoću L1 i L2)
3.	$\Box\neg\Box\mathsf{G_T} \to \Box(\Box\mathsf{G_T} \to \bot)$	(iz 6.1)
4.	$\Box\mathsf{G_T} \to (\Box\Box\mathsf{G_T} \to \Box\bot)$	(iz 2 i 3 te upotrebom L2)
5.	$\Box\mathsf{G_T} \to \Box\Box\mathsf{G_T}$	(L3)
6.	$\Box\mathsf{G_T} \to \Box\bot$	(iz 4 i 5)
7.	$\neg\Box\bot \to \neg\Box\mathsf{G_T}$	(iz 6)

Kako je $\mathsf{Con_T} =_{\text{def}} \neg\Box\bot$, ovime je dokazano da $T \vdash \mathsf{Con_T} \to \neg\mathsf{Prov_T}(\ulcorner \mathsf{G_T} \urcorner)$. □

6.2. Nedokazivost $\mathsf{Con_T}$

Teorem 6.4 govori nam da se Gödelov prvi teorem za teoriju T koja je konzistenta, p.r. aksiomatizabilna, p.r. adekvatna te zadovoljava Löbove uvjete dokazivosti (definicija 6.1) može dokazati unutar same teorije T. Dokaz Gödelovog drugog teorema nepotpunosti, odnosno činjenice da teorija T ne može dokazati $\mathsf{Con_T}$, sada je vrlo jednostavan.

Dokaz. Pretpostavimo, kontradikcije radi, da T može dokazati svoju konzistentnost, tj. $T \vdash \mathsf{Con_T}$. Iz teorema 6.4 se dalje dobiva $T \vdash \neg\mathsf{Prov_T}(\ulcorner \mathsf{G_T} \urcorner)$, gdje je $\mathsf{G_T}$ fiksna točka za $\neg\mathsf{Prov_T}(\mathsf{x})$ čije postojanje dokazuje dijagonalna lema. Upravo iz dijagonalne leme proizlazi $T \vdash \mathsf{G_T} \leftrightarrow \neg\mathsf{Prov_T}(\ulcorner \mathsf{G_T} \urcorner)$, pa sada dobivamo, dakle, $T \vdash \mathsf{G_T}$. Ovaj je rezultat proturječan Gödelovom prvom teoremu nepotpunosti, iz čega zaključujemo da mora vrijediti $T \nvdash \mathsf{Con_T}$. □

Posebno, dokazali smo da vrijedi $\mathsf{PA} \nvdash \mathsf{Con_{PA}}$. Ako pretpostavimo da je PA adekvatna u odnosu na standardni model (svi teoremi teorije istiniti su na standardnom modelu), tada je ona i konzistentna, pa je $\mathsf{Con_{PA}}$ istinita rečenica. U tom je slučaju, dakle, $\mathsf{Con_{PA}}$ još jedan primjer rečenice koja je istinita, a nije dokaziva u PA.

Sljedeći teorem također se jednostavno dokazuje:

Teorem 6.5. *Ako je T konzistentna, p.r. aksiomatizabilna i p.r. adekvatna teorija koja zadovoljava Löbove uvjete dokazivosti, tada $T \vdash \neg\mathsf{Prov_T}(\ulcorner \varphi \urcorner) \to \mathsf{Con_T}$ za svaku rečenicu φ jezika teorije T.*

Dokaz. Neka je φ proizvoljna rečenica jezika teorije T. Ranije smo pokazali da $T \vdash \neg\bot$. Dodavanjem disjunkcije dobivamo $T \vdash \neg\bot \vee \varphi$, odnosno $T \vdash \bot \to \varphi$. Iz uvjeta L1 i L2 (definicija 6.1) slijedi $T \vdash \mathsf{Prov_T}(\ulcorner \bot \urcorner) \to \mathsf{Prov_T}(\ulcorner \varphi \urcorner)$. Obratom po kontrapoziciji odmah se dobiva $T \vdash \neg\mathsf{Prov_T}(\ulcorner \varphi \urcorner) \to \mathsf{Con_T}$, što je i trebalo dokazati. □

Primijetimo da gornji teorem pokazuje da teorija T *zna* da je ona konzistentna ako postoji rečenica φ koju ne može dokazati. Iz teorema 6.5 i drugog teorema nepotpunosti sada očito proizlazi i sljedeća tvrdnja:

Korolar 6.6. *Za svaku rečenicu* φ, $T \nvdash \neg\mathsf{Prov_T}(\ulcorner \varphi \urcorner)$.

Lemom 5.5 dokazali smo da teorija T zna za svaki svoj teorem. S druge strane, sada vidimo da T ne može znati ništa o tome što ona *nije u mogućnosti dokazati.*

Kao što je to slučaj s Gödelovim prvim teoremom, i drugi se teorem nepotpunosti može izvesti unutar teorije T.

Teorem 6.7. $T \vdash \mathsf{Con_T} \to \neg\mathsf{Prov_T}(\ulcorner \mathsf{Con_T} \urcorner)$.

Dokaz. Iz teorema 6.4 i 6.5 slijedi $T \vdash \mathsf{Con_T} \leftrightarrow \neg\mathsf{Prov_T}(\ulcorner \mathsf{G_T} \urcorner)$. Upotrebom dijagonalne leme nad $\neg\mathsf{Prov_T}(\mathsf{x})$ sada se dobiva posebno i $T \vdash \mathsf{Con_T} \to \mathsf{G_T}$. Uvjeti dokazivosti L1 i L2 odmah povlače $T \vdash \mathsf{Prov_T}(\ulcorner \mathsf{Con_T} \urcorner) \to \mathsf{Prov_T}(\ulcorner \mathsf{G_T} \urcorner)$. Obratom po kontrapoziciji iz teorema 6.4 dolazi se do $T \vdash \mathsf{Prov_T}(\ulcorner \mathsf{G_T} \urcorner) \to \neg\mathsf{Con_T}$. Kombinacijom prethodna dva rezultata i obratom po kontrapoziciji dobiva se tvrdnja ovog teorema. □

Na kraju ovog poglavlja osvrnimo se na mogućnost dokazivanja konzistentnosti teorije kao što je Peanova aritmetika. Evidentno $\mathsf{Con_{PA}}$ ne možemo dokazati u nekoj slabijoj teoriji – u tom slučaju bi vrijedilo i $\mathsf{PA} \vdash \mathsf{Con_{PA}}$ (budući da PA dokazuje sve što i slabije teorije), što se protivi Gödelovom drugom teoremu nepotpunosti. S druge strane, drugi teorem nepotpunosti ne pobija mogućnost dokazivanja $\mathsf{Con_{PA}}$ u nekoj jačoj teoriji (kao što je, primjerice, ZFC). Međutim, tada se postavlja pitanje kako dokazati konzistentnost takve jače teorije, a to zasigurno nije lakši posao od dokazivanja konzistentnosti Peanove aritmetike.

Jedina mogućnost koja nam sada preostaje je uzeti teoriju koja je *u nekim pogledima* jača, a u drugim slabija od PA. Drugim riječima, takva teorija ne može dokazati sve što i PA, ali dokazuje i neke tvrdnje koje PA ne može. Upravo je jednu takvu slabiju teoriju (teoriju PRA, tzv. primitivno rekurzivnu aritmetiku), no s dodatkom principa *transfinitne indukcije*, koristio G. Gentzen u svojem čuvenom dokazu konzistentnosti aritmetike iz 1936. godine (vidi [2] i [10] za više detalja).

7 Zaključak

Matematičari su početkom 20. stoljeća nastojali osmisliti aksiomatski sustav u kojem bi se mogla formalizirati cjelokupna matematika. U ovom radu pokazano je kako tako nešto nije ostvarivo već ni za jednostavne teorije poput Robinsonove aritmetike. Dapače, kakav god skup aksioma odabrali (pod uvjetom da rezultirajuća teorija može dokazati barem one teoreme koje i Q), uvijek će postojati istinite aritmetičke tvrdnje koje neće biti moguće dokazati. Dakle, pojmovi istinitosti i dokazivosti, kao što je Gödel pokazao, nikako nisu ekvivalentni.

Gödelovi teoremi nepotpunosti primjenjivi su i na jače teorije, poput primjerice Zermelo-Fraenkelove teorije skupova s aksiomom izbora, u kojoj se može formalizirati većina dosadašnjih matematičkih spoznaja. Naime, u ZFC mogu se izvesti Peanovi aksiomi, pa je ZFC također primitivno rekurzivno adekvatna teorija. Dakako, jezik te teorije različit je od L_A te su funkcije sljedbenika, zbrajanja i množenja drugačije definirane; ipak, postoji rečenica $\mathsf{G}_{\mathsf{ZFC}}$ jezika teorije skupova koja nije dokaziva u ZFC.

Implikacije Gödelovih teorema vrlo su zanimljive. Primjerice, ZFC je dovoljno jaka teorija da se u njoj može govoriti o *modelima* same te teorije. Međutim, kada bi ZFC mogla dokazati postojanje modela za samu sebe, dokazala bi svoju konzistentnost (ona proizlazi iz Gödelovog teorema potpunosti koji se također može formalizirati u ZFC), što bi značilo da je ona u stvari nekonzistentna (posljedica Gödelovog drugog teorema nepotpunosti). Ipak, u ZFC se mogu definirati tzv. *unutrašnji modeli* (koji su klase, a ne skupovi) – jedan takav, u kojem uz aksiome teorije ZFC vrijedi još i *hipoteza kontinuuma*, definirao je sam Gödel 1940. godine. Više o posljedicama Gödelovih teorija u aksiomatskoj teoriji skupova može se pročitati, primjerice, u [3].

Sama rečenica G_{PA}, koja za sebe govori da nije dokaziva, nije matematički posebno zanimljiva tvrdnja. Međutim, nedugo nakon objave Gödelovih rezultata pokazalo se da postoje tvrdnje koje nisu dokazive u PA, a teoremi su nekih drugih grana matematike. Najpoznatiji primjeri su vjerojatno Goodsteinov teorem te verzija Ramseyevog teorema za relativno velike skupove, o kojima se može čitati u [4].

Literatura

[1] G. S. Boolos, J. P. Burgess, R. C. Jeffrey, *Computability and Logic*, 5th Edition, Cambridge University Press, 2007.

[2] S. R. Buss, *Handbook of Proof Theory*, Elsevier Science, 1998.

[3] W. Just, M. Weese, *Discovering Modern Set Theory, Volume I*, American Mathematical Society, 1996.

[4] J. Kovačić, *Nedokazive formule u Peanovoj aritmetici*, diplomski rad, PMF-MO, 2011.

[5] E. Mendelson, *Introduction to Mathematical Logic*, 4th Edition, Chapman & Hall, 1997.

[6] K. H. Rosen, *Elementary Number Theory and Its Applications*, 5th Edition, Addison Wesley, 2005.

[7] M. Sipser, *Introduction to the Theory of Computation*, 2nd Edition, Thomson Course Technology, 2006.

[8] P. Smith, *An Introduction to Gödel's Theorems*, Cambridge University Press, 2007.

[9] R. M. Smullyan, *Gödel's Incompleteness Theorems*, Oxford University Press, 1992.

[10] G. Takeuti, *Proof Theory*, Elsevier Science, 1975.

[11] M. Vuković, *Matematička logika*, Element, Zagreb, 2009.

[12] M. Vuković, *Izračunljivost*, skripta, `http://web.math.hr/~vukovic/`, 2007.

Naslov: Gödelovi teoremi nepotpunosti

Sažetak: Gödelovi teoremi nepotpunosti ukazuju na inherentna ograničenja aksiomatske metode u matematici. U ovom se radu dokazuju Gödelovi teoremi, pri čemu se posebno obraća pozornost na aritmetizaciju sintakse i reprezentabilnost funkcija, ključne ideje sadržane u Gödelovim dokazima. Na početku se definiraju Robinsonova i Peanova aritmetika, dvije aksiomatske aritmetičke teorije. Nakon toga se opisuje način pridjeljivanja kodova izrazima aritmetičkog jezika L_A te se pokazuje kako je Robinsonova aritmetika dovoljno jaka da se u njoj mogu dokazati tvrdnje o dokazivosti u samoj toj teoriji. Iz toga se lako dobiva dokaz Gödelovog prvog teorema nepotpunosti (definiranjem rečenice G koja nije dokaziva u teoriji PA), dijagonalne leme te nekih zanimljivih srodnih rezultata. Konačno, razmatra se pitanje konzistentnosti Peanove aritmetike te se dokazuje Gödelov drugi teorem nepotpunosti.

Ključne riječi: Gödel, Robinsonova aritmetika, Peanova aritmetika, nepotpunost aritmetike, dijagonalizacija, reprezentabilnost, aritmetizacija, dijagonalna lema

Title: Gödel's incompleteness theorems

Summary: Kurt Gödel's incompleteness theorems establish inherent limitations of the axiomatic method in mathematics. The main focus of this paper are Gödel's proofs, with emphasis on two key ideas: arithmetization of syntax and representability of functions. First, we define two first-order theories of arithmetic: Robinson arithmetic Q and Peano arithmetic PA. Afterwards, Gödel's idea of assigning natural numbers to L_A expressions is described. Robinson arithmetic is shown to be strong enough to be able to reason (via Gödel coding), to some extent, about it's own theorems. Proof for the first theorem then quickly follows by constructing a sentence G such that neither G nor it's negation can be derived from PA (assuming it's ω-consistent). Diagonal lemma is also proved, as well as some of the related theorems. Finally, PA's inability to prove it's own consistency is demonstrated, proving Gödel's second incompleteness theorem.

Keywords: Gödel, Robinson arithmetic, Peano arithmetic, incompleteness, diagonalization, representability, arithmetization of syntax, diagonal lemma