Sveučilište u Zagrebu
PMF–Matematički odjel

Mladen Vuković

IZRAČUNLJIVOST

predavanja

Zagreb, srpanj 2015.

Sadržaj

Predgovor

Ovaj materijal nastao je na osnovu zabilješki iz kolegija *Izračunljivost* koji već niz godina predajem na Prirodoslovno–matematičkom fakultetu – Matematički odsjek Sveučilišta u Zagrebu. Ovaj materijal je prije svega namijenjen studentima koji slušaju navedeni kolegij, odnosno trebaju polagati ispit iz tog kolegija.

Želim naglasiti da ovo nije skripta. To znači da nije proveden postupak recenzije. Naravno, time ne želim reći da imam opravdanje za greške (raznih vrsta) kojih sigurno ima. Svaki ispravak, ili pak sugestiju, koji bi mogli doprinijeti poboljšanju ovog teksta, rado ću prihvatiti.

Zahvaljujem se svim studentima koji su me upozorili na greške, a posebno asistentima dr. sc. Vedranu Čačiću, dr. sc. Zvonku Iljazoviću i Marku Doki.

U Zagrebu, 2015. Mladen Vuković

Poglavlje 1

Izračunljivost

1.1 Uvod

Prilikom proučavanja matematičke logike naveli smo sljedeći **Churchov teorem:**

> Logika prvog reda je **neodlučiva teorija**, tj. ne postoji algoritam koji bi za svaku formulu u konačno mnogo koraka određivao je li dana formula valjana.

Kako bi izreka Churchovog teorema bila sasvim jasna svakako prvo moramo strogo definirati pojam algoritma. Algoritam je jedan od osnovnih pojmova matematike. Prvo ćemo kratko opisati povijest tog pojma.

Riječ **algoritam** dolazi od latiniziranog imena arapskog matematičara **Al-Khwarizmija** koji je u IX. stoljeću dao pravila kako se izvršavaju četiri računske operacije u decimalnom sustavu. Naziv za pojam u današnjem značenju uveo je **G. W. Leibniz** (1646.–1716.) Naziv **algebra** dolazi od *al jabr*, riječi koja je sadržana u naslovu jedne Al-Khwarizmijeve knjige. Knjiga je prevedena na latinski u 13. stoljeću i imala je dubok utjecaj na razvoj europske matematike u doba renesanse. Prijevodom te knjige stigle su u Europu i arapske brojke.

Navodimo neke primjere iz matematike gdje se susrećemo s algoritmima.

Primjer 1.1. *Svakako najpoznatiji algoritmi su algoritmi za zbrajanje, oduzimanje, množenje i dijeljenje decimalnih brojeva koje se uče još u osnovnoj školi. Već smo bili naveli da ih je prvi zapisao Al-Khwarizmi.*

Primjer 1.2. *Jedan od najstarijih algoritama je svakako* **Euklidov algoritam.** *Euklidov algoritam rješava sljedeći problem: za dane prirodne brojeve n*

i m treba odrediti najveću zajedničku mjeru. Algoritam se prvi puta spominje u Euklidovim **Elementima***, ali u geometrijskom obliku. Jednako se naziva i sličan algoritam za određivanje najveće zajedničke mjere dvaju polinoma. Koraci algoritma su sljedeći:*

a) Usporedite prirodne brojeve n i m. Ako je $n = m$ tada postupak staje i rezultat je n. Ako je $n \neq m$ tada prijeđite na sljedeću instrukciju.

b) Neka je $x = \max\{n, m\}$ i $y = \min\{n, m\}$.

c) Označimo $n = x - y$ i $m = y$. Nakon toga prijeđemo na instrukciju a).

Primjer 1.3. *Sada ćemo opisati algoritam za određivanje* **drugog korijena** *proizvoljnog decimalnog broja. Kako bi algoritam bio jasniji primjenjujemo ga za određivanje $\sqrt{34507}$. Koraci algoritma su sljedeći:*

1. *Susjedne znamenke danog broja A spojimo u parove od desna na lijevo. Označimo prvi par slijeva, odnosno znamenku prvu slijeva s L.*

   Za broj 34 507 potcrtamo parove znamenaka: $\underline{3}$, $\underline{45}$ i $\underline{07}$. Sa L označimo broj 3.

2. *Odredimo najveći prirodni broj y čiji je kvadrat manji ili jednak L. Neka je $R = L - y^2$, $x_1 = y$ i $n = 2$.*

   Za broj 34 507 imamo da je $y = 1$, $R = 3 - 1^2 = 2$ i $x_1 = 1$.

3. *Ako više nema parova znamenki zadanog broja koje još nisu uzete u obzir, te je $R = 0$ ili pak ne želimo računati decimalna mjesta drugog korijena prelazimo na instrukciju 6.*

   Ako nema više parova znamenki zadanog broja, te ako je $R \neq 0$, tada ako želimo računati i decimalna mjesta drugog korijena broju R dopišemo dvije nule. Označimo dobiveni broj sa S.

   Ako još ima parova znamenki zadanog broja koje još nisu uzete u obzir tada broju R dopišemo sljedeći par znamenki danog broja. Označimo dobiveni broj sa S.

   Za broj 34 507 imamo da je za $n = 2$ broj S jednak 245.

4. *Odredimo najveći prirodni broj x koji ima svojstvo da vrijedi*

   $$(20 \cdot y + x) \cdot x \leq S.$$

   Neka je $x_n = x$ ako smo broju R dopisali par znamenki danog broja, odnosno neka je $z_n = x$ ako smo broju R dopisali dvije nule jer više nije bilo parova znamenki zadanog broja.

Za zadani broj 34 507 je $x_2 = 8$*, jer je* $(20 \cdot 1 + 8) \cdot 8 < 245$ *i* $(20 \cdot 1 + 9) \cdot 9 > 245$.

5. *Neka je* $R = S - (20 \cdot y + x) \cdot x$*, te n povećamo za jedan (odnosno "programerski":* $n = n + 1$*), te se vratimo na instrukciju 3.*

   Za zadani broj 34 507 i n=2 je $R = 245 - (20 \cdot 1 + 8) \cdot 8 = 21$.

6. *Tada je* $\sqrt{A} = x_1 x_2 \ldots, z_1 z_2 z_3 \ldots$ *i algoritam staje.*

   Za zadani broj 34 507 vrijedi da je $\sqrt{34\ 507} = 185,76059\ldots$

Primjer 1.4. *U ovom primjeru navodimo algoritam za rješavanje Cramerovog sustava. Neka su* a_1, a_2, b_1, b_2, c_1, *i* c_2, *realni brojevi. Treba odrediti rješenja linearnog sistema jednadžbi:*

$$\begin{array}{ccccc} a_1 x & + & b_1 y & = & c_1 \\ a_2 x & + & b_2 y & = & c_2 \end{array}$$

Koraci algoritma:

a) *Neka je* $D = a_1 \cdot b_2 - a_2 \cdot b_1$.

b) *Ako je* $D = 0$ *tada sistem nema rješenja i postupak staje.*

c) *Ako je* $D \neq 0$ *tada neka je* $D_x = c_1 \cdot b_2 - b_1 \cdot c_2$, *a* $D_y = a_1 \cdot c_2 - c_1 \cdot a_2$. *U ovom slučaju sistem ima jedinstveno rješenje koje je dano formulama:*

$$x = \frac{D_x}{D}, \quad y = \frac{D_y}{D}.$$

Pojam algoritma je precizno definiran tek u XX. stoljeću. Prirodno se postavlja pitanje kako to da su se tako dugo matematičari bezbrižno snalazili s nepreciznim pojmom algoritma. Potreba za definicijom pojavila se tek kada se željelo dokazati da ne postoji algoritam za rješavanje nekog problema.

Sada ističemo dva vjerojatno povijesno najpoznatija problema za koje se pokazalo da ne postoje algoritmi za njihovo rješavanje.

Primjer 1.5. Diofantske jednadžbe
Neka je $P(x_1, \ldots, x_n)$ *polinom s cjelobrojnim koeficijentima. Jednadžba oblika* $P(x_1, \ldots, x_n) = 0$ *naziva se diofantska jednadžba. Takve su npr. jednadžbe*

$$x^2 + y^2 - z^2 = 0$$
$$6x^{18} - x + 3 = 0.$$

Postavlja se pitanje ima li dana diofantska jednadžba cjelobrojna rješenja. Za neke posebne slučajeve odavno su poznati algoritmi. To su npr. diofantske jednadžbe s jednom nepoznanicom, te linearne diofantske jednadžbe s dvije nepoznanice. Ovdje navodimo algoritme za njihovo rješavanje.

a) Diofantske jednadžbe s jednom nepoznanicom su jednadžbe oblika

$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 = 0,$$

gdje su a_i cijeli brojevi. Ako je x_0 cjelobrojno rješenje gornje jednadžbe tada je očito x_0 djelitelj slobodnog koeficijenta a_0. Dakle, da bismo ispitali ima li dana jednadžba cjelobrojnih rješenja dovoljno je uvrstiti u jednadžbu sve djelitelje koeficijenta a_0 (pozitivne i negativne), te ispitati je li neki od njih rješenje.

b) Linearne diofantske jednadžbe s dvije nepoznanice, tj. jednadžbe oblika

$$ax + by = c,$$

gdje su a, b i c cijeli brojevi, pri čemu je $a^2 + b^2 \neq 0$. Nužan i dovoljan uvjet za egzistenciju cjelobrojnih rješenja je da najveća zajednička mjera brojeva a i b dijeli c.

Na drugom svjetskom kongresu matematičara u Parizu 1900. godine njemački matematičar David Hilbert (1862.–1943.) održao je predavanje pod naslovom Matematički problemi. *Iznio je 23 problema*[1] *za koje je smatrao da su ključni za razvitak matematike u novom mileniju. Deseti Hilbertov problem je glasio:*

> Neka je zadana proizvoljna diofantska jednadžba s proizvoljnim brojem nepoznanica. Treba pronaći postupak pomoću kojeg je nakon konačno mnogo koraka moguće odrediti ima li ta jednadžba rješenje u skupu cijelih brojeva.

J. V. Matijasević je 1969. godine dokazao da traženi algoritam ne postoji (vidi B. Golub, O Hilbertovom desetom problemu, diplomski rad, PMF–MO, Zagreb, 2003.).

Primjer 1.6. Problem riječi

Kako bismo uopće mogli izreći problem riječi moramo podsjetiti na neke jednostavne činjenice iz teorije grupa. Svaka grupa reda n može se zadati sa n slova i n^2 definicionih jednakosti ("tablica množenja" dane grupe). Npr. grupa $(\mathbf{Z}_2, +)$ je zadana tablicom

+	0	1
0	0	1
1	1	0

[1] Popis svih Hilbertovih problema možete vidjeti npr. u [9].

Za konačnu grupu interesantno je odrediti kako se može zadati sa što manjim brojem simbola i definicionih jednakosti. Ako je $(G, \circ)$ grupa, te $a_1, \ldots, a_k \in G$ tada izraz $a_1 \circ \ldots \circ a_k$ nazivamo **riječ** *u grupi G. Problem riječi za grupe glasi:*

> *odrediti algoritam koji će za proizvoljnu grupu $(G, \circ)$, te $n, m \in \mathbb{N}$ i $a_1, \ldots, a_n, b_1, \ldots, b_m \in G$ odrediti vrijedi li $a_1 \circ \ldots \circ a_n = b_1 \circ \ldots \circ b_m$.*

Nerješivost problema, tj. nepostojanje traženog algoritma, dokazali su nezavisno P. S. Novikov i W. W. Boone. Točnije dokazali su da postoji grupa s 11 simbola i 30 definicionih jednakosti s nerješivim problemom riječi.

Zadaci:

1. Neka je $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ polinom s relanim koeficijentima stupnja n i $c \in \mathbb{R}$. Dijeljenjem polinoma f sa $x - c$ dobivamo polinom $g(x) = b_0 x^{n-1} + b_1 x^{n-2} + \ldots + b_{n-2}x + b_{n-1}$, a primjenom Bézoutovog teorema znamo da je ostatak jednak $f(c)$. Koeficijenti polinoma g dobivaju se na sljedeći način:

   $$\begin{aligned} b_0 &= a_0 \\ b_1 &= a_1 + cb_0 \\ b_2 &= a_2 + cb_1 \\ &\vdots \\ b_{n-1} &= a_{n-1} + cb_{n-2}, \end{aligned}$$

   a ostatak $f(c) = a_n + cb_{n-1}$. Opisani postupak se naziva Hornerova shema (W. G. Horner, 1786.–1837., eng. matematičar). Taj se algoritam koristi za brzo računanje vrijednosti polinoma.

   Primjenom Hornerove sheme izračunajte $f(4)$, ako je $f(x) = 3x^4 + 2x^3 - 5x^2 - 7x + 2$.

2. Opisat ćemo igru gomilice za dva igrača. Neka su $n, m \in \mathbb{N}$ tako da vrijedi $0 < n < m$. Na stolu se nalazi m novčića. Igrači naizmjence uzimaju sa hrpe, i to u svakom potezu igrač može uzeti bilo koji broj novčića k, tako da vrijedi $1 \leq k \leq n$. Pobjednik u igri je onaj igrač koji uzme posljednji novčić sa stola. Odredite uvjete kada postoji pobjednička strategija za prvog, odnosno drugog igrača. [2]

3. Po legendi, u indijskom gradu Benaresu u hramu boga Brahme postojala je metalna ploča na kojoj su bile učvršćene tri dijamantne igle. Na jednoj igli

[2]O igri gomilice možete čitati u Matematičko–fizičkom listu broj 116.

> su bila postavljena 64 koluta. Najveći kolut se nalazio na dnu. Svećenici su neprekidno, i dan i noć, premještali kolutove s jedne igle na drugu, koristeći treću kao pomoćnu. U svakom potezu su smjeli premjestiti samo jedan disk na neku od igala, pazeći pri tome da uvijek stavljaju manji disk na veći, a nikako ne obratno. Navedeni problem se naziva **Hanojske kule**.
>
> Dokažite da je problem Hanojskih kula rješiv za svaki broj kolutova. Opišite algoritam premještanja za problem Hanojskih kula. Dokažite da je minimalan broj premještanja za n kolutova jednak $2^n - 1$.

1.1.1 Opisne definicije osnovnih pojmova

Sada želimo dati opisne definicije pojmova koje ćemo razmatrati, tj. kasnije strogo definirati.

Izračunavanje je proces kod kojeg iz nekih početno danih objekata s fiksiranim skupom pravila dobivamo krajnji rezultat. Početne objekte nazivamo **ulazni podaci**. Fiksirani skup pravila naziva se **algoritam** ili **program**. Krajnji rezultati se nazivaju **izlazni podaci**.

Mi ćemo uvijek pretpostavljati da postoji najviše **jedan** izlazni podatak. Ako se želi promatrati izračunavanje s k izlaznih podataka može se promatrati k izračunavanja od kojih svako ima samo jedan izlazni rezultat.

U drugu ruku **dozvoljavamo svaki konačan broj ulaznih podataka,** uključujući i nula ulaznih podataka.

Pretpostavljamo da je za svaki pojedini algoritam ili program fiksiran broj ulaznih podataka (fiksirana "mjesnost").

Ne zahtijevamo da za sve ulazne podatke svaki algoritam daje izlazni rezultat. To znači da neki algoritam za neke ulazne podatke može računati **a da nikad ne stane.**

Kod algoritma mora biti točno precizirano što je akcija, odnosno **instrukcija**, koja se izvodi u svakom koraku. Instrukcije moraju biti u dovoljnoj mjeri "mehaničke" (npr. kako bi se mogle izvoditi i na računalu).

Neka je $f : S \subseteq \mathbb{N}^k \to \mathbb{N}$. Smatramo da algoritam A s k ulaznih podataka **izračunava** funkciju f ako vrijedi:

> prirodni brojevi $x_1, \ldots, x_k$ su u domeni funkcije f ako i samo ako algoritam A prilikom izračunavanja s ulaznim podacima $x_1, \ldots, x_k$ stane, i izlazni rezultat je u tom slučaju jednak $f(x_1, \ldots, x_k)$.

Smatramo da je neka funkcija $f : S \subseteq \mathbb{N}^k \to \mathbb{N}$ **izračunljiva** ako postoji neki algoritam koji je izračunava.

Mogli bismo pomisliti da čim je zadana neka funkcija $f : \mathbb{N} \to \mathbb{N}$ onda odmah imamo i "efektivni postupak" za izračunavanje njenih vrijednosti $f(n)$. Sljedeći jednostavan primjer pokazuje da je pojam "efektivne izračunljivosti" vrlo suptilan. Neka je funkcija $f : \mathbb{N} \to \mathbb{N}$ zadana s:

$$f(n) = \begin{cases} 1, & \text{ako postoji } \ n \text{ uzastopnih petica u decimalnom zapisu } \sqrt{2}; \\ 0, & \text{inače.} \end{cases}$$

Znamo da je $\sqrt{2}$ iracionalan broj, te nije periodički decimalni broj. Danas ne postoji način da za svaki $n \in \mathbb{N}$ znamo odrediti postoji li n uzastopnih petica u decimalnom zapisu broja $\sqrt{2}$. Iz ovog primjera vidimo da vrijednosti $f(n)$ općenito nisu izračunljive, tj. nema još efektivnog postupka za izračunavanje $f(n)$, iako je funkcija f korektno definirana.

Bilo je dosta teško prethodno navedene pojmove opisati precizno. Iz tog razloga ćemo dati definicije tih pojmova na dva različita načina.

Definirat ćemo klasu RAM-izračunljivih funkcija i klasu parcijalno rekurzivnih funkcija. Iz definicije će biti jasno da je svaka ta funkcija izračunljiva u prije navedenom intuitivnom smislu. Nakon proučavanja obje klase dat ćemo argumente za tvrdnju da svaka izračunljiva funkcija pripada tim klasama.

1.1.2 Termini i oznake

Sa $\mathbb{N}$ označavamo skup $\{0, 1, 2, 3, \ldots\}$ i njegove elemente nazivamo prirodni brojevi. Mi ćemo promatrati samo algoritme čiji su ulazni podaci i izlazni podatak prirodni brojevi.

Kada pišemo "skup" mislimo uvijek na neki podskup skupa $\mathbb{N}^k$, za neki $k \in \mathbb{N}$ $(k > 0)$.

Često ćemo umjesto uređene k-torke prirodnih brojeva $(x_1, \ldots, x_k)$ pisati samo kratko $\vec{x}$.

Kada pišemo "k-mjesna funkcija" tada mislimo na neku funkciju čija je domena podskup od $\mathbb{N}^k$, a kodomena je skup $\mathbb{N}$. Ako kažemo samo "funkcija" tada mislimo na neku k-mjesnu funkciju.

Funkcija je **totalna** ako je njena domena skup $\mathbb{N}^k$. Ako želimo naglasiti da neka funkcija moguće nije totalna tada kažemo da je ona **parcijalna**.

k-mjesna relacija je proizvoljan podskup od $\mathbb{N}^k$. Ako je R neka relacija tada činjenicu $\vec{x} \in R$ zapisujemo i $R(\vec{x})$. Ako je R dvomjesna relacija tada umjesto $R(x, y)$ pišemo i xRy.

Ako je R relacija tada sa χ_R označavamo **karakterističnu funkciju** relacije R, koja je definirana s

$$\chi_R(\vec{x}) = \begin{cases} 1, & \text{ako vrijedi } \ R(\vec{x}); \\ 0, & \text{inače.} \end{cases}$$

Primijetite da je χ_R totalna funkcija za svaku relaciju R.

Smatramo da je relacija R izračunljiva ako je pripadna funkcija χ_R izračunljiva. Kada relaciji pridjeljujemo neka funkcijska svojstva mislimo uvijek na svojstva karakteristične funkcije.

1.2 RAM–stroj

Sada ćemo definirati RAM–stroj (eng. random access machines) i klasu RAM–izračunljivih funkcija. To će biti jedan način strogog definiranja klase izračunljivih funkcija. Kasnije ćemo definirati parcijalno rekurzivne funkcije.

RAM–stroj je idealizirano računalo s beskonačno velikom memorijom koje nikad ne radi greške. Definicija RAM–stroja, koja slijedi, je opisna. Mogli bismo dati definiciju koja bi bila stroža ("RAM–stroj je uređena n-torka ...") i "više" matematička, ali smatramo da tada taj pojam ne bi bio toliko jasan.

Definicija 1.7. *Osnovni dijelovi RAM–stroja su:*

- *registri;*
- *spremnik za program;*
- *brojač.*

Za svaki prirodan broj k stroj ima registar koji označavamo s $\mathcal{R}_k$. U svakom trenutku rada stroja svaki registar $\mathcal{R}_k$ sadrži neki prirodan broj.

U spremniku za program je smješten program. Program je konačan niz instrukcija. Ako je n broj instrukcija u programu tada su one numerirane s 1., 2., $\ldots$, n.

U brojaču se u svakom trenutku rada RAM–stroja nalazi redni broj instrukcije koja se izvršava.

Postoje četiri tipa instrukcija:

- *INC* $\mathcal{R}_k$
  Kada stroj izvodi tu instrukciju tada povećava broj u registru $\mathcal{R}_k$ za jedan, te broj u brojaču poveća za jedan.
- *DEC* $\mathcal{R}_k$, m.
  Broj m je obavezno redni broj neke instrukcije u programu. Ako je broj u registru $\mathcal{R}_k$ različit od nule tada se prilikom izvršenja navedene instrukcije broj u $\mathcal{R}_k$ smanji za jedan, a broj u brojaču se poveća za jedan. Ako je broj u registru $\mathcal{R}_k$ jednak nuli tada se prilikom izvršenja navedene instrukcije samo broj u brojaču promijeni u m.
- *GO TO* m
  Broj m je obavezno redni broj neke instrukcije u programu.
  Kada stroj izvodi tu instrukciju on jednostavno broj u brojaču mijenja u m.
- *STOP*
  Kada stroj dođe na tu instrukciju tada izračunavanje bezuvjetno stane.

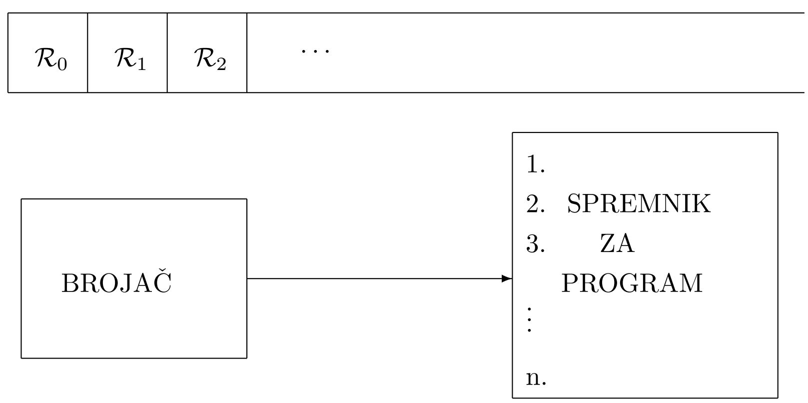
Za primjenu stroja prvo stavljamo program u spremnik programa. Zatim upisujemo odgovarajuće brojeve u registre (ulazni podaci). Ako se radi o programu s k ulaznih podataka, tada smatramo da su oni redom zapisani u registrima $\mathcal{R}_1$, $\ldots$, $\mathcal{R}_k$. *U brojaču je na početku broj* 1 *(to znači da se svaki program počinje izvršavati od prve instrukcije). Tada startamo stroj.*

Stroj tada počinje izvršavati instrukcije. U svakom koraku stroj izvršava instrukciju u programu čiji je redni broj u brojaču. Na kraju izvršenja instrukcije mijenja se broj u brojaču.

Ako je izračunavanje došlo na instrukciju STOP, ili pak je broj u brojaču veći od svakog rednog broja instrukcija u programu, tada stroj staje. U tom slučaju je izlazni rezultat zapisan u registru $\mathcal{R}_0$. *Ako se to nikad ne dogodi stroj radi "vječno".*

Napomena 1.8. *Na početku smo rekli da je RAM–stroj neka vrsta idealiziranog računala koja nikad ne griješi. Ako stroj nikad ne stane prilikom izvršenja nekog programa to ne znači da stroj griješi, već je program takav. (Sjetimo se samo koliko puta su nam probleme stvarale beskonačne petlje koje se znaju dogoditi prilikom nepažljivog programiranja.) Beskonačni rad stroja ne dopuštamo samo kako bismo mogli opravdati grešku u programu, već će nam ta neodređenost biti oznaka za jedno svojstvo funkcije čija se vrijednost izračunava.*

Sljedećom slikom dajemo skicu RAM–stroja.



Sada dajemo neke jednostavne primjere RAM–programa.

Primjer 1.9.

a) Program koji broj u registru $\mathcal{R}_k$ povećava za tri.

1. *INC* $\mathcal{R}_k$
2. *INC* $\mathcal{R}_k$
3. *INC* $\mathcal{R}_k$

b) Program koji broj u registru $\mathcal{R}_k$ zamijeni s nulom.

1. *DEC* $\mathcal{R}_k$, 3
2. *GO TO 1*
3. *STOP*

c) Program koji nikad ne staje.

1. *GO TO 2*
2. *GO TO 1*

Važno je naglasiti da nam nije cilj učenje principa programiranja (s minimalnim brojem instrukcija!). Glavni cilj je dati dvije različite definicije koje opisuju izračunljive funkcije, te dokazati da se te dvije klase funkcija poklapaju.

Definicija 1.10. *Za svaki program P za RAM–stroj i svaki $k \in \mathbb{N}$ uređeni par (P, k) nazivamo* **algoritam**, *te označavamo sa A_k^P.*

Definicija 1.11. *Neka je $f : S \subseteq \mathbb{N}^k \to \mathbb{N}$ i A_k^P neki algoritam. Kažemo da algoritam A_k^P* **izračunava** *funkciju f ako za sve prirodne brojeve $x_1, \ldots, x_k$ vrijedi da je $(x_1, \ldots, x_k) \in S$ ako i samo ako RAM–stroj s programom P u spremniku i s $(x_1, \ldots, x_k)$ kao ulaznim podacima stane, i u tom slučaju je na kraju rada stroja u registru $\mathcal{R}_0$ zapisan broj $f(x_1, \ldots, x_k)$. Često ćemo i reći da program P izračunava funkciju f, i to u situacijama kada nije potrebno naglašavati mjesnost ulaznih podataka.*

Kažemo da je **funkcija** *f* **RAM–izračunljiva** *ako postoji algoritam A_k^P koji je izračunava. Kažemo da je* **relacija** *R* **RAM–izračunljiva** *ako je njena karakteristična funkcija RAM-izračunljiva.*

Želimo posebno naglasiti da iz prethodne definicije slijedi da ako je A_k^P algoritam koji izračunava funkciju f, te su u RAM–stroju ulazni podaci koji ne pripadaju domeni funkcije f, tada RAM–stroj nikada neće stati.

Važno je naglasiti da smatramo da je svaka RAM–izračunljiva funkcija izračunljiva. (Sve instrukcije RAM–programa su jasne i "mehaničke".) Kasnije ćemo dati nekoliko primjera RAM–izračunljivih funkcija, te dokazati da je jedna velika klasa funkcija RAM–izračunljiva.

Dosta je teško pisati programe za RAM–stroj jer na raspolaganju imamo samo četiri tipa instrukcija. Sada ćemo uvesti nove tipove instrukcija. To će zapravo biti pokrate za čitave nizove osnovnih instrukcija. Ideja uvođenja novih instrukcija je slična kao kod programiranja - primjenjujemo potprogame, odnosno makroe, koje ćemo sada definirati.

Definicija 1.12. *Za svaki program P za RAM-stroj uvodimo novu instrukciju koju označavamo s P^* i nazivamo* **makro** *za P.* **Makro-stroj** *se sastoji od istih dijelova kao i RAM-stroj, te za svaki program P za RAM-stroj prepoznaje instrukciju P^*.*

Kada makro-stroj počinje izvršavati instrukciju oblika P^* on počinje izvršavati zapravo program P (s podacima koji su trenutno u registrima). Ako izvršavanje program P s danim podacima nikad ne stane tada smatramo da izvršavanje instrukcije P^* nije kompletirano, tj. makro-stroj ne staje.
Ako izvršavanje programa P stane tada se broj u brojaču poveća za jedan (u odnosu na broj u brojaču na početku izvršavanja instrukcije P^*), te makro-stroj nastavlja izvršavati daljnje instrukcije programa.

Pojam **makro–izračunljive** funkcije se definira na isti način kao pojam RAM-izračunljive funkcije.

U sljedećoj definiciji definiramo pojam ekvivalentnih algoritama. Uočite da je definicija općenita, tj. ne odnosi se samo na RAM–strojeve i makro–strojeve.

Definicija 1.13. *Neka su S i S' strojevi (RAM ili makro). Za svaki $k \in \mathbb{N}$ označimo s $\mathcal{R}_k$ registar stroja S, a s $\mathcal{R}'_k$ registar stroja S'. Neka je A_k^P algoritam za stroj S, a B_k^Q algoritam za stroj S'.*

Kažemo da su algoritmi A_k^P i B_k^Q **ekvivalentni** *ako za sve $\vec{x} \in \mathbb{N}^k$, koji su zapisani u S i S' kao ulazni podaci, oba stroja ili rade beskonačno, ili pak oba stanu i u registrima $\mathcal{R}_0$ i $\mathcal{R}'_0$ je zapisan isti broj.*

Propozicija 1.14. *Za svaki algoritam za makro–stroj postoji neki algoritam za RAM–stroj koji je ekvivalentan s njim.*

Dokaz. Neka je Q neki program za makro–stroj. Svaki makro P^* u programu Q zamijenimo nizom instrukcija programa P. Zatim prenumeriramo na odgovarajući način redne brojeve instrukcija, te brojeve u instrukcijama oblika DEC $\mathcal{R}_i,\ n$ i GO TO n. Očito je dobiveni algoritam ekvivalentan s algoritmom određenim programom Q. $\square$

Korolar 1.15. *Klase RAM–izračunljivih funkcija i makro–izračunljivih funkcija su jednake.*

Sada uvodimo oznake za makroe koje ćemo češće koristiti.

a) Makro programa iz primjera 1.9., koji broj u registru $\mathcal{R}_k$ izjednačava s nulom, označavat ćemo sa **ZERO** $\mathcal{R}_k$.

b) Sljedeći program za makro–stroj broj iz registra $\mathcal{R}_i$ prepisuje u registar $\mathcal{R}_j$, pri čemu na kraju izvršavanja programa broj u registru $\mathcal{R}_i$ nije promijenjen. Za izvršavanje tog programa koristimo kao pomoćni registar $\mathcal{R}_k$. Naravno, smatramo da su $i,\ j$ i k međusobno različiti prirodni brojevi.

   1. ZERO $\mathcal{R}_j$
   2. ZERO $\mathcal{R}_k$
   3. DEC $\mathcal{R}_i,\ 7$
   4. INC $\mathcal{R}_j$
   5. INC $\mathcal{R}_k$
   6. GO TO 3
   7. DEC $\mathcal{R}_k,\ 10$
   8. INC $\mathcal{R}_i$
   9. GO TO 7
   10. ZERO $\mathcal{R}_k$

   Makro za prethodni program označavamo sa:

   MOVE $\mathcal{R}_i$ **TO** $\mathcal{R}_j$ **USING** $\mathcal{R}_k$

   Obično ćemo ispuštati pisanje pomoćnog registra $\mathcal{R}_k$. Smatrat ćemo da je pomoćni registar izabran tako da je različit od svih drugih registara koji se koriste u programu. To znači da ćemo obično koristiti oznaku **MOVE** $\mathcal{R}_i$ **TO** $\mathcal{R}_j$.

c) Neka je f k-mjesna RAM-izračunljiva funkcija, te neka je P program za RAM-stroj koji je izračunava. Neka je m za jedan veći prirodan broj od najvećeg indeksa registra koji se koriste u instrukcijama programa P. Označimo s Q sljedeći program za makro–stroj:

1.	MOVE $\mathcal{R}_1$ TO $\mathcal{R}_{m+1}$ USING $\mathcal{R}_m$
$\vdots$	
(m-1).	MOVE $\mathcal{R}_{m-1}$ TO $\mathcal{R}_{2m-1}$ USING $\mathcal{R}_m$ (Brojevi iz registara $\mathcal{R}_1, \ldots, \mathcal{R}_{m-1}$ se prepisuju redom u registre $\mathcal{R}_{m+1}, \ldots, \mathcal{R}_{m+(m-1)}$.)
m.	ZERO $\mathcal{R}_0$
(m+1).	ZERO $\mathcal{R}_{k+1}$
$\vdots$	
(2m-k).	ZERO $\mathcal{R}_{m-1}$ (Brojevi u registrima $\mathcal{R}_0$, $\mathcal{R}_{k+1}, \ldots, \mathcal{R}_{m-1}$ se brišu.)
(2m-k+1).	P^* (Program P koristi registre $\mathcal{R}_0$, $\mathcal{R}_1$, ..., $\mathcal{R}_k$, ..., $\mathcal{R}_{m-1}$).
(2m-k+2).	MOVE $\mathcal{R}_{m+1}$ TO $\mathcal{R}_1$ USING $\mathcal{R}_m$
$\vdots$	
(3m-k+1).	MOVE $\mathcal{R}_{2m-1}$ TO $\mathcal{R}_{m-1}$ USING $\mathcal{R}_m$ (Brojevi iz registara $\mathcal{R}_{m+1}, \ldots, \mathcal{R}_{m+(m-1)}$ se vraćaju redom u registre $\mathcal{R}_1, \ldots, \mathcal{R}_{m-1}$.)

Provjerite da vrijedi: ako je program Q pokrenut s ulaznim podacima x_1, ..., x_k u registrima $\mathcal{R}_1$, ..., $\mathcal{R}_k$ tada će se makro-stroj zaustaviti ako i samo ako je $f(x_1, \ldots, x_k)$ definirano, i u tom slučaju je broj u registru $\mathcal{R}_0$ jednak $f(x_1, \ldots, x_k)$, a brojevi u registrima $\mathcal{R}_i$ su nepromijenjeni osim možda u registrima s indeksom i, gdje je $i = 0$ ili vrijedi $m \le i < 2m$.

Makro za prethodni program označavamo sa $f(\mathcal{R}_1, \ldots, \mathcal{R}_k) \to \mathcal{R}_0$.

Zadaci:

1. Neka je u registru $\mathcal{R}_1$ zapisan broj n, a u registru $\mathcal{R}_2$ broj m. Napišite program za makro–stroj koji provjerava je li n strogo veći od m. Ako jest neka stroj stane i u registru $\mathcal{R}_0$ neka bude zapisan broj 0. Ako pak nije, neka također stroj stane, a u registru $\mathcal{R}_0$ neka bude zapisan broj 1.

Rješenje.

1. ZERO $\mathcal{R}_0$
2. INC $\mathcal{R}_0$
3. MOVE $\mathcal{R}_1$ TO $\mathcal{R}_3$
4. MOVE $\mathcal{R}_2$ TO $\mathcal{R}_4$
5. DEC $\mathcal{R}_3$, 9
6. DEC $\mathcal{R}_4$, 8
7. GO TO 5
8. ZERO $\mathcal{R}_0$
9. STOP

2. Napišite program za makro–stroj koji prepoznaje je li broj n u registru $\mathcal{R}_1$ djeljiv s tri. Ako je djeljiv tada neka stroj stane i neka u registru $\mathcal{R}_0$ bude zapisana nula. Ako pak broj n nije djeljiv s tri neka stroj ne stane.

   Rješenje.

   1. ZERO $\mathcal{R}_2$
   2. MOVE $\mathcal{R}_1$ TO $\mathcal{R}_2$
   3. DEC $\mathcal{R}_2, 9$
   4. DEC $\mathcal{R}_2, 7$
   5. DEC $\mathcal{R}_2, 7$
   6. GO TO 3
   7. GO TO 8
   8. GO TO 9
   9. ZERO $\mathcal{R}_0$

3. Napišite program za makro–stroj koji izračunava funkciju $f : \mathbb{N} \to \mathbb{N}$, $f(x) = x^2$. Postoji li program za RAM–stroj koji izračunava funkciju f?

4. Neka je funkcija $\dot{-} : \mathbb{N}^2 \to \mathbb{N}$ definirana sa:

$$x \dot{-} y = \begin{cases} 0, & \text{ako je } x \leq y; \\ x - y, & \text{inače.} \end{cases}$$

   Napišite program za makro–stroj koji izračunava funkciju $\dot{-}$.

5. Napišite program za makro–stroj koji izračunava funkciju $n \mapsto \lfloor \sqrt{n} \rfloor$ (najveće cijelo drugog korijena od n).

   Rješenje. Označimo s $\mathcal{R}_i^2 \to \mathcal{R}_j$ makro za program koji broj iz registra $\mathcal{R}_i$ kvadrira i zapisuje u registar $\mathcal{R}_j$ (smatramo da je nakon toga broj u registru $\mathcal{R}_i$ nepromijenjen).

Označimo s IF $\mathcal{R}_i \leq \mathcal{R}_j < \mathcal{R}_k$ THEN p ELSE q makro za program koji provjerava je li broj zapisan u registru $\mathcal{R}_i$ manji od broja zapisanog u registru $\mathcal{R}_j$, a taj je strogo manji od broja u zapisanog u registru $\mathcal{R}_k$. Ako je to ispunjeno program se nastavlja izvršavati od p. instrukcije, a ako nije program se nastavlja izvršavati od q. instrukcije.

Sada prvo dajemo program za makro–stroj koji u registar $\mathcal{R}_0$ zapisuje $\lfloor\sqrt{n}\rfloor$ (ako je na početku u registru $\mathcal{R}_1$ zapisan broj n.) Nakon toga ćemo dati programe za makro–stroj koji će opravdati uvođenje gornjih makroa.

1. ZERO $\mathcal{R}_0$
2. ZERO $\mathcal{R}_2$
3. INC $\mathcal{R}_2$
4. $\mathcal{R}_0^2 \to \mathcal{R}_3$
5. $\mathcal{R}_2^2 \to \mathcal{R}_4$
6. IF $\mathcal{R}_3 \leq \mathcal{R}_1 < \mathcal{R}_4$ THEN 9 ELSE 7
7. INC $\mathcal{R}_0$
8. GO TO 2
9. STOP

Sada navodimo jedan program za makro–stroj koji broj zapisan u registru $\mathcal{R}_i$ kvadrira i rezultat zapisuje u registar $\mathcal{R}_j$. (Registri $\mathcal{R}_k$ i $\mathcal{R}_m$ su pomoćni u ovom programu).

1. ZERO $\mathcal{R}_j$
2. ZERO $\mathcal{R}_m$
3. MOVE $\mathcal{R}_i$ TO $\mathcal{R}_k$
4. GO TO 7
5. $\mathcal{R}_i + \mathcal{R}_j \to \mathcal{R}_m$
6. MOVE $\mathcal{R}_m$ TO $\mathcal{R}_j$
7. DEC $\mathcal{R}_k$, 9
8. GO TO 5
9. STOP

(Makro $\mathcal{R}_i + \mathcal{R}_j \to \mathcal{R}_m$ nećemo posebno opisivati, jer smatramo da je jasan.)

Preostalo je napisati program za makro–stroj koji opravdava makro IF $\mathcal{R}_i \leq \mathcal{R}_j < \mathcal{R}_k$ THEN p ELSE q koji smo prije koristili. Registre $\mathcal{R}_l$, $\mathcal{R}_m$

i $\mathcal{R}_s$ koristimo kao pomoćne.

1. MOVE $\mathcal{R}_i$ TO $\mathcal{R}_l$
2. MOVE $\mathcal{R}_j$ TO $\mathcal{R}_m$
3. MOVE $\mathcal{R}_k$ TO $\mathcal{R}_s$
4. DEC $\mathcal{R}_s$, q
5. DEC $\mathcal{R}_m$, 8
6. DEC $\mathcal{R}_l$, 4
7. GO TO 4
8. DEC $\mathcal{R}_l$, p
9. GO TO q

(Uočite da ovo posljednje nije korektni program za makro–stroj jer u njemu ne postoje instrukcije s rednim brojevima p i q No, to nije problem, jer smo mogli ovaj posljedni program napisati u programu koji rješava zadatak umjesto makro–instrukcije IF $\mathcal{R}_i \leq \mathcal{R}_j < \mathcal{R}_k$ THEN 9 ELSE 7 .)

6. Napišite program za makro–stroj koji izračunava funkciju

$$f(n) = \begin{cases} 0, & \text{ako je } n = 0; \\ \lfloor \log n \rfloor, & \text{inače} \end{cases}$$

Rješenje. Označimo s $10^{\mathcal{R}_i} \to \mathcal{R}_j$ makro za program koji čita broj iz registra $\mathcal{R}_i$ i računa potenciju broja 10, te rezultat zapisuje u registar $\mathcal{R}_j$ (smatramo da je nakon toga broj u registru $\mathcal{R}_i$ nepromijenjen).

Označimo s IF $\mathcal{R}_i \leq \mathcal{R}_j < \mathcal{R}_k$ THEN p ELSE q makro kao u zadatku 5. Prvo dajemo program za makro–stroj koji u registar $\mathcal{R}_0$ zapisuje $f(n)$ (ako je na početku u registru $\mathcal{R}_1$ zapisan broj n).

1. ZERO $\mathcal{R}_0$
2. MOVE $\mathcal{R}_1$ TO $\mathcal{R}_5$
3. DEC $\mathcal{R}_5$, 12
4. ZERO $\mathcal{R}_0$
5. ZERO $\mathcal{R}_2$
6. INC $\mathcal{R}_2$
7. $10^{\mathcal{R}_0} \to \mathcal{R}_3$
8. $10^{\mathcal{R}_2} \to \mathcal{R}_4$
9. IF $\mathcal{R}_3 \leq \mathcal{R}_1 < \mathcal{R}_4$ THEN 12 ELSE 10
10. INC $\mathcal{R}_0$
11. GO TO 6
12. STOP

Sada dajemo program za makro–stroj koji računa i zapisuje broj 10^n u registar $\mathcal{R}_j$, ako je na početku u registru $\mathcal{R}_i$ zapisan broj n. (Registri $\mathcal{R}_k$ i $\mathcal{R}_m$ su pomoćni u ovom programu).

1. ZERO $\mathcal{R}_j$
2. INC $\mathcal{R}_j$
3. ZERO $\mathcal{R}_m$
4. MOVE $\mathcal{R}_i$ TO $\mathcal{R}_k$
5. GO TO 7
6. $10 \cdot \mathcal{R}_j \to \mathcal{R}_m$
7. MOVE $\mathcal{R}_m$ TO $\mathcal{R}_j$
8. DEC $\mathcal{R}_k$, 10
9. GO TO 6
10. STOP

Makro $10 \cdot \mathcal{R}_j \to \mathcal{R}_m$ nećemo posebno opisivati.

U zadacima koji slijede razmatraju se Turingovi strojevi. Definirali su ih manje–više istovremeno 1936. godine Alan Turing (1912.–1954.) i Emil Post (1897.–1954.). Dajemo prvo definiciju Turingovog stroja.

Definicija 1.16. *Turingov stroj je uređena šestorka* $(\mathcal{S}, \Gamma, q_0, s_0, F, \Pi)$, *gdje je redom:*

$\mathcal{S}$ *konačan skup, čije elemente nazivamo stanja;*

Γ *je konačan skup, čije elemente nazivamo dozvoljeni simboli;*

q_0 *je element iz* $\mathcal{S}$ *i nazivamo ga početno stanje;*

s_0 *je element od* Γ *i nazivamo ga prazni simbol;*

F *je podskup od* $\mathcal{S}$ *i njegove elemente nazivamo završna stanja;*

Π *je proizvoljna funkcija sa* $\Gamma \times \mathcal{S}$ *u skup* $\Gamma \times \{L, D, H\} \times \mathcal{S}$ *i nazivamo je program za Turingov stroj.*

Možemo reći da je Turingov stroj automat koji manipulira simbolima na beskonačnoj traci, pri čemu su ti simboli iz fiksiranog alfabeta. Traka je podijeljena u registre (kao filmska traka). U svakom registru može biti zapisan samo jedan simbol. Traka je beskonačan slijeva i zdesna. U jednom trenutku glava čitača može promatrati samo jedan registar. Turingov stroj ima samo konačan broj stanja. Turingov stroj može izvršavati četiri akcije:

a) pomaknuti glavu čitača za jedan registar lijevo;
b) pomaknuti glavu čitača za jedan registar desno;
c) pročitati simbol iz registra kojeg promatra;
d) napisati simbol (iz danog skupa simbola) u registar (odnosno, izbrisati postojeći simbol i napisati novi).

Za funkcije oblika $f : S \subseteq \mathbb{N}^k \to \mathbb{N}$ se definira pojam Turing–izračunljivosti na sasvim analogni način kao i RAM–izračunljivost. Važno je naglasiti da se klase RAM–izračunljivih i Turing–izračunljivih funkcija poklapaju.

Turingov stroj obično zadajemo tablicom iz koje se može iščitati skup stanja i dozvoljenih simbola. To ćemo ilustrirati u zadacima koji slijede.

7. Na traci se nalazi zapisan prirodan broj veći od nule u unarnom zapisu (npr. broj 5 je zapisan kao IIIII). Sastavite Turingov stroj koji određuje binarni zapis tog broja. Glava čitača se na početku nalazi na krajnjem lijevom znaku.
Rješenje. Prvo dajemo opis rada stroja po koracima, a onda ćemo ga točno zadati tablicom.

1) pomak na zadnji desni znak I;
2) obrisati zadnji desni znak I;
3) pomak na prvo lijevo prazno mjesto;
4) na prazno mjesto pišemo 1;
5) pomak na zadnji desni znak I;
6) obrisati zadnji desni znak I;
7) pomak lijevo do prve znamenke zdesna;
8) ako je znamenka 0 tada je treba obrisati i napisati 1, te primijenimo korak 10);
ako je znamenka 1 tada je treba obrisati i napisati 0, te pomaknuti se jedno mjesto lijevo;
9) ako je opet pročitana neka znamenka (0 ili 1) tada se vratimo na korak 8);
10) vraćamo se na korak 5) ako još ima znakova I, a inače stroj stane.

Sada traženi Turingov stroj zadajemo tablicom.

	q_0	q_1	q_2
0	$0Dq_0$	$0Hq_{STOP}$	$1Dq_0$
1	$1Dq_0$	$1Hq_{STOP}$	$0Lq_2$
s_0	s_0Lq_1	s_0Hq_{STOP}	$1Dq_0$
I	IDq_0	s_0Lq_2	ILq_2

Dakle, dani Turingov stroj ima četiri moguća stanja: q_0, q_1, q_2 i q_{STOP} (završno stanje). Skup dozvoljenih simbola je $\{s_0, I, 0, 1\}$.

8. Na traci se nalazi zapisan prirodan broj u unarnom zapisu. Sastavite Turingov stroj koji odredjuje dekadski zapis tog broja. Glava čitača se na početku nalazi na krajnjem desnom znaku.

9. Na traci je zapisan realan broj u unarnom zapisu koji ima samo konačno mnogo decimala različitih od nule, pri čemu je na početku zapisan predznak broja. Konstruirajte Turingov stroj koji računa najveće cijelo danog realnog broja, koje je zapisano u unarnom zapisu. Na početku se glava za čitanje nalazi na predznaku broja.
Rješenje. Prvo dajemo opis rada stroja.

   1) Pročitati predznak broja.
      Ako je predznak + tada neka stroj pređe u stanje q_1;
      Ako je predznak $-$ tada neka stroj pređe u stanje q_3.
   2) Glavu za čitanje pomaknuti do decimalne točke.
   3) Ako je pročitan predznak + (tj. stroj se nalazi u stanju q_1) umjesto decimalne točke se napiše simbol s_0 i stroj stane (ili pak se obrišu svi znakovi I desno od decimalne točke).
   4) Ako je pročitan predznak $-$ tada se umjesto decimalne točke napiše prvo simbol I. Zatim se glava pomakne desno, napiše prazno mjesto s_0, te stroj stane.

Sada traženi Turingov stroj zadajemo sljedećom tablicom.

	q_0	q_1	q_2	q_3
+	$+Dq_1$			
$-$	$-Dq_3$			
.		s_0Dq_2		IDq_2
1		IDq_1	s_0Dq_2	IDq_3
s_0			s_0Hq_{STOP}	

10. Konstruirajte Turingov stroj čiji je ulazni podatak neki niz iz alfabeta $\{0, 1, 2\}$, a kao izlazni rezultat daje isti niz u obrnutom poretku. U toku rada smiju se koristiti samo znakovi alfabeta $\{0, 1, 2, a, b, c\}$. Ulazni niz je sa svake strane omeđen jednim praznim znakom. Izlazni rezultat treba biti također omeđen sa svake strane s praznim znakovima. Glava za čitanje se na početku nalazi na proizvoljnom mjestu unutar niza, dok konačan položaj glave nije bitan.
Rješenje. Prvo dajemo opis rada stroja koji izvršava traženu operaciju.

1) Pomaknuti glavu za čitanje na krajnji desni znak niza.
2) Čitanje znaka koji će se kopirati (prijelaz u određeno stanje q_a, q_b ili q_c), te umjesto pročitanog znaka pišemo odgovarajuću "šifru" (ako je pročitani znak 0 tada na njegovo mjesto pišemo a, ako je 1 tada pišemo b, te ako je pročitani znak 2 tada pišemo c).
3) Pomak glave do praznog mjesta gdje će se pročitani znak kopirati, te samo kopiranje.
4) Ponavljanje postupka sve dok ima nepročitanih znakova.

Kako bi upravo navedeni opis rada stroja bio jasniji ilustrirat ćemo rad stroja za koji je niz $s_0 21021 s_0$ ulazni podatak.

$$s_0 21021 s_0 \mapsto s_0 2102b s_0 \mapsto s_0 2102b s_0 1 s_0 \mapsto s_0 210cb s_0 1 s_0$$
$$\mapsto s_0 210cb s_0 12 s_0 \mapsto s_0 21acb s_0 12 s_0 \mapsto s_0 21acb s_0 120 s_0$$
$$\mapsto s_0 2bacb s_0 120 s_0 \mapsto s_0 2bacb s_0 1201 s_0 \mapsto s_0 cbacb s_0 1201 s_0$$
$$\mapsto s_0 cbacb s_0 12012 s_0$$

Skup stanja Turingovog stroja koji upravo definiramo je $\{q_0, q_1, q_a, q_b, q_c, q_{aa}, q_{bb}, q_{cc}, q_l, q_{STOP}\}$. Sada dajemo opis svakog pojedinog stanja stroja.

- q_0 je početno stanje, i znači još pomak glave za čitanje na krajnji desni znak niza;
- q_1 stanje služi za nalaženje prvog znaka zdesna koji još nije kopiran (tj. još nije zamijenjen s nekim od slova a, b, c);
- stanja q_a, q_b, q_c znače pomak glave desno do prve praznine, (to je praznina između početnog niza i stvaranog), a onda prelazi u jedno od stanja: q_{aa}, q_{bb}, q_{cc};
- stanja q_{aa}, q_{bb}, q_{cc} uzrokuju pomak glave do prve sljedeće praznine zdesna, te tu piše znak $[x]$, pri čemu je:

  $$[x] = \begin{cases} 0, & \text{ako je } x = a; \\ 1, & \text{ako je } x = b; \\ 2, & \text{ako je } x = c. \end{cases}$$

  Zatim stroj prelazi u stanje q_1.
- stanje q_l znači pomak glave lijevo do prve praznine, a onda prelazak u stanje q_1 (ponavljanje postupka);
- q_{STOP} je završno stanje.

Traženi Turingov stroj zadajemo sa sljedeće dvije tablice:

	q_0	q_1	q_a	q_b	q_c
s_0	s_0Lq_1	s_0Hq_{STOP}	s_0Dq_{aa}	s_0Dq_{bb}	s_0Dq_{cc}
0	0Dq_0	aDq_a	0Dq_a	0Dq_b	0Dq_c
1	1Dq_0	bDq_b	1Dq_a	1Dq_b	1Dq_c
2	2Dq_0	cDq_c	2Dq_a	2Dq_b	2Dq_c
a		aLq_1	aDq_a	aDq_b	aDq_c
b		bLq_1	bDq_a	bDq_b	bDq_c
c		cLq_1	cDq_a	cDq_b	cDq_c

	q_{aa}	q_{bb}	q_{cc}	q_l
s_0	0Lq_l	1Lq_l	2Lq_l	s_0Lq_1
0	0Dq_{aa}	0Dq_{bb}	0Dq_{cc}	0Lq_l
1	1Dq_{aa}	1Dq_{bb}	1Dq_{cc}	1Lq_l
2	2Dq_{aa}	2Dq_{bb}	2Dq_{cc}	2Lq_l

11. Konstruirajte Turingov stroj koji prirodan broj na ulazu množi s 3. Znakovi na traci su iz alfabeta $\{0, 1, \ldots, 9\}$. Broj je odijeljen sa svake strane jednim praznim mjestom. Glava čitača se na početku nalazi na prvoj znamenci.
Rješenje.

Traženi Turingov stroj zadan je sljedećom tablicom:

	q_p	q_0	q_1	q_2	q_3
0	Dq_p	Lq_0	1Lq_0	2Lq_0	s_0Sq_{STOP}
1	Dq_p	3Lq_0	4Lq_0	5Lq_0	s_0Sq_{STOP}
2	Dq_p	6Lq_0	7Lq_0	8Lq_0	s_0Sq_{STOP}
3	Dq_p	9Lq_0	0Lq_1	1Lq_1	s_0Sq_{STOP}
4	Dq_p	2Lq_1	3Lq_1	4Lq_1	s_0Sq_{STOP}
5	Dq_p	5Lq_1	6Lq_1	7Lq_1	s_0Sq_{STOP}
6	Dq_p	8Lq_1	9Lq_1	0Lq_2	s_0Sq_{STOP}
7	Dq_p	9Lq_2	2Lq_2	3Lq_2	s_0Sq_{STOP}
8	Dq_p	4Lq_2	5Lq_2	6Lq_2	s_0Sq_{STOP}
9	Dq_p	7Lq_2	8Lq_2	9Lq_2	s_0Sq_{STOP}
s_0	Lq_0	Hq_{STOP}	1Lq_3	2Lq_3	s_0Hq_{STOP}

12. Definirajte Turingov stroj koji izračunava funkciju $n \mapsto n+1$, pri čemu je prirodan broj dan u dekadskom zapisu.

13. Definirajte Turingov stroj koji niz znamenki iz skupa $\{0,1,2,3\}$ sortira u neopadajućem poretku. Ulazni niz je omeđen s praznim simbolima. Izlazni niz treba biti omeđen također praznim simbolima. Za ilustraciju navodimo primjer:

    ulazni niz $s_0 3201213 s_0$
    izlazni niz $s_0 0112233 s_0$

1.3 Rekurzivne funkcije

Sada definiramo još jednu klasu funkcija za koje ćemo se odmah iz definicije biti jasno da su izračunljive u intuitivnom smislu. Tada ćemo dokazati da se ta novo definirana klasa funkcija poklapa s klasom RAM–izračunljivih funkcija.

Definicija 1.17. *Funkciju* $Z : \mathbb{N} \to \mathbb{N}$ *definiranu sa* $Z(x) = 0$ *nazivamo* **nul–funkcija.**

Funkciju $Sc : \mathbb{N} \to \mathbb{N}$ *definiranu sa* $Sc(x) = x + 1$ *nazivamo* **funkcija sljedbenika** *(eng. successor).*

Neka je $n \in \mathbb{N} \setminus \{0\}$ *i* $k \in \{1, \ldots, n\}$. *Funkciju* $I_k^n : \mathbb{N}^n \to \mathbb{N}$ *definiranu s* $I_k^n(x_1, \ldots, x_n) = x_k$ *nazivamo* **projekcija.**

Funkcije Z, Sc *i* I_k^n $(n \in \mathbb{N} \setminus \{0\},\ k \le n)$ *nazivamo* **inicijalne funkcije***.*

Uočite da je svaka inicijalna funkcija totalna.

Propozicija 1.18. *Svaka inicijalna funkcija je RAM–izračunljiva.*

Dokaz. Redom za svaku inicijalnu funkciju pišemo program za makro–stroj koji je izračunava.

Za nul–funkciju:	0. ZERO $\mathcal{R}_0$
Za funkciju sljedbenika:	0. MOVE $\mathcal{R}_1$ TO $\mathcal{R}_0$ 1. INC $\mathcal{R}_0$
Za projekciju I_k^n:	0. MOVE $\mathcal{R}_k$ TO $\mathcal{R}_0$

□

U daljnjim izlaganjima promatrat ćemo i funkcije koje nisu totalne, pa ćemo se često susretati s izrazima koji za neke prirodne brojeve nisu definirani. Npr. izraz $\frac{x^2-4}{x-2}$ je nedefiniran za $x = 2$, a za sve ostale $x \in \mathbb{N}$ vrijednost izraza je prirodan broj. Važno je naglasiti da mi promatramo samo izraze i funkcije koji uvrštavanjem prirodnih brojeva poprimaju vrijednost koja je prirodan broj ili pak su nedefinirani. Ako je izraz X nedefiniran za neki $\vec{x} \in \mathbb{N}^k$ tada pišemo $X(\vec{x}) \uparrow$, a inače $X(\vec{x}) \downarrow$. Analogno, ako je f parcijalna funkcija, te $\vec{x} \in \mathbb{N}^k$ koji nije u domeni funkcije f, tada to kratko označavamo s $f(\vec{x}) \uparrow$. Ako pak je $\vec{x}$ u domeni funkcije tada to kratko označavamo s $f(\vec{x}) \downarrow$.

Posebno nam je važna relacija jednakosti na izrazima, odnosno između parcijalnih funkcija. Neka su X i Y neki izrazi. Sa $X \simeq Y$ označavamo činjenicu da za svaku uređenu k–torku prirodnih brojeva vrijedi:

$$X(\vec{x})\downarrow,\ Y(\vec{x})\downarrow \quad \text{i} \quad X(\vec{x}) = Y(\vec{x});$$
$$\text{ili}$$
$$X(\vec{x})\uparrow \quad \text{i} \quad Y(\vec{x})\uparrow$$

Primjer 1.19.

1. *Vrijedi* $2 \simeq \frac{2(x+1)}{x+1}$.
2. *Ne vrijedi* $7 \simeq \frac{7(x-y)}{x-y}$ *jer u slučaju* $x = y$ *izraz* $\frac{7(x-y)}{x-y}$ *je nedefiniran.*
3. *Neka je* $S = \{0, 2, 4, 6, 8\}$ *i* $F, G : S \to \mathbb{N}$ *funkcije koje su definirane ovako:* $F(n) = n + 1$, $G(n) = \frac{n^2-1}{n-1}$. *Tada vrijedi* $F \simeq G$.

Kako bi definirali pojam rekurzivne funkcije moramo definirati još tri operacije: kompoziciju, primitivnu rekurziju i μ-operator. U sljedećoj definiciji prvo definiramo kompoziciju.

Definicija 1.20. *Neka su* $G, H_1, \ldots H_n$ *funkcije. Neka je funkcija* F *definirana sa:*

$$F(\vec{x}) \simeq G(H_1(\vec{x}), \ldots, H_n(\vec{x})).$$

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

Propozicija 1.21. *Klasa RAM–izračunljivih funkcija je zatvorena za kompoziciju, tj. točnije ako su i* G, H_1, $\ldots$ H_n *RAM–izračunljive funkcije, tada je i funkcija* F *koja je dobivena kompozicijom iz funkcija* G, H_1, $\ldots$ H_n *također RAM–izračunljiva.*

Dokaz. Navodimo jedan program za makro–stroj koji izračunava funkciju F.

0. $H_1(\mathcal{R}_1, \ldots, \mathcal{R}_k) \to \mathcal{R}_{k+1}$

$\vdots$

(n-1). $H_n(\mathcal{R}_1, \ldots, \mathcal{R}_k) \to \mathcal{R}_{k+n}$

n. $G(\mathcal{R}_{k+1}, \ldots, \mathcal{R}_{k+n}) \to \mathcal{R}_0$

(Uočite da je ovdje važno da nakon niti jednog koraka prilikom izvršavanja programa nisu promijenjeni ulazni podaci u registrima $\mathcal{R}_1, \ldots, \mathcal{R}_k$). □

Definicija 1.22. *Neka je* $k > 0$, *te* G *totalna* k*–mjesna funkcija i* H *totalna* $(k+2)$*–mjesna funkcija. Neka je* $(k+1)$*–mjesna funkcija* F *definirana na sljedeći način:*

$$\begin{aligned} F(0, \vec{x}) &= G(\vec{x}) \\ F(y+1, \vec{x}) &= H(F(y, \vec{x}), y, \vec{x}) \end{aligned}$$

Tada kažemo da je funkcija F definirana pomoću **primitivne rekurzije.**
Ako je $k = 0$ tada definicija funkcije F pomoću primitivne rekurzije izgleda:

$$\begin{array}{rcl} F(0) & = & a \qquad (a \in \mathbb{N}) \\ F(y+1) & = & H(F(y), y) \end{array}$$

Propozicija 1.23. *Klasa RAM–izračunljivih funkcija je zatvorena za primitivnu rekurziju, tj. ako su G i H RAM–izračunljive totalne funkcije tada je funkcija F, koja je definirana pomoću primitivne rekurzije iz G i H, također RAM–izračunljiva.*

Dokaz. Radi kraćeg zapisivanja promatramo slučaj kada je $k = 1$. Sada ćemo navesti jedan program za makro–stroj koji izračunava funkciju F.

0. $G(\mathcal{R}_2) \to \mathcal{R}_0$
1. MOVE $\mathcal{R}_1$ TO $\mathcal{R}_3$
2. ZERO $\mathcal{R}_1$
3. DEC $\mathcal{R}_3, 8$
4. $H(\mathcal{R}_0, \mathcal{R}_1, \mathcal{R}_2) \to \mathcal{R}_4$
5. MOVE $\mathcal{R}_4$ TO $\mathcal{R}_0$
6. INC $\mathcal{R}_1$
7. GO TO 3
8. STOP

□

Definicija 1.24. *Najmanja klasa totalnih funkcija koja sadrži inicijalne funkcije, te je zatvorena za kompoziciju i primitivnu rekurziju, naziva se klasa* **primitivno rekurzivnih funkcija.**

Za relaciju $R \subseteq \mathbb{N}^k$ kažemo da je **primitivno rekurzivna relacija** *ako je njena karakteristična funkcija primitivno rekurzivna.*

Analogno, za skup $S \subseteq \mathbb{N}^k$ kažemo da je **primitivno rekurzivan skup** *ako je njegova karakteristična funkcija primitivno rekurzivna.*

Uočeno je da inicijalne funkcije, te kompozicija i primitivna rekurzija, nisu dovoljne kako bi se definirala svaka izračunljiva funkcija. Jedan primjer izračunljive funkcije koja nije primitivno rekurzivna je **Ackermanova funkcija**.[3] Kako bismo potpuno opisali klasu izračunljivih funkcija definirat ćemo kasnije još jedan operator.

Sljedeća propozicija govori o "virtualnim" varijablama. Bit će nam vrlo korisna u kasnijim razmatranjima.

[3] O Ackermanovoj funkciji možete čitati u Dodatku.

Propozicija 1.25. *Neka je g primitivno rekurzivna k–mjesna funkcija, te x_1, $\ldots$, x_n različite varijable. Neka je za sve i, gdje je $1 \le i \le k$, z_i jedna od varijabli $x_1, \ldots, x_n$. Neka je funkcija f definirana s*

$$f(x_1, \ldots, x_n) = g(z_1, \ldots, z_k).$$

Tada je funkcija f primitivno rekurzivna.

Dokaz. Neka je $z_i = x_{j_i}$, gdje je $1 \le j_i \le n$, $1 \le i \le k$. Tada za sve $i \in \{1, \ldots, k\}$ vrijedi

$$I^n_{j_i}(x_1, \ldots, x_n) = z_i.$$

Time imamo

$$f(x_1, \ldots, x_n) = g(I^n_{j_1}(x_1, \ldots, x_n), \ldots, I^n_{j_k}(x_1, \ldots, x_n)).$$

To znači da je funkcija f definirana pomoću kompozicije primitivno rekurzivnih funkcija, pa je primitivno rekurzivna po definiciji. $\square$

Primjenom prethodne propozicije odmah slijedi rekurzivnost nul-funkcije proizvoljne mjesnosti. To ističemo u sljedećoj propoziciji.

Propozicija 1.26. *Za svaki $k > 0$ neka je funkcija $N : \mathbb{N}^k \to \mathbb{N}$ definirana s $N(\vec{x}) = 0$ (opća nul–funkcija). Zatim, neka je za svaki $k > 0$ i $n \in \mathbb{N}$ funkcija $C_n : \mathbb{N}^k \to \mathbb{N}$ definirana s $C_n(\vec{x}) = n$ (konstanta funkcija). Za sve $k > 0$ i $n \in \mathbb{N}$ funkcije N i C_n su primitivno rekurzivne.*

Dokaz. Primjenom prethodne propozicije uzimajući $g(x) = Z(x)$ slijedi da je funkcija N primitivno rekurzivna za svaki $k > 0$.

Za funkcije C_n, $n \in \mathbb{N}$, dokaz provodimo indukcijom po n. Za $n = 0$ to je funkcija N za koju smo upravo dokazali da je primitivno rekurzivna. Očito za sve $n \in \mathbb{N}$ vrijedi

$$C_{n+1}(\vec{x}) = Sc(C_n(\vec{x})).$$

$\square$

Propozicija 1.27. *Funkcije $(x, y) \mapsto x+y$, $(x, y) \mapsto x\cdot y$, $x \mapsto x!$ i $(x, y) \mapsto x^y$ su primitivno rekurzivne. (Po dogovoru stavljamo $0^0 = 1$, kako bi funkcija potenciranja bila totalna).*

Dokaz. Radi ilustracije dokazujemo za zbrajanje. Očito vrijedi:

$$\begin{array}{rcl} x + 0 & = & I^1_1(x) \\ x + (y + 1) & = & Sc(I^3_1(x + y, y, x)). \end{array}$$

$\square$

Sada definiramo μ–operator na funkcijama, te tako dobivamo klasu parcijalno rekurzivnih funkcija. Kao što smo prije već bili spomenuli, svaka izračunljiva funkcija nije primitivno rekurzivna. Upravo je μ-operator ta bitna razlika između primitivno rekurzivnih i izračunljivih funkcija.

Definicija 1.28. *Neka je f funkcija. S $\mu y(f(\vec{x}, y) \simeq 0)$ označavamo funkciju definiranu na sljedeći način:*

$$\mu y(f(\vec{x}, y) \simeq 0) \simeq \begin{cases} \text{najmanji } y, \text{ ako postoji, takav da je } f(\vec{x}, z) \downarrow \\ \text{za sve } z < y, \text{ te je } f(\vec{x}, y) = 0. \end{cases}$$

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

Kao što smo već prije bili spomenuli μ–operator nam omogućava da definiramo klasu parcijalno rekurzivnih funkcija.

Definicija 1.29. *Najmanja klasa funkcija koja sadrži sve inicijalne funkcije, te je zatvorena za kompoziciju, primitivnu rekurziju i μ-operator, naziva se klasa* **parcijalno rekurzivnih funkcija.** *Funkcija iz klase parcijalno rekurzivnih funkcija koja je totalna naziva se i* **rekurzivna funkcija**. *Kažemo da je* **relacija rekurzivna** *ako je njena karakteristična funkcija rekurzivna. Specijalno, kažemo da je* **skup rekurzivan** *ako je njegova karakteristična funkcija rekurzivna.*

Iz definicija slijedi da je svaka primitivno rekurzivna funkcija ujedno i rekurzivna, a onda i parcijalno rekurzivna.

Oduzimanje nije totalna funkcija na skupu $\mathbb{N}$. Iz tog razloga definiramo sljedeću funkciju (**modificiranog oduzimanja**).

$$x \dot{-} y = \begin{cases} x - y, & \text{ako je } x \geq y; \\ 0, & \text{inače.} \end{cases}$$

Da bismo dokazali da je funkcija $\dot{-}$ primitivno rekurzivna prvo definiramo funkciju pr (**funkcija prethodnik**) pomoću primitivne rekurzije ovako:

$$\begin{aligned} pr(0) &= 0 \\ pr(x+1) &= x \end{aligned}$$

Sada funkciju $\dot{-}$ možemo definirati pomoću primitivne rekurzije ovako:

$$\begin{aligned} x \dot{-} 0 &= x \\ x \dot{-} (y+1) &= pr(x \dot{-} y) \end{aligned}$$

Napomena 1.30. *U daljnjim razmatranjima koristit ćemo i sljedeću definiciju funkcije pomoću μ–operatora i relacije. Neka je R neka $(k+1)$–mjesna relacija. Sa $\mu y R(\vec{x}, y)$ označavamo funkciju definiranu na sljedeći način:*

$$\mu y R(\vec{x}, y) \;\simeq\; \left\{ \begin{array}{l} \text{najmanji } z \text{ tako da ne vrijedi } R(\vec{x}, y) \;\; \text{niti za jedan } y < z \text{ i} \\ \text{vrijedi } \; R(\vec{x}, z), \; \text{ako takav } z \text{ postoji.} \end{array} \right.$$

Očito vrijedi

$$\mu y R(\vec{x}, y) \;\simeq\; \mu y \Big(1 \dot{-} \chi_R(\vec{x}, y) \simeq 0 \Big)$$

Iz toga slijedi da je za svaku rekurzivnu relaciju R funkcija $\mu y R$ parcijalno rekurzivna. To znači da primjenom μ–operatora na rekurzivne relacije nismo proširili klasu parcijalno rekurzivnih funkcija.

Sljedeća napomena je jako važna jer naglašava čestu grešku prilikom definicije μ–operatora.

Napomena 1.31. *Neka je $f(\vec{x}, y)$ parcijalno rekurzivna funkcija. Zatim, neka je sa M označen operator definiran s*

$$M(f)(\vec{x}) \simeq \left\{ \; \text{najmanji } y \text{ takav da je } f(\vec{x}, y) = 0, \; \text{ako takav } y \text{ postoji.} \right.$$

Uočite da se operator M razlikuje od μ–operatora u tome što nema zahtjeva da je funkcija f definirana za sve prirodne brojeve z koji su manji od y. U točki 1.9 ćemo pokazati da klasa RAM–izračunljivih funkcija nije zatvorena za operator M.

Propozicija 1.32. *Klasa RAM-izračunljivih funkcija je zatvorena za μ-operator, tj. ako je funkcija f RAM-izračunljiva, tada je funkcija $\mu y(f(\vec{x}, y) \simeq 0)$ također RAM-izračunljiva.*

Dokaz. Neka je f neka $(k+1)$–mjesna funkcija. Pišemo program za makro–stroj koji izračunava funkciju $\mu y(f(\vec{x}, y) \simeq 0)$.

0. ZERO $\mathcal{R}_0$
1. $f(\mathcal{R}_1, \ldots, \mathcal{R}_k, \mathcal{R}_0) \to \mathcal{R}_{k+1}$
2. DEC $\mathcal{R}_{k+1}$, 5
3. INC $\mathcal{R}_0$
4. GO TO 1
5. STOP

□

Tvrdnja sljedećeg teorema slijedi iz prethodnih propozicija 1.18., 1.21., 1.23. i 1.32.

Teorem 1.33. *Svaka parcijalno rekurzivna funkcija je RAM-izračunljiva.*

U daljnjim razmatranjima cilj nam je dokazati obrat prethodnog teorema.

Sada navodimo primjere primitivno rekurzivnih funkcija koje ćemo kasnije koristiti. Funkcija **apsolutne vrijednosti razlike** je dvomjesna funkcija čiju vrijednost označavamo s $|x-y|$, a definirana je s

$$|x-y| = (x \dot{-} y) + (y \dot{-} x)$$

Pošto su funkcije $\dot{-}$ i $+$ primitivno rekurzivne, tada je i funkcija apsolutne vrijednosti razlike primitvno rekurzivna.

Sa sg označavamo **funkciju predznaka**, tj. funkciju signum, definiranu sa:

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

Pošto funkciju sg možemo definirati pomoću primitivne rekurzije na sljedeći način:

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

slijedi da je funkcija signum primitivno rekurzivna.

Označimo sa $\overline{sg}$ funkciju definiranu sa:

$$\overline{sg}(x) = \begin{cases} 1, & \text{ako je } \ x = 0; \\ 0, & \text{inače.} \end{cases}$$

Očito vrijedi $\overline{sg}(x) = 1 \dot{-} x$, pa je funkcija $\overline{sg}$ primitivno rekurzivna.

Sljedeću propoziciju ćemo često koristiti.

Propozicija 1.34. *Neka su R i P (primitivno) rekurzivne relacije. Tada su i relacije $\neg R$, $R \wedge P$, $R \vee P$, $R \rightarrow P$ i $R \leftrightarrow P$ (primitivno) rekurzivne.*

Dokaz. Očito vrijedi

$$\begin{aligned} &\chi_{\neg R}(\vec{x}) = 1 \dot{-} \chi_R(\vec{x}) \\ &\chi_{R \wedge P}(\vec{x}) = \chi_R(\vec{x}) \cdot \chi_P(\vec{x}) \end{aligned}$$

Pošto je $\{\neg, \wedge\}$ baza za skup svih propozicionalnih veznika, sve druge relacije koje su navedene u iskazu propozicije, možemo shvatiti kao pokrate. □

Korolar 1.35. *Neka su A i B rekurzivni skupovi. Tada su i A^c, $A \cap B$ i $A \cup B$ rekurzivni skupovi. Presjek, odnosno unija, konačno mnogo rekurzivnih skupova je rekurzivan skup.*

Propozicija 1.36. *Relacije* $\leq$, $\geq$, $<$, $>$ *i* $=$ *su primitivno rekurzivne.*

Dokaz. Lako je provjeriti da redom vrijedi:

$$\begin{array}{l}
\chi_{>}(x,y) = sg(x \dot{-} y) \\
x \leq y \ \text{ ako i samo ako vrijedi } \ \neg(x > y) \\
x \geq y \ \text{ ako i samo ako vrijedi } y \leq x \\
x < y \ \text{ ako i samo ako vrijedi } \ \neg(y \leq x) \\
x = y \ \text{ ako i samo ako vrijedi } \ (x \leq y \ \wedge \ y \leq x)
\end{array}$$

Sada primjenom propozicije 1.34. slijedi tvrdnja ove propozicije. □

Propozicija 1.37. *Neka su* $R_1, \ldots R_n$ *(primitivno) rekurzivne relacije koje imaju svojstvo da za sve* $\vec{x}$ *postoji točno jedan* $i \in \{1, \ldots, n\}$ *tako da vrijedi* $R_i(\vec{x})$. *Neka su* $F_1, \ldots, F_n$ *(primitivno) rekurzivne funkcije. Tada je funkcija* $F : \mathbb{N}^k \to \mathbb{N}$ *definirana sa:*

$$F(\vec{x}) = \begin{cases} F_1(\vec{x}), & \textit{ako vrijedi } \ R_1(\vec{x}), \\ \quad \vdots & \\ F_n(\vec{x}), & \textit{ako vrijedi } \ R_n(\vec{x}) \end{cases}$$

također (primitivno) rekurzivna.

Dokaz. Očito vrijedi

$$F(\vec{x}) = F_1(\vec{x}) \cdot \chi_{R_1}(\vec{x}) + \ \ldots \ + F_n(\vec{x}) \cdot \chi_{R_n}(\vec{x}).$$

Sada primjenom propozicije 1.27. slijedi tražena tvrdnja. □

Prethodnu propoziciju ćemo često upotrebljavati. Radi ilustracije navodimo jedan primjer funkcije čiju rekurzivnost slijedi upravo iz prethodne propozicije.

Primjer 1.38. *Neka je funkcija* F *definirana po slučajevima na sljedeći način:*

$$F(x,y) = \begin{cases} x, & \textit{ako vrijedi } \ x < y; \\ y+2, & \textit{ako vrijedi } \ y \leq 4 \ \ i \ \ x = 4; \\ 3, & \textit{inače.} \end{cases}$$

Kako bi dokazali rekurzivnost funkcije F *uvodimo sljedeće oznake. Neka su funkcije* F_1, F_2 *i* F_3 *definirane redom sa:* $F_1(x,y) = x$, $F_2(x,y) = y + 2$ *i* $F_3(x,y) = 3$. *Pošto je* $F_1 = I_1^2$ *tada je funkcija* F_1 *rekurzivna po definiciji. Očito vrijedi* $F_2(x,y) = Sc(Sc(I_2^2(x,y)))$, *a iz toga slijedi rekurzivnost funkcije* F_2. *Funkcija* F_3 *je konstantna funkcija, pa njena rekurzivnost slijedi iz propozicije 1.26.*

Relacije $<$, $\leq$ i $=$ su rekurzivne (propozicija 1.36.) Rekurzivnost relacije "$y \leq x$ i $x = 4$" slijedi iz propozicije 1.34. Ako sa R_1 označimo relaciju $<$, a sa $R_2(x, y)$ relaciju $y \leq x \wedge x = 4$, tada je relacija R_3 (tj. "inače" koje se navodi u definiciji funkcije F), ekvivalenta sa $\neg(R_1 \vee R_2)$. Rekurzivnost relacije R_3 slijedi iz propozicije 1.34. Očito relacije R_i imaju svojstvo da za sve $x, y \in \mathbb{N}$ postoji točno jedan $i \in \{1, 2, 3\}$ takav da vrijedi $R_i(x, y)$.

Time smo pokazali da je funkcija F definirana po slučajevima pomoću rekurzivnih funkcija i rekurzivnih relacija, pa iz propozicije 1.37. slijedi rekurzivnost funkcije F.

Propozicija 1.39. *Neka je F (primitivno) rekurzivna funkcija, a G totalna funkcija koja ima svojstvo da vrijedi $G(\vec{x}) = F(\vec{x})$, osim možda za konačno mnogo $\vec{x}$. Tada je funkcija G također (primitivno) rekurzivna.*

Dokaz. Neka su $\vec{a}_1, \ldots, \vec{a}_m$ sve uređene k-torke $\vec{x}$ prirodnih brojeva za koje vrijedi $F(\vec{x}) \neq G(\vec{x})$. Neka su $b_1, \ldots, b_m$ prirodni brojevi za koje vrijedi $b_i = G(\vec{a}_i)$. Tada očito vrijedi

$$G(\vec{x}) = \begin{cases} b_1, & \text{ako } \vec{x} = \vec{a}_1; \\ & \quad\vdots \\ b_m, & \text{ako } \vec{x} = \vec{a}_m; \\ F(\vec{x}), & \text{inače.} \end{cases}$$

Primjenom propozicije 1.26. slijedi da su funkcije $\vec{x} \mapsto b_i$ primitivno rekurzivne. Iz propozicije 1.36. znamo da je jednakost primitivno rekurzivna relacija. Sada primjenom propozicije 1.37. slijedi da je funkcija G (primitivno) rekurzivna. $\square$

Korolar 1.40. *Neka je R relacija za koju postoji najviše konačno mnogo $\vec{x}$ takvih da vrijedi $R(\vec{x})$. Tada je relacija R primitivno rekurzivna.*

Dokaz. Iz pretpostavke korolara slijedi da je $\chi_R(\vec{x}) = 0$, osim možda za konačno mnogo $\vec{x}$. Sada primjenom prethodne propozicije i propozicije 1.26. slijedi tvrdnja. $\square$

Budući da svaki skup možemo promatrati kao unarnu relaciju, iz prethodnog korolara direktno slijedi sljedeća tvrdnja.

Korolar 1.41. *Svaki konačan skup je primitivno rekurzivan.*

U sljedećoj propoziciji ističemo da su ograničene sume i produkti rekurzivne funkcije.

Propozicija 1.42. *Neka su g, α i β (primitivno) rekurzivne funkcije. Tada su (primitivno) rekurzivne i sljedeće funkcije:*

$$a)\quad f(\vec{x},y)=\sum_{i=0}^{y} g(\vec{x},i).$$

$$b)\quad f(\vec{x},y,z)=\begin{cases} \displaystyle\sum_{i=y}^{z} g(\vec{x},i), & \textit{ako je}\ \ y\le z;\\ 0, & \textit{inače.}\end{cases}$$

$$c)\quad f(\vec{x})=\begin{cases} \displaystyle\sum_{i=\alpha(\vec{x})}^{\beta(\vec{x})} g(\vec{x},i), & \textit{ako je}\ \ \alpha(\vec{x})\le\beta(\vec{x});\\ 0, & \textit{inače.}\end{cases}$$

$$d)\quad f(\vec{x},y)=\prod_{i=0}^{y} g(\vec{x},i).$$

$$e)\quad f(\vec{x},y,z)=\begin{cases} \displaystyle\prod_{i=y}^{z} g(\vec{x},i), & \textit{ako je}\ \ y\le z;\\ 1, & \textit{inače.}\end{cases}$$

$$f)\quad f(\vec{x})=\begin{cases} \displaystyle\prod_{i=\alpha(\vec{x})}^{\beta(\vec{x})} g(\vec{x},i), & \textit{ako je}\ \ \alpha(\vec{x})\le\beta(\vec{x});\\ 1, & \textit{inače.}\end{cases}$$

Dokaz. Za ilustraciju dokazujemo tvrdnje a) i b). Funkciju f iz tvrdnje a) moguće je definirati pomoću primitivne rekurzije na sljedeći način:

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

Lako je provjeriti da za funkciju f iz tvrdnje b) vrijedi sljedeće:

$$f(\vec{x},y,z)=\left(\sum_{i=0}^{z} g(\vec{x},i)\right)\dot{-}\left(\sum_{i=0}^{y} g(\vec{x},i)\right)\ +\ g(\vec{x},y)\cdot\overline{sg}(y\dot{-}z).$$

□

Ako je $R(\vec{x}, y)$ rekurzivna relacija tada općenito relacije $\exists y R(\vec{x}, y)$ i $\forall y R(\vec{x}, y)$ ne moraju biti rekurzivne. To ćemo pokazati kasnije u točki 1.9. Nije teško dokazati da je primjenom ograničene kvantifikacije sačuvana rekurzivnost. To ističemo u sljedećoj propoziciji.

Propozicija 1.43. *Neka je R (primitivno) rekurzivna relacija. Tada su (primitivno) rekurzivne i sljedeće relacije:* $(\exists y < z)\ R(\vec{x}, y)$, $(\exists y \le z)\ R(\vec{x}, y)$, $(\forall y < z)\ R(\vec{x}, y)$ *i* $(\forall y \le z)\ R(\vec{x}, y)$.

Dokaz. Označimo sa $P(\vec{x}, z)$ relaciju $(\exists y < z)\ R(\vec{x}, y)$. Lako je vidjeti da vrijedi

$$\chi_P(\vec{x}, z) = \begin{cases} sg(\sum_{y=0}^{z \dot{-} 1} \chi_R(\vec{x}, y)), & \text{ako je } z \neq 0; \\ 0, & \text{ako je } z = 0. \end{cases}$$

(Primitivna) rekurzivnost karakteristične funkcije χ_P slijedi iz propozicije 1.42.

Označimo sa Q relaciju $(\forall y \le z)\ R(\vec{x}, y)$. Lako je provjeriti da vrijedi

$$\chi_Q(\vec{x}, z) = \prod_{y=0}^{z} \chi_R(\vec{x}, y).$$

Iz posljednje jednakosti očito slijedi (primitivna) rekurzivnost relacije Q. $\square$

Korolar 1.44. *Neka je R (primitivno) rekurzivna relacija. Tada su (primitivno) rekurzivne i sljedeće relacije:* $\exists y_{z_1 < y < z_2}\ R(\vec{x}, y)$, $\exists y_{z_1 \le y \le z_2}\ R(\vec{x}, y)$, $\forall y_{z_1 < y < z_2}\ R(\vec{x}, y)$ *i* $\forall y_{z_1 \le y \le z_2}\ R(\vec{x}, y)$.

Korolar 1.45. *Neka su α i β (primitivno) rekurzivne funkcije, a R (primitivno) rekurzivna relacija. Tada su (primitivno) rekurzivne i sljedeće relacije:* $\exists y_{\alpha(\vec{x}) < y < \beta(\vec{x})}\ R(\vec{x}, y)$, $\exists y_{\alpha(\vec{x}) \le y \le \beta(\vec{x})}\ R(\vec{x}, y)$, $\forall y_{\alpha(\vec{x}) < y < \beta(\vec{x})}\ R(\vec{x}, y)$ *i* $\forall y_{\alpha(\vec{x}) \le y \le \beta(\vec{x})}\ R(\vec{x}, y)$.

Sljedeća propozicija govori da primjenom "ograničenog" μ-operatora na rekurzivnu relaciju dobivamo rekurzivnu (totalnu!) funkciju.

Propozicija 1.46. *Neka je R (primitivno) rekurzivna relacija. Neka je funkcija $f : \mathbb{N}^{k+1} \to \mathbb{N}$ definirana sa:*

$$f(\vec{x}, z) = \begin{cases} \text{najmanji } y \text{ takav da vrijedi } R(\vec{x}, y) \ \text{ i } \ y < z, \\ \text{ako takav } y \text{ postoji;} \\ \\ z, \ \text{inače.} \end{cases}$$

Tada je funkcija f (primitivno) rekurzivna. Obično se vrijednost tako definirane funkcije f označava i sa $(\mu y < z)\ R(\vec{x}, y)$.

Dokaz. Lako je vidjeti da vrijedi

$$(\mu y < z)\ R(\vec{x}, y) = \begin{cases} \displaystyle\sum_{y=0}^{z \dot{-} 1} \prod_{i=0}^{y} \overline{sg}(\chi_R(\vec{x}, i)), & \text{ako je } z \neq 0; \\ 0, & \text{ako je } z = 0. \end{cases}$$

Iz ovog posljednjeg odmah slijedi (primitivna) rekurzivnost dane funkcije. □

Korolar 1.47. *Neka su α i β (primitivno) rekurzivne funkcije, a R (primitivno) rekurzivna relacija. Neka je funkcija $f : \mathbb{N}^k \to \mathbb{N}$ definirana s:*

$$f(\vec{x}) = \begin{cases} \textit{najmanji } y \textit{ takav da vrijedi } R(\vec{x}, y) \textit{ i } \alpha(\vec{x}) < y < \beta(\vec{x}), \\ \textit{ako takav } y \textit{ postoji;} \\ \\ \beta(\vec{x}), \quad \textit{inače.} \end{cases}$$

Ovako definiranu funkciju f obično označavamo s $\mu y_{\alpha(\vec{x})<y<\beta(\vec{x})}\ R(\vec{x}, y)$. Analogno se definiraju i funkcije: $\mu y_{\alpha(\vec{x})\le y\le\beta(\vec{x})}\ R(\vec{x}, y)$, $\mu y_{\alpha(\vec{x})<y\le\beta(\vec{x})}\ R(\vec{x}, y)$ i $\mu y_{\alpha(\vec{x})\le y<\beta(\vec{x})}\ R(\vec{x}, y)$. Sve te funkcije su (primitivno) rekurzivne.

Zadaci:

1. Dokažite da su sljedeće funkcije primitivno rekurzivne:

   a) $\lfloor x/y \rfloor$ = *najveće cijelo prilikom dijeljenja x sa y*, pri čemu radi totalnosti funkcije definiramo $\lfloor x/0 \rfloor = x$, za sve $x \in \mathbb{N}$.

   b) $res(x, y)$ = *ostatak pri dijeljenju x sa y*, pri čemu definiramo $res(x, 0) = x$, za sve $x \in \mathbb{N}$.

   c)
   $$div(x, y) = \begin{cases} 1, & \text{ako } y \text{ dijeli } x; \\ 0, & \text{inače.} \end{cases}$$

   d) $nd(x)$ = *broj djelitelja od x*, pri čemu definiramo $nd(0) = 0$.

   e)
   $$\sigma(x) = \begin{cases} \text{suma svih djelitelja broja } x, & \text{ako je } x \neq 0; \\ 0, & \text{ako je } x = 0. \end{cases}$$

f)

$$f(n,m) = \begin{cases} \binom{n}{m}, & \text{ako je } \ n \geq m; \\ \\ 0, & \text{inače.} \end{cases}$$

Rješenje.

a) $\lfloor x/y \rfloor = \sum_{i=1}^{x} \overline{sg}(i \cdot y \dot{-} x)$.

(drugo rješenje:

$$\lfloor x/y \rfloor = \begin{cases} \mu z \leq x (z \cdot y \leq x \ \text{ i } \ (z+1) \cdot y > x), & \text{ako je } \ y \neq 0; \\ x, & \text{ako je } \ y = 0) \end{cases}$$

b) $res(x,y) = x \dot{-} (y \cdot \lfloor x/y \rfloor)$.

c) $div(x,y) = \overline{sg}(res(x,y))$.

d)

$$nd(x) = \begin{cases} \sum_{i=1}^{x} div(x,i), & \text{ako je } \ x \neq 0; \\ 0, & \text{ako je } \ x = 0. \end{cases}$$

e)

$$\sigma(x) = \begin{cases} \sum_{i=1}^{x} i \cdot div(x,i), & \text{ako je } \ x \neq 0; \\ 0, & x = 0. \end{cases}$$

f) Vrijedi:

$$f(n,m) = \begin{cases} \mu z \leq n! \big(z \cdot m! \cdot (n-m)! = n! \big), & \text{ako je } \ n \geq m; \\ 1, & \text{inače.} \end{cases}$$

Sada primitivna rekurzivnost funkcije f slijedi iz propozicija 1.27. i 1.37., te korolara 1.47.

2. Dokažite da je funkcija $p : \mathbb{N} \to \mathbb{N}$ koja svakom $n \in \mathbb{N}$ pridružuje n-ti po redu prosti broj, RAM–izračunljiva.
Rješenje. Znamo da je svaka rekurzivna funkcija RAM-izračunljiva, pa je dovoljno dokazati da je funkcija p rekurzivna. Označimo s Pr unarnu relaciju na $\mathbb{N}$ koja je definirana s

$$Pr(x) \quad \Leftrightarrow \quad x \text{ je prosti broj.}$$

Primitivna rekurzivnost relacije Pr slijedi iz ekvivalencije

$$Pr(x) \text{ ako i samo ako } nd(x) = 2$$

(primitivna rekurzivnost funkcije nd je dokazana u zadatku 1).

Očito vrijedi:

$$\begin{array}{rcl} p(0) & = & 2 \\ p(n+1) & = & \mu\, y[y > p(n) \ \wedge \ Pr(y)], \end{array}$$

pa je funkcija p rekurzivna, a onda i RAM–izračunljiva.

3. Označimo s $\Pi(x)$ broj svih prostih djelitelja broja x, pri čemu definiramo $\Pi(0) = 0$. Dokažite da je funkcija Π primitivno rekurzivna.

   Rješenje. Lako je provjeriti da vrijedi $\Pi(x) = \displaystyle\sum_{i=0}^{x} \chi_{Pr}(i) \cdot div(x, i)$.

   (Relacija Pr je definirana u rješenju prethodnog zadatka).

4. Za svaki $n \in \mathbb{N}$, $n \geq 2$, definirane su funkcije min i max s:

$$\begin{array}{l} min(x_1, \ldots, x_n) \ = \ \textit{najmanji element skupa} \ \{x_1, \ldots, x_n\}; \\ max(x_1, \ldots, x_n) \ = \textit{najveći element skupa} \ \{x_1, \ldots, x_n\}. \end{array}$$

   Dokažite da su za svaki $n \in \mathbb{N}$ funkcije min i max primitivno rekurzivne.
   Rješenje. Za $n = 2$ za funkciju min očito vrijedi $min(x, y) = x \dot{-} (x \dot{-} y)$, pa je ta funkcija primitivno rekurzivna. Primitivna rekurzivnost n-mjesne funkcije min lako se dokaže indukcijom po n.

   Uočite da vrijedi $max(x, y) = x + y - min(x, y)$.

5. Neka je za sve $x \in \mathbb{N}$ s $\varphi(x)$ označen broj svih prirodnih brojeva manjih od x koji su relativno prosti s x (uočite da je posebno $\varphi(0) = 0$). Dokažite da je funkcija φ primitivno rekurzivna. Funkcija φ se naziva Eulerova funkcija.
   Rješenje. Označnimo s rp dvomjesnu relaciju definiranu s:

$$rp(x, y) \ \Leftrightarrow \ \text{brojevi } \ x \ \text{ i } \ y \ \text{ su relativno prosti ili } x \cdot y = 0.$$

Pošto vrijedi:

$$\chi_{rp}(x,y) = \overline{sg} \sum_{i=2}^{min(x,y)} div(x,i) \cdot div(y,i),$$

tada je relacija rp primitivno rekurzivna. (Funkcija div je definirana u zadatku 1). Sada iz $\varphi(x) = \sum_{i=1}^{x} \chi_{rp}(x,i)$ slijedi primitivna rekurzivnost Eulerove funkcije.

6. Neka je za $x \neq 0$ definirano $f(x) =$ *broj eksponenata različitih od nule u rastavu broja x na proste faktore*, te neka je $f(0) = 0$. Dokažite da je f primitivno rekurzivna funkcija.

7. Dokažite da je funkcija $x \mapsto \lfloor \sqrt{x} \rfloor$ primitivno rekurzivna. Je li funkcija $f : \mathbb{N} \to \mathbb{N}$ definirana s

$$f(x) = \begin{cases} \sqrt{x}, & \text{ako je } \sqrt{x} \in \mathbb{N}; \\ 0, & \text{inače,} \end{cases}$$

primitivno rekurzivna?
Rješenje. $\lfloor \sqrt{x} \rfloor = \mu y \leq x \big(y^2 \leq x \ \wedge (y+1)^2 > x \big)$.

8. Dokažite da je funkcija $\lfloor \sqrt[y]{x} \rfloor$ primitivno rekurzivna, gdje smo definirali $\lfloor \sqrt[0]{x} \rfloor = x$, za sve $x \in \mathbb{N}$.

9. Funkcija $f : \mathbb{N} \to \mathbb{N}$ definirana je s $f(x) = \lfloor \log_2 x \rfloor$. Dokažite da je funkcija f RAM–izračunljiva.

10. Neka je funkcija $f : \mathbb{N} \to \mathbb{N}$ definirana s:

$$f(x) = \left\lfloor \ \sqrt[7]{\log_2 \tfrac{2x+1}{2} + 3} \quad \right\rfloor$$

Dokažite da je funkcija f primitivno rekurzivna.
Rješenje. Očito vrijedi

$$f(x) = (\mu y < x)(2^{y^7 \dot{-} 3} \cdot 2 \dot{-} 1 \leq 2x < 2^{(y+1)^7 \dot{-} 3} \cdot 2 \dot{-} 1),$$

iz čega slijedi primitivna rekurzivnost funkcije f.

11. Dokažite da je sljedeća funkcija f primitivno rekurzivna:

$$f(x_1, \ldots, x_n) = 2^{max(x_2,\ldots,x_n)} \ + \ \lfloor \log \ min(x_1+1, \ldots, x_{n-1}+1) \rfloor.$$

12. Dokažite da su sljedeće relacije primitivno rekurzivne:

    a) *x je savršen broj*;
    b) *znamenka jedinica broja $3x$ je jednaka 7*;
    c) *x je kvadrat prostog broja*;
    d) *x je djeljiv s 2, 3 ili 5, i s niti jednim drugim prostim brojem*;
    e) *x u svom zapisu s bazom 3 nema znamenku 1.*

13. a) Relacija $P(x)$ je zadana s $(\exists n \in \mathbb{N})(x = 1 + 2 + \ldots + n)$. Je li relacija P primitivno rekurzivna?

    b) Relacija $P(x)$ je zadana s $(\exists n \in \mathbb{N})(x = 1^2 + 2^2 + \ldots + n^2)$. Dokažite da je relacija P primitivno rekurzivna.

    Rješenje b). Označimo s f funkciju definiranu s:

    $$\begin{aligned} &f(0) = 0 \\ &f(n+1) = f(n) + (n+1)^2. \end{aligned}$$

    Očito je funkcija f primitivno rekurzivna. Karakteristična funkcija relacije P je dana sa $\chi_P(x) = \sum_{i=0}^{x} \chi_=(f(i), x)$. Iz ovog posljednjeg vidimo da je relacija P primitivno rekurzivna.

14. Dokažite da su sljedeći skupovi rekurzivni: $\emptyset$, $\mathbb{N}$, svaki podskup od $\mathbb{N}$ čiji je komplement konačan, skup svih parnih i skup svih neparnih prirodnih brojeva.

15. Neka je f monotono padajuća funkcija. Dokažite da je tada slika od f rekurzivan skup, te da je f primitivno rekurzivna funkcija.

16. Dokažite da je svaka funkcija s konačnom domenom parcijalno rekurzivna.
    Rješenje. Neka je f n-mjesna, te neka je domena

    $$Dom(f) = \{(a_{11}, \ldots, a_{1n}), \ldots, (a_{m1}, \ldots, a_{mn})\}.$$

    Označimo $f(a_{i1}, \ldots, a_{in}) = b_i$, za sve $i = 1, \ldots, m$. Tada imamo:

    $$f(\vec{x}) \simeq \sum_{i=1}^{m} b_i \cdot \overline{sg}\Big(|x_1 - a_{i1}| + \ldots + |x_n - a_{in}|\Big) +$$

    $$\mu z\Big(z + \prod_{j=1}^{m} (|x_1 - a_{j1}| + \ldots + |x_n - a_{jn}|) = 0\Big).$$

    Iz ovog posljednjeg slijedi parcijalna rekurzivnost funkcije f.

17. Dokažite da se pomoću nul-funkcije i projekcija primjenom pravila kompozicije i primitivne rekurzije ne može izraziti funkcija $Sc(x) = x + 1$.
Rješenje. Neka je $f(\vec{x})$ funkcija dobivena pomoću nul-funkcije i projekcija primjenom kompozicije i primitivne rekurzije. Tvrdimo da je tada $f(0, \ldots, 0) = 0$. (Uočite da iz toga slijedi da se funkcija Sc ne može izraziti pomoću danih jer je $Sc(0) = 1$).

Neka je $f_1, \ldots, f_m = f$ konačan niz funkcija takav da za svaki $i \in \{1, \ldots, m\}$ vrijedi barem jedno od:

a) f_i je nul-funkcija;
b) f_i je neka projekcija;
c) f_i je nastala kompozicijom iz nekih f_j $(j < i)$;
d) f_i je nastala pomoću primitivne rekurzije iz nekih f_j $(j < i)$;

Indukcijom po m lako se dokaže da za sve i vrijedi $f_i(0, \ldots, 0) = 0$. Tada je posebno $f_m(0, \ldots, 0) = 0$, tj. $f(0, \ldots, 0) = 0$.

18. Neka je $a_0, a_1 a_2 \ldots$ decimalni prikaz broja $\sqrt[3]{5}$. Dokažite da je funkcija $n \mapsto a_n$ primitivno rekurzivna.
Rješenje. Neka je $n \geq 1$. Iz

$$a_0, a_1 ... a_n < \sqrt[3]{5} < a_0, a_1 ... a_n + 10^{-n}$$

slijedi da je

$$(\overline{a_0 a_1 ... a_n})^3 < 5 \cdot 10^{3n} < (\overline{a_0 a_1 ... a_n} + 1)^3$$

pa je $\overline{a_0 a_1 ... a_n}$ najmanji prirodan broj k takav da je $(k+1)^3 > 5 \cdot 10^{3n}$. Stoga je a_n ostatak pri dijeljenju s 10 broja

$$\mu k((k+1)^3 > 5 \cdot 10^{3n}) = \mu k \leq 5 \cdot 10^{3n}((k+1)^3 > 5 \cdot 10^{3n})$$

iz čega slijedi da je funkcija $n \mapsto a_n$ primitivno rekurzivna.

19. Neka je funkcija f definirana s $f(n) = \lfloor e \cdot n \rfloor$, gdje je e baza prirodnog logaritma. Dokažite da je funkcija f primitivno rekurzivna.
Rješenje. Definirajmo funkciju $S : \mathbb{N} \to \mathbb{N}$ sa

$$S(n) = n! + \frac{n!}{1!} + \frac{n!}{2!} + \ldots + \frac{n!}{n!}.$$

Funkcija S je primitivno rekurzivna jer se može definirati pomoću primitivne rekurzije na sljedeći način:

$$\begin{aligned} S(0) = &\quad 1 \\ S(n+1) = &\quad (n+1)\cdot S(n) + 1 \end{aligned}$$

Za svaki $n \in \mathbb{N}$ označimo

$$R(n) = \sum_{k=n+1}^{\infty} \frac{1}{k!}$$

Primijetimo da za sve $n \in \mathbb{N}$ vrijedi

$$\begin{aligned} R(n) = &\quad \frac{1}{n!}\cdot\left(\frac{1}{n+1} + \frac{1}{(n+1)(n+2)} + \frac{1}{(n+1)(n+2)(n+3)} + \ldots\right) \\ < &\quad \frac{1}{n!}\cdot\left(\frac{1}{n+1} + \frac{1}{(n+1)^2} + \frac{1}{(n+1)^3} + \ldots\right) \\ = &\quad \frac{1}{n!}\cdot\left(\frac{1}{n+1}\cdot\frac{1}{1-\frac{1}{n+1}}\right) = \frac{1}{n\cdot n!} < \frac{1}{n!} \end{aligned}$$

Znamo da vrijedi

$$\begin{aligned} e = &\quad 1 + \frac{1}{1!} + \ldots + \frac{1}{n!} + \frac{1}{(n+1)!} + \ldots \\ = &\quad \frac{1}{n!}\Big(n! + \frac{n!}{1!} + \ldots + \frac{n!}{n!}\Big) + \frac{1}{(n+1)!} + \ldots = \frac{1}{n!}\cdot S(n) + R(n) \end{aligned}$$

Iz ovog posljednjeg, te činjenice da vrijedi $R(n) < \frac{1}{n!}$, slijedi

$$e < \frac{1}{n!}\cdot S(n) + \frac{1}{n!}.$$

Pošto je očito $\frac{1}{n!}S(n) < e$, tada slijedi

$$\frac{1}{n!}S(n) < e < \frac{1}{n!}\cdot S(n) + \frac{1}{n!}.$$

Množenjem s n dobivamo

$$\frac{1}{(n-1)!}S(n) < e\cdot n < \frac{S(n)+1}{(n-1)!},$$

iz čega slijedi

$$f(n) = \lfloor e \cdot n \rfloor = \mu z \leq S(n) \Big(S(n) \leq z \cdot (n-1)! < S(n) + 1 \Big).$$

20. Dokažite da je funkcija $n \mapsto \lfloor e^n \rfloor$ primitivno rekurzivna.

21. Neka je $e = 2 + \sum_{n=1}^{\infty} \frac{a_n}{10^n}$, gdje za sve $n \in \mathbb{N}$ vrijedi $a_n \in \{0, 1, \dots, 9\}$, te definiramo $a_0 = 2$. Dokažite da je funkcija $n \mapsto a_n$ primitivno rekurzivna.

22. Neka je $\pi = 3 + \sum_{n=1}^{\infty} \frac{a_n}{10^n}$, gdje za sve $n \in \mathbb{N}$ vrijedi $a_n \in \{0, 1, \dots, 9\}$, te definiramo $a_0 = 3$. Dokažite da je funkcija $n \mapsto a_n$ primitivno rekurzivna.
Uputa. Pošto je

$$\frac{1}{1+x^2} = 1 - x^2 + x^4 - x^6 + x^8 - \dots,$$

integriranjem dobivamo

$$\operatorname{arctg} x = \sum_{n=0}^{\infty} (-1)^n \frac{x^{2n+1}}{2n+1}$$

Tada iz toga i $\pi = 6 \cdot \operatorname{arctg} \frac{1}{\sqrt{3}}$ slijedi

$$\pi = \frac{6}{\sqrt{3}} \sum_{n=0}^{\infty} \frac{(-1)^n}{3^n(2n+1)}$$

23. Neka je $k \in \mathbb{N} \setminus \{0\}$, proizvoljan, ali fiksiran. Dokažite da je skup

$$\{(a_0, \dots, a_k) \in \mathbb{N}^{k+1} : \text{ polinom } a_0 + \dots + a_k x^k \text{ ima cjelobrojni korijen}\}$$

primitivno rekurzivan.
Rješenje. Definiramo funkciju $f : \mathbb{N}^{k+2} \to \mathbb{N}$ na sljedeći način. Ako je k paran, neka je

$$f(x, a_0, ..., a_k) = |(a_0 + a_2 x^2 + ... + a_k x^k) - (a_1 x + a_3 x^3 ... + a_{k-1} x^{k-1})|,$$

a ako je k neparan, neka je

$$f(x, a_0, ..., a_k) = |(a_0 + a_2 x^2 + ... + a_{k-1} x^{k-1}) - (a_1 x + a_3 x^3 ... + a_k x^k)|.$$

Funkcija f je primitivno rekurzivna i vrijedi da je $f(x, a_0, ..., a_k) = 0$ ako i samo ako je $a_0 + a_1(-x) + ... + a_k(-x)^k = 0$. Ako je $(a_0, ..., a_k) \in \mathbb{N}^{k+1}$, $a_0 \neq 0$, te α cjelobrojna nultočka polinoma $a_0 + a_1 x + ... + a_k x^k$, tada je α djelitelj od a_0 te se nalazi u skupu $\{0, -1, ..., -a_0\}$. Stoga je

$$\chi_S(a_0, ..., a_k) = \overline{sg}\left(\prod_{x=0}^{a_0} f(x, a_0, ..., a_k)\right)$$

pa slijedi da je S primitivno rekurzivan skup.

24. Neka su g i h primitivno rekurzivne funkcije. Funkcija f definirana je sa:

$$\begin{array}{rcl} f(0, x) & = & g(x) \\ f(z+1, x) & = & f(z, h(z, x)). \end{array}$$

Dokažite da je funkcija f primitivno rekurzivna.
Rješenje. Neka su funkcije f_0 i f_1 definirane ovako:

$$\begin{array}{rcl} f_0(0, z, x) & = & x \\ f_0(n+1, z, x) & = & h(z \dot{-} n, f_0(n, z, x)) \\ & & \\ f_1(z, x) & = & g(f_0(z, z \dot{-} 1, x)). \end{array}$$

Dokazujemo da vrijedi $f = f_1$.

Prvo indukcijom po n dokazujemo da za sve $z \in \mathbb{N}$ vrijedi

$$f_0(n+1, z, x) = f_0(n, z \dot{-} 1, h(z, x)).$$

Za $n = 0$ imamo

$$f_0(1, z, x) = h(z \dot{-} 0, f_0(0, z, x)) = h(z, x) = f_0(0, z \dot{-} 1, h(z, x)).$$

Pretpostavimo da za neki $n \in \mathbb{N}$ vrijedi $f_0(n+1, z, x) = f_0(n, z \dot{-} 1, h(z, x))$. Tada imamo

$$f_0(n+2, z, x) = h(z \dot{-} (n+1), f_0(n+1, z, x)) = f_0(n+1, z \dot{-} 1, h(z, x))$$

$$= h((z \dot{-} 1) \dot{-} n, f_0(n, z \dot{-} 1, h(z,x))) = h(z \dot{-} (n+1), f_0(n, z \dot{-} 1, h(z,x)))$$

Slično se indukcijom po z dokaže (koristeći prethodno dokazanu tvrdnju) da za sve $x \in \mathbb{N}$ vrijedi

$$f_1(z,x) = f(z,x).$$

Funkcija f_1 je očito primitivno rekurzivna, pa slijedi da je i funkcija f primitivno rekurzivna.

25. Neka su g, h i p primitivno rekurzivne funkcije. Neka je funkcija f definirana sa:

$$\begin{array}{l} f(0,x) = g(x) \\ f(z+1,x) = h(z,x,f(z,p(z,x))). \end{array}$$

Dokažite da je funkcija f primitivno rekurzivna.
Rješenje. Neka su funkcije f_0, f_1, f_2 i f_3 definirane ovako:

$$\begin{array}{rcl} f_0(0,z,x) & = & x \\ f_0(n+1,z,x) & = & f_0(n, z \dot{-} 1, p(z \dot{-} 1, x)) \\ \\ f_1(n,z,x,y) & = & h(z \dot{-} (n+1), f_0(n,z,x), y) \\ \\ f_2(0,z,x,y) & = & y \\ f_2(n+1,z,x,y) & = & f_2(n,z,x,f_1(n,z,x,y)) \\ \\ f_3(z,x) & = & f_2(z,z,x,g(f_0(z,z,x))) \end{array}$$

Primitivna rekurzivnost funkcija f_0 i f_2 slijedi iz prethodnog zadatka. Primitivna rekurzivnost funkcija f_1 i f_3 tada je očita.

Indukcijom po n lako je dokazati da za sve $z, x, y \in \mathbb{N}$ vrijedi

$$f_1(n+1, z+1, x, y) = f_1(n, z, p(z,x), y) \quad \text{i}$$

$$f_2(n+1, z+1, x, y) = h(z, x, f_2(n, z, p(z,x), y)).$$

Na kraju indukcijom po z dokažite da za svaki $x \in \mathbb{N}$ vrijedi $f_3(z,x) = f(z,x)$.

1.4 Kodiranje konačnih nizova. Primjene

Na početku smo definirali da promatramo izračunljivost funkcija $f : S \subseteq \mathbb{N}^k \to \mathbb{N}$. Sada želimo opisati postupak prevođenja drugih funkcija i problema.

Pretpostavimo da je zadana neka klasa I koja nije podskup skupa $\mathbb{N}^k$, za neki $k \in \mathbb{N}$. Razmatramo algoritme čiji su ulazni i izlazni podaci iz skupa I. Osnovna ideja je da svakom članu klase I pridružimo prirodni broj, koji ćemo nazivati **kod** danog člana. Naravno, svakako želimo da je dano pridruživanje **injektivno**. Time smo prije svega ulaznim podacima pridružili kodove. Zatim provedemo izračunavanje (npr. na RAM-stroju) s numeričkim podacima. Ako stroj stane dobit ćemo numerički izlazni podatak. Sada slijedi postupak **dekodiranja**, tj. treba provjeriti je li dobiveni izlazni podatak kod nekog člana od I, te ako jeste treba odrediti član klase I čiji je kod upravo izlazni podatak.

Istaknimo sada što ćemo zahtijevati od kodiranja. Neka je I neka klasa, tj. skup koji nije podskup od $\mathbb{N}$. Funkciju $F : I \to \mathbb{N}$ ćemo nazivati **kodiranje** ako vrijedi sljedeće:

- funkcija F je injekcija;
- postoji algoritam koji određuje $F(i)$, za svaki $i \in I$;
- postoji algoritam koji za svaki $n \in \mathbb{N}$ određuje postoji li $i \in I$ tako da vrijedi $F(i) = n$. Ako takav i postoji tada ga algoritam efektivno određuje.

Mi se nećemo baviti proučavanjem funkcija kodiranja. Za naša daljnja proučavanja posebno će biti značajno kodiranje skupa svih konačnih nizova prirodnih brojeva. U tu svrhu označimo s p_k $k-$ti prosti broj, tj. neka je

$$p_0,\ p_1,\ p_2,\ \ldots$$

strogo rastući niz svih prostih brojeva. (To znači da je $p_0 = 2,\ p_1 = 3,\ p_2 = 5, \ldots$). Neka je $k \in \mathbb{N}$ proizvoljan, te $x_0,\ x_1,\ \ldots,\ x_{k-1}$ proizvoljan niz prirodnih brojeva duljine k. Tada ćemo danom nizu pridružiti broj

$$p_0^{x_0+1} \cdot p_1^{x_1+1}\ \ldots\ p_{k-1}^{x_{k-1}+1}$$

koji ćemo nazivati kod konačnog niza $x_0,\ x_1,\ \ldots,\ x_{k-1}$. Po definiciji praznom nizu pridružujemo broj 1.

Iz osnovnog teorema aritmetike slijedi da različiti nizovi imaju različite kodove. No, primijetite da to ne vrijedi ako u eksponentima ispustimo pribrojnik 1. (Tada bi npr. za nizove $2,1,0,3$ i $2,1,0,3,0,0,0$ vrijedilo $p_0^2 \cdot p_1^1 \cdot p_2^0 \cdot p_3^3 = p_0^2 \cdot p_1^1 \cdot p_2^0 \cdot p_3^3 \cdot p_4^0 \cdot p_5^0 \cdot p_6^0$).

Sada nam je cilj dokazati da je upravo definirano preslikavanje konačnih nizova prirodnih brojeva rekurzivno. U tu svrhu redom definiramo funkcije i relacije, te dokazujemo da su rekurzivne.

Sa Div označimo binarnu relaciju na $\mathbb{N}$ koja je definirana sa:

$$Div(x, y) \text{ ako i samo ako } \text{"}\textit{broj } x \textit{ je djeljiv brojem } y\text{"}.$$

Očito vrijedi:

$$Div(x, y) \text{ ako i samo ako } y \neq 0 \ \wedge \ \exists z(x = y \cdot z).$$

No, iz toga ne možemo zaključiti da je relacija Div rekurzivna, jer se radi o neograničenoj kvantifikaciji $\exists z$. To možemo popraviti na sljedeći način:

$$Div(x, y) \text{ ako i samo ako } y \neq 0 \ \wedge \ (\exists z \leq x)(x = y \cdot z),$$

iz čega slijedi primitivna rekurzivnost relacije Div.

Označimo s Pr unarnu relaciju "*broj x je prosti broj*". Primjenom relacije Div dobivamo da vrijedi:

$$Pr(x) \text{ ako i samo ako } x > 1 \ \wedge \ (\forall y < x)(y > 1 \to \neg Div(x, y))$$

Primjenom primitivne rekurzivnosti relacije Div i prije dokazanih propozicija slijedi da je relacija Pr primitivno rekurzivna. (Primitivna rekurzivnost relacije Pr dokazana je na drugi način i u točki 1.3 u zadatku 2).

Primijetimo da tada vrijedi

$$\begin{array}{rcl} p_0 & = & 2 \\ p_{i+1} & = & (\mu x \leq p_i! + 1)(Pr(x) \ \wedge \ x > p_i) \end{array}$$

No, to je upravo definicija funkcije $n \mapsto p_n$ pomoću primitivne rekurzije. To znači da je funkcija $n \mapsto p_n$, tj. funkcija koja prirodnom broju n pridružuje n–ti po redu prosti broj, primitivno rekurzivna.

Za sve $k \in \mathbb{N}$, pri čemu je $k > 0$, definiramo k–mjesnu totalnu funkciju $\langle . \rangle$ na $\mathbb{N}^k$ na sljedeći način:

$$\langle x_0, \ldots, x_{k-1} \rangle = p_0^{x_0+1} \ \ldots \ p_{k-1}^{x_{k-1}+1}$$

Zatim, definiramo da je $\langle \rangle = 1$ (tj. kod praznog niza je jednak 1).

Broj $\langle x_0, \ldots, x_{k-1} \rangle$ nazivamo **kod** niza $x_0, \ldots, x_{k-1}$. Primjenom prethodnih rezultata slijedi da je funkcija kodiranja primitivno rekurzivna. (Uočite da koristimo istu oznaku za funkcije kodiranja različitih mjesnosti).

Sada nam je cilj dokazati da je "dekodiranje" efektivan postupak, tj. da postoji algoritam koji za svaki $n \in \mathbb{N}$ određuje postoje li prirodni brojevi $k, x_0, \ldots, x_{k-1}$ tako da vrijedi $n = \langle x_0, \ldots, x_{k-1} \rangle$. U tu svrhu redom promatramo sljedeće relacije i funkcije, te dokazujemo da su rekurzivne.

Neka je sa $exp(x,i)$ označen eksponent prostog broja p_i u rastavu broja x na proste faktore. Pošto želimo da funkcija exp bude totalna po dogovoru stavljamo $exp(0,i) = 0$, za sve $i \in \mathbb{N}$. Očito vrijedi:

$$exp(x,i) = \begin{cases} \mu y < x \ (Div(x, p_i^y) \land \neg Div(x, p_i^{y+1})), & \text{ako je } \ x \neq 0; \\ 0, & \text{ako je } \ x = 0, \end{cases}$$

iz čega slijedi da je funkcija exp primitivno rekurzivna.

Definiramo jednomjesnu totalnu funkciju lh (eng. length) i dvomjesnu totalnu funkciju $(x,i) \mapsto (x)_i$ na sljedeći način:

$$\begin{array}{l} lh(x) = (\mu i < x)(exp(x,i) = 0) \\ (x)_i = exp(x,i) \dot{-} 1 \end{array}$$

Ako je $x = \langle x_0, x_1, \ldots, x_{k-1} \rangle$ tada očito vrijedi:

$$\begin{array}{l} lh(x) = k, \\ (x)_i = \begin{cases} x_i, & \text{za sve } \ i < k; \\ 0, & \text{za sve } \ i \geq k. \end{cases} \end{array}$$

Očito su funkcije lh i $(.)$ primitivno rekurzivne.

(Uočimo npr. da 3 nije kod niti jednog konačnog niza, no $lh(3)$ je definirano i vrijedi $lh(3) = 0$. Ni broj 50 nije kod niti jednog konačnog niza. No, iz $50 = 2 \cdot 5^2$ slijedi da je $lh(50) = 1$, te $(50)_2 = 1$ i $(50)_i = 0$, za sve $i \neq 2$.)

Označimo sa Seq jednomjesnu relaciju definiranu sa:

$Seq(x)$ ako i samo ako "*x je kod nekog konačnog niza prirodnih brojeva.*

Pošto očito vrijedi:

$$Seq(x) \ \text{ako i samo ako} \ \ x = 1 \ \lor \ \Big(x \neq 0 \ \land \ (\forall i < x)(Div(x, p_i) \to i < lh(x)) \Big),$$

tada je relacija Seq primitivno rekurzivna.

Važna binarna operacija na konačnim nizovima je konkatenacija. To je dvomjesna funkcija na $\mathbb{N}$ koju označavamo s $*$ i ima sljedeće svojstvo: ako je $x = \langle x_0, \ldots, x_{k-1} \rangle$ i $y = \langle y_0, \ldots, y_{l-1} \rangle$ tada je $x * y$ kod niza $x_0, \ldots, x_{k-1}, y_0, \ldots, y_{l-1}$.

Nije teško vidjeti da vrijedi

$$\begin{aligned} x * y &= \mu z(Seq(z) \ \wedge \ lh(z) = lh(x) + lh(y) \ \wedge \\ &\quad (\forall i < lh(x))((z)_i = (x)_i) \ \wedge \\ &\quad (\forall i < lh(y))((z)_{lh(x)+i} = (y)_i)) \\ &= \prod_{i<lh(x)} p_i^{(x)_i+1} \cdot \prod_{i<lh(y)} p_{lh(x)+i}^{(y)_i+1} \end{aligned}$$

Iz posljednje jednakosti slijedi da je funkcija konkatenacije primitivno rekurzivna.

Sada ćemo navesti neke primjene kodiranja konačnih nizova. Kao prvu primjenu kodiranja pokazat ćemo kako k–mjesne funkcije i relacije možemo svesti na jednomjesne.

Ako je F neka k–mjesna funkcija, definiramo jednomjesnu funkciju, koju označavamo s $\langle F \rangle$, na sljedeći način:

$$\langle F \rangle(x) \simeq F((x)_0. \dots, (x)_{k-1}).$$

Funkciju $\langle F \rangle$ nazivamo **kontrakcija** funkcije F. Iz funkcije $\langle F \rangle$ možemo ponovno dobiti funkciju F pomoću očiglednog identiteta

$$F(x_1, \dots, x_k) \simeq \langle F \rangle(\langle x_1, \dots, x_k \rangle).$$

Iz prethodna dva identiteta slijedi:

> funkcija F je parcijalno rekurzivna ako i samo ako je funkcija $\langle F \rangle$ parcijalno rekurzivna.

Kao drugu primjenu kodiranja promatramo definiciju funkcije pomoću **simultane primitivne rekurzije**.

Propozicija 1.48. *Neka su G_1, G_2, H_1 i H_2 rekurzivne funkcije. Definiramo funkcije F_1 i F_2 na sljedeći način:*

$$\begin{aligned} F_1(0, \vec{x}) &= G_1(\vec{x}) \\ F_2(0, \vec{x}) &= G_2(\vec{x}) \\ F_1(y+1, \vec{x}) &= H_1(y, \vec{x}, F_1(y, \vec{x}), F_2(y, \vec{x})) \\ F_2(y+1, \vec{x}) &= H_2(y, \vec{x}, F_1(y, \vec{x}), F_2(y, \vec{x})) \end{aligned}$$

Tada su funkcije F_1 i F_2 rekurzivne.

Dokaz. U svrhu dokaza definiramo funkciju F pomoću primitivne rekurzije na sljedeći način:

$$\begin{array}{rcl} F(0,\vec{x}) & = & \langle G_1(\vec{x}), G_2(\vec{x})\rangle \\ F(y+1,\vec{x}) & = & \langle\ H_1(y,\vec{x},(F(y,\vec{x}))_0,(F(y,\vec{x}))_1), \\ & & H_2(y,\vec{x},(F(y,\vec{x}))_0,(F(y,\vec{x}))_1)\ \rangle. \end{array}$$

Očito je funkcija F rekurzivna, te vrijedi:

$$F_1(y,\vec{x}) = (F(y,\vec{x}))_0 \ \text{ i } \ F_2(y,\vec{x}) = (F(y,\vec{x}))_1.$$

Iz posljednjih jednakosti slijedi da su funkcije F_1 i F_2 rekurzivne. □

Lako je poopćiti definiranje funkcija pomoću simultane rekurzije na više od dvije funkcije.

Kao treću primjenu kodiranja navodimo općenitiju formu definiranja funkcija pomoću primitivne rekurzije. Kod (obične) primitivne rekurzije vrijednost funkcije f na $y+1$ ovisi samo o vrijednosti funkcije na y. Sada ćemo definirati funkciju za koju će vrijednost na $y+1$ ovisiti o svim prethodnim vrijednostima, tj. o $f(0), \ldots f(y)$.

Neka je F neka $(k+1)$–mjesna funkcija. Želimo definirati $(k+1)$–mjesnu funkciju $\overline{F}$ koja bi imala sljedeće svojstvo:

$$\overline{F}(y,\vec{x}) \simeq \langle F(0,\vec{x}), \ldots, F(y \dot{-} 1,\vec{x})\rangle.$$

Uočite da to ne može biti definicija funkcije $\overline{F}$ iz koje će slijediti rekurzivnost te funkcije. Naravno, problem je što definicija ovisi od varijabli y, tj. funkcija $\overline{F}$ ne može biti prikazana kao kompozicija dvije funkcije.

Kako bi izbjegli taj problem, funkciju $\overline{F}$ definiramo pomoću primitivne rekurzije ovako:

$$\begin{array}{rcl} \overline{F}(0,\vec{x}) & = & 1 \\ \overline{F}(y+1,\vec{x}) & = & \overline{F}(y,\vec{x}) * \langle F(y,\vec{x})\rangle. \end{array}$$

Tada očito vrijedi: $F(y,\vec{x}) \simeq (\overline{F}(y+1,\vec{x}))_y$. Iz toga slijedi:

> funkcija F je parcijalno (primitivno) rekurzivna ako i samo ako je funkcija $\overline{F}$ parcijalno (primitivno) rekurzivna.

Sada konačno možemo definirati općenitiju primitivnu rekurziju (tzv. course-of-values recursion).

Propozicija 1.49. *Neka je G parcijalno (primitivno) rekurzivna funkcija. Zatim, neka je funkcija F definirana na sljedeći način:*

$$F(y,\vec{x}) \simeq G(\overline{F}(y,\vec{x}), y, \vec{x}).$$

Tada je funkcija F parcijalno (primitivno) rekurzivna.

Dokaz. Uočite da iz definicije funkcije $\overline{F}$ slijedi da je općenito $\overline{F}(0,\vec{x}) = \langle\rangle$, tj. $\overline{F}(0,\vec{x}) = 1$. Sada imamo da za funkciju F iz pretpostavke ove propozicije vrijedi $F(0,\vec{x}) \simeq G(0,y,\vec{x})$.

Po prethodnim razmatranjima za parcijalnu (primitivnu) rekurzivnost funkcije F dovoljno je dokazati da je funkcija $\overline{F}$ parcijalno (primitivno) rekurzivna. No, funkciju $\overline{F}$ možemo definirati pomoću primitivne rekurzije na sljedeći način:

$$\begin{aligned} \overline{F}(0,\vec{x}) &\simeq 1 \\ \overline{F}(y+1,\vec{x}) &\simeq \overline{F}(y,\vec{x}) * \langle G(\overline{F}(y,\vec{x}),y,\vec{x})\rangle. \end{aligned}$$

□

Zadaci:

1. Niz $1, 1, 2, 3, 5, 8, 13, 21, \ldots$ naziva se Fibonaccijev niz. Dokažite da je funkcija f koja prirodnom broju n pridružuje n-ti član Fibonaccijevog niza prmitivno rekurzivna.
   Rješenje: Po uvjetima zadatka vrijedi
   $$f(0) = 0, \qquad f(1) = 1$$
   $$f(n+2) = f(n) + f(n+1)$$
   Neka je funkcija F definirana pomoću primitivne rekurzije s
   $$\begin{aligned} F(0) &= \langle 0\rangle \\ F(n+1) &= \begin{cases} \langle 0,1\rangle, & \text{ako je } n = 0; \\ F(n) * ((F(n))_{n \dot{-} 1} + (F(n))_n), & \text{ako je } n > 0. \end{cases} \end{aligned}$$
   Očito je funkcija F primitivno rekurzivna. Indukcijom je lako dokazati da vrijedi $F(n) = \langle f(0),\ldots,f(n)\rangle$. Iz toga slijedi da je $f(n) = (F(n))_n$, tj. funkcija f je primitivno rekurzivna.

2. Funkcija f je zadana sa sljedeće dvije jednakosti:
   $$f(0) = 5$$
   $$f(n+1) = (n+1)^{f(n)} + n \cdot f(n \dot{-} 3)$$
   Dokažite da je funkcija f RAM-izračunljiva.
   Rješenje: Pošto je svaka rekurzivna funkcija i RAM-izračunljiva, dovoljno je dokazati da je dana funkcija rekurzivna. U svrhu dokaza rekurzivnosti funkcije f definiramo prvo dvomjesnu funkciju h s:

$$h(x,y) = (x+1)^{(y)_x} \ + \ x \cdot (y)_{x \dot{-} 3}$$

Funkcija h je očito primitivno rekurzivna. Sada pomoću primitivne rekurzije definiramo funkciju F :

$$\begin{array}{rcl} F(0) & = & \langle 5 \rangle \\ F(n+1) & = & h(n, F(n)). \end{array}$$

Funkcija F je primitivno rekurzivna, te vrijedi: $F(n) = \langle f(0), \ldots, f(n) \rangle$ i $f(n) = (F(n))_n$. Iz toga odmah slijedi da je i funkcija f primitivno rekurzivna.

3. Funkcija f je zadana sa sljedeće dvije jednakosti:

$$f(0) = 13$$

$$f(n+1) = (n+1)^{f(n \dot{-} 1)} + 4 \cdot f(n \dot{-} 2)$$

Dokažite da je funkcija f Turing izračunljiva. (pojam Turingovog stroja je definiran u točki 1.2 na strani 22).

4. Funkcije f i g su definirana s:

$$\begin{array}{rcl} f(0,y) & = & 1 \\ f(x+1,y) & = & (y+g(x)) \cdot f(x,y) \\ g(x) & = & f(x,x) \end{array}$$

Dokažite da su funkcije f i g primitivno rekurzivne.
Rješenje: Očito je dovoljno dokazati primitivnu rekurzivnost funkcije f jer tada odmah slijedi i primitivna rekurzivnost funkcije g. Očito vrijedi $f(x+1,y) = (y + f(x,x)) \cdot f(x,y)$. U svrhu dokaza definiramo funkciju F s:

$$F(x,y) = \begin{cases} \langle \ f(0,0), \ldots, f(0,y), \\ \quad f(1,0), \ldots, f(1,y), \\ \qquad \vdots \\ \quad f(x,0), \ldots, f(x,y) \ \rangle, & \text{ako je } \ x \le y; \\ \langle \ f(0,0), \ldots, f(0,x), \\ \quad f(1,0), \ldots, f(1,x), \\ \qquad \vdots \\ \quad f(x,0), \ldots, f(x,x) \ \rangle, & \text{ako je } \ x > y. \end{cases}$$

Dokažimo da je funkcija F primitivno rekurzivna. Lako je provjeriti da je funkciju F moguće definirati pomoću primitivne rekurzije na sljedeći način:

$$F(0,y) = \langle 1,\ldots,1\rangle \qquad ((y+1)\text{-puta jedinica})$$

$$F(x+1,y) = \begin{cases} (y + (F(x,y)))_{y+(x\dot{-}1)(y+1)+x+1} \cdot (F(x,y))_{(x+1)(y+1)}, \\ \hfill \text{ako je } x \le y; \\ (y + (F(x,y)))_{(x+1)(y+1)} \cdot (F(x,y))_{x+(x\dot{-}1)(x+1)+y+1}, \\ \hfill \text{ako je } x > y. \end{cases}$$

Iz toga slijedi da je funkcija F primitivno rekurzivna. Pošto vrijedi:

$$f(x,y) = \begin{cases} (F(x,y))_{(x+1)(y+1)}, & \text{ako je } \ x \le y; \\ (F(x,y))_{x+(x\dot{-}1)(x+1)+y+1}, & \text{ako je } \ x > y. \end{cases}$$

tada slijedi da je funkcija f primitivno rekurzivna.

5. Neka su g i h primitivno rekurzivne funkcije. Dokažite da je tada i sljedeća funkcija f primitivno rekurzivna:

$$f(0,\vec{x}) = f(1,\vec{x}) = g(\vec{x})$$

$$f(y+2,\vec{x}) = h(f(y,\vec{x}), f(y+1,\vec{x}), y, \vec{x})$$

Rješenje: Prvo definiramo funkciju F ovako:

$$F(0,\vec{x}) = \langle g(\vec{x})\rangle$$
$$F(y+1,\vec{x}) = \begin{cases} \langle g(\vec{x})\rangle, & \text{ako } y = 0; \\ F(y,\vec{x}) * h((F(y,\vec{x}))_{y\dot{-}1}, (F(y,\vec{x}))_y, y\dot{-}1, \vec{x}), & \text{inače.} \end{cases}$$

Funkcija F je primitivno rekurzivna, te vrijedi $(F(y,\vec{x}))_y = f(y,\vec{x})$.

6. Neka je funkcija $\beta : \mathbb{N}^3 \to \mathbb{N}$ definirana s $\beta(x, y, z) = res(x, 1 + y(z + 1))$ (funkcija res je definirana u točki 1.3 u zadatku 1). Funkcija β se naziva Gödelova β–funkcija. Dokažite da za svaki konačan niz prirodnih brojeva $a_0, a_1, \dots, a_n$ sistem jednadžbi

$$\begin{gathered} \beta(x, y, 0) = a_0 \\ \beta(x, y, 1) = a_1 \\ \vdots \\ \beta(x, y, n) = a_n \end{gathered}$$

ima jedinstveno rješenje po x i y.
(Uočite da iz toga slijedi da možemo definirati kodiranje konačnih nizova s $(a_0, a_1, \dots, a_n) \mapsto (x, y)$).
Rješenje. Neka je $j = \max\{n, a_0, \dots, a_n\}$ i $c = j!$. Za svaki $k \in \{0, \dots, n\}$ definiramo broj $u_k = 1 + c(k + 1)$. Lako je dokazati da su za svaki $k \neq l$ brojevi u_k i u_l relativno prosti. Primjenom kineskog teorema o ostacima, tj. teorema o egzistenciji rješenja sistema kongruencija, slijedi da postoji jedinstveni prirodan broj $b < u_0 \cdot u_1 \dots u_n$ tako da vrijedi:

$$\begin{gathered} b \equiv a_1 \pmod{u_1} \\ b \equiv a_2 \pmod{u_2} \\ \vdots \\ b \equiv a_n \pmod{u_n} \end{gathered}$$

Iz toga slijedi da za sve $k \in \{0, \dots, n\}$ vrijedi $res(b, u_k) = a_k$, tj.

$$\beta(b, c, k) = res(b, 1 + c(k + 1)) = res(b, u_k) = a_k.$$

7. Neka je funkcija $C^2 : \mathbb{N}^2 \to \mathbb{N}$ definirana s

$$C^2(x, y) = \frac{(x + y)^2 + 3x + y}{2}$$

Ova funkcija se naziva Cantorova funkcija. Dokažite da je C bijekcija i primitivno rekurzivna. Uočite da Cantorova funkcija definira kodiranje parova prirodnih brojeva. Za svaki $n \in \mathbb{N}$, $n \geq 2$ definiramo

$$C^{n+1}(x_1, \dots, x_{n+1}) = C^2(C^n(x_1, \dots, x_n), x_{n+1}).$$

Dokažite da je za svaki $n \leq 3$ funkcija C^n bijekcija i primitivno rekurzivna.

Zatim, dokažite da postoje primitivno rekurzivne funkcije $l, r : \mathbb{N} \to \mathbb{N}$ tako da vrijedi:

$$l(C^2(x,y)) = x, \quad r(C^2(x,y)) = y \ \text{ i } \ C^2(l(x), r(x)) = x.$$

Uputa. Neka je funkcija $f : \mathbb{N} \to \mathbb{N}$ definirana s

$$f(x) = \mu z\left(\overline{sg}\lfloor\frac{(z+1)(z+2)}{2}\rfloor \dot{-} x) = 0\right).$$

Tada definiramo

$$l(x) = x \dot{-} \lfloor\frac{f(x)(f(x)+1)}{2}\rfloor \quad \text{i} \quad r(x) = f(x) \dot{-} l(x).$$

1.5 Indeksi

Dokazali smo da je svaka parcijalno rekurzivna funkcija RAM–izračunljiva. Sada ćemo dokazati obrat. U tu svrhu ćemo kodirati RAM–stroj, tj. cjelokupni rad RAM–stroja.

Prisjetimo se dijelova RAM–stroja. To su: traka s registrima, spremnik za program i brojač. Kako bi RAM–stroj mogao raditi u spremnik za program mora biti stavljen neki program P (koji ima zadanu mjesnost ulaznih podataka k), te u registre $\mathcal{R}_1, \ldots, \mathcal{R}_k$ moraju biti zapisani ulazni podaci.

Želimo ovoj početnoj konfiguraciji pridružiti neki kod. Prije svega moramo definirati kod svakog programa za RAM–stroj. Program je konačan niz instrukcija. To znači da moramo definirati kod svake instrukcije za RAM–stroj, a onda ćemo kod programa definirati kao kod konačnog niza (kodova instrukcija koje nastupaju u tom programu). Krenimo redom. Prvo svakoj instrukciji RAM-programa pridružujemo kod na sljedeći način:

$$\begin{array}{rcl} INC\ \mathcal{R}_i & \mapsto & \langle 0, i\rangle \\ DEC\ \mathcal{R}_i, n & \mapsto & \langle 1, i, n\rangle \\ GO\ TO\ n & \mapsto & \langle 2, n\rangle \\ STOP & \mapsto & \langle 3\rangle \end{array}$$

Ako je P program za RAM-stroj koji sadrži N instrukcija čiji su pripadni kodovi redom $y_1, \ldots, y_N$ tada po definiciji programu P pridružujemo kod

$$\langle y_1, \ldots, y_N\rangle$$

Obično ćemo kod programa P kratko označavati s e.

Sada želimo dokazati da je dekodiranje efektivan postupak. U tu svrhu prvo označimo s Ins jednomjesnu unarnu relaciju na $\mathbb{N}$ koja je definirana s:

$Ins(x)$ ako i samo ako "*x je kod neke instrukcije za RAM-stroj*".

Lako je vidjeti da vrijedi:

$$\begin{array}{ll} Ins(x) & \text{ako i samo ako} \\ & x = \langle 0, (x)_1\rangle \ \vee\ x = \langle 1, (x)_1, (x)_2\rangle \ \vee\ x = \langle 2, (x)_1\rangle \ \vee\ x = \langle 3\rangle \end{array}$$

Iz toga slijedi da je relacija Ins primitivno rekurzivna.

Označimo s $Prog$ jednomjesnu unarnu relaciju na $\mathbb{N}$ koja je definirana s:

$Prog(x)$ ako i samo ako "*x je kod nekog programa za RAM-stroj*".

Lako je vidjeti da vrijedi:

$$\begin{array}{lll} Prog(x) & \text{ako i samo ako} & Seq(x) \ \wedge \ (\forall i < lh(x))[Ins((x)_i) \wedge \\ & & (((x)_i)_0 = 1 \to ((x)_i)_2 < lh(x)) \wedge \\ & & (((x)_i)_0 = 2 \to ((x)_i)_1 < lh(x))]. \end{array}$$

Iz posljednje ekvivalencije slijedi da je relacija $Prog$ primitivno rekurzivna. Objasnimo ukratko navedenu ekvivalenciju. Uvjet $Seq(x)$ znači da je x kod nekog konačnog niza prirodnih brojeva. Zatim, za sve i, koji su strogo manji od duljine niza čiji je kod x, vrijedi redom sljedeće:

a) broj $(x)_i$ je kod neke instrukcije za RAM-program;

b) ako je $((x)_i)_0 = 1$, tj. $(x)_i$ je kod neke instrukcije oblika DEC $\mathcal{R}_i, n$, tada n mora biti strogo manji od duljine niza $x_0, \ldots, x_{k-1}$ (tj. u programu mora postojati instrukcija s rednim brojem n);

c) analogno kao b), ali za instrukciju oblika GO TO n.

Ako je P program za RAM–stroj i $\vec{x}$ k-torka ulaznih podataka tada rad RAM-stroja kada je P u spremniku programa, a $\vec{x}$ su ulazni podaci nazivamo **P-izračunavanje s $\vec{x}$**.

Sada želimo definirati kod P–izračunavanja s $\vec{x}$. To ćemo napraviti tako da nakon svakog koraka rada RAM–stroja izračunamo kod relevantnih registara za to izračunavanje. Iz definicije rada RAM–stroja jasno je da za svako P–izračunavanje sa $\vec{x}$ dovoljno samo konačno mnogo registara. Odredimo neku među za relevantne registre prilikom nekog P–izračunavanja s $\vec{x}$.

Neka je s e označen kod programa P. Tada za indeks i proizvoljnog registra koji se pojavljuje u P vrijedi $i < e$. To znači da su za P–izračunavanje s $\vec{x}$ (moguće) značajni samo registri s indeksima i, pri čemu je $i < e + k$.

Označimo s q_i prirodan broj zapisan u registru $\mathcal{R}_i$ (u nekom trenutku rada stroja). Definiramo **kod registara** stroja prilikom P–izračunavanja s $\vec{x}$ (u nekom trenutku rada stroja!) kao broj $\langle q_0, \ldots, q_{e+k \dot{-} 1}\rangle$. (Uočite da uzimamo u obzir samo registre za koje smo prije primijetili da su relevantni za P–izračunavanje s $\vec{x}$.) [4]

Ako P–izračunavanje s $\vec{x}$ stane nakon m koraka tada s r_i označimo kod registara stroja nakon i–tog koraka, za $i = 0, \ldots, m$. Tada broj $r = \langle r_0, \ldots, r_m\rangle$

[4] Ne možemo govoriti o kodu registara nakon izvršenja i–te instrukcije, već nakon i–tog koraka. Moramo govoriti o koracima, jer se neka instrukcija može izvršavati više puta prilikom izvršavanja programa.

nazivamo **kod P-izračunavanja s $\vec{x}$.** Ako P–izračunavanje s $\vec{x}$ stane izlazni rezultat označimo s **U(r),** tj. $U(r)$ je broj zapisan u registru $\mathcal{R}_0$ nakon m–tog koraka. Uočite da vrijedi:

$$U(r) = \big((r)_{lh(r)\dot{-}1}\big)_0$$

To znači da U možemo promatrati kao funkciju definiranu na skupu $\mathbb{N}$. Štoviše, iz prethodnog identiteta slijedi da je U primitivno rekurzivna funkcija.

Da bismo do kraja kodirali rad RAM-stroja moramo još definirati funkcije koje opisuju rad brojača i upisa u registre.

Neka je s $Count(e, x, n)$ označen broj koji je zapisan u brojaču nakon izvršenja n–tog koraka P-izračunavanja sa $\vec{x}$, gdje je e kod programa P, a $x = \langle x_0, \dots, x_k\rangle$.

Neka je s $Reg(j, e, x, n)$ označen broj koji je zapisan u j–tom registru nakon izvršenja n–tog koraka P–izračunavanja sa $\vec{x}$, gdje je e kod programa P, a $x = \langle x_1, \dots, x_k\rangle$. Da bismo dokazali da su funkcije $Count$ i Reg primitivno rekurzivne definiramo ove dvije funkcije pomoću simultane primitivne rekurzije. Radi kratkoće i jasnoće zapisa u sljedećoj definiciji funkcija $Count$ i Reg umjesto izraza $(e)_{Count(e,x,n)}$ pisat ćemo samo i.

$$\begin{aligned}
Count(e, x, 0) &= 0\\
Reg(j, e, x, 0) &= \begin{cases} (x)_{j\dot{-}1}, & \text{ako } 0 < j < lh(x);\\ 0, & \text{inače.}\end{cases}
\end{aligned}$$

$$Count(e, x, n+1) = \begin{cases} (i)_2, & \text{ako } (i)_0 = 1 \text{ i } Reg((i)_1, e, x, n) = 0;\\ (i)_1, & \text{ako } (i)_0 = 2;\\ Count(e, x, n) + 1, & \text{inače.}\end{cases}$$

$$Reg(j, e, x, n+1) = \begin{cases} Reg(j, e, x, n) + 1, & \text{ako } (i)_0 = 0 \text{ i } j = (i)_1;\\ Reg(j, e, x, n)\dot{-}1, & \text{ako } (i)_0 = 1 \text{ i } j = (i)_1;\\ Reg(j, e, x, n), & \text{inače.}\end{cases}$$

Primitivna rekurzivnost funkcija $Count$ i Reg slijedi iz propozicije 1.48.

Dajemo kratko objašnjenje navedenih jednakosti. Prvo govorimo o funkciji $Count$. Neka je y_i kod i–te instrukcije, te $e = \langle y_1, \dots, y_m\rangle$. U zapisu smo koristili pokratu $i = (e)_{Count(e,n,x)}$. Uočite da je to kod instrukcije čiji redni broj se nalazi u brojaču prije n–tog koraka. Ako je $(i)_0 = 1$ (radi se o instrukciji oblika $DEC\ \mathcal{R}_j, k$) i u $(i)_1$-tom registru prije izvršenja n–tog koraka je nula (tj. $Reg((i)_1, e, x, n) = 0$) tada je u brojaču broj $(i)_2$ nakon izvršenja n–tog koraka. Ako je $(i)_0 = 2$ (radi se o instrukciji oblika $GO\ TO\ k$) tada je u brojaču nakon izvršenja n–tog koraka broj $(i)_1$. U svim ostalim slučajevima se brojač povećava za jedan.

Sada još nekoliko riječi o funkciji Reg. Ako je $(i)_0 = 0$ (radi se o instrukciji oblika $INC\ \mathcal{R}_j$), te je $(i)_1$ upravo j, tada se broj u registru $\mathcal{R}_j$ poveća za jedan. Ako je $(i)_0 = 1$ tada se radi o instrukciji oblika $DEC\ \mathcal{R}_j, m$ pa se s registrom $\mathcal{R}_j$ postupa u skladu s definicijom te instrukcije. U svim ostalim slučajevima broj u registru se ne mijenja.

Označimo sa $Step$ tromjesnu relaciju koja je definirana sa: $Step(e,x,n)$ ako i samo ako e je kod nekog programa P i $x = \langle \vec{x} \rangle$, te P–izračunavanje s $\vec{x}$ završava u n–koraka. Lako je vidjeti da vrijedi:

$$\begin{array}{ll} Step(e,x,n) & \text{ako i samo ako} \\ & (Count(e,x,n) \geq lh(e)\ \lor\ (e)_{Count(e,x,n)} = \langle 3 \rangle) \land \\ & (\forall i < n)(Count(e,x,i) < lh(e)\ \land\ (e)_{Count(e,x,i)} \neq \langle 3 \rangle) \end{array}$$

Iz prethodne ekvivalencije slijedi da je relacija $Step$ primitivno rekurzivna.

Navodimo kratko objašnjenje navedene ekvivalencije. Uvjet $Count(e,x,n) \geq lh(e)$ znači da je broj u brojaču nakon izvršenja n–tog koraka veći od rednog broja svake instrukcije u programu (tj. RAM–stroj će stati nakon izvršenja n–tog koraka). Uvjet $(e)_{Count(e,x,n)} = \langle 3 \rangle$ znači da je nakon izvršenja n–tog koraka u brojaču redni broj instrukcije koja je oblika $STOP$. Za sve ostale korake je broj u brojaču strogo manji od broja svih instrukcija u programu, odnosno instrukcija koja se izvršava nije oblika $STOP$.

Za svaki $k \in \mathbb{N}$ s T_k označavamo $(k+2)$–mjesnu relaciju koja je definirana s:

> $T_k(e,\vec{x},y)$ ako i samo ako e je kod programa P, $\vec{x}$ je uređena k–torka prirodnih brojeva, a y je kod P–izračunavanja s $\vec{x}$.

Iz definicije relacije T_k slijedi da vrijedi:

$T_k(e,\vec{x},y)$ ako i samo ako

$$Prog(e)\ \land\ Seq(y)\ \land\ Step(e,\langle \vec{x} \rangle, lh(y) \dot{-} 1)\ \land$$

$$(\forall i < lh(y))((y)_i = \overline{Reg}(e+k,e,\langle \vec{x} \rangle, i)).$$

Iz prethodno navedene ekvivalencije slijedi da je za svaki $k \in \mathbb{N}$ relacija T_k primitivno rekurzivna.

Objasnimo kratko prethodnu ekvivalenciju. Broj e mora biti kod nekog programa P za RAM-stroj. Broj y mora biti kod nekog konačnog niza. P–izračunavanje s $\vec{x}$ mora stati nakon $lh(y) \dot{-} 1$ koraka. Svaka koordinata od y, tj. $(y)_i$ mora biti kod registara nakon svakog koraka P–izračunavanja s $\vec{x}$. Sjetimo se još da je $\overline{Reg}(e+k,e,\langle \vec{x} \rangle, i))$ jednako

$$\langle Reg(0, e, \langle \vec{x} \rangle, i),\ Reg(1, e, \langle \vec{x} \rangle, i),\ \ldots,\ Reg(e + k \dot{-} 1, e, \langle \vec{x} \rangle, i) \rangle.$$

Uočite da se promatraju samo registri $\mathcal{R}_0, \ldots, \mathcal{R}_{e+k\dot{-}1}$, jer su samo oni relevantni prilikom P-izračunavanja s $\vec{x}$.

Definicija 1.50. *Neka su $e, k \in \mathbb{N}$ i $\vec{x} \in \mathbb{N}^k$. Ako je e kod nekog programa P za RAM–stroj mjesnosti k, te ako P–izračunavanje s $\vec{x}$ stane, tada s $\{e\}^k(\vec{x})$ označavamo izlazni rezultat. U svim ostalim slučajevima smatramo da izraz $\{e\}^k(\vec{x})$ nije definiran.*

Ako P–izračunavanje s $\vec{x}$ stane tada vrijedi $U(r) = \{e\}^k(\vec{x})$ i $r = \mu y T_k(e, \vec{x}, y)$. Ako pak P–izračunavanje s $\vec{x}$ ne stane tada ne postoji $y \in \mathbb{N}$ tako da bi vrijedilo $T_k(e, \vec{x}, y)$, a to znači da izraz $U(\mu y T_k(e, \vec{x}, y))$ nije definiran. Iz ovih razmatranja slijedi da za sve $e, k \in \mathbb{N}$ i $\vec{x} \in \mathbb{N}^k$ vrijedi

$$\{e\}^k(\vec{x}) \simeq U(\mu y T_k(e, \vec{x}, y)) \qquad (*).$$

Time smo dokazali sljedeći važan teorem:

Teorem 1.51. *(***Kleenijev teorem o normalnoj formi za parcijalno rekurzivne funkcije***)*
Postoji primitivno rekurzivna funkcija U, i za svaki $k \geq 1$ postoji primitivno rekurzivna relacija T_k tako da za svaku k–mjesnu parcijalno rekurzivnu funkciju φ postoji $e \in \mathbb{N}$ tako da vrijede sljedeće tvrdnje:

a) $\varphi(\vec{x}) \downarrow$ *ako i samo ako postoji y tako da vrijedi $T_k(e, \vec{x}, y)$;*

b) $\varphi(\vec{x}) \simeq U(\mu y T_k(e, \vec{x}, y))$.

Kleenijev teorem smo dokazali prethodnim razmatranjima. No, ipak ukratko ćemo ponoviti skicu tog dokaza. Neka je φ neka k–mjesna parcijalno rekurzivna funkcija. Iz teorema 1.33. slijedi da je ta funkcija RAM–izračunljiva. Neka je P neki program za RAM-stroj koji izračunava funkciju φ, tj. za sve $\vec{x} \in \mathbb{N}^k$ vrijedi:

> $\varphi(\vec{x}) \downarrow$ ako i samo ako P–izračunavanje s $\vec{x}$ stane, te je tada u registru $\mathcal{R}_0$ zapisan broj $\varphi(\vec{x})$.

Označimo s e kod programa P. Ako stroj stane, označimo s y_0 kod P–izračunavanja s $\vec{x}$. Po definiciji relacije T_k tada imamo da vrijedi $T_k(e, \vec{x}, y_0)$. To znači da postoji $y \in \mathbb{N}$ tako da vrijedi $T_k(e, \vec{x}, y)$, odnosno funkcija U je definirana za $\mu y T_k(e, \vec{x}, y)$. No, sjetimo se da je $U(r)$ upravo broj zapisan u registru $\mathcal{R}_0$ na kraju izvršenja programa (ako stroj stane!). Dakle, ako stroj stane tada vrijedi $\varphi(\vec{x}) = U(\mu y T_k(e, \vec{x}, y))$. Lako je vidjeti da vrijedi $\varphi(\vec{x}) \uparrow$ ako i samo ako ne postoji y takav da vrijedi $T_k(e, \vec{x}, y)$.

Definicija 1.52. *Neka je $\varphi : S \subseteq \mathbb{N}^k \to \mathbb{N}$ neka funkcija. Kažemo da za funkciju φ postoji* **indeks** *ako postoji $e \in \mathbb{N}$ takav da za sve $\vec{x} \in \mathbb{N}^k$ vrijedi $\varphi(\vec{x}) \simeq \{e\}^k(\vec{x})$.*

Teoremi koji slijede su posljedice Kleenijevog teorema.

Teorem 1.53. *Funkcija $f : S \subseteq \mathbb{N}^k \to \mathbb{N}$ je parcijalno rekurzivna ako i samo ako postoji indeks za f.*

Dokaz. Ako je funkcija f RAM–izračunljiva tada egzistencija indeksa slijedi iz prethodnih razmatranja.

Pretpostavimo da postoji indeks e za funkciju f. Tada iz Kleenijevog teorema, tj. iz $(*)$ sa stane 63, slijedi:

$$f(\vec{x}) \simeq \{e\}^k(\vec{x}) \simeq U(\mu y T_k(e, \vec{x}, y)).$$

Desna strana posljednje jednakosti je parcijalno rekurzivna funkcija, a onda je i lijeva strana. To znači da je funkcija f parcijalno rekurzivna. $\square$

Napomena 1.54. *Za sve prirodne broj e i k ima smisla napisati $\{e\}^k$, jer iz Kleenijevog teorema imamo da je $\{e\}^k(\vec{x}) \simeq U(\mu y T_k(e, \vec{x}, y)$. Dakle, za sve $e, k \in \mathbb{N}$ je definirana funkcija $\{e\}^k$. Ako e nije kod nekog programa za RAM–stroj tada za sve $k \in \mathbb{N}$ i $\vec{x} \in \mathbb{N}^k$ vrijedi $\{e\}^k(\vec{x}) \uparrow$. Posebno to znači da ako e nije kod nekog programa za RAM–stroj tada ne možemo govoriti o fiksnoj mjesnosti funkcije. Npr. broj 5 nije kod niti jednog RAM-programa, pa izrazi $\{5\}^2(1,2)$, $\{5\}^4(1,2,34,5)$ i $\{5\}^6(6,78,9,567,0,1)$ nisu definirani.*

Teorem 1.55. *Funkcija je RAM-izračunljiva ako i samo ako je parcijalno rekurzivna.*

Dokaz. Ako je funkcija parcijalno rekurzivna tada iz teorema 1.33. slijedi da je i RAM-izračunljiva.

Ako je funkcija f RAM-izračunljiva tada iz definicije slijedi da postoji program P za RAM–stroj koji je izračunava. Označimo s e kod programa P. Iz dokaza Kleenijevog teorema slijedi da je e jedan indeks funkcije f. Iz prethodnog teorema slijedi da je funkcija f parcijalno rekurzivna. $\square$

Dokazali smo da je funkcija definirana po slučajevima pomoću rekurzivnih funkcija i rekurzivnih disjunktnih relacija, također rekurzivna. Sada ćemo primjenom indeksa to dokazati za parcijalno rekurzivne funkcije.

Teorem 1.56. *Neka su $R_1, \ldots, R_n$ rekurzivne relacije koje imaju svojstvo da za svaki $\vec{x} \in \mathbb{N}^k$ postoji najviše jedan $i \in \{1, \ldots, n\}$ za kojeg vrijedi $R_i(\vec{x})$. Neka* *su $F_1, \ldots, F_n$ k–mjesne parcijalno rekurzivne funkcije. Funkciju F definiramo po slučajevima ovako:*

$$F(\vec{x}) \simeq \begin{cases} F_1(\vec{x}), & \textit{ako vrijedi } R_1(\vec{x}); \\ \quad\vdots & \\ F_n(\vec{x}), & \textit{ako vrijedi } R_n(\vec{x}). \end{cases}$$

Tada je funkcija F parcijalno rekurzivna.

Dokaz. Iz teorema 1.53. znamo da za svaku funkciju F_i postoji indeks. Označimo sa e_i indeks funkcije F_i, za $i = 1, \ldots, n$. Lako je vidjeti da je $\{3\}$ primjer jedne parcijalno rekurzivne funkcije čija je domena prazan skup. Definiramo funkciju G ovako:

$$G(\vec{x}) = \begin{cases} e_1, & \text{ako vrijedi } R_1(\vec{x}); \\ \ \vdots & \\ e_n, & \text{ako vrijedi } R_n(\vec{x}); \\ 3, & \text{inače.} \end{cases}$$

Iz propozicije 1.37. slijedi da je funkcija G rekurzivna. Očito vrijedi

$$F(\vec{x}) \simeq \{G(\vec{x})\}(\vec{x}).$$

Iz Kleenijevog teorema, tj. iz $(*)$ sa strane 63, imamo

$$\{G(\vec{x})\}(\vec{x}) \simeq U(\mu y\ T_k(G(\vec{x}), \vec{x}, y).$$

Pošto je desna strana posljednje jednakosti parcijalno rekurzivna funkcija tada je i lijeva, tj. funkcija $\{G(\vec{x})\}$ je parcijalno rekurzivna. Iz toga slijedi da je parcijalno rekurzivna i funkcija F. □

Teorem 1.57. *Za svaku parcijalno rekurzivnu funkciju φ postoji definicija u kojoj se μ-operator pojavljuje najviše jednom.*

Dokaz. Iz Kleenijevog teorema slijedi da postoji $e \in \mathbb{N}$ tako da za sve $\vec{x} \in \mathbb{N}^k$ vrijedi $\varphi(\vec{x}) \simeq U(\mu y T_k(e, \vec{x}, y))$. No, funkcija U i relacija T_k su primitivno rekurzivne. □

Zadaci:

1. Odredite $\{128\}(127)$ i $\{63\}(64)$.
   Rješenje. Odredimo program čiji je kod 128. Pošto je $128 = 2^7 = 2^{6+1}$ tada se traženi program za RAM–stroj sastoji samo od jedne instrukcije. Kod te jedne instrukcije je 6. Pošto je $6 = 2^{1+0} \cdot 3^{1+0}$, tj. $6 =< 0, 0 >$ tada je 6 kod instrukcije INC $\mathcal{R}_0$. Dakle, 128 je kod programa:

   $$1.\ \text{INC} \quad \mathcal{R}_0.$$

   Očito taj program izračunava funkciju f definiranu s $f(x) = 1$. Dakle, 128 je indeks funkcije f. Iz toga zaključujemo da je $\{128\}(127) = 1$.

   Broj 63 nije kod niti jednog programa jer je neparan. To znači da funkcija $\{63\}$ nije definirana niti za jedna prirodan broj. Posebno, izraz $\{63\}(64)$ nije definiran.

2. Dokažite da postoji parcijalno rekurzivna funkcija f koja se ne može proširiti do rekurzivne funkcije.
   Rješenje. Neka je funkcija f definirana sa

   $$f(x) \simeq \{x\}(x) + 1.$$

   Funkcija f je parcijalