Sveučilište u Zagrebu
Prirodoslovno-matematički fakultet
Matematički odsjek

Jelena Kovačić

Nedokazive formule u Peanovoj aritmetici

Diplomski rad

Zagreb, siječanj 2011.

Sveučilište u Zagrebu
Prirodoslovno-matematički fakultet
Matematički odsjek

Jelena Kovačić

Nedokazive formule u Peanovoj aritmetici

Diplomski rad

Voditelj rada:
Doc. dr. sc. Mladen Vuković

Zagreb, siječanj 2011.

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

1. ______________________________, predsjednik
2. ______________________________, član
3. ______________________________, član

Povjerenstvo je rad ocijenilo ocjenom ________________.

Potpisi članova povjerenstva:

1. ______________________________
2. ______________________________
3. ______________________________

Sadržaj

Uvod

Priču o nedokazivim formulama Peanove aritmetike nemoguće je započeti bez priče o nepotpunosti. Još prije no što je 1920. godine Hilbert svojim programom potaknuo pitanje formalizacije cijele matematike, matematičari su pokušavali konstruirati formalni sistem koji bi opisivao prirodne brojeve i unutar kojeg bi bilo moguće dokazati sve istinite tvrdnje o njima. Poželjna svojstva takvog sistema bila su potpunost i konzistentnost, to jest, definirana teorija je trebala biti takva da je unutar nje moguće dokazati svaku u njoj izrazivu tvrdnju ili njenu negaciju, i to točno jednu od njih.

Odgovor na pitanje je li moguće definirati konzistentnu i potpunu teoriju prvog reda koja bi opisivala prirodne brojeve dao je Gödel. Jedanaest godina nakon objave Hilbertovog programa Gödel dokazuje svoje teoreme nepotpunosti, iz kojih je slijedila nepotpunost Peanove aritmetike, do danas najprihvaćenije teorije prvog reda čiji aksiomi opisuju prirodne brojeve. Situacija je zapravo bila još i gora jer je Gödel pokazao da je svaka konzistentna teorija prvog reda koja je dovoljno jaka da dokaže osnovna svojstva prirodnih brojeva nužno nepotpuna.

Iako su Gödelovi teoremi nepotpunosti bili izrazito negativan rezultat u kontekstu Hilbertovog programa, još uvijek je postojala nada da ćemo koristeći Peanove aksiome moći dokazati svaku istinitu tvrdnju o prirodnim brojevima. Naime, Gödel je dokazao svoje teoreme konstruiravši rečenicu koja je, u jeziku aritmetike, govorila sama za sebe da je nedokaziva te je kao takvu nije bilo moguće izraziti kao matematički zanimljivu tvrdnju u prirodnom jeziku. Ipak, u međuvremenu su se pojavili primjeri u Peanovoj aritmetici nedokazivih tvrdnji koji su istovremeno bili teoremi nekih drugih matematičkih disciplina, kao što su kombinatorika ili teorija brojeva.

Fenomen matematičke nepotpunosti te njegov utjecaj na logiku i, općenito, poimanje ljudskog uma, načina na koji razmišlja, zaključuje i za što je sposoban, i filozofski je zanimljiva tema te se u literaturi može naći mnoštvo tekstova koji koriste Gödelove teoreme u argumentaciji ovakvih tvrdnji. U ovom se radu nećemo baviti takvim razmatranjima, već ćemo se držati matematičke strane problema. Zanimat će nas tvrdnje o prirodnim brojevima koje su istinite i izrazive u formalnom sistemu Peanove aritmetike, ali nisu dokazive unutar teorije. Najveći dio rada posvećen je jednoj takvoj, Ramseyjevom teoremu za relativno velike skupove. U radu ćemo dokazati istinitost tvrdnje teorema, kao i njegovu nedokazivost u Peanovoj aritmetici, te pokušati dati objašnjenje zašto ga, s matematičkog gledišta, ne možemo dokazati koristeći samo Peanove aksiome.

Rad je podijeljen na četiri poglavlja. U prvom poglavlju dajemo pregled osnovnih definicija i rezultata potrebnih za razumijevanje ostatka rada. U drugom poglavlju navodimo i dokazujemo Ramseyjev teorem te njegovu verziju za relativno velike skupove koja, iako izraziva, nije dokaziva u formalnom sistemu Peanove aritmetike. U trećem poglavlju provodimo dokaz da ta verzija Ramseyjevog teorema nije dokaziva u Peanovoj arimetici. Naposljetku, u četvrtom poglavlju navodimo primjere još nekih istinitih tvrdnji koje nisu dokazive u Peanovoj aritmetici.

Na kraju, koristim priliku da se zahvalim profesoru Vukoviću, čija su predavanja u meni pobudila fascinaciju ovim područjem, što je bio iznimno strpljiv dok sam ja bila iznimno neodlučna u izboru teme. Također se zahvaljujem svim onima koji su korisnim savjetima i kritikama pridonijeli konačnom izgledu rada.

POGLAVLJE 1

Osnovni pojmovi i rezultati

Kroz cijeli rad podrazumijevat ćemo predznanje obuhvaćeno kolegijem Matematička logika, čiji sadržaj prati [25], te osnovno predznanje o rekurzivnim funkcijama i kodiranju, obuhvaćeno kolegijem Izračunljivost (kao literatura za navedeno gradivo može poslužiti [2]). U ovom poglavlju dajemo pregled rezultata koji će biti korišteni u nastavku rada te uvodimo neke nestandardne oznake. Prvo dajemo par komentara o skupovima i njihovim oznakama.

U cijelom ćemo radu s ω označavati skup prirodnih brojeva, uključujući nulu. Prirodne ćemo brojeve interpretirati i u smislu teorije skupova pa ćemo tako simbol za prirodan broj n ujedno koristiti i kao oznaku za početni segment skupa ω kardinalnosti n, $n = \{0, \ldots, n-1\}$. Pritom se početni segment definira na standardan način: $X \subseteq \omega$ je početni segment od ω ako $x \in X$ i $y < x$ povlače $y \in X$. Proizvoljne podskupove od ω, ne nužno početne segmente, označavat ćemo masno tiskanim simbolima (npr. $\boldsymbol{h}$). Za $\boldsymbol{h}, \boldsymbol{h'} \subseteq \omega$, pišemo $\boldsymbol{h} < \boldsymbol{h'}$ ukoliko za svako $x \in \boldsymbol{h}$ i $y \in \boldsymbol{h'}$ vrijedi $x < y$ (sličan komentar vrijedi i za ostale skupovne nejednakosti).

U ostatku poglavlja navest ćemo neke metateoreme o teorijama prvog reda te reći nešto o Peanovoj aritmetici i rekurzivnim funkcijama.

1.1 Neki rezultati za teorije prvog reda

U ovom odjeljku ističemo samo pojmove važne za ovaj rad i za njih vezane rezultate koje ćemo u nastavku rada koristiti. Navedeni rezultati odnosit će se na proizvoljnu teoriju prvog reda T. Teorija prvog reda te pojmovi vezani za jezik teorije prvog reda, kao što su term, formula i rečenica, definiraju se na standardan način. Standardne su i definicije strukture i modela teorije, uključujući definiciju istinitosti formule u strukturi te za nju vezanih pojmova poput ispunjivosti i valjanosti formule. Iz istog razloga preskačemo definicije dokaza, izvoda i teorema (sve se definicije mogu naći u [25]). Činjenicu da je formula φ teorem teorije T označavat ćemo s $\mathsf{T} \vdash \varphi$. Slično, s $\mathsf{T} \nvdash \varphi$ označavamo da formula φ nije teorem teorije T.

Sad navodimo definiciju konzistentnosti te dva teorema korisna za dokazivanje konzistentnosti neke teorije.

Definicija 1.1.1. *Teorija T je **konzistentna** ako ne postoji formula φ teorije T takva da*

$$\mathsf{T} \vdash \varphi \quad i \quad \mathsf{T} \vdash \neg\varphi.$$

*Ako teorija nije konzistentna, kažemo da je **inkonzistentna**.*

Slično možemo definirati i konzistentnost skupa formula u teoriji: skup formula Γ teorije T bit će konzistentan u T ako ne postoji formula φ teorije T takva da se i φ i $\neg\varphi$ mogu izvesti iz Γ. Prvo navodimo propoziciju koja se može naći u [25].

Propozicija 1.1.2. *Neka je Γ skup formula teorije T. Ako postoji model teorije T koji je model i za skup Γ, tada je skup Γ konzistentan u teoriji T.*

Uzmemo li za Γ skup aksioma teorije T, kao korolar dobivamo sljedeći teorem.

Teorem 1.1.3. *Ako teorija T ima model, tada je konzistentna.*

Sad navodimo verziju teorema kompaktnosti za teorije prvog reda čiji se dokaz može naći u [21].

Teorem 1.1.4 (Teorem kompaktnosti)**.** *Teorija T ima model ako i samo ako svaki konačan podskup aksioma od T ima model.*

Osim konzistentnosti, važno svojstvo svake teorije je potpunost.

Definicija 1.1.5. *Teorija T je **potpuna** ako za svaku zatvorenu formulu φ teorije T vrijedi*

$$\mathsf{T} \vdash \varphi \quad ili \quad \mathsf{T} \vdash \neg\varphi.$$

*Ako teorija nije potpuna, kažemo da je **nepotpuna**.*

Uz nepotpune teorije vezan je pojam neodlučivih formula, „svjedoka nepotpunosti".

Definicija 1.1.6. *Formula φ teorije T je **neodlučiva** u teoriji T ako vrijedi*

$$\mathsf{T} \nvdash \varphi \quad i \quad \mathsf{T} \nvdash \neg\varphi.$$

Naposljetku, navodimo teorem potpunosti, koji daje vezu između dokazivosti i valjanosti formula teorije prvog reda.

Teorem 1.1.7 (Teorem potpunosti)**.** *Neka je φ formula teorije T. Tada vrijedi*

$$\mathsf{T} \vdash \varphi \quad \textit{ako i samo ako} \quad \mathfrak{M} \models \varphi, \ \textit{za svaki model}\ \mathfrak{M}\ \textit{od}\ \mathsf{T}.$$

1.2 Peanova aritmetika

Peanova aritmetika je teorija prvog reda koja opisuje prirodne brojeve. Skup nelogičkih simbola Peanove aritmetike sastoji se od dva dvomjesna funkcijska simbola, $+$ i $\cdot$, i jednog jednomjesnog funkcijskog simbola, s, čije su željene interpretacije funkcije zbrajanja, množenja i sljedbenika, te jednog konstantskog simbola, 0. Jedini relacijski simbol je $=$, čija je željena interpretacija relacija jednakosti.

Standardno, pisat ćemo $x + y$ i $x \cdot y$ umjesto $+(x, y)$ i $\cdot(x, y)$ te $x \neq y$ umjesto $\neg(x = y)$ (iste se primjedbe odnose na formule dobivene zamjenom individualnih varijabli proizvoljnim termima).

Za $n \in \omega$, s $\overline{n}$ ćemo označavati term čija je željena interpretacija prirodan broj n,

$$\overline{n} = \underbrace{s(s(\ldots s}_{n \text{ puta}}(0)\ldots)).$$

Terme ovog oblika nazivat ćemo **numerali**.

Sad zadajemo nelogičke aksiome Peanove aritmetike.

Definicija 1.2.1. *Nelogički aksiomi Peanove aritmetike su:*

(i) aksiomi jednakosti,

- $x = x$ *te*
- $x = y \to (\varphi(x) \to \varphi'(y))$, *gdje je* $\varphi(x)$ *atomarna formula, a* $\varphi'(y)$ *formula dobivena zamjenom nekih, možda i svih, slobodnih nastupa varijable* x *varijablom* y,

(ii) aksiomi koji opisuju svojstva koja treba zadovoljavati funkcija sljedbenika,

- $s(x) = s(y) \to x = y$ *te*
- $0 \neq s(x)$,

(iii) aksiomi zbrajanja,

- $x + 0 = x$ *te*
- $x + s(y) = s(x + y)$,

(iv) aksiomi množenja,

- $x \cdot 0 = 0$ *te*
- $x \cdot s(y) = x \cdot y + x$,

(v) te shema aksioma indukcije,

$$\varphi(0) \to (\forall x(\varphi(x) \to \varphi(s(x))) \to \forall x \varphi(x)) ,$$

gdje je $\varphi(x)$ proizvoljna formula.

U daljnjem ćemo tekstu često za Peanovu aritmetiku koristiti oznaku PA.

Može se pokazati da su mnoga svojstva zbrajanja i množenja prirodnih brojeva te, štoviše, i glavni teoremi teorije brojeva, dokazivi u PA (za neke primjere i dokaze vidi [17]).

Teorija PA ima model kojem je nosač skup prirodnih brojeva ω, funkcijski simboli $+$, $\cdot$ i s interpretirani su standardnim funkcijama zbrajanja, množenja i sljedbenika na skupu ω, a konstantski simbol 0 interpretiran je prirodnim brojem nula. Ovu strukturu označavat ćemo s $\langle \omega; +, \cdot, s, 0 \rangle$ i zvat ćemo je **standardnim modelom** za PA.

Svaki model za PA koji nije izomorfan standardnom zvat ćemo **nestandardnim modelom** za PA.

Budući da PA ima model, iz teorema 1.1.3 slijedi da je konzistentna. Međutim, može se pokazati da teorija PA nije potpuna, o čemu govori Gödelov prvi teorem nepotpunosti.

Teorem 1.2.2 (Gödelov prvi teorem nepotpunosti)**.** *Postoji zatvorena formula G teorije PA za koju vrijedi*

$$\mathsf{PA} \nvdash G \quad i \quad \mathsf{PA} \nvdash \neg G.$$

Također, osim što je nepotpuna, iz drugog Gödelovog teorema nepotpunosti slijedi da teorija PA ne može dokazati ni svoju konzistentnost. Označimo li s $\mathrm{Con}_{\mathsf{PA}}$ formulu teorije PA koja izražava njenu konzistentnost, drugi teorem nepotpunosti možemo iskazati u sljedećem obliku.

Teorem 1.2.3 (Gödelov drugi teorem nepotpunosti)**.**

$$\mathsf{PA} \nvdash \mathrm{Con}_{\mathsf{PA}}.$$

Gödelova rečenica G iz teorema 1.2.2 bila je prvi svjedok nepotpunosti teorije PA. Međutim, iako teoretski važna, rečenica G ne može se interpretirati kao tvrdnja o prirodnim brojevima.

U ovom ćemo se radu baviti primjerima neodlučivih formula teorije PA koje govore nešto zanimljivo o prirodnim brojevima te čiju istinitost možemo dokazati. Kako su takve tvrdnje istinite u standardnom modelu, iz teorema 1.1.7 slijedi da je, da bismo dokazali njihovu neodlučivost, dovoljno pokazati da nisu dokazive u PA.

1.3 Rekurzivne funkcije

U ovom odjeljku navodimo definiciju i najvažnije rezultate vezane za rekurzivne funkcije. Rekurzivne funkcije predstavljaju klasu funkcija koje smatramo u intuitivnom smislu izračunljivima i važan su alat za rad unutar teorije PA. Naime, mnoge tvrdnje o prirodnim brojevima, kao i mnoge tvrdnje o samoj teoriji, mogu se izraziti pomoću rekurzivnih funkcija te zatim i zapisati pomoću formula teorije PA. Ovim se često koristi kad se želi pokazati da je neka tvrdnja (ne)dokaziva u PA.

Da bismo mogli definirati klasu rekurzivnih funkcija, potrebno je prvo definirati jednu užu klasu funkcija, primitivno rekurzivne funkcije.

Primitivno rekurzivne funkcije

Prvi korak u definiranju primitivno rekurzivnih funkcija je definicija inicijalnih funkcija.

Definicija 1.3.1. *Funkciju $Z\colon \omega \to \omega$ definiranu sa $Z(x) = 0$ nazivamo* ***nul-funkcija****.*

Funkciju $Sc\colon \omega \to \omega$ definiranu sa $Sc(x) = x + 1$ nazivamo ***funkcija sljedbenika****.*

Za $n \in \omega$ i $1 \leq k \leq n$, funkciju $I^n_k\colon \omega^n \to \omega$ definiranu sa $I^n_k(x_1, \dots, x_n) = x_k$ nazivamo ***projekcija****.*

Funkcije Z, Sc i $I^n_k (n \in \omega, 1 \leq k \leq n)$ nazivamo ***inicijalne funkcije****.*

Neka su $f, g\colon \omega^k \to \omega$, za neko $k \geq 1$. Sa $f \simeq g$ označavamo da za svaku uređenu k-torku $\vec{\boldsymbol{x}} \in \omega^k$ vrijedi

$$\begin{gathered} f(\vec{\boldsymbol{x}}) \text{ i } g(\vec{\boldsymbol{x}}) \text{ su definirani i vrijedi } f(\vec{\boldsymbol{x}}) = g(\vec{\boldsymbol{x}}) \\ \text{ili} \\ f(\vec{\boldsymbol{x}}) \text{ i } g(\vec{\boldsymbol{x}}) \text{ su nedefinirani.} \end{gathered}$$

Sad uvodimo definicije funkcija pomoću kompozicije i primitivne rekurzije.

Definicija 1.3.2. *Neka su $g, h_1, \dots, h_n$ funkcije. Neka je funkcija f definirana sa*

$$f(\vec{\boldsymbol{x}}) \simeq g(h_1(\vec{\boldsymbol{x}}), \dots, h_n(\vec{\boldsymbol{x}})).$$

Tada kažemo da je funkcija f definirana pomoću ***kompozicije*** *funkcija.*

Definicija 1.3.3. *Neka je g totalna funkcija mjesnosti k, a h totalna funkcija mjesnosti $k+2$. Neka je funkcija f mjesnosti $k+1$ definirana na sljedeći način:*

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

Tada kažemo da je funkcija f definirana pomoću ***primitivne rekurzije****. Ukoliko je $k=0$, funkciju f definiramo pomoću primitivne rekurzije na sljedeći način:*

$$\begin{aligned} f(0) &= a \ (a \in \omega), \\ f(y+1) &= h(f(y),y). \end{aligned}$$

Naposljetku, definiramo klasu primitivno rekurzivnih funkcija.

Definicija 1.3.4. *Najmanja klasa totalnih funkcija koja sadrži sve inicijalne funkcije te je zatvorena za kompoziciju i primitivnu rekurziju naziva se klasa* ***primitivno rekurzivnih funkcija****.*

(Parcijalno) rekurzivne funkcije

Pokazuje se da klasa primitivno rekurzivnih funkcija nije dovoljna da obuhvatimo sve u intuitivnom smislu izračunljive funkcije. Zbog toga se za definiranje klase rekurzivnih funkcija uvodi još i μ-operator.

Definicija 1.3.5. *Neka je f funkcija. S $\mu y(f(\vec{\boldsymbol{x}},y) \simeq 0)$ označavamo funkciju koja $(\vec{\boldsymbol{x}},y)$ pridružuje najmanji z, ukoliko postoji, takav da je izraz $f(\vec{\boldsymbol{x}},y)$ definiran za sve $y<z$ te je $f(\vec{\boldsymbol{x}},z)=0$. Ako takav ne postoji, vrijednost $\mu y(f(\vec{\boldsymbol{x}},y) \simeq 0)$ je nedefinirana.*

*Kažemo da je funkcija $\mu y(f(\vec{\boldsymbol{x}},y) \simeq 0)$ definirana pomoću μ-**operatora**.*

Definicija 1.3.6. *Najmanja klasa funkcija koja sadrži sve inicijalne funkcije te je zatvorena za kompoziciju, primitivnu rekurziju i μ-operator naziva se klasa* ***parcijalno rekurzivnih funkcija****. Parcijalno rekurzivna funkcija koja je totalna naziva se* ***rekurzivna funkcija****.*

Kažemo da je ***relacija rekurzivna*** *ako je njena karakteristična funkcija rekurzivna.*

Ponekad se koristi i definicija funkcije pomoću μ-operatora i relacije. Neka je R relacija mjesnosti $k+1$, za neko $k \in \omega$. Tada s $\mu y R(\vec{\boldsymbol{x}},y)$ označavamo funkciju koja $(\vec{\boldsymbol{x}},y)$ pridružuje najmanji z, ukoliko postoji, takav da vrijedi $\neg R(\vec{\boldsymbol{x}},y)$ sve $y<z$ te vrijedi $R(\vec{\boldsymbol{x}},z)$. Ako takav ne postoji, vrijednost $\mu y R(\vec{\boldsymbol{x}},y)$ je nedefinirana.

Ako je R rekurzivna relacija, lako se vidi da je tada $\mu y R(\vec{\boldsymbol{x}}, y)$ parcijalno rekurzivna funkcija pa je klasa parcijalno rekurzivnih funkcija zatvorena i na ovako definirane funkcije.

Ackermannova funkcija

Ackermannova je funkcija primjer funkcije koja je rekurzivna, ali nije primitivno rekurzivna.

Definiramo prvo pomoću primitivne rekurzije funkciju $B\colon \omega^2 \to \omega$,

$$\begin{aligned} B(0,y) &= 2+y, \\ B(x+1,0) &= sg(x), \\ B(x+1,y+1) &= B(x, B(x+1,y)). \end{aligned}$$

Ovdje smo sa sg označili funkciju predznaka, definiranu sa

$$sg(x) = \begin{cases} 0, \text{ ako je } x = 0, \\ 1, \text{ ako je } x > 0. \end{cases}$$

Ackermannova funkcija $A\colon \omega \to \omega$ tada je definirana s

$$A(x) = B(x,x).$$

Spomenimo još i da Ackermannovu funkciju karakterizira jako brzi rast, što se može vidjeti već i na malim ulaznim vrijednostima.

Reprezentabilnost rekurzivnih funkcija u PA

Sad dajemo par komentara o reprezentabilnosti rekurzivnih funkcija (i njihovih grafova) u PA. Prvo definiramo pojam grafa funkcije.

Definicija 1.3.7. *Neka je f k-mjesna funkcija.* ***Graf*** *od f je relacija G_f mjesnosti $k+1$ definirana s*

$$G_f(\vec{\boldsymbol{x}}, y) \quad \text{ako i samo ako} \quad f(\vec{\boldsymbol{x}}) \simeq y.$$

Teorem 1.3.8 (Teorem o grafu)**.** *Funkcija f je rekurzivna ako i samo ako je njen graf rekurzivna relacija.*

Sad definiramo što znači da neku funkciju ili relaciju možemo izraziti u PA.

Definicija 1.3.9. *Neka je R relacija mjesnosti k te $D(x_1, \ldots, x_k)$ formula teorije* PA *sa slobodnim varijablama $x_1, \ldots, x_k$. Kažemo da je relacija R definirana formulom $D(x_1, \ldots, x_k)$ u teoriji* PA *ako vrijede sljedeća dva uvjeta:*

- $\mathsf{PA} \vdash D(\overline{n_1}, \ldots, \overline{n_k})$, *za sve* $n_1, \ldots, n_k$ *takve da* $R(n_1, \ldots, n_k)$,
- $\mathsf{PA} \vdash \neg D(\overline{n_1}, \ldots, \overline{n_k})$, *za sve* $n_1, \ldots, n_k$ *takve da* $\neg R(n_1, \ldots, n_k)$.

Kažemo da je relacija R ***definabilna*** *u* PA *ako postoji formula koja je definira.*

Definicija 1.3.10. *Neka je* $f\colon \omega^k \to \omega$ *funkcija te* $F(x_1, \ldots, x_k, y)$ *formula teorije* PA *sa slobodnim varijablama* $x_1, \ldots, x_k, y$. *Kažemo da je funkcija* f *reprezentirana u teoriji* PA *formulom* $F(x_1, \ldots, x_k, y)$ *ako za sve* $n_1, \ldots, n_k \in \omega$ *vrijedi*

$$\mathsf{PA} \vdash \forall y(F(\overline{n_1}, \ldots, \overline{n_k}, y) \leftrightarrow y = \overline{m}), \ \ gdje\ je\ m = f(n_1, \ldots, n_k).$$

Kažemo da je funkcija ***reprezentabilna*** *u* PA *ako postoji formula koja je reprezentira.*

Prije nego iskažemo teorem o reprezentabilnosti rekurzivnih funkcija u PA, potrebno je još definirati pojam Σ_1-formule.

Definicija 1.3.11. *Za formulu teorije prvog reda kažemo da je* Δ_0-***formula*** *ako ne sadrži neograničene kvantifikatore (može sadržavati proizvoljno mnogo ograničenih kvantifikatora). Kažemo da je formula* Σ_1-***formula*** *ako je oblika* $\exists x\varphi$, *gdje je* φ *neka* Δ_0*-formula.*

Teorem 1.3.12. *Svaka rekurzivna funkcija reprezentabilna je u* PA *nekom* Σ_1*-formulom. Svaka rekurzivna relacija definabilna je u* PA *nekom* Σ_1*-formulom.*

Iz ovoga slijedi da rekurzivne funkcije i njihove grafove možemo izraziti Σ_1-formulama u PA.

POGLAVLJE 2

Ramseyjev teorem

2.1 Uvod

Ramseyjev teorem proizašao je iz starog kombinatornog pitanja: koliki je minimalan broj ljudi koji trebaju biti nazočni na zabavi da bismo mogli naći *homogenu* trojku - trojku unutar koje se ili svi međusobno poznaju ili nitko ne poznaje nikog? Rješenje je problema poznato, a do brojke od šest osoba brzo se dođe jednostavnim raščlanjivanjem na moguće slučajeve. Promatramo li pak umjesto trojki veće grupe, i problem postaje teži i općenito nije jasno kako bismo za proizvoljan broj r jednostavno odredili broj uzvanika koji bi osigurao barem jednu homogenu r-torku.

Zamijenimo li grupe ljudi skupovima i relaciju poznavanja nekom relacijom ekvivalencije, dolazimo do Ramseyjevog teorema:

> Neka su r, s i n, pri čemu je $n \geq r$, prirodni brojevi. Tada postoji prirodan broj m i n-člani podskup H skupa $M = \{0, 1, \ldots, m-1\}$ takav da, bez obzira na način na koji su r-člani podskupovi skupa M particionirani u s klasa, svi r-člani podskupovi skupa H pripadaju istoj klasi.

Ramseyjev teorem i dokaz koristili su samo konačne skupove. Upotrebom prikladnog kodiranja takvih skupova, teorem je moguće iskazati te provesti dokaz analogan originalnom unutar Peanove aritmetike. Druga verzija dokaza koristi „beskonačnu" verziju Ramseyjevog teorema, poopćenje teorema na beskonačne skupove.

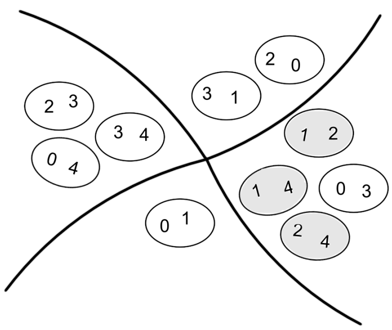
Postoje i druga poopćenja Ramseyjevog teorema, i upravo je jedno takvo učinilo teorem toliko značajnim. Naime, jednostavno proširenje teorema na tzv. *relativno velike* skupove iznjedrilo je primjer u Peanovoj aritmetici neodlučive formule koju je istovremeno bilo moguće izraziti kao matematički problem u prirodnom jeziku i dokazati matematičkim aparatom.

U daljnjem tekstu iskazat ćemo i dokazati verziju Ramseyjevog teorema za beskonačne skupove. Definirat ćemo pojam relativno velikih skupova te iskazati pripadnu verziju Ramseyjevog teorema. Na kraju ćemo pokazati kako se pomoću beskonačne verzije Ramseyjevog teorema, primjenom teorema kompaktnosti, mogu dokazati gore navedeni teorem i njegov analogon za relativno velike skupove. Cilj idućeg poglavlja bit će pokazati da se taj dokaz ne može provesti u Peanovoj aritmetici.

2.2 Beskonačna verzija Ramseyjevog teorema

Prije samog iskaza i dokaza verzije teorema za beskonačne skupove, potrebno je dati par komentara vezanih za notaciju.

Za prirodan broj r i dani skup $\boldsymbol{m}$ uvodimo oznaku $[\boldsymbol{m}]^r$ za skup svih njegovih r-članih podskupova. Proizvoljnu s-članu particiju P takvog skupa predstavljat ćemo funkcijom kojoj je kodomena s-člani skup ($P\colon [\boldsymbol{m}]^r \to s$). Pritom ćemo dopuštati da neke od klasa budu prazne. Dalje, činjenicu da svi r-člani podskupovi skupa $\boldsymbol{h}$ pripadaju istoj klasi particije P možemo izraziti tako da kažemo da je skup $\operatorname{Im} P|_{[\boldsymbol{h}]^r}$ jednočlan (kažemo još da je $\boldsymbol{h}$ **homogen** za P). Ovdje smo s $P|_{[\boldsymbol{h}]^r}$ označili restrikciju od P na skup $[\boldsymbol{h}]^r$.



Slika 2.1: Prikazana je particija $P\colon [5]^2 \to 4$. Skup $\{1, 2, 4\}$ homogen je za P

Sad je sve spremno za iskaz beskonačne verzije Ramseyjevog teorema:

Teorem 2.2.1 (Beskonačna verzija Ramseyjevog teorema)**.** *Neka su r, s prirodni brojevi te $f\colon [\omega]^r \to s$. Tada postoje prebrojivo beskonačni podskup $\boldsymbol{h}$ od ω i prirodan broj $j \in s$ takvi da je* $\operatorname{Im} f|_{[\boldsymbol{h}]^r} = \{j\}$.

Dokaz. Neka je s proizvoljan prirodan broj. Za fiksni s, dokaz se provodi matematičkom indukcijom po r.

Neka je $r = 1$ i $f\colon [\omega]^1 \to s$ proizvoljna. Definiramo $\boldsymbol{a}_k = \{x\colon f(\{x\}) = k\}$, za $1 \leq k \leq s$. Budući da je ω beskonačan, mora postojati $k \in s$ takav da je $\boldsymbol{a}_k$ beskonačan. Označimo s j najmanji takav. Tada je očito $f|_{[\boldsymbol{a}_j]^1} = \{j\}$.

Pretpostavimo sad da tvrdnja vrijedi za neki prirodan broj r te neka je $f\colon [\omega]^{r+1} \to s$. Za svaki prirodan broj i definiramo prirodne brojeve b_i, j_i, prebrojivo beskonačne skupove $\boldsymbol{y}_i$, $\boldsymbol{w}_i$, $\boldsymbol{z}_i$, te funkciju $f_i\colon [\omega]^r \to s$, na način koji ćemo sada opisati.

Neka je $\boldsymbol{y}_0 = \omega$. Pretpostavimo da je $\boldsymbol{y}_i$ definiran te definirajmo b_i kao njegov najmanji element. Sad definiramo $\boldsymbol{z}_i = \boldsymbol{y}_i \setminus \{b_i\}$. Primijetimo da je, budući da je $\boldsymbol{y}_i$ beskonačan, i $\boldsymbol{z}_i$ prebrojivo beskonačan. Dakle, $\boldsymbol{z}_i$ možemo napisati u obliku $\boldsymbol{z}_i = \{z_0^{(i)} < z_1^{(i)} < z_2^{(i)} < \dots\}$. Sad definiramo $f_i\colon [\omega]^r \to s$. Za proizvoljni r-člani podskup $\boldsymbol{k} = \{k_1, \dots, k_r\}$ od ω, stavimo

$$f_i(\{k_1, \dots, k_r\}) = f(\{b_i, z_{k_1}^{(i)}, \dots, z_{k_r}^{(i)}\}).$$

Budući da su svi $z_{k_1}^{(i)}, \dots, z_{k_r}^{(i)}$ međusobno različiti i različiti od b_i, f_i je dobro definirana. Sad, po pretpostavci indukcije, postoje prebrojivo beskonačan skup $\boldsymbol{w}_i$ i prirodan broj j_i takvi da je $\operatorname{Im} f_i|_{[\boldsymbol{w}_i]^r} = \{j_i\}$. Na kraju, definiramo $\boldsymbol{y}_{i+1} = \{z_k^{(i)}\colon k \in \boldsymbol{w}_i\}$. Primijetimo da vrijedi $\boldsymbol{y}_{i+1} \subseteq \boldsymbol{z}_i \subset \boldsymbol{y}_i$. Također, budući da je b_i manji od bilo kojeg člana skupa $\boldsymbol{z}_i$, vrijedi $b_{i+1} < b_i$.

Neka je sad $\boldsymbol{a}_k = \{i : j_i = k\}$, za $1 \leq k \leq s$. Označimo sa j najmanji prirodan broj takav da je $\boldsymbol{a}_j$ beskonačan (takav očito postoji). Definirajmo $\boldsymbol{h} = \{b_i : i \in \boldsymbol{a}_j\} = \{b_i : j_i = j\}$ te pokažimo da je $\boldsymbol{h}$ traženi skup. Budući da je $\boldsymbol{a}_j$ beskonačan te da je $b_l \neq b_k$ za $l \neq k$, $\boldsymbol{h}$ je također prebrojivo beskonačan. Preostaje još pokazati da je $\operatorname{Im} f|_{[\boldsymbol{h}]^{r+1}} = \{j\}$.

Neka je $\boldsymbol{b}$ proizvoljan $r+1$-člani podskup od $\boldsymbol{h}$. Možemo ga napisati u obliku $\boldsymbol{b} = \{b_i < b_{i_1} < \dots < b_{i_r}\}$. Budući da je $(\boldsymbol{y}_i)_{i \geq 0}$ padajući niz skupova, $b_{i_1}, \dots, b_{i_r}$ se nalaze u skupu $\boldsymbol{y}_{i+1} = \{z_k^{(i)} : k \in \boldsymbol{w}_i\}$. Dakle, vrijedi $b_{i_1} = z_{k_1}^{(i)}, \dots, b_{i_r} = z_{k_r}^{(i)}$, za neke $k_1, \dots, k_r \in \boldsymbol{w}_i$. Brojevi $b_{i_1}, \dots, b_{i_r}$ su međusobno različiti, iz čega slijedi da je $\{k_1, \dots, k_r\}$ r-člani podskup od $\boldsymbol{w}_i$. Iz konstrukcije skupa $\boldsymbol{w}_i$ slijedi $f_i(k_1, \dots, k_r) = j_i$. Sad je

$$f(\boldsymbol{b}) = f(\{b_i, b_{i_1}, \dots, b_{i_r}\}) = f(\{b_i, z_{k_1}^{(i)}, \dots, z_{k_r}^{(i)}\}) = f_i(\{k_1, \dots, k_r\}) = j_i = j,$$

gdje posljednja jednakost slijedi iz $i \in \boldsymbol{a}_j$. $\square$

2.3 Verzije Ramseyjevog teorema za konačne skupove

Prije nego prijeđemo na dokaze drugih verzija Ramseyjevog teorema, trebat će nam pojam stabla i jedan rezultat vezan za njega.

Definicija 2.3.1. ***Stablo*** *se sastoji od:*

- *nepraznog skupa T čije elemente nazivamo* ***čvorovima*** *stabla,*
- *particije skupa T,*

$$T = T_0 \cup T_1 \cup \dots,$$

  na konačan ili beskonačan broj skupova koje nazivamo ***razinama*** *stabla,*
- *dvomjesne relacije R na skupu T. Pritom relacija R zadovoljava sljedeće uvjete:*
  - *ni za koje $a \in T$ i $b \in T_0$ ne vrijedi aRb,*
  - *za $b \in T_{n+1}$, aRb vrijedi za točno jedan $a \in T$ i pritom je $a \in T_n$.*

  Ako vrijedi aRb, kažemo da je a ***točno ispod*** *b, odnosno da je b* ***točno iznad*** *a.*

Kažemo da je stablo ***konačno (beskonačno)*** *ako je skup T konačan (beskonačan).* ***Grana*** *stabla je niz (konačan ili beskonačan) čvorova stabla $G = (a_n) \subseteq T$ takvih da je a_n točno ispod a_{n+1}, za sve $a_n, a_{n+1} \in G$.*

Lema 2.3.2 (Königova lema)**.** *Neka je T beskonačno stablo te neka je skup čvorova na svakoj razini od T konačan. Tada T ima barem jednu beskonačnu granu.*

Dokaz. Danom stablu T pridružujemo alfabet teorije prvog reda na sljedeći način. Označimo s $c_1^{(i)}, \dots, c_{k_i}^{(i)}$ čvorove koji se nalaze na i-toj razini stabla, za $i \geq 0$. Skup konstantskih simbola tada definiramo kao skup

$$\bigcup_{i \geq 0} \{\mathbf{c}_1^{(i)}, \dots, \mathbf{c}_{k_i}^{(i)}\}.$$

Skup relacijskih sadržavat će samo jedan jednomjesni relacijski simbol G (željena interpretacija izraza $G(x)$ je 'x pripada grani'), a skup funkcijskih simbola bit će prazan.

Sad definiramo prebrojiv skup S formula te teorije. Skup S sastojat će se od tri vrste formula:

(i) $G(\mathbf{c}_1^{(0)}) \vee \dots \vee G(\mathbf{c}_{k_0}^{(0)})$,

(ii) $\neg(G(\mathbf{c}_j^{(i)}) \wedge G(\mathbf{c}_l^{(i)}))$, $i \geq 0$, $1 \leq j, l \leq k_i$,i

(iii) $\neg G(\mathbf{c}_j^{(i)}) \vee G(\mathbf{c}_{j_1}^{(i+1)}) \vee \cdots \vee G(\mathbf{c}_{j_m}^{(i+1)})$, za sve $i \geq 0$, pri čemu su sa $c_{j_1}^{(i+1)}, \ldots, c_{j_m}^{(i+1)}$ označeni čvorovi točno iznad $c_j^{(i)}$. Ukoliko takvih nema, pripadna je formula $\neg G(\mathbf{c}_j^{(i)})$.

Ako postoji model za S, T ima beskonačnu granu. Naime, istinitost formule (i) povlači da u nultoj razini stabla postoji barem jedan čvor $c_r^{(0)}$ za koji je $G(\mathbf{c}_r^{(0)})$ istinita. Zbog istinitosti formula oblika (ii) za $i = 0$ zaključujemo da postoji točno jedan takav čvor. Iz (iii) za $i = 0$ i $j = r$ i (2) za $i = 1$ dobivamo da postoji točno jedan čvor točno iznad $c_r^{(0)}$ za koji je pripadna atomarna formula istinita. Analognim zaključivanjem dolazimo do prebrojivog niza čvorova sa svojstvom da je svaki član niza točno iznad svog neposrednog prethodnika, tj. dolazimo do beskonačne grane.

Preostaje pokazati da postoji model za S. Iz teorema kompaktnosti slijedi da je dovoljno pokazati da svaki konačan podskup od S ima model.

Neka je S' neki konačan podskup od S. Za $k \geq 0$, označimo sa S_k podskup od S koji sadrži formulu (i) te sve formule oblika (ii) i (iii) za $i \leq k$. Označimo s l najmanji broj takav da je $S' \subseteq S_l$. Dovoljno je pokazati da postoji model (M, φ) za S_l.

Definirajmo nosač M kao skup svih čvorova stabla T te definirajmo vrijednosti od φ na skupu konstantskih simbola tako da svakom kostantskom simbolu pridružimo odgovarajući čvor. Uzmimo sad proizvoljni čvor koji se nalazi na l-toj razini stabla i definirajmo relaciju $\varphi(G)$ na skupu M na način da relaciju zadovoljavaju točno oni čvorovi koji leže na grani od odabranog čvora do nekog čvora iz nulte razine. Sad se lako vidi da je (M, φ) model za S_l. $\square$

Iskažimo sad Ramseyjev teorem u malo drugačijoj formi i dokažimo ga primjenom dosad navedenih rezultata.

Teorem 2.3.3 (Ramseyjev teorem)**.** *Neka su r, s i n ($n \geq r$) prirodni brojevi. Tada postoji prirodan broj M takav da za svaku funkciju $f\colon [M]^r \to s$ postoje n-člani podskup $\boldsymbol{h}$ od M i prirodan broj $j \in s$ takvi da je $\operatorname{Im} f|_{[\boldsymbol{h}]^r} = \{j\}$.*

Dokaz. Pretpostavimo da tvrdnja teorema ne vrijedi. U tom slučaju postoje prirodni brojevi r, s i n takvi da za svako $m \geq n$ postoji particija P skupa $[m]^r$ za koju ne možemo naći nijedan n-člani homogeni podskup skupa m. Pridružimo toj particiji, na jedinstven način, funkciju

$$f_P\colon [m]^r \to s$$

te zatim od svih takvih particija formirajmo stablo na sljedeći način. Na k-tu razinu stabla stavimo sve funkcije koje određuju particije skupa $[n+k]^r$ za koje ne postoji n-člani homogeni podskup od $n + k$. Pritom funkciju $f\colon [m+1]^r \to s$ smještamo točno iznad funkcije $g\colon [m]^r \to s$ ukoliko f proširuje g, tj. ukoliko vrijedi $f|_{[m]^r} = g$.

Lako je vidjeti da za danu funkciju f postoji točno jedna ovakva funkcija na razini ispod. Naime, takva je funkcija jedinstveno određena vrijednostima funkcije $f|_{[m]^r}$. Također, funkcija $f|_{[m]^r}$ ne može određivati niti jedan n-člani homogeni podskup od m jer bi tada to bio i n-člani homogeni podskup od $m+1$ funkcije f. Iz ovoga slijedi da opisana struktura zaista zadovoljava definiciju stabla.

Budući da za svako $m \geq n$ postoji barem jedna funkcija na pripadnoj razini stabla, zaključujemo da stablo ima beskonačno mnogo čvorova. Iz konstrukcije stabla slijedi da svaka razina stabla sadrži najviše konačno mnogo čvorova (svih s-članih particija skupa $[m]^r$ ima konačno mnogo, za svaki m). Primjenom Königove leme sad slijedi da stablo mora sadržavati barem jednu beskonačnu granu.

Označimo s f_k čvor te grane koji se nalazi na k-toj razini. Iz definicije grane slijedi da f_k proširuje f_{k-1}, za svako $k \geq 1$. Sad ćemo definirati funkciju $F\colon [\omega]^r \to s$.

Za dani r-člani podskup $\boldsymbol{x}$ od ω, nađimo najmanji $k \geq 0$ takav da je $\boldsymbol{x} \subseteq n+k$ te stavimo $F(\boldsymbol{x}) = f_k(\boldsymbol{x})$, što je, zbog svojstva proširenja, jednako $f_l(\boldsymbol{x})$, za svako $l \geq k$. Funkcija F određuje jednu s-članu particiju na skupu svih r-članih podskupova od ω pa primjenom teorema 2.2.1 slijedi da postoji prebrojivo beskonačni podskup $\boldsymbol{y}$ od ω homogen za tu particiju. Označimo s $\boldsymbol{y}_n$ skup koji sadrži n najmanjih elemenata tog skupa. Najveći element tog skupa je tada oblika $n+l$, za neko $l \geq 0$. Budući da je $\boldsymbol{y}_n$ homogen za F, iz definicije od F slijedi da je homogen i za particiju određenu s f_l, što je u kontradikciji s pretpostavkom da f_l pripada stablu. $\square$

Na koncu, iskažimo i dokažimo verziju Ramseyjevog teorema za relativno velike skupove.

Definicija 2.3.4. *Kažemo da je konačan skup prirodnih brojeva* $\boldsymbol{h}$ ***relativno velik*** *ukoliko je* $\operatorname{card} \boldsymbol{h} \geq \min \boldsymbol{h}$.

Teorem 2.3.5 (Ramseyjev teorem za relativno velike skupove)**.** *Neka su r, s i n ($n \geq r$) prirodni brojevi. Tada postoji prirodan broj M takav da za svaku funkciju $f\colon [M]^r \to s$ postoje relativno velik podskup $\boldsymbol{h}$ od M, kardinalnosti barem n, i prirodan broj $j \in s$ takvi da je $\operatorname{Im} f|_{[\boldsymbol{h}]^r} = \{j\}$ (pišemo $M \underset{*}{\longrightarrow} (n)^r_s$).*

Dokaz. Pretpostavimo da tvrdnja teorema ne vrijedi. Analogno kao u dokazu Teorema 2.3.3, možemo konstruirati stablo s beskonačnim brojem čvorova. Funkcija će pripadati k-toj razini stabla ako su svi relativno veliki podskupovi od $n+k$, kadinalnosti barem n, nehomogeni za particiju koju ta funkcija određuje. Na isti način kao prije dolazimo do niza funkcija $(f_n)_{n\in\mathbb{N}}$ koje leže na istoj grani stabla, funkcije F koja određuje particiju skupa ω i prebrojivo beskonačnog skupa $\boldsymbol{y}$ homogenog za tu particiju. Označimo s p najmanji element tog skupa i definirajmo $\boldsymbol{h}$ kao skup koji sadrži najmanjih q elemenata skupa $\boldsymbol{y}$, gdje je $q = \max(p, n)$. Tada je $\boldsymbol{h}$ relativno velik skup kardinalnosti barem n, homogen za particiju od ω određenu s F. Označimo li s l najmanji prirodan broj takav da je $\boldsymbol{h} \subseteq n + l$, zaključujemo da je $\boldsymbol{h}$ relativno velik podskup tog skupa, homogen za particiju određenu s f_l, što je kontradikcija s pretpostavkom da f_l pripada stablu. $\square$

POGLAVLJE 3

Nedokazivost Ramseyjevog teorema u Peanovoj aritmetici

3.1 Uvod

Cilj je ovog poglavlja dokazati sljedeći teorem:

Teorem 3.1.1 (Paris-Harrington). *Ramseyjev teorem za relativno velike skupove (teorem 2.3.5) nije dokaziv u teoriji* PA.

Nekoliko verzija dokaza teorema dostupno je u literaturi. Prvi i najpoznatiji dokaz objavili su Paris i Harrington u [21]. Isti autori zaslužni su i za alternativni dokaz teorema [19, 12] koji koristi takozvane indikatorske funkcije, proizašle iz rada Parisa i Kirbyja (vidi npr. [14] i [20]). Za razliku od ovog dokaza koji koristi rezultate teorije modela, dokaz kombinatorne prirode ponudili su Ketonen i Solovay [13]. Još jedan dokaz može se izvesti iz [11], gdje su Kanamori i McAloon pokazali da Ramseyjev teorem za relativno velike skupove u PA povlači jedan drugi kombinatorni princip nedokaziv u PA.

Ideja je dokaza objavljenog u [21] pokazati da Ramseyjev teorem za relativno velike skupove povlači $\mathrm{Con}_{\mathsf{PA}}$, gdje je s $\mathrm{Con}_{\mathsf{PA}}$ označena formula teorije PA koja izražava njenu konzistentnost. Tada iz Gödelovog drugog teorema nepotpunosti slijedi tvrdnja teorema 3.1.1. U dokazu se prvo definira teorija T čiji su aksiomi skrojeni na način da je početni segment određenog oblika modela za T ujedno i model teorije PA. Zatim se pokaže kako se, koristeći Ramseyjev teorem za relativno velike skupove, za svaki konačan podskup aksioma od T može konstruirati model. Tada, koristeći teorem kompaktnosti i svojstva konzistentnosti, dobivamo da konzistentnost teorije T povlači konzistentnost teorije PA.

Važno je napomenuti da ovdje treba razlikovati ono što se događa „unutar” i „van” teorije. „Van” teorije znamo da PA ima model (skup prirodnih brojeva sa standardnim operacijama zbrajanja, množenja i sljedbenika) te je i konzistentna, no konzistentnost ne možemo dokazati unutar teorije (Gödelov drugi teorem nepotpunosti). Dakle, čitanje dokaza van teorije ne daje ništa novo te tvrdnju teorema 3.1.1 dobivamo tek kad dokaz provedemo unutar PA.

Kodiranje i teorija rekurzivnih funkcija omogućili su da o svojstvima teorije pričamo unutar nje same. Gödelovi teoremi nepotpunosti primjer su kako je kodiranjem alfabeta teorije, te zatim i sintaktičkih objekata poput rečenice ili dokaza, moguće izraziti neka svojstva teorije jezikom PA. Iz opisa je dokaza jasno da je ovdje potrebno ići još dalje i kodirati i semantiku, kako bismo unutar PA mogli izraziti, primjerice, da je neka formula ispunjiva ili pak da teorija ima model.

Iako ćemo u daljnjem tekstu provesti sve korake dokaza, u njihovu se formalizaciju ovdje nećemo upuštati (za neke primjere formalizacije semantičkih svojstava vidi [10] i [12]). Umjesto toga, iskoristit ćemo ih na način sličan onome koji se može naći u [23] da dobijemo izravniji dokaz teorema 3.1.1. Ovaj će pristup ujedno dati i jasnije objašnjenje zašto Ramseyjev teorem za relativno velike skupove nije dokaziv u teoriji PA. Naposljetku, dat ćemo i par komentara o dokazu koji koristi indikatorske funkcije, kao i o dokazu navedenom u [13], te njihovoj vezi s dokazom koji ovdje provodimo.

3.2 Dokaz Paris-Harringtonovog teorema

Dokaz koji ćemo ovdje provesti oslanjat će se na svojstva funkcije $f\colon \omega \to \omega$ definirane s

$$f(x) = \mu y[y \underset{*}{\longrightarrow} (x+1)^x_x].$$

Funkcija f prirodnom broju x pridružuje najmanji $y \in \omega$ takav da za proizvoljnu particiju $P\colon [y]^x \to x$ postoji podskup od y kardinalnosti barem $x+1$ homogen za P. Iz Ramseyjevog teorema za relativno velike skupove slijedi da je f totalna funkcija, no, kao što ćemo u nastavku pokazati, to ne možemo dokazati u PA. Naime, iako je u PA za svako $n \in \omega$ moguće dokazati $\exists y\,(y \underset{*}{\longrightarrow} (\overline{n+1})^{\overline{n}}_{\overline{n}})$ (vidi [21]), ne može se pokazati $\forall x \exists y\,(y \underset{*}{\longrightarrow} (x+1)^x_x)$. Kad bismo htjeli dati intuitivno objašnjenje za to, rekli bismo da je problem u tome što f raste prebrzo te je za općeniti x vrijednost $f(x)$ toliko velika da PA ne može dokazati da uopće postoji. Budući da se totalnost funkcije f u PA može dokazati iz Ramseyjevog teorema za relativno velike skupove, iz nedokazivosti totalnosti funkcije f odmah će slijediti i tvrdnja teorema 3.1.1.

Dokaz počinjemo zadavanjem alfabeta i aksioma teorije T. Alfabet teorije T sadržavat će alfabet teorije PA te prebrojivo mnogo konstantskih simbola c_i, gdje je $i \in \omega$.

Prije nego krenemo dalje, dajemo par primjedbi vezanih za oznake koje će biti korištene u ovom poglavlju. Primjedbe se odnose kako na formule teorije T, tako i na formule teorije PA. Obično tiskanim simbolima, kao x, y, z, označavat ćemo individualne varijable, a masno tiskanim simbolima ($\boldsymbol{x}$, $\boldsymbol{y}$, $\boldsymbol{z}$) nizove varijabli, s indeksima u rastućem poretku. Za formulu ψ koristimo oznaku $\psi(\boldsymbol{x})$ kako bismo naglasili da je ψ formula u kojoj se kao slobodne pojavljuju neke varijable iz $\boldsymbol{x}$ (možda i sve). Standardno, pišemo $x < y$ umjesto $\exists z(z \neq 0 \land x + z = y)$. Izraze oblika $\exists x < y\ \psi$ pisat ćemo kao pokratu za $\exists x(x < y \land \psi)$, a izraz $\forall x < y\ \psi$ kao pokratu za $\forall x(x < y \rightarrow \psi)$. Slično kao kod oznaka skupova, ako je $\boldsymbol{y} = y_{i_1}, \ldots, y_{i_k}$, $\boldsymbol{y} < z$ koristit ćemo umjesto $(y_{i_1} < z) \land \cdots \land (y_{i_k} < z)$ (sličan komentar vrijedi i za $z < \boldsymbol{y}$). Također ćemo koristiti standardnu pokratu $x \leq y$ za formulu $(x < y) \lor (x = y)$ te $x > y$ i $x \geq y$ umjesto $y < x$, odnosno $y \leq x$ (iste se primjedbe odnose na formule dobivene zamjenom individualnih varijabli proizvoljnim termima). Naposljetku, u formulama teorije T nekad ćemo pisati $c(\boldsymbol{k})$ za niz konstantskih simbola s indeksima određenim skupom $\boldsymbol{k} \subset \omega$.

Definicija 3.2.1. *Aksiomi teorije* T *su:*

(i) *aksiomi teorije* PA*, pri čemu instance sheme aksioma indukcije sadrži samo* Δ_0*-formule,*

(ii) *za svaki* $i \in \omega$*, aksiom* $c_i \cdot c_i < c_{i+1}$*, te*

(iii) *za svako* $i < \boldsymbol{k}, \boldsymbol{k'}$*, gdje su* $\boldsymbol{k}$ *i* $\boldsymbol{k'}$ *podskupovi prirodnih brojeva iste kardinalnosti, i svaku* Δ_0*-formulu* $\psi(\boldsymbol{y}, \boldsymbol{z})$ *koja ne sadrži konstantske simbole aksiom*

$$\forall \boldsymbol{y} < c_i[\psi(\boldsymbol{y}, c(\boldsymbol{k})) \leftrightarrow \psi(\boldsymbol{y}, c(\boldsymbol{k'}))].$$

Pritom podrazumijevamo da je broj elemenata u $\boldsymbol{z}$ *jednak broju elemenata u* $\boldsymbol{k}$ *i* $\boldsymbol{k'}$*.*

Za danu σ-strukturu $\mathfrak{M} = (M, \varphi)$ obično ćemo pisati $+^{\mathfrak{M}}$, $\cdot^{\mathfrak{M}}$, $s^{\mathfrak{M}}$ te $=^{\mathfrak{M}}$ za odgovarajuće funkcije, odnosno relacije, na elementima nosača. Ako je $\mathfrak{M}$ model za teoriju T, iz aksioma oblika (ii) i standardnih svojstava zbrajanja i množenja slijedi $c_i^{\mathfrak{M}} <^{\mathfrak{M}} c_{i+1}^{\mathfrak{M}}$, za svako $i \in \omega$ (ovdje pod $c_i^{\mathfrak{M}} <^{\mathfrak{M}} c_{i+1}^{\mathfrak{M}}$ zapravo podrazumijevamo pripadnu formulu u kojoj se pojavljuju samo $+^{\mathfrak{M}}$ i $=^{\mathfrak{M}}$, a slično ćemo podrazumijevati i ubuduće).

Označimo s $\mathfrak{I}$ strukturu kojoj je nosač skup

$$I = \{a \in M : \text{ postoji } i \in \omega \text{ t.d. } a <^{\mathfrak{M}} c_i^{\mathfrak{M}}\},$$

a funkcijski i relacijski simboli interpretirani su pripadnim funkcijama i relacijama na M, restringiranima na I. Pokazat ćemo da je, ukoliko je $\mathfrak{M}$ model za T, $\mathfrak{I}$ model za PA. Za to će nam prvo trebati sljedeća lema.

Lema 3.2.2. *Vrijede sljedeće tvrdnje:*

(i) *Skup I zatvoren je na zbrajanje i množenje.*

(ii) *Ako je $\varphi(\boldsymbol{x})$ Δ_0-formula u kojoj su sve kvantifikacije oblika $\forall x < t$, $\exists x < t$, gdje je t term u kojem se ne pojavljuju konstantski simboli ili je $t = c_i$ za neko $i \in \omega$, tada vrijedi*

$$\mathfrak{I} \models \varphi(\boldsymbol{a}) \text{ ako i samo ako } \mathfrak{M} \models \varphi(\boldsymbol{a}),$$

za svaki niz $\boldsymbol{a} \subseteq I$.

Dokaz. Pokažimo zatvorenost na zbrajanje. Primijetimo prvo da za $i_0 < i_1 < i_2$ i $p <^{\mathfrak{M}} c_{i_0}^{\mathfrak{M}}$ vrijedi $p +^{\mathfrak{M}} c_{i_1}^{\mathfrak{M}} <^{\mathfrak{M}} c_{i_2}^{\mathfrak{M}}$. Naime, u slučaju $p +^{\mathfrak{M}} c_{i_1}^{\mathfrak{M}} \geq^{\mathfrak{M}} c_{i_2}^{\mathfrak{M}}$, iz svojstava zbrajanja slijedilo bi da postoji $p' <^{\mathfrak{M}} c_{i_0}^{\mathfrak{M}}$ takav da je $p' +^{\mathfrak{M}} c_{i_1}^{\mathfrak{M}} =^{\mathfrak{M}} c_{i_2}^{\mathfrak{M}}$. Iz definicije 3.2.1 (iii) tada zaključujemo $p' +^{\mathfrak{M}} c_{i_1}^{\mathfrak{M}} =^{\mathfrak{M}} c_j^{\mathfrak{M}}$, za svako $j > i_2$, što je kontradikcija s komentarom da svi konstantski simboli u nosaču moraju biti interpretirani kao različiti elementi. Dakle, vrijedi $p +^{\mathfrak{M}} c_{i_1}^{\mathfrak{M}} <^{\mathfrak{M}} c_{i_2}^{\mathfrak{M}}$, za svako $p <^{\mathfrak{M}} c_{i_0}^{\mathfrak{M}}$, iz čega slijedi da je za svako $q <^{\mathfrak{M}} c_{i_1}^{\mathfrak{M}}$, $p +^{\mathfrak{M}} q <^{\mathfrak{M}} c_{i_2}^{\mathfrak{M}}$. Time smo dokazali zatvorenost na zbrajanje. Također, za $i_0 < i_1 < i_2$ vrijedi $c_{i_0}^{\mathfrak{M}} +^{\mathfrak{M}} c_{i_1}^{\mathfrak{M}} \leq^{\mathfrak{M}} c_{i_2}^{\mathfrak{M}}$.

Pretpostavimo sad da I nije zatvoren na množenje. U tom slučaju iz svojstava zbrajanja i množenja slijedi da postoji $p <^{\mathfrak{M}} c_{i_0}^{\mathfrak{M}}$ takav da $p \cdot^{\mathfrak{M}} c_{i_1}^{\mathfrak{M}} < c_{i_2}^{\mathfrak{M}} \leq s^{\mathfrak{M}}(p) \cdot^{\mathfrak{M}} c_{i_1}^{\mathfrak{M}}$. Dodamo li $c_{i_1}^{\mathfrak{M}}$ s obje strane prve nejednakosti, dobivamo $s^{\mathfrak{M}}(p) \cdot^{\mathfrak{M}} c_{i_1}^{\mathfrak{M}} < c_{i_1}^{\mathfrak{M}} +^{\mathfrak{M}} c_{i_2}^{\mathfrak{M}}$ pa iz komentara za dokaz zatvorenosti na zbrajanje i definicije 3.2.1 (iii) slijedi $s^{\mathfrak{M}}(p) \cdot^{\mathfrak{M}} c_{i_1}^{\mathfrak{M}} \leq c_j^{\mathfrak{M}}$, za svako $j > i_3 > i_2$. S druge strane, iz definicije 3.2.1 (iii) i druge nejednakosti, $c_{i_2}^{\mathfrak{M}} \leq s^{\mathfrak{M}}(p) \cdot^{\mathfrak{M}} c_{i_1}^{\mathfrak{M}}$, dobivamo $c_j^{\mathfrak{M}} \leq s^{\mathfrak{M}}(p) \cdot^{\mathfrak{M}} c_{i_1}^{\mathfrak{M}}$, za svako $j > i_3$, što je kontradikcija. Time smo dokazali tvrdnju (i).

Dokaz za (ii) ide indukcijom po složenosti formule (pod složenosti podrazumijevamo broj veznika $\wedge$, $\vee$, $\neg$ te kvantifikatora $\forall$ i $\exists$ u formuli). Tvrdnja očito vrijedi za sve formule složenosti 0 jer su sve takve atomarne. Pretpostavimo sad da tvrdnja vrijedi za sve formule složenosti najviše n, za neko $n \in \omega$, te neka je $\theta(\boldsymbol{x})$ formula složenosti $n+1$.

Ako je $\theta(\boldsymbol{x})$ formula oblika $\theta_1(\boldsymbol{x}) \wedge \theta_2(\boldsymbol{x})$, tada za $\boldsymbol{a} \subseteq I$ vrijedi

$$\begin{array}{rlcl} & \mathfrak{I} \models \theta(\boldsymbol{a}) & & \\ \Leftrightarrow & \mathfrak{I} \models \theta_1(\boldsymbol{a}) & \text{i} & \mathfrak{I} \models \theta_2(\boldsymbol{a}) \\ \Leftrightarrow & \mathfrak{M} \models \theta_1(\boldsymbol{a}) & \text{i} & \mathfrak{M} \models \theta_2(\boldsymbol{a}) \\ \Leftrightarrow & \mathfrak{M} \models \theta(\boldsymbol{a}), & & \end{array}$$

pri čemu druga ekvivalencija slijedi iz pretpostavke indukcije za formule $\theta_1(\boldsymbol{x})$, $\theta_2(\boldsymbol{x})$. Analogan dokaz možemo provesti ukoliko je $\theta(\boldsymbol{x})$ oblika $\theta_1(\boldsymbol{x}) \vee \theta_2(\boldsymbol{x})$ ili $\neg\theta_1(\boldsymbol{x})$.

U slučaju kad je $\theta(\boldsymbol{x})$ oblika $\forall y < t(\boldsymbol{x})\, \theta_1(\boldsymbol{x}, y)$ i $t(\boldsymbol{x})$ term u kojem se ne pojavljuje niti jedan konstantski simbol, za $\boldsymbol{a} \subseteq I$ vrijedi

$$\mathfrak{I} \models \theta(\boldsymbol{a}) \text{ ako i samo ako za svako } b <^{\mathfrak{I}} t(\boldsymbol{a}), \mathfrak{I} \models \theta_1(\boldsymbol{a}, b).$$

Budući da je I početni segment od M zatvoren na zbrajanje i množenje, slijedi

$$\{b \in I : b <^{\mathfrak{I}} t(\boldsymbol{a})\} = \{b \in M : b <^{\mathfrak{M}} t(\boldsymbol{a})\}$$

pa, koristeći pretpostavku indukcije, zaključujemo

$$\begin{aligned} & \mathfrak{I} \models \theta(\boldsymbol{a}) \\ \Leftrightarrow \quad & \text{za svako } b <^{\mathfrak{M}} t(\boldsymbol{a}), \mathfrak{M} \models \theta_1(\boldsymbol{a}, b) \\ \Leftrightarrow \quad & \mathfrak{M} \models \theta(\boldsymbol{a}). \end{aligned}$$

Ako je $\theta(\boldsymbol{x})$ oblika $\forall y < c_i\, \theta_1(\boldsymbol{x}, y)$ za neko $i \in \omega$, možemo provesti isti dokaz, uz komentar da u ovom slučaju $\{b \in I : b <^{\mathfrak{I}} c_i^{\mathfrak{I}}\} = \{b \in M : b <^{\mathfrak{M}} c_i^{\mathfrak{M}}\}$ vrijedi po definiciji skupa I. Potpuno analogno dokazuju se slučajevi kad je $\theta(\boldsymbol{x})$ oblika $\exists y < t(\boldsymbol{x})\, \theta_1(\boldsymbol{x}, y)$ ili $\exists y < c_i\, \theta_1(\boldsymbol{x}, y)$. □

Propozicija 3.2.3. *Ako je $\mathfrak{M}$ model za* T*, tada je $\mathfrak{I}$ model za* PA*.*

Dokaz. Budući da je $\mathfrak{M}$ struktura za T i alfabet teorije PA je podskup alfabeta teorije T, $\mathfrak{I}$ je struktura za PA. Iz definicije 3.2.1 (i) i leme 3.2.2 slijedi da su u $\mathfrak{I}$ istiniti svi aksiomi teorija PA koji se odnose na definicije zbrajanja, množenja i funkcije sljedbenika. Preostaje još pokazati da $\mathfrak{I}$ zadovoljava sve instance sheme aksioma indukcije.

Neka je $\theta(\boldsymbol{x})$ proizvoljna formula teorije PA te neka je $\exists y_1 \forall y_2 \ldots \exists y_k \varphi(\boldsymbol{x}, \boldsymbol{y})$ njen zapis u preneksnoj normalnoj formi. Tada za $\boldsymbol{a} \subset I$, $\boldsymbol{a} <^{\mathfrak{M}} c_{i_0}^{\mathfrak{M}}$, vrijedi

$$\begin{aligned} & \mathfrak{I} \models \exists y_1 \forall y_2 \ldots \exists y_k \varphi(\boldsymbol{a}, \boldsymbol{y}) \\ \Leftrightarrow \quad & \exists i_1 > i_0 \forall i_2 > i_1 \ldots \exists i_k > i_{k-1} \text{ t.d. } \mathfrak{I} \models \exists y_1 < c_{i_1} \forall y_2 < c_{i_2} \ldots \exists y_k < c_{i_k} \varphi(\boldsymbol{a}, \boldsymbol{y}) \\ \Leftrightarrow \quad & \exists i_1 > i_0 \forall i_2 > i_1 \ldots \exists i_k > i_{k-1} \text{ t.d. } \mathfrak{M} \models \exists y_1 < c_{i_1} \forall y_2 < c_{i_2} \ldots \exists y_k < c_{i_k} \varphi(\boldsymbol{a}, \boldsymbol{y}) \\ \Leftrightarrow \quad & \mathfrak{M} \models \exists y_1 < c_{i_0+1} \forall y_2 < c_{i_0+2} \ldots \exists y_k < c_{i_0+k} \varphi(\boldsymbol{a}, \boldsymbol{y}). \end{aligned}$$

Ovdje smo u drugoj ekvivalenciji iskoristili lemu 3.2.2 (ii) ($\varphi(\boldsymbol{x}, \boldsymbol{y})$ je formula teorije PA pa se u njoj ne pojavljuju konstantski simboli), a treća je posljedica istinitosti aksioma (iii) iz definicije 3.2.1. Iz ovoga slijedi da indukciju za bilo kakve formule u $\mathfrak{I}$ možemo zamijeniti indukcijom za ograničene formule u $\mathfrak{M}$, što će biti zadovoljeno zbog istinitosti aksioma (i) iz definicije 3.2.1. □

Sljedeći je korak pokazati da svaki konačan podskup aksioma od T ima model. Za to će nam biti potrebno nekoliko lema vezanih za particije skupova.

Lema 3.2.4. *Neka su M, e, r_0 i r_1 prirodni brojevi te $P_0 \colon [M]^e \to r_0$ i $P_1 \colon [M]^e \to r_1$ particije. Tada postoji particija $P \colon [M]^e \to r_0 \cdot r_1$ takva da je $\boldsymbol{h} \subseteq M$ homogen za P ako i samo ako je homogen za P_0 i P_1.*

Dokaz. Za e-člani podskup $\boldsymbol{a}$ od M definiramo $P'(\boldsymbol{a})$ kao kod niza $P_0(\boldsymbol{a})$, $P_1(\boldsymbol{a})$,

$$P'(\boldsymbol{a}) = \langle P_0(\boldsymbol{a}), P_1(\boldsymbol{a})\rangle = 2^{P_0(\boldsymbol{a})+1} \cdot 3^{P_1(\boldsymbol{a})+1}.$$

Ako je $\boldsymbol{h} \subseteq M$ homogen za P_0 i za P_1, iz definicije particije P' odmah slijedi da je homogen i za P'. Obratno, ako je $\boldsymbol{h}$ homogen za P', iz injektivnosti funkcije kodiranja slijedi da je homogen i za P_0 i P_1.

Particija P' definirana je tako da poprima najviše $r_0 \cdot r_1$ različitih vrijednosti. Pomicanjem ovih vrijednosti unutar skupa $r_0 \cdot r_1$ dobivamo particiju $P\colon [M]^e \to r_0 \cdot r_1$ koja zadovoljava tražene uvjete. □

Lema 3.2.5. *Neka su M, e i r prirodni brojevi te $P\colon [M]^e \to r$ particija skupa $[M]^e$. Tada je $\boldsymbol{h} \subseteq M$ homogen za P ako i samo ako je svaki podskup od $\boldsymbol{h}$ kardinalnosti $e+1$ homogen za P.*

Dokaz. Ako je $\boldsymbol{h} \subseteq M$ homogen za P, tada je očito i svaki njegov podskup kardinalnosti $e+1$ homogen za P.

Obratno, neka je $\boldsymbol{h} \subseteq M$ takav da je svaki njegov podskup kardinalnosti $e+1$ homogen za P i pretpostavimo da $\boldsymbol{h}$ nije homogen za P. Označimo s $\boldsymbol{a} = \{a_1 < \cdots < a_e\}$ najmanjih e elemenata skupa $\boldsymbol{h}$. Budući da $\boldsymbol{h}$ nije homogen za P, postoji e-člani podskup $\boldsymbol{b}$ od $\boldsymbol{h}$ takav da je $P(\boldsymbol{a}) \neq P(\boldsymbol{b})$. Odaberimo takav $\boldsymbol{b} = \{b_1 < \cdots < b_e\} \subseteq \boldsymbol{h}$ koji zadovoljava $P(\boldsymbol{a}) \neq P(\boldsymbol{b})$ i pritom je suma $\sum_{l=1}^{e} b_l$ minimalna. Označimo s i minimalni indeks takav da je $a_i \neq b_i$ ($a_i < b_i$) i definirajmo $\boldsymbol{c} = \{a_1, \ldots, a_i, b_i, \ldots, b_e\}$. Tada je $\boldsymbol{c}$ podskup od $\boldsymbol{h}$ kardinalnosti $e+1$. Budući da je $\boldsymbol{c}$ po pretpostavci homogen za P i $\boldsymbol{b} \subseteq \boldsymbol{c}$, mora vrijediti i $P(\{a_1, \ldots, a_i, b_i, \ldots, b_{e-1}\}) = P(\boldsymbol{b})$. Također, zbog $a_i < b_i < b_e$, vrijedi

$$\sum_{j=1}^{i} a_j + \sum_{l=i}^{e-1} b_l = \sum_{l=1}^{e-1} b_l + a_i < \sum_{l=1}^{e} b_l,$$

što je kontradikcija s izborom skupa $\boldsymbol{b}$. □

Za prirodan broj r, definirajmo $\sqrt{r}$ kao najmanji prirodan broj s takav da je $s^2 \geq r$. Lako se vidi da za sve $r \geq 7$ vrijedi $r \geq 1 + 2\sqrt{r}$.

Lema 3.2.6. *Neka su M, e i r prirodni brojevi te $P\colon [M]^e \to r$ particija skupa $[M]^e$. Tada postoji particija $P'\colon [M]^{e+1} \to 1 + 2\sqrt{r}$ takva da za svaki $\boldsymbol{h} \subseteq M$ kardinalnosti barem $e+2$ vrijedi da je $\boldsymbol{h}$ homogen za P ako i samo ako je homogen za P'.*

Dokaz. Neka je $s = \sqrt{r}$. Za proizvoljni e-člani podskup $\boldsymbol{a}$ od M vrijedi

$$P(\boldsymbol{a}) \leq r - 1 \leq s^2 - 1 = s(s-1) + (s-1),$$

iz čega slijedi da $P(\boldsymbol{a})$ možemo napisati u obliku

$$P(\boldsymbol{a}) = s \cdot Q_{\boldsymbol{a}} + R_{\boldsymbol{a}},$$

pri čemu su $Q_{\boldsymbol{a}}, R_{\boldsymbol{a}} \in s$. Na ovaj način dolazimo do particija $Q, R\colon [M]^e \to s$, definiranih s $Q(\boldsymbol{a}) = Q_{\boldsymbol{a}}$, $R(\boldsymbol{a}) = R_{\boldsymbol{a}}$.

Definirajmo sad particiju P'. Za $\boldsymbol{b} = \{b_1 < \cdots < b_{e+1}\} \subseteq M$ označimo s $\boldsymbol{b}'$ skup koji sadrži njegovih e najmanjih elemenata, $\boldsymbol{b} = \{b_1 < \cdots < b_e\}$, i stavimo

$$P'(\boldsymbol{b}) = \begin{cases} \quad 0, \quad & \text{, ako je } \boldsymbol{b} \text{ homogen za } P, \\ \big\langle 0, R(\boldsymbol{b}')\big\rangle, & \text{ako je } \boldsymbol{b} \text{ homogen za } Q, \text{ ali ne i za } P, \\ \big\langle 1, Q(\boldsymbol{b}')\big\rangle, & \text{inače.} \end{cases}$$

Primijetimo da P' poprima najviše $2s+1$ različitih vrijednosti koje po potrebi možemo skalirati tako da kodomena bude $2s+1$, kao što bi i trebala. Pokažimo još da P' zadovoljava željeno svojstvo. Neka je $\boldsymbol{h}$ proizvoljan podskup od M kardinalnosti barem $e+2$. Označimo s $h_1 < \cdots < h_{e+2}$ najmanjih $e+2$ elemenata skupa $\boldsymbol{h}$.

Pretpostavimo da je $\boldsymbol{h}$ homogen za P i da nije homogen za P'. Tada možemo naći skupove $\boldsymbol{c}_1, \boldsymbol{c}_2$, podskupove od $\boldsymbol{h}$ kardinalnosti $e+1$, takve da je $P'(\boldsymbol{c}_1) \neq P'(\boldsymbol{c}_2)$. Iz definicije particije P' tada slijedi da ili $\boldsymbol{c}_1$ ili $\boldsymbol{c}_2$ nije homogen za P, što je kontradikcija s tvrdnjom leme 3.2.5.

Obratno, neka je $\boldsymbol{h}$ homogen za P'. Označimo sa $\boldsymbol{c}$ skup koji sadrži $e+1$ najmanjih elemenata skupa $\boldsymbol{h}$, $\boldsymbol{c} = \{h_1 < \cdots < h_{e+1}\}$ i pokažimo da je $P'(\boldsymbol{c}) = 0$.

Pretpostavimo da vrijedi $P'(\boldsymbol{c}) \neq 0$. Tada vrijedi ili $P'(\boldsymbol{c}) = \langle 1, Q(\boldsymbol{c}')\rangle$ ili $P'(\boldsymbol{c}) = \langle 0, R(\boldsymbol{c}')\rangle$.

U slučaju $P'(\boldsymbol{c}) = \langle 1, Q(\boldsymbol{c}')\rangle$, iz definicije particije P' zaključujemo da $\boldsymbol{c}$ nije homogen ni za P ni za Q. Slijedi da možemo naći $\boldsymbol{c}_1 \subset \boldsymbol{c}$ kardinalnosti e takav da je $Q(\boldsymbol{c}') \neq Q(\boldsymbol{c}_1)$. Tada mora biti $P'(\boldsymbol{c}_1 \cup \{h_{e+2}\}) \neq P'(\boldsymbol{c})$, što je kontradikcija s pretpostavkom da je $\boldsymbol{h}$ homogen za P'.

U slučaju $P'(\boldsymbol{c}) = \langle 0, R(\boldsymbol{c}')\rangle$, iz definicije particije P' zaključujemo da je $\boldsymbol{c}$ homogen za P Q, ali ne i za P. Slijedi da možemo naći $\boldsymbol{c}_1 \subset \boldsymbol{c}$ kardinalnosti e takav da je $P(\boldsymbol{c}') \neq P(\boldsymbol{c}_1)$. Zbog $Q(\boldsymbol{c}') = Q(\boldsymbol{c}_1)$, mora vrijediti $R(\boldsymbol{c}') \neq R(\boldsymbol{c}_1)$. Na sličan način kao prije dolazimo do $P'(\boldsymbol{c}_1 \cup \{h_{e+2}\}) \neq P'(\boldsymbol{c})$, što je opet kontradikcija s pretpostavkom da je $\boldsymbol{h}$ homogen za P'.

Dakle, mora vrijediti $P'(\boldsymbol{c}) = 0$. Sad, budući da je $\boldsymbol{h}$ homogen za P', vrijedi $P'(\boldsymbol{d}) = 0$, za svaki $\boldsymbol{d} \subset \boldsymbol{h}$ kardinalnosti $e+1$. Iz definicije particije P' slijedi da je svaki podskup od $\boldsymbol{h}$ kardinalnosti $e+1$ homogen za P pa primjenom leme 3.2.5 zaključujemo da je $\boldsymbol{h}$ homogen za P. $\square$

Lema 3.2.7. *Neka su M, n, e_i, $r_i (0 \leq i < n)$ prirodni brojevi te $P_i\colon [M]^{e_i} \to r_i$, $i = 0, \ldots, n-1$, particije. Označimo $e = \max_i e_i$ te $r = \prod_i \max(r_i, 7)$. Tada postoji* *particija* $P\colon [M]^e \to r$ *takva da za svaki* $\boldsymbol{h} \subseteq M$ *kardinalnosti barem* $e+1$ *vrijedi da je* $\boldsymbol{h}$ *homogen za* P *ako i samo ako je homogen za* P_i, $0 \leq i < n$.

Dokaz. Svakoj od particija P_j, $0 \leq j < n$, pridružujemo particiju $P'_j\colon [M]^e \to \max(r_j, 7)$ sa svojstvom da je svaki $\boldsymbol{h} \subseteq M$ kardinalnosti barem $e+1$ homogen za P_j ako i samo ako je homogen za P'_j.

Ukoliko je $e_j = \max_i e_i$, do P'_j dolazimo tako da samo eventualno proširimo kodomenu.

Ako je pak $e_j < \max_i e_i$, od P_j prvo, koristeći lemu 3.2.6, dolazimo do particije

$$P_j^{(1)}\colon [M]^{e_j+1} \to 1 + 2\sqrt{r_j}.$$

Ako je $e_j^{(1)} = e_j + 1 < \max_i e_i$, postupak nastavljamo s $P_j^{(1)}$. Budući da je $r_j^{(1)} = 1 + 2\sqrt{r_j} \leq \max(r_j, 7)$ (vidi napomenu prije leme 3.2.6), postupak možemo nastaviti tako da u svakom koraku kodomena ostane $\max(r_j, 7)$. Jasno je da ćemo na ovaj način nakon konačno koraka doći do particije P'_j sa željenim svojstvom.

Naposljetku, primjenom leme 3.2.4 na particije P'_j, $0 \leq j < n$, u konačno koraka dobivamo particiju P koja zadovoljava tvrdnju leme. □

Lema 3.2.8. *Neka je* M *prirodan broj. Za svaki prirodan broj* p *postoji particija* $Q\colon [M]^1 \to p+1$ *takva da za svaki* $\boldsymbol{h} \subseteq M$ *kardinalnosti barem* 2 *koji je homogen za* Q *vrijedi* $\min \boldsymbol{h} \geq p$.

Dokaz. Za $a \in M$, definirajmo $Q(\{a\}) = \min(a, p)$. Tada je $Q\colon [M]^1 \to p+1$.

Neka je sad $\boldsymbol{h} \subseteq M$ homogen za Q i kardinalnosti barem 2. U slučaju da postoji element skupa $\boldsymbol{h}$ manji od p, Q bi poprimala barem dvije različite vrijednosti na $\boldsymbol{h}$, što je kontradikcija s pretpostavkom homogenosti. □

Za proizvoljnu funkciju f i prirodan broj k označimo s $f^{(k)}$ funkciju koju dobijemo komponiranjem funkcije f same sa sobom k puta. Definirajmo induktivno

$$\begin{aligned} f_0(x) &= x+2, \text{ te} \\ f_{n+1}(x) &= f_n^{(x)}(2), \text{ za } n \geq 0. \end{aligned}$$

Za ovako definirane funkcije karakteristično je da rastu jako brzo (slično kao Ackermannova funkcija), što je svojstvo koje će biti bitno u glavnom dijelu dokaza. Primjerice, lako se vidi da vrijedi $f_1(x) \geq 2x$, $f_2(x) \geq 2^x$, $f_3(x) \geq 2^{2^{\cdot^{\cdot^{2}}}}$ (izraz je sastavljen od x dvojki), i tako dalje.

Također, može se pokazati da je za svako $n \in \omega$ funkcija f_n primitivno rekurzivna.

Lema 3.2.9. *Neka su* M *i* r *prirodni brojevi. Za svaki prirodan broj* m *postoji particija* $R\colon [M]^2 \to r$, *pri čemu* r *ovisi samo o* m, *takva da za svaki relativno velik* $\boldsymbol{h} \subseteq M$ *kardinalnosti barem* 3 *koji je homogen za* R *i* $x, y \in \boldsymbol{h}$ *vrijedi da* $x < y$ *povlači* $f_m(x) < y$.

Dokaz. Za $0 \leq i \leq m$, definiramo particiju $P_i \colon [M]^2 \to 2$,

$$P_i(\{a < b\}) = \begin{cases} 0, \text{ ako je } f_i(a) < b, \\ 1, \text{ inače.} \end{cases}$$

Označimo $p = f_m(3)$ i, koristeći lemu 3.2.8, pridružimo mu particiju $Q \colon [M]^1 \to p + 1$. Iskoristimo lemu 3.2.7 da od particija P_i, $0 \leq i \leq m$, i Q dobijemo particiju $R \colon [M]^2 \to r$. Pritom je r dobiven kao $(\prod_{0 \leq i \leq m} \max(2, 7)) \cdot \max(f_m(3) + 1, 7)$, stoga ovisi samo o m.

Neka je sad $\boldsymbol{h} \subseteq M$ homogen za R i kardinalnosti barem 3. Označimo $a = \min \boldsymbol{h}$ i $b = \max \boldsymbol{h}$. Induktivno se lagano vidi da za svaki $i \leq m$ vrijedi $f_i(a) < b$. Tada, budući da je $\boldsymbol{h}$ homogen za R, stoga i za P_i, slijedi da za sve $x, y \in \boldsymbol{h}$ vrijedi $f_i(x) < y$. Posebno, za $i = m$ i sve $x, y \in \boldsymbol{h}$ vrijedi $f_m(x) < y$, kao što je i traženo. □

Lema 3.2.10. *Neka su M, m, e ($e \geq 2$) i s prirodni brojevi i $P \colon [M]^e \to s$ particija skupa $[M]^e$. Tada postoji particija $P^* \colon [M]^e \to s'$, pri čemu s' ovisi samo o m i s, takva da za svaki relativno velik $\boldsymbol{y} \subseteq M$ kardinalnosti barem $e+1$ koji je homogen za P^* postoji relativno velik $\boldsymbol{x} \subseteq M$ homogen za P i kardinalnosti barem* $\max(e + 1, f_m(\min \boldsymbol{x}))$.

Dokaz. Za $a \in M$ označimo s $h(a)$ najveći $x \in M$ takav da je $f_m(x) \leq a$ (ukoliko takav postoji). Zatim definirajmo particiju $S \colon [M]^e \to s + 1$,

$$S(\boldsymbol{a}) = S(\{a_1 < \cdots < a_e\}) = \begin{cases} P(h(\boldsymbol{a})), \text{ ako je } h(a_1) < \cdots < h(a_e), \\ \quad s \quad\;, \text{ inače.} \end{cases}$$

Za dano m uzmimo particiju $R \colon [M]^2 \to r$ kao u tvrdnji leme 3.2.9. Primjenom leme 3.2.7 na particije R i S dolazimo do particije $P^* \colon [M]^e \to s'$. Pritom s' ovisi samo o r i s, odnosno, o m i s (r ovisi samo o m).

Neka je sad $\boldsymbol{y} \subseteq M$ relativno velik skup homogen za P^* i kardinalnosti barem $e + 1 > 2$. Budući da je, iz tvrdnje leme 3.2.7, $\boldsymbol{y}$ homogen i za R, zaključujemo da $\boldsymbol{y}$ zadovoljava uvjete leme 3.2.9, odnosno, za bilo koja dva elementa y i y' skupa $\boldsymbol{y}$ vrijedi da $y' < y''$ povlači $f_m(y') < y''$. Definirajmo $\boldsymbol{x} = h(\boldsymbol{y})$ i pokažimo da je $\boldsymbol{x}$ skup s traženim svojstvima.

Pokažimo prvo da $\boldsymbol{x}$ i $\boldsymbol{y}$ imaju jednak broj elemenata. Neka su y', $y'' \in \boldsymbol{y}$ i neka vrijedi $y' < y''$. Tada je $f_m(y') < y''$ pa zaključujemo $y' \leq h(y'')$. Iz definicije $h(y')$ i svojstava funkcije f_m tada slijede nejednakosti $f_m(h(y')) \leq y' < f_m(y') \leq f_m(h(y''))$ pa imamo $h(y') < h(y'')$.

Dakle, vrijedi $\operatorname{card} \boldsymbol{x} = \operatorname{card} \boldsymbol{y} \geq e + 1$. Također, budući da je $\boldsymbol{y}$ homogen za S (tvrdnja leme 3.2.7), iz definicije od S slijedi da je $\boldsymbol{x}$ homogen za P. Vrijedi još i

$$\operatorname{card} \boldsymbol{x} = \operatorname{card} \boldsymbol{y} \geq \min \boldsymbol{y} \geq f_m(\min \boldsymbol{x}) > \min \boldsymbol{x}.$$

Prva nejednakost vrijedi jer je $\boldsymbol{y}$ relativno velik, a druga zbog $h(\min \boldsymbol{y}) = \min \boldsymbol{x}$. Iz ovoga slijedi da $\boldsymbol{x}$ zadovoljava sva tražena svojstva. $\square$

Sad možemo prijeći na konstrukciju modela za T. Model za konačni podskup aksioma od T konstruirat ćemo koristeći sljedeću propoziciju, koju dokazujemo pomoću Ramseyjevog teorema za relativno velike skupove i lema za particije dokazanih u ovom poglavlju.

Propozicija 3.2.11. *Neka su e, k i r prirodni brojevi. Tada postoji prirodan broj M takav da za bilo koju familiju $(P_i : i < 2^M)$ particija $P_i \colon [M]^e \to r$ postoji $\boldsymbol{x} \subseteq M$ kardinalnosti barem k takav da vrijedi:*

(i) za bilo koje $a, b \in \boldsymbol{x}$, $a < b$ povlači $a^2 < b$, i

(ii) ako je $a \in \boldsymbol{x}$ te $i < 2^a$, tada je $\boldsymbol{x} \setminus (a+1)$ homogen za P_i.

Dokaz. Označimo $e' = 2e + 1$ te odaberimo $p \in \omega$ takav da je za svako $a \geq p$ $f_3(a)$ „puno veći” od e, r, k i a (iz zadnjeg dijela dokaza bit će jasno koliko „puno veći”).

Za bilo koji $N > 0$ i bilo koju familiju particija $Q_i \colon [N]^e \to r$, $i < 2^N$, možemo provesti postupak koji ćemo sad opisati i doći do s' koji ovisi samo o e' i p. Prvo definiramo particiju $S_N : [N]^{e'} \to 2$ tako da za $a \in N$ te $\boldsymbol{b}$, $\boldsymbol{c} \subseteq N$ kardinalnosti e stavimo

$$S_N(a, \boldsymbol{b}, \boldsymbol{c}) = \begin{cases} 0, \text{ ako je } Q_i(\boldsymbol{a}) = Q_i(\boldsymbol{b}), \text{ za svako } i < 2^a \\ 1, \text{ inače.} \end{cases}$$

Zatim iz leme 3.2.8 dobijemo particiju $Q_N \colon [N]^1 \to p+1$, te iz leme 3.2.9 za $m = 2$ particiju $R_N \colon [M]^2 \to r$. Koristeći lemu 3.2.7, od Q_N, S_N i R_N dobivamo particiju P_N. Naposljetku, pomoću leme 3.2.10 za $m = 3$ dobivamo $P_N^* \colon [M]^{e'} \to s'$. Iz konstrukcije slijedi da s' ovisi samo o e' i p.

Sad za e' i s', koristeći Ramseyjev teorem za relativno velike skupove, nađimo M takav da $M \underset{*}{\longrightarrow} (e'+1)^{e'}_{s'}$. Uzmimo proizvoljnu particiju $(P_i \colon i < 2^M)$ te definirajmo particije $S \colon [M]^{e'} \to 2$, $Q \colon [M]^1 \to p+1$ te $R \colon [M]^2 \to r$ na analogan način kao prije. Koristeći lemu 3.2.7, od Q, S i R konstruirajmo particiju P te od nje, opet kao prije, pomoću leme 3.2.10 za $m = 3$ dobijmo $P^* \colon [M]^{e'} \to s'$.

Iz Ramseyjevog teorema za relativno velike skupove slijedi da postoji relativno velik $\boldsymbol{h} \subseteq M$, kardinalnosti barem $e + 1$ i homogen za P^*. Budući da $\boldsymbol{h}$ zadovoljava uvjete leme 3.2.10, možemo naći relativno velik $\boldsymbol{x} \subseteq M$, homogen za P (pa onda i za Q, R i S) i kardinalnosti barem $\max(e'+1, f_3(\min \boldsymbol{x}))$. Pokažimo da je $\boldsymbol{x}$ traženi skup.

Budući da je $\boldsymbol{x}$ homogen za R, relativno velik i kardinalnosti barem $e'+1 = 2e+2 > 2$, iz leme 3.2.9 zaključujemo da za svako $a, b \in \boldsymbol{x}$ t.d. $a < b$ vrijedi $f_2(a) < b$. Zbog $f_2(x) \geq x^2$, za svako x, slijedi $a^2 < b$ pa $\boldsymbol{x}$ zadovoljava (i).

Pokažimo još da je, za proizvoljno $a \in \boldsymbol{x}$, $\boldsymbol{x} \setminus \{0, \dots, a\}$ homogen za P_i, za svako $i < 2^a$. Iz definicije particije S slijedi da je dovoljno pokazati da vrijedi $S(a, \boldsymbol{b}, \boldsymbol{c}) = 0$, za sve $\boldsymbol{b}, \boldsymbol{c} \subseteq \boldsymbol{x} \setminus (a+1)$. Kako je $\boldsymbol{x}$ homogen za S, bit će dovoljno pronaći neke $a' \in \boldsymbol{x}$ te $\boldsymbol{b}', \boldsymbol{c}' \subseteq \boldsymbol{x}$ kardinalnosti e t.d. vrijedi $S(a', \boldsymbol{b}', \boldsymbol{c}') = 0$. Uzmimo $a' = \min \boldsymbol{x}$. Budući da je $\boldsymbol{x}$ homogen za Q, vrijedi $a' \geq p$. Također, vrijedi $\operatorname{card} \boldsymbol{x} \geq f_3(a')$. Iz načina kako smo birali p na početku dokaza, vidimo da smo $\operatorname{card} \boldsymbol{x}$ mogli odabrati da bude dovoljno velik u odnosu na r i a', odnosno, toliko velik da svih e-članih podskupova od $\boldsymbol{x}$ ima više od r^{2^a}. Budući da za proizvoljni e-člani skup $\boldsymbol{z}$ postoji r^{2^a} različitih mogućnosti za niz $(P_i(\boldsymbol{z}) : i < 2^a)$, možemo naći dva e-člana podskupa $\boldsymbol{b}'$ i $\boldsymbol{c}'$ od $\boldsymbol{x}$ takva da je $P_i(\boldsymbol{b}') = P_i(\boldsymbol{c}')$, za svako $i < 2^a$. Tada je $S(a', \boldsymbol{b}', \boldsymbol{c}') = 0$, kao što je i traženo. □

Propozicija 3.2.12. *Svaki konačan podskup aksioma od* T *ima model.*

Dokaz. Neka je dan konačan podskup S aksioma od T te neka su $c_0, \dots, c_{k-1}$ svi konstantski simboli koji se pojavljuju u S. Konstruirat ćemo model za S kojem je nosač skup ω, funkcijski simboli $+$, $\cdot$ i s interpretirani su standardnim operacijama zbrajanja, množenja i funkcije sljedbenika na ω, a konstantski simboli elementima $x_0, \dots, x_{k-1}$ skupa $\boldsymbol{x}$ kojeg ćemo dobiti koristeći propoziciju 3.2.11. Ovakvu strukturu označit ćemo s $\langle \omega; +, \cdot, s, x_0, \dots, x_{k-1} \rangle$.

Neka je $N \in \omega$ proizvoljan te neka je za svaku ograničenu formulu $\psi(\boldsymbol{y}, \boldsymbol{z})$ koja se pojavljuje u nekom od aksioma oblika (iii) dana bilo kakva particija $Q_\psi \colon [M]^{\operatorname{len}(\boldsymbol{z})} \to 2$, gdje smo s $\operatorname{len}(\boldsymbol{z})$ označili duljinu niza $\boldsymbol{z}$. Tada, koristeći lemu 3.2.7, particijama Q_ψ možemo pridružiti particiju $P \colon [M]^e \to r$, pri čemu e i r ovise samo o broju i obliku aksioma iz skupa S.

Za te e, r i k nađimo $M \in \omega$ iz propozicije 3.2.11. Zatim za svaku ograničenu formulu $\psi(\boldsymbol{y}, \boldsymbol{z})$ koja se pojavljuje u nekom od aksioma oblika (iii) iz S i svako $\xi \in \omega$ duljine $\operatorname{len}(\boldsymbol{y})$ definirajmo particije $F_{\psi,\xi} \colon [M]^{\operatorname{len}(\boldsymbol{z})} \to 2$ na način koji ćemo sada opisati. Broj $\xi \in \omega$ interpretiramo kao kod niza prirodnih brojeva $\boldsymbol{a}(\xi)$ i pritom smatramo da je svaki podskup skupa $b = \{0, \dots, b-1\}$ kodiran nekim brojem manjim od 2^b. Za niz $\boldsymbol{c}$ iz M duljine $\operatorname{len}(\boldsymbol{z})$ tada stavljamo $F_{\psi,\xi}(\boldsymbol{c}) = 0$, ako je $\psi(\boldsymbol{a}(\xi), \boldsymbol{c})$ istinita u $\langle \omega; +, \cdot, s \rangle$, a $F_{\psi,\xi}(\boldsymbol{c}) = 1$, inače. Budući da formula $\psi(\boldsymbol{y}, \boldsymbol{z})$ ne sadrži konstantske simbole, interpretabilna je u $\langle \omega; +, \cdot, s \rangle$ pa je $F_{\psi,\xi}$ dobro definirana. Sad za fiksno ξ, koristeći lemu 3.2.7, particijama $F_{\psi,\xi}$ možemo pridružiti particiju $P_\xi \colon [M]^e \to r$. Za familiju particija $(P_\xi : \xi < 2^M)$ tada možemo naći $\boldsymbol{x} \subseteq M$ koji zadovoljava uvjete (i) i (ii) iz propozicije 3.2.11.

Označimo s $x_0 < \cdots < x_{k-1}$ najmanjih k elemenata skupa $\boldsymbol{x}$ i pokažimo da je $\langle \omega; +, \cdot, s, x_0, \dots, x_{k-1} \rangle$ model za S.

Jasno je da su svi aksiomi oblika (i) za T zadovoljeni, a istinitost aksioma oblika (ii) odmah slijedi iz 3.2.11(i).

Pokažimo još da su svi aksiomi oblika (iii) za T zadovoljeni. Uzmimo proizvoljan takav. Neka je $i < k$, $\theta(\boldsymbol{y}, \boldsymbol{z})$ ograničena formula te $i < \boldsymbol{l}$, $\boldsymbol{l'} < k$, gdje su $\boldsymbol{l}$ i $\boldsymbol{l'}$ nizovi iste duljine. Pripadni je aksiom $\forall \boldsymbol{y} < c_i[\theta(\boldsymbol{y}, c(\boldsymbol{l})) \leftrightarrow \theta(\boldsymbol{y}, c(\boldsymbol{l'}))]$.

Budući da je c_i interpretiran brojem x_i, da bismo provjerili istinitost aksioma, gledamo valuacije za koje je svaki član niza $\boldsymbol{y}$ interpretiran prirodnim brojem manjim od x_i. Treba pokazati da za svaku takvu v formule $\theta(v(\boldsymbol{y}), \boldsymbol{x}(\boldsymbol{l}))$ i $\theta(v(\boldsymbol{y}), \boldsymbol{x}(\boldsymbol{l'}))$ imaju istu istinitosnu vrijednost.

Pridružimo valuaciji v kod ζ njenih vrijednosti na $\boldsymbol{y}$, pri čemu je $\zeta < 2^{x_i}$. Iz propozicije 3.2.11 slijedi da je $\boldsymbol{x} \setminus (x_i + 1)$ homogen za P_ζ, pa onda i za $F_{\theta,\zeta}$, iz čega zaključujemo da za proizvoljne $\boldsymbol{x}(\boldsymbol{j})$, $\boldsymbol{x}(\boldsymbol{j'}) \in \boldsymbol{x} \setminus (x_i + 1)$ formule $\theta(\boldsymbol{a}(\zeta), \boldsymbol{x}(\boldsymbol{j}))$ i $\theta(\boldsymbol{a}(\zeta), \boldsymbol{x}(\boldsymbol{j'}))$ imaju istu istinitosnu vrijednost. Posebno, $\theta(\boldsymbol{a}(\zeta), \boldsymbol{x}(\boldsymbol{l}))$ i $\theta(\boldsymbol{a}(\zeta), \boldsymbol{x}(\boldsymbol{l'}))$ imaju istu istinitosnu vrijednost. Iz ovoga slijedi istinitost aksioma. □

Sad prelazimo na dokaz glavnog teorema ovog poglavlja. Kao jednostavnu posljedicu teorema dobit ćemo i dokaz teorema 3.1.1. Za iskaz teorema bit će nam potrebna definicija dokazivo rekurzivne funkcije.

Neka je g rekurzivna funkcija. Iz teorema o grafu tada slijedi da joj je graf rekurzivna relacija te je definabilan Σ_1-formulom u PA. Označimo s $g(x) \simeq y$ Σ_1-formulu teorije PA koja izražava da (x, y) pripada grafu od g.

Definicija 3.2.13. *Rekurzivna funkcija g je PA-**dokazivo rekurzivna** ako*

$$\mathsf{PA} \vdash \forall x \exists y \, (g(x) \simeq y).$$

Dakle, rekurzivna funkcija je PA-dokazivo rekurzivna ako PA može dokazati njenu totalnost. Poznato je da klasa PA-dokazivo rekurzivnih funkcija sadrži sve primitivno rekurzivne funkcije [10]. Posebno su sve elementarne funkcije, kao što su zbrajanje, množenje, dijeljenje, eksponencijalna funkcija, PA-dokazivo rekurzivne. Primjer funkcije koja nije primitivno rekurzivna, a PA dokazuje njenu totalnost, je Ackermannova funkcija. Ipak, nisu sve rekurzivne funkcije PA-dokazivo rekurzivne. Jedna je takva, kao što ćemo uskoro vidjeti, funkcija f definirana na početku ovog poglavlja.

Teorem 3.2.14. *Ako je $g \colon \omega \to \omega$ PA-dokazivo rekurzivna funkcija, tada postoji prirodan broj n takav da $m \geq n$ povlači $f(m) > g(m)$, za svaki prirodan broj m .*

Prije nego krenemo na dokaz teorema, vratit ćemo se na komentar s početka ovog poglavlja. Kad smo htjeli dati intuitivno objašnjenje zašto je Ramseyjev teorem za relativno velike skupove nedokaziv u PA, rekli smo da je, za općeniti x, vrijednost $f(x)$ „toliko velika da PA ne može dokazati da uopće postoji".

Ovaj teorem daje malo jasniju sliku o tome što se ovdje zapravo događa. Rekurzivne su funkcije ono što smatramo dobrim funkcijama - funkcije koje znamo izračunati, za svaku ulaznu vrijednost, i izraziti formulama teorije PA. Dokazivo rekurzivne funkcije možemo u tom smislu zamišljati kao aparat koji smijemo koristiti za opisivanje drugih objekata unutar PA. Dakle, problem s kojim se ovdje susrećemo je sljedeći: znamo da za svaki konkretni prirodan broj a vrijednost $f(a)$ postoji, međutim, kad bismo za neki općeniti x htjeli opisati $f(x)$ jezikom PA (ili barem postaviti gornju među za tu vrijednost), u opisu ne bismo mogli upotrijebiti nijednu takvu funkciju.

Sad dajemo dokaz teorema 3.2.14.

Dokaz. Za potrebe ovog dokaza alfabetu teorije T dodat ćemo još jedan konstantski simbol c (bit će jasno da će sve tvrdnje koje budemo koristili vrijediti i za ovako promijenjenu teoriju). Pretpostavimo da za svako $n \in \omega$ postoji $m \geq n$ takav da je $f(m) \leq g(m)$ i pokažimo da g tada nije PA-dokazivo rekurzivna.

Neka je S proizvoljan konačan podskup aksioma od T i neka je $k \in \omega$ takav da su svi konstantski simboli koji se pojavljuju u S sadržani u $c(k)$. Iz dokaza propozicija 3.2.11 i 3.2.12 vidljivo je da za dovoljno velik n možemo naći $a \geq n$ takav da je $f(a) \leq g(a)$ i da je k elemenata skupa $\boldsymbol{x}$, koji će interpretirati konstantske simbole, sadržano u intervalu $[a, f(a)]$.

Označimo sa S' skup formula koji dobijemo kad skupu S dodamo formulu $c \leq c_0$ te za svako $i < k$ formulu $\forall x < c_i \, \neg(g(c) \simeq x)$. Iz dokaza propozicije 3.2.12 i početne pretpostavke slijedi da S' ima model kojem je nosač skup prirodnih brojeva s operacijama zbrajanja, množenja i sljedbenika, pri čemu su $c_0, \ldots, c_{k-1}$ interpretirani elementima skupa $\boldsymbol{x}$, a c se interpretira kao a. Iz teorema kompaktnosti sad zaključujemo da skup T' koji sadrži aksiome teorije T i formule $c \leq c_0$ te za svako $i \in \omega$ formulu $\forall x < c_i \, \neg(g(c) \simeq x)$ ima model $\mathfrak{M} = (M, \varphi)$. Iz propozicije 3.2.3 tada slijedi da je struktura $\mathfrak{I}$ kojoj je nosač I početni komad skupa M određen s $c_i^{\mathfrak{M}}$, $i \in \omega$, model za PA.

Kad bi postojao $d \in I$ takav da $\mathfrak{I} \models g(c) \simeq d$, vrijedilo bi $\mathfrak{M} \models g(c) \simeq d \land d < c_i$ za neko $i \in \omega$, što je kontradikcija s pretpostavkom da je $\mathfrak{M}$ model za T'. Dakle, mora vrijediti $\mathsf{PA} \not\vdash \forall x \exists y \, (g(x) \simeq y)$ pa g nije PA-dokazivo rekurzivna. $\square$

Iz definicije funkcije f jasno je da je f parcijalno rekurzivna funkcija, a iz Ramseyjevog teorema za relativno velike skupove slijedi da je i totalna. Iz ovoga odmah dobivamo sljedeći korolar:

Korolar 3.2.15. $\mathsf{PA} \not\vdash \forall x \exists y \, (f(x) \simeq y)$.

Iz ovog korolara slijedi da Ramseyjev teorem za relativno velike skupove nije dokaziv u PA (lako je vidjeti da je dokaz da Ramseyjev teorem za relativno velike skupove povlači $\forall x \exists y \, (f(x) \simeq y)$ moguće provesti u PA). Ovim razmatranjima dokazali smo teorem 3.1.1.

3.3 Indikatori

U ovom dijelu dajemo kratak osvrt na dokaz Paris-Harringtonovog teorema pomoću indikatora. Indikatori su formule teorije PA koje zadovoljavaju određene uvjete i glavni su nositelji općenite tehnike razvijene za dokazivanje neodlučivosti formula u PA.

Da bismo mogli definirati indikatore, potrebno je prvo nešto reći o početnim segmentima modela za PA. Prisjetimo se, ako je $\mathfrak{M} = (M, \varphi)$ model za PA, tada je $I \subseteq M$ početni segment od M (s obzirom na φ) ukoliko za svako $a \in I$ i $b <^{\mathfrak{M}} a$ vrijedi $b \in I$. U svakom modelu za PA možemo naći barem dva početna segmenta, prazan skup i M. Nas će ovdje zanimati početni segmenti različiti od ova dva trivijalna, pravi početni segmenti, koji još imaju dodatno svojstvo zatvorenosti na funkciju sljedbenika.

Definicija 3.3.1. *Neka je $\mathfrak{M} = (M, \varphi)$ model za* PA *te $I \subset M$ pravi početni segment od M. Kažemo da je I **usjek** od M (s obzirom na φ) ako je I zatvoren na $s^{\mathfrak{M}}$. U tom slučaju pišemo $I \subset_e M$.*

Iz definicije slijedi da je usjek zatvoren i na $+^{\mathfrak{M}}$ i $\cdot^{\mathfrak{M}}$ pa inducira jednu strukturu za PA, s funkcijama zbrajanja, množenja i sljedbenika naslijeđenima iz $\mathfrak{M}$.

Za svaki model $\mathfrak{M}$ od PA koji nije izomorfan standardnom (skup ω s operacijama zbrajanja, množenja i funkcijom sljedbenika) možemo naći usjek N od M izomorfan skupu ω. Krenimo od najmanjeg elementa u M (s obzirom na $<^{\mathfrak{M}}$), $0^{\mathfrak{M}}$. Tada pomoću funkcije sljedbenika možemo doći do sljedećeg najmanjeg elementa $s^{\mathfrak{M}}(0^{\mathfrak{M}})$, pa do sljedećeg, $s^{\mathfrak{M}}(s^{\mathfrak{M}}(0^{\mathfrak{M}}))$, i tako dalje. Na ovaj način dolazimo do skupa N koji izgleda kao ω i čiji elementi zadovoljavaju aksiome zbrajanja i množenja. Iz ovoga slijedi da je N, zajedno s funkcijama zbrajanja, množenja i sljedbenika naslijeđenima iz $\mathfrak{M}$, i sam model za PA (ovakav ćemo model označavati s $\mathfrak{N}$). U skladu s oznakama uvedenima u poglavlju 1, s $a >^{\mathfrak{M}} N$ ćemo označavati činjenicu da je a veći, s obzirom na $<^{\mathfrak{M}}$, od bilo kojeg elementa iz N (takav ćemo a zvati nestandardnim elementom od M).

Spomenimo još da za svaki nestandardni model od PA možemo pronaći usjeke različite od ovako dobivenog N koji su također nosači modela za PA (vidi [8]).

Usjeci nisi definabilni aritmetičkim formulama u PA. Naime, kad bi postojala formula $\theta(x)$ takva da

$$\mathfrak{M} \models \theta(a) \text{ ako i samo ako } a \in I,$$

gdje je $I \subset_e M$, tada bi moralo vrijediti

$$\mathfrak{M} \models \theta(0) \wedge \forall x(\theta(x) \to \theta(s(x))) \wedge \neg \forall x \theta(x)$$

pa jedna instanca sheme aksioma indukcije ne bi bila istinita u $\mathfrak{M}$. Ipak, iako usjeke nije moguće izravno izraziti u PA, često je moguće definirati formule koje ukazuju na prisustvo usjeka s određenim svojstvom $\mathcal{P}$. Takve formule bit će indikatori.

Definicija 3.3.2. *Formula $Y(x, y, z)$ je **indikator** za usjeke sa svojstvom $\mathcal{P}$ ako vrijedi:*

(i) $Y(x, y, z)$ *je* Σ_1*-formula,*

(ii) $\mathsf{PA} \vdash \forall x \forall y \exists! z\, Y(x, y, z)$,

što nam omogućuje da formuli Y u danom modelu $\mathfrak{M}$ za PA *pridružimo funkciju $Y^{\mathfrak{M}} \colon M \times M \to M$, definiranu s*

$$Y^{\mathfrak{M}}(a, b) = c \text{ ako i samo ako } \mathfrak{M} \models Y(a, b, c).$$

Naposljetku, treba vrijediti

(iii) $Y^{\mathfrak{M}}(a, b) >^{\mathfrak{M}} N$ *ako i samo ako postoji* $I \subset_e M$ *sa svojstvom* $\mathcal{P}$ *takav da je* $a \in I$ *i* $b >^{\mathfrak{M}} I$.

Dakle, „velika" (veća od svakog standardnog elementa u M) vrijednost $Y^{\mathfrak{M}}(a, b)$ pokazatelj je da postoji usjek I od M sa svojstvom $\mathcal{P}$ kojem je desni rub smješten unutar $[a, b\rangle$.

Slika 3.1: Indikatori nam pomažu da odredimo položaj usjeka.

Može se pokazati da za dosta zanimljivih svojstava $\mathcal{P}$ postoje indikatori. Mi ćemo se ovdje detaljnije pozabaviti indikatorima za svojstvo da je usjek model za PA, važnima za dokazivanje neodlučivosti formula u PA. Da bismo mogli objasniti vezu između ovakvih indikatora i neodlučivosti, potreban nam je teorem koji ćemo sad iskazati (za dokaz vidi [19]).

Teorem 3.3.3. *Neka je $\mathfrak{M}$ model teorije* PA *te Y indikator za modele* PA*. Označimo s $Y(x, y) > z$ formulu $\exists t (Y(x, y, t) \wedge t > z)$. Tada vrijedi:*

(i) $\mathsf{PA} \vdash \forall x \exists y\, (Y(x, y) > \overline{n})$, *za svako* $n \in \omega$,

(ii) $\mathfrak{N} \models \forall x \forall z \exists y\, (Y(x,y) > z)$, *te*

(iii) $\mathsf{PA} \not\vdash \forall x \forall z \exists y\, (Y(x,y) > z)$.

Iz tvrdnji (ii) i (iii) odmah slijedi da je, ako je $Y(x,y,z)$ indikator modela teorije PA, formula $\forall x \forall z \exists y\, (Y(x,y) > z)$ neodlučiva u PA.

Da bismo dokazali neodlučivost neke formule u PA, cilj je zapisati je u obliku

$$\forall x \forall z \exists y\, (Y(x,y) > z),$$

gdje je $Y(x,y,z)$ indikator modela teorije PA. Naputak kako konstruirati formulu Y čitamo iz (iii): naša tvrdnja zapisana u terminima x, y, z trebala bi biti takva da vrijednost od y raste jako brzo u usporedbi s vrijednostima x i z.

Pogledajmo sad kako ove primjedbe možemo iskoristiti da dobijemo drugi dokaz Paris-Harringtonovog teorema. S obzirom da nam je ovdje glavni cilj objasniti ideju dokaza i usporediti ga s onim danim u prethodnom dijelu, većinu tvrdnji komentirat ćemo samo neformalno (detaljniji dokaz može se naći u [16]).

Prisjetimo se funkcije f, definirane u prethodnom dijelu ovog poglavlja, koja je broju x pridruživala najmanji y takav da $y \underset{*}{\longrightarrow} (x+1)^x_x$ (odnosno, najmanji y takav da za svaku particiju $P\colon [y]^x \to x$ postoji podskup od y kardinalnosti barem $x+1$ homogen za P). Bitno svojstvo funkcije f bilo je da f raste jako brzo, brže od bilo koje PA-dokazivo rekurzivne funkcije, uključujući Ackermannovu funkciju. U skladu s tim, definiramo $Y(x,y,z)$ kao aritmetički zapis rečenice

$$\text{„}z \text{ je makismalan t.d. } [x,y] \underset{*}{\longrightarrow} (z+1)^z_z\text{"}\ .$$

Objasnimo prvo zašto bi iz pretpostavke $\mathsf{PA} \not\vdash \forall x \forall z \exists y\, (Y(x,y) > z)$ slijedila nedokazivost teorema 2.3.5 u PA.

Lako je vidjeti da ako za neke x, y, z vrijedi $[x,y] \underset{*}{\longrightarrow} (z+1)^z_z$, tada vrijedi i $[x,y] \underset{*}{\longrightarrow} (u+1)^u_u$ za svako $u < z$. Naime, proizvoljnu particiju P skupa svih u-članih podskupova od $[x,y]$ možemo proširiti na particiju P' skupa svih z-članih podskupova od $[x,y]$ tako da svakom z-članom podskupu od $[x,y]$ pridružimo vrijednost od P na njegovih najmanjih u elemenata. Tada je najmanjih $u+1$ elemenata skupa $\boldsymbol{x}$ kardinalnosti $z+1$, homogenog za P', skup homogen za P. Nakon provođenja dokaza u PA, dobivamo da $\mathsf{PA} \not\vdash \forall x \forall z \exists y\, (Y(x,y) > z)$ povlači $\mathsf{PA} \not\vdash \forall x \forall z \exists y\, ([x,y] \underset{*}{\longrightarrow} (z+1)^z_z)$. Iz ovoga slijedi $\mathsf{PA} \not\vdash \forall z \exists y\, (y \underset{*}{\longrightarrow} (z+1)^z_z)$ (ovdje pod $\forall x \forall z \exists y\, ([x,y] \underset{*}{\longrightarrow} (z+1)^z_z)$ i $\forall z \exists y\, (y \underset{*}{\longrightarrow} (z+1)^z_z)$ zapravo podrazumijevamo formule teorije PA koje izražavaju odgovarajuće tvrdnje). Dokaz teorema 3.1.1 tada dobivamo na isti način kao u dokazu iz prethodnog dijela.

Dokaz da je Y zaista indikator modela za PA nešto je zahtjevniji i ovdje ga nećemo provoditi. Spomenimo samo da se svojstvo (i) iz definicije 3.3.2 provjerava raspisivanjem, a svojstvo (ii) slijedi iz Ramseyjevog teorema za relativno velike skupove (teorem 2.3.5) i primjedbe da je vrijednost od z omeđena odozgo s vrijednosti od y. Za svojstvo (iii) potrebno se malo više pomučiti i dokazati rezultat analogan onome iz propozicije 3.2.3. Pritom ovdje, ponovno koristeći teorem 2.3.5, za proizvoljni model $\mathfrak{M} = (M, \varphi)$ za PA treba naći niz c_i, gdje je $i \in \omega$, elemenata iz M koji zadovoljavaju (ii) i (iii) iz definicije 3.2.1.

U literaturi je moguće pronaći još formula sličnih $\forall z \exists y\, (y \underset{*}{\longrightarrow} (z+1)^z_z)$ koje se također mogu povezati s indikatorima za modele teorije PA. Na taj je način u [22] pokazano da je rečenica $\forall z \exists y\, (y \underset{*}{\longrightarrow} (z+1)^z_3)$ neodlučiva u PA, dok se u [12] može pronaći dokaz za neodlučivost rečenice $\forall z \exists y\, (y \underset{*}{\longrightarrow} (2z)^z_3)$. Iz metode s indikatorima proizašli su i razni drugi primjeri u PA neodlučivih rečenica (vidi [19], [20], [12] i [10]).

Za kraj, pogledajmo jedno obrazloženje, dano u [20], zašto su tvrdnje koje možemo povezati s indikatorima modela za PA nedokazive u PA. Zanimljivo je da je ovo obrazloženje slično onome koje smo dali kad smo, proučavajući dokaz Paris-Harringtonovog teorema koji nije koristio indikatore, pokušali dati odgovor na pitanje zašto teorem 2.3.5 nije dokaziv u PA.

Za svaki prirodan broj m definirajmo funkciju $g_m \colon \omega \to \omega$,

$$g_m(k) = \text{ najmanji } l \text{ t.d. } Y(\overline{k}^{\mathfrak{N}}, \overline{l}^{\mathfrak{N}}) >^{\mathfrak{N}} \overline{m}^{\mathfrak{N}}.$$

Iz definicije 3.3.2(i) i teorema 3.3.3(i) slijedi da je funkcija g_m PA-dokazivo rekurzivna, za svako $m \in \omega$. Također, može se pokazati da vrijedi sljedeći rezultat (za dokaz vidi [19]).

Teorem 3.3.4. *Ako je h PA-dokazivo rekurzivna funkcija, tada postoji $m \in \omega$ takav da je $h(k) < g_m(k)$, za svako $k \in \omega$.*

Definirajmo sad funkciju $g \colon \omega \to \omega$,

$$g(k) = g_k(k) = \text{ najmanji } l \text{ t.d. } Y(\overline{k}^{\mathfrak{N}}, \overline{l}^{\mathfrak{N}}) >^{\mathfrak{N}} \overline{k}^{\mathfrak{N}}.$$

Budući da je $g(k) > g_m(k)$ za sve osim eventualno konačno mnogo k-ova, iz teorema 3.3.4 slijedi da g nije PA-dokazivo rekurzivna te, štoviše, da je ne možemo opisati ni omeđiti nijednom takvom funkcijom. Dakle, opet možemo reći da je za općenite x i z vrijednost y za koju je $Y(x, y) > z$ „toliko velika da PA ne može dokazati da uopće postoji”.

3.4 Hijerarhija brzo rastućih funkcija

U prethodnim smo odjeljcima komentirali dva različita dokaza neodlučivosti Ramseyjevog teorema za relativno velike skupove u PA. Vidjeli smo da u pozadini oba dokaza leži brzo rastuća funkcija koja svugdje, osim u eventualno konačno mnogo točaka, postiže vrijednosti veće od proizvoljne PA-dokazivo rekurzivne funkcije. U ovom ćemo odjeljku malo jasnije dočarati koliko brzo takva funkcija zapravo treba rasti.

Pitanje koliko brz rast je stvarno brz rast uvelike ovisi o kontekstu te je nemoguće dati univerzalan odgovor na njega. Hijerarhije brzo rastućih funkcija su u tom smislu pokušaj stupnjevanja funkcija po brzini rasta. Takva je hijerarhija definirana na način da pri svakom skoku na iduću razinu dobivamo funkciju s puno bržom stopom rasta od funkcije na trenutnoj razini.

Sad definiramo hijerarhiju na način opisan u [13], gdje se koristi ponešto izmijenjena Wainerova hijerarhija [27]. Definiramo $\omega_0 = \omega$, $\omega_{k+1} = \omega^{\omega_k}$, te $\varepsilon_0 = \lim_{k\to\infty} \omega_k$. Zatim, za granični ordinal λ s $(\{\lambda\}(n) : n \in \omega)$ označavamo kanonski rastući niz ordinala kojem je limes λ (detalji konstrukcije takvog niza mogu se naći u [13]). Kao prije, s $F^{(k)}$ označavamo funkciju dobivenu komponiranjem funkcije F same sa sobom k puta.

Za $0 \leq \alpha \leq \varepsilon_0$ definiramo funkcije $F_\alpha \colon \omega \to \omega$,

$$\begin{aligned} F_0(x) &= x+1, \\ F_{\eta+1}(x) &= F_\eta^{(x+1)}(x), \end{aligned}$$

te, za granični ordinal λ,

$$F_\lambda(x) = \max\{F_{\{\lambda\}(j)} : j \leq x\}.$$

Kako bismo ilustrirali kolike su razlike u stopama rasta među funkcijama na susjednim razinama, navodimo ocjene za brzine rasta prvih nekoliko funkcija u hijerarhiji. Tako je $F_1(x) \approx 2x$, $F_2(x) \approx 2^x$, $F_3(x) \approx 2^{2^{\cdot^{\cdot^{\cdot^{2^x}}}}}$ (u izrazu se pojavljuje x dvojki), a funkcija F_4 već raste toliko brzo da se, za razliku od prve četiri funkcije, ne može opisati ni na koji elementarniji način. Funkcija F_ω raste kao Ackermannova funkcija.

Može se pokazati da je za svaki $\alpha \leq \varepsilon_0$ funkcija F_α strogo rastuća, za $\alpha < \omega$ primitivno rekurzivna, te, za $\alpha < \varepsilon_0$, PA-dokazivo rekurzivna. Osim toga, svaka PA-dokazivo rekurzivna funkcija g dominirana je nekom funkcijom iz hijerarhije (točnije, za danu PA-dokazivo rekurzivnu funkciju g postoje $\alpha < \varepsilon_0$ i $n \in \omega$ takvi da je $g(m) < F_\alpha(m)$, za sve $m \geq n$). Također se može pokazati da je za $\alpha, \beta \leq \varepsilon_0$ funkcija F_α dominirana funkcijom F_β ako i samo ako je $\alpha < \beta$ [13]. Dakle, funkcija F_{ε_0} je prva funkcija u hijerarhiji koja je dominantna nad svim PA-dokazivo rekurzivnim funkcijama.

Hijerarhija brzo rastućih funkcija je, osim za karakterizaciju rekurzivnih funkcija, važna i za bolje razumijevanje fenomena nedokazivosti istinitih i prirodnih matematičkih tvrdnji u Peanovoj aritmetici. Jedna tehnika za dokazivanje neodlučivosti takve tvrdnje u PA je pokazati da generira funkciju koja je po stupnju brzine rasta usporediva s F_{ε_0} (u svjetlu toga, razinu ε_0 možemo doživljavati kao granicu Peanove aritmetike). Na taj je način u [13] pokazano da Ramseyjev teorem za relativno velike skupove nije dokaziv u PA. Navodimo glavne rezultate iz [13].

Označimo sa σ funkciju definiranu s

$$\sigma(x,y) = \mu z[z \underset{*}{\longrightarrow} (x+1)^x_y].$$

Tada je $\sigma(x,x) = f(x)$, gdje je f funkcija definirana na početku odjeljka 3.2, te je $\sigma(x,x)$ reda veličine $F_{\varepsilon_0}(x-2)$. Naime, za $x \geq 20$ vrijede sljedeće ocjene:

$$\begin{array}{rcccl} F_{\varepsilon_0}(x-3) & \leq & \sigma(x,8) & \leq & F_{\varepsilon_0}(x-2), \\ F_{\varepsilon_0}(x-4) & \leq & \sigma(x,7) & \leq & F_{\varepsilon_0}(x-2). \end{array}$$

Također, vrijedi

$$\sigma(x,x-7) \leq F_{\varepsilon_0}(x-2) \quad \text{te} \quad \sigma(x,x) \leq F_{\varepsilon_0}(x-1).$$

POGLAVLJE 4

Još neke nedokazive formule u Peanovoj aritmetici

U prethodnim poglavljima bavili smo se primjerom jedne u Peanovoj arimetici neodlučive rečenice, Ramseyjevim teoremom za relativno velike skupove (teorem 2.3.5). Teorem smo iskazali i dokazali te smo proveli dokaz da teorem nije dokaziv u teoriji PA. Također smo naveli par primjera nedokazivih rečenica usko povezanih s teoremom 2.3.5.

U ovom poglavlju navodimo još neke druge primjere u Peanovoj aritmetici neodlučivih rečenica. Iako ćemo definirati i objasniti sve potrebne pojmove, nećemo ništa dokazivati.

4.1 Goodsteinov teorem

Prvi primjer koji navodimo je jedan teorem teorije brojeva, Goodsteinov teorem.

Za prirodne brojeve m i n prvo definiramo reprezentaciju broja m u bazi n na sljedeći način. Zapišimo m kao zbroj potencija broja n,

$$m = \alpha_k n^k + \alpha_{k-1} n^{k-1} + \cdots + \alpha_1 n + \alpha_0,$$

gdje je $\alpha_k \neq 0$ i $0 \leq \alpha_i < n$ za $i \leq k$ (poznato je da za svaki prirodan broj m ovo možemo napraviti na jedinstven način). Sad isti postupak ponovimo s eksponentima, zatim s eksponentima eksponenata i tako dalje dok svaki broj u zapisu ne bude manji ili jednak n. Primjerice, zapis u bazi 2 za broj 515 dobivamo ovako:

$$515 = 2^9 + 2 + 1 = 2^{2^3+1} + 2 + 1 = 2^{2^{2+1}+1} + 2 + 1.$$

Sad definiramo Goodsteinov niz $G(m)$ broja m, $G(m) = (m_k)_{k \in \omega}$. Prvi član niza je m. Ako je m jednak 0, sljedeći član niza je 0. Ako je m različit od 0, zapišemo ga u bazi

2, kao što je opisano. Sljedeći član niza m_1 dobivamo tako da sve nastupe broja 2 u tom zapisu zamijenimo s 3 i oduzmemo 1. Zatim m_2 dobivamo iz m_1 tako da sve nastupe broja 3 zamijenimo s 4 i oduzmemo 1 i tako dalje. Općenito, u k-tom koraku m_k dobivamo tako da sve nastupe broja $k+1$ u zapisu m_{k-1} u bazi $k+1$ zamijenimo s $k+2$ i oduzmemo 1. Kao primjer navodimo prvih nekoliko članova niza $G(14)$:

$$\begin{aligned}
14_0 &= 2^{2+1} + 2^2 + 2, \\
14_1 &= 3^{3+1} + 3^3 + 2 = 110, \\
14_2 &= 4^{4+1} + 4^4 + 1 = 1281, \\
14_3 &= 5^{5+1} + 5^5 = 18750.
\end{aligned}$$

Ovim smo opisali Goodsteinove nizove koji počinju sa zapisom u bazom 2. Na analogan način mogu se definirati nizovi koji počinju s bazom n, za bilo koji $n > 1$.

Goodsteinovi nizovi već za male vrijednosti broja m rastu jako brzo. Tako niz koji počinje s 19 u samo pet koraka premašuje vrijednost $10^{500\,000}$. Tim više iznenađuje sljedeći rezultat. Štoviše, može se pokazati da isti rezultat vrijedi za nizove koji počinju s bazom n ($n > 1$) [15].

Teorem 4.1.1 (Goodstein)**.** *Za svaki m postoji $k \in \omega$ takav da je $m_k = 0$.*

Dokaz Goodsteinovog teorema koristi svojstva ordinalnih brojeva (vidi [26]) te se ne može formalizirati u Peanovoj aritmetici. Prvi dokaz nedokazivosti Goodsteinovog teorema u PA pomoću teorije indikatora dan je u [15], a još jedan dokaz može se naći u [7].

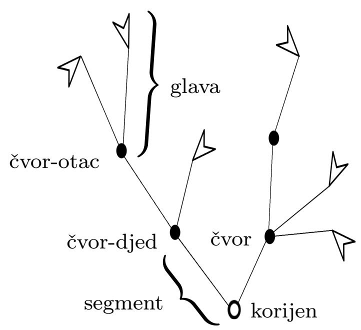
Uz Goodsteinov teorem veže se brzo rastuća Goodsteinova funkcija $\mathcal{G}$ koja prirodnom broju m pridružuje najmanji k takav da je $m_k = 0$. Goodsteinova funkcija raste kao F_{ϵ_0} definirana u odjeljku 3.4. Za ilustraciju navodimo prvih nekoliko vrijednosti funkcije $\mathcal{G}$:

$$\begin{aligned}
\mathcal{G}(1) &= 1, \\
\mathcal{G}(2) &= 3, \\
\mathcal{G}(3) &= 5, \\
\mathcal{G}(4) &= 3 \cdot 2^{402\,653\,211} - 3.
\end{aligned}$$

Izvod za vrijednost $\mathcal{G}(4)$ može se naći u [24].

4.2 Heraklo i Hidra

Još jedan primjer u Peanovoj aritmetici nedokazive formule proizašao je iz igre inspirirane pričom o borbi grčkog junaka Herakla s nemani Hidrom. U igri je Hidra predstavljena stablom s jednim istaknutim čvorom na nultoj razini, korijenom (vidi sliku 4.1). Relacije među čvorovima prikazane su segmentima. Čvor koji nema nasljednika (čvorova koji su točno iznad njega), zajedno s pripadnim segmentom, nazivamo glava. Čvor koji je točno ispod takvog čvora je njegov čvor-otac, a čvor točno ispod čvora-oca (ukoliko takav postoji) njegov čvor-djed.

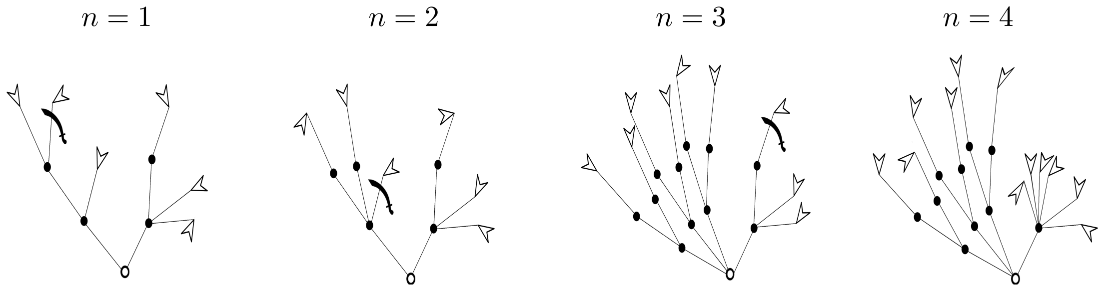


Slika 4.1: Hidra

U n-tom vremenskom trenutku Heraklo odsijeca jednu glavu Hidri. Ukoliko je čvor-otac odsječene glave korijen, ne događa se ništa. Ako čvor-otac nije korijen, u sljedećem trenutku iz čvora-djeda odsječene glave niče još n kopija ovako osakaćenog podstabla (vidi sliku 4.2). Heraklo pobjeđuje ako uspije obezglaviti Hidru, to jest, sasijeći je do korijena, u konačnom broju koraka.

Čini se da broj Hidrinih glava sa svakim korakom nezaustavljivo buja pa je pomalo iznenađujuća tvrdnja da Heraklo uvijek pobjeđuje, bez obzira kojim redom odsijecao glave. Definiramo li strategiju kao funkciju koja prirodnom broju n pridružuje glavu koju Heraklo odsijeca u n-tom vremenskom trenutku, ovu tvrdnju možemo iskazati u obliku sljedećeg teorema. Dokaz teorema, slično kao i dokaz Goodsteinovog teorema, koristi svojstva ordinala [15].

Teorem 4.2.1. *Svaka Heraklova strategija vodi do pobjede.*



Slika 4.2: Heraklo odsijeca glave Hidri

Štoviše, može se pokazati da isti rezultat vrijedi i promijenimo li pravila igre na način da u svakom koraku odsječenu glavu zamjenjuje proizvoljan prirodan broj pripadnih podstabala.

Neformalno, Hidra tokom igre postaje šira, ali i niža. Naime, svaku glavu možemo strpljivim odsijecanjem nakon nekog vremena srezati do podstabla s konačnim brojem glava na prvoj razini, odmah iznad korijena, a takve glave više ne mogu dati nove glave. Kad jednom sve glave snizimo na prvu razinu, u svakom sljedećem trenutku smanjujemo broj glava za jedan te Hidra naposljetku umire.

Strategije su općenito beskonačni objekti pa tvrdnju da Heraklo uvijek pobjeđuje ne možemo izraziti u Peanovoj aritmetici. Ipak, u PA je moguće izraziti sljedeći teorem:

Teorem 4.2.2. *Svaka rekurzivna Heraklova strategija vodi do pobjede.*

Iako je ovu tvrdnju moguće izraziti u Peanovoj aritmetici, nije je moguće dokazati unutar PA. Kao moguće objašnjenje obično se navodi velik broj koraka potreban da bitka završi [18].

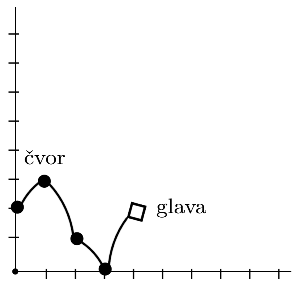
Prvi dokaz neodlučivosti pomoću indikatora može se naći u [15], a još jedan dokaz dan je u [5].

4.3 Bitka s crvom

Bitka s crvom je primjer još jedne igre iz koje je proizašla tvrdnja nedokaziva u Peanovoj aritmetici.

Crv se sastoji od čvorova, kao što je prikazano na slici 4.3. Posljednji čvor je istaknut i nazivamo ga glava. Cilj je igre obezglaviti crva, no, kao što ćemo vidjeti, igra je u ovom slučaju potpuno deterministička.

Formalno, u bilo kojem vremenskom trenutku crva možemo promatrati kao funkciju kojoj je domena neki prirodan broj m, a kodomena skup ω. Tako crvu na slici 4.3 pridružujemo funkciju $f\colon 5 \to \omega$ s vrijednostima $f(0) = 2$, $f(1) = 3$, $f(2) = 1$, $f(3) = 0$ i $f(4) = 2$. Često koristimo jednostavniji zapis, niz $(f(0), \dots, f(m-1))$, pa tako crvu na slici 4.3 pridružujemo niz $(2, 3, 1, 0, 2)$ ili, još jednostavnije, broj 23102 (ovaj zapis koristimo samo kad su sve vrijednosti niza manje od 10).



Slika 4.3: Crv

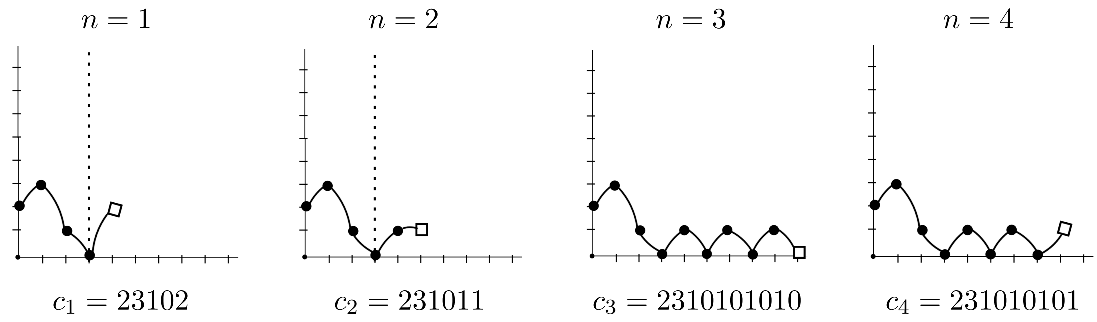
Pravila igre ilustrirana su na slici 4.4. Ako u n-tom vremenskom trenutku glava crva $c_n = (f(0), \dots, f(m))$ ima vrijednost 0, posljednji čvor nestaje, a pretposljednji preuzima ulogu glave. Tada u trenutku $n + 1$ ostaje crv $c_{n+1} = (f(0), \dots, f(m-1))$. Ako je pak $f(m)$ različito od 0, tražimo najveći k takav da je $f(k) < f(m)$. Označimo s r prvih $k + 1$ čvorova crva, $r = (f(0), \dots, f(k))$, te sa s ostatak s vrijednosti glave umanjene za 1, $s = (f(k+1), \dots, f(m) - 1)$. Pritom dopuštamo da r bude prazan (u slučaju da ne postoji k takav da je $f(k) < f(m)$). U sljedećem trenutku c_{n+1} dobijemo tako da spojimo niz r s $n + 1$ kopija niza s,

$$c_{n+1} = r * \underbrace{s * \cdots * s}_{n+1 \text{ puta}}.$$

Crv u kratkom vremenskom roku može nabujati do jako velikog broja čvorova. Ipak, može se pokazati da vrijedi sljedeći teorem.

Teorem 4.3.1. *Svaki crv umire.*

Neformalno objašnjenje za ovakav rezultat slično je kao kod Herakla i Hidre: tokom vremena crv raste samo u širinu, ne i u visinu. Budući da se glava u svakom koraku miče za



Slika 4.4: Crv $c_0 = 23103$ u sljedeća četiri vremenska trenutka

jedno mjesto dolje ili ulijevo, crv nakon nekog vremena postaje sve kraći i niži te naposljetku umire.

Teorem 4.3.1, iako izraziv, nije dokaziv u PA. Zanimljivo je još da je neodlučivost tvrdnje teorema 4.3.1 u Peanovoj aritmetici usko povezana s neodlučivosti tvrdnje teorema 4.2.2 (vidi [1]). Naime, može se pokazati da je ova igra ekvivalentna (do na neke detalje) igri Herakla i Hidre - bitka Herakla i Hidre može se skoro korak po korak prevesti u bitku s crvom i obratno (za detalje vidi [6]).

Dokaz da je teorem 4.3.1 nedokaziv u Peanovoj aritmetici može se naći u [1].

4.4 Kruskalov teorem o konačnim stablima

U ovom ćemo odjeljku, da bismo iskazali Kruskalov teorem u izvornom obliku, koristiti nešto drugačiju definiciju stabla od one uvedene u odjeljku 2.3. Reći ćemo da je $(T, \leq_T)$ stablo ako je $\leq_T$ parcijalni uređaj na skupu T s dodatnim svojstvima da T ima minimalni element (korijen) te da je za svaki $t \in T$ skup $\{s \in T : s \leq_T t\}$ linearno uređen. Lako je vidjeti da smo ovim obuhvatili i definiciju 2.3.1 (za stablo S koje zadovoljava 2.3.1 mogli bismo definirati $a \leq_S b$ ako postoji niz $s_1, \ldots, s_k$ iz S takav da je $s_1 = a$, $s_k = b$ te je s_{i+1} točno iznad s_i, za svako $i < k$).

Za $t, t' \in T$ s $\inf_T(t, t')$ označavamo najveći element skupa T takav da je $\inf_T(t, t') \leq_T t$ i $\inf_T(t, t') \leq_T t'$ (neformalno, $\inf_T(t, t')$ je prvi čvor u kojem se putevi iz t i t' prema korijenu susreću). Kažemo da stablo $(S, \leq_S)$ možemo **uložiti** u $(T, \leq_T)$ i pišemo $S \trianglelefteq T$ ako postoji injektivna funkcija $h \colon S \to T$ takva da vrijedi $h(inf_S(s, s')) = inf_T(h(s), h(s'))$ za sve $s, s' \in S$.

Sad možemo iskazati verziju Kruskalovog teorema za konačna stabla.

Teorem 4.4.1 (Kruskalov teorem o konačnim stablima)**.** *Neka je k prirodan broj. Tada postoji prirodan broj n takav da za proizvoljna konačna stabla $T_1, \ldots, T_n$ koja zadovoljavaju*

$$\operatorname{card} T_i \leq k + i \quad (i \leq n)$$

postoje $i < j \leq n$ takvi da vrijedi $T_i \trianglelefteq T_j$.

Friedman je dokazao da ova verzija Kruskalovog teorema nije dokaziva u Peanovoj aritmetici (svi se dokazi mogu naći u [9]). Ono što Kruskalov teorem čini posebno zanimljivim je da nije dokaziv ni u nekim teorijama jačim od Peanove aritmetike. Također, i uz Kruskalov se teorem veže jedna funkcija koja raste izuzetno brzo.

Definirajmo $\mathcal{T}$ kao funkciju koja prirodnom broju k pridružuje najmanji n koji zadovoljava tvrdnju teorema 4.4.1. Tada funkcija $\mathcal{T}$ raste brže od bilo koje rekurzivne funkcije čiju totalnost možemo dokazati metodama predikatne matematike, uključujući sve PA-dokazivo rekurzivne funkcije. Poznato je, primjerice, da vrijedi $\mathcal{T}(100) \geq 2^{2^{\cdot^{\cdot^{\cdot^{2}}}}}$ (u izrazu s desne strane 2 se pojavljuje 1000 puta).

Na kraju, navodimo jedan noviji rezultat. Još primjera nedokazivih formula u Peanovoj aritmetici može se naći u [4].

4.5 Friedmanov teorem

Teorem 4.5.1 (Friedman)**.** *Neka je k prirodan broj. Tada postoji prirodan broj n takav da za proizvoljne racionalne brojeve $x_1, \ldots, x_n$ možemo naći $0 < p_1 < \cdots < p_{k+1} \leq n$ takve da vrijedi*

$$\begin{aligned}
&\big|\sin(x_{p_1} x_{p_2} \cdots x_{p_k}) - \sin(x_{p_1} x_{p_3} \cdots x_{p_{k+1}})\big| < 4^{-p_1} \ \ i \\
&\big|\sin(x_{p_2} x_{p_3} \cdots x_{p_{k+1}}) - \sin(x_{p_2} x_{p_4} \cdots x_{p_{k+2}})\big| < 4^{-p_2}.
\end{aligned}$$

Kao što se navodi u [3], ovaj teorem nije dokaziv u Peanovoj aritmetici. U istom se radu može pronaći dokaz nedokazivosti teorema sličnog ovome. Također se navodi da je funkcija koja prirodnom broju k pridružuje najmanji prirodan broj n za koji vrijedi tvrdnja teorema reda veličine F_{ε_0} te je dominantna nad bilo kojom PA-dokazivo rekurzivnom funkcijom.

Zaključak

Osvrnemo li se na rezultate iznesene u ovom radu, mogli bismo reći da je priča o prirodnim matematičkim tvrdnjama koje nisu dokazive u Peanovoj aritmetici priča o velikim brojevima i brzo rastućim funkcijama. Pritom ovdje govorimo o vrijednostima koje su toliko ekstremno velike da daleko nadilaze sva naša uobičajena poimanja „velikog", bilo u svakodnevnom životu, bilo u standardnoj matematici.

Koliko god ovo objašnjenje bilo lijepo i jednostavno, ipak valja biti oprezan pri donošenju ovakvih zaključaka. U literaturi se može naći još puno tekstova s različitim pristupima u dokazivanju nedokazivosti kojih se ovdje nismo dotakli i za očekivati je da bi tek pručavanje ostalih dokaza dalo potpuniju sliku problema. Zbog toga ovaj rad treba čitati prvenstveno kao dokaz nedokazivosti verzije Ramseyjevog teorema te uvod u nedokazivost u Peanovoj aritmetici, nipošto kao potpuni pregled. Kao početna točka za dublja istraživanja može poslužiti [4], u kojem se može naći opsežni pregled literature o nedokazivosti.

Napokon, teško je povjerovati da je priča o nedokazivim formulama u Peanovoj aritmetici završena. Potraga za matematičkim tvrdnjama koje nisu dokazive u Peanovoj aritmetici relativno je kratkog vijeka - nedokazivost prvih ovakvih primjera dokazana je tek krajem sedamdesetih godina prošlog stoljeća, a najnoviji su primjeri otkriveni u posljednjih nekoliko godina. Možemo zaključiti da nas u budućnosti očekuje nastavak priče, s novim rezultatima i interpretacijama.

Bibliografija

[1] L. D. Beklemishev, *The Worm Principle*, Logic Group Preprint Series, Utrecht University, 2003., `http://www.phil.uu.nl/preprints/lgps/list.html`.

[2] G. Boolos, J.P. Burgess, i R. Jeffrey, *Computability and Logic*, Cambridge University Press, 2002.

[3] A. Bovykin, *Unprovability of Sharp Versions of Friedman's Sine-Principle*, Proceedings of the American Mathematical Society (2007.), br. 135, 2967–2973.

[4] ______, *Brief Introduction to Unprovability*, Logic Colloquium 2006, Lecture Notes in Logic, 2009., 38–64.

[5] L. Carlucci, *A New Proof-Theoretic Proof of the Independence of Kirby-Paris' Hydra Theorem*, Theoretical Computer Science (2003.), br. 300, 365–378.

[6] ______, *Worms, Gaps, and Hydras*, Mathematical Logic Quarterly **51** (2005.), br. 4, 342–350.

[7] A. Cichon, *A Short Proof of Two Recently Discovered Independence Results Using Recursion Theoretic Methods*, Proceedings of American Mathematical Society, sv. 87, 1983., 704–706.

[8] H. Friedman, *Some Applications of Kleene's Methods for Intuitionistic Systems*, Cambridge Summer School of Mathematical Logic (A.R.D. Mathias i H. Rogers, ur.), Lecture Notes in Mathematics, sv. 337, Springer-Verlag, 1971., 113–170.

[9] J.H. Gallier, *What's So Special About Kruskal's Theorem and the Ordinal* Γ_0*? A Survey of Some Results in Proof Theory*, Annals of Pure and Applied Logic **53** (1991.), br. 3, 199–260.

[10] P. Hájek i P. Pudlák, *Metamatemathics of First-Order Arithmetic*, Perspectives in Mathematical Logic, Springer-Verlag, 1998.

[11] A. Kanamori i K. McAloon, *On Gödel Incompleteness and Finite Combinatorics*, Annals of Pure and Applied Logic **33** (1987.), 23–41.

[12] R. Kaye, *Models of Peano Arithmetic*, Clarendon Press, Oxford, 1991.

[13] J. Ketonen i R. Solovay, *Rapidly Growing Ramsey Functions*, Annals of Mathematics **113** (1981.), 267–314.

[14] L. Kirby i J. Paris, *Initial Segments of Models of Peano's Axioms*, Proceedings of the Bierutowice Conference, Springer-Verlag, 1976.

[15] ______, *Accessible Independence Results for Peano Arithmetic*, Bulletin of London Mathematical Society (1982.), br. 14, 285–293.

[16] D. Lascar, *Une indicatrice de type "Ramsey" pour l'arithmétique de Peano et la formule de Paris-Harrington*, Modèles de l'arithmétique (K. McAloon, ur.), Société Mathématique de France, 1980.

[17] E. Mendelson, *Introduction to Mathematical Logic*, Chapman & Hall, 1997.

[18] G. Moser, *The Hydra Battle and Cichon's Principle*, Applicable Algebra in Engineering, Communication and Computing **20** (2009.), br. 2, 133–158.

[19] J. Paris, *Some Independence Results for Peano Arithmetic*, The Journal of Symbolic Logic **43** (1978.), br. 4, 725–731.

[20] ______, *Combinatorial Statements Independent of Arithmetic*, Mathematics of Ramsey Theory (E.J. Nesetril i V. Rodl, ur.), Springer-Verlag, 1991., 232–245.

[21] J. Paris i L. Harrington, *A Mathematical Incompleteness in Peano Arithmetic*, Handbook of Mathematical Logic (J. Barwise, ur.), Studies in Logic and the Foundations of Mathematics, sv. 90, North Holland Publishing Company, 1977., 1133–1142.

[22] J. E. Quinsey, *Some Problems in Logic*, Disertacija, Oxford University, 1980.

[23] T. von der Twer, *Some Remarks on the Mathematical Incompleteness of Peano's Arihmetic Found by Paris and Harrington*, Set Theory and Model Theory (R.B. Jensen i A. Prestel, ur.), Lecture Notes in Mathematics, sv. 872, Springer-Verlag, 1981., 157–174.

[24] M. Vuković, *Matematička indukcija i Goodsteinov teorem*, Poučak (2003.), br. 13, 5–13.

[25] ______, *Matematička logika*, Element, 2009.

[26] ______, *Teorija skupova*, predavanja, 2010., `http://web.math.hr/~vukovic/Diplomski-kolegiji/TS-skripta-2010.pdf`.

[27] S.S. Wainer, *A Classification of the Ordinal Recursive Functions*, Archiv für mathematische Logik und Grundlagenforschung **13** (1970.), 136–153.

Sažetak

U ovom diplomskom radu pokazuje se nedokazivost Ramseyjevog teorema za relativno velike skupove u Peanovoj aritmetici. Definirani su svi pojmovi vezani za teorem te je teorem iskazan i dokazan pomoću beskonačne verzije Ramseyjevog teorema i teorema kompaktnosti.

Dokaz nedokazivosti Ramseyjevog teorema za relativno velike skupove uglavnom slijedi dokaz Paris-Harringtonovog teorema, uz dodatno korištenje svojstava dokazivo rekurzivnih funkcija Peanove aritmetike. Osim Ramseyjevog teorema za relativno velike skupove, u radu su također opisani primjeri nekih drugih u Peanovoj aritmetici nedokazivih formula.

Summary

In this graduate thesis the unprovability of Ramsey's theorem for relatively large sets in Peano arithmetic is shown. The theoretical background necessary for the understanding of proofs is given. The theorem is proved using infinitary Ramsey's theorem and the compactness theorem.

The unprovability proof mostly follows the proof of Paris-Harrington theorem. Additionally, the properties of Peano arithmetic provably recursive functions are used. Besides Ramsey's theorem for relatively large sets, some other examples of formulae unprovable in Peano arithmetic are described.

Životopis

Rođena sam 26. ožujka 1987. godine u Splitu. U Omišu sam pohađala osnovnu školu Josip Pupačić i srednju školu Jure Kaštelan, gdje sam maturirala 2005. godine. Iste godine upisala sam Preddiplomski sveučilišni studij Matematike na Matematičkom odsjeku Prirodoslovno-matematičkog fakulteta u Zagrebu. Godine 2008., nakon završenog preddiplomskog studija, upisala sam Diplomski sveučilišni studij Matematičke statistike na istom odsjeku. Od svibnja do kolovoza 2010. godine radila sam na projektu *Medical Image Automatic Annotation* na sveučilištu Universidade da Beira Interior u Portugalu.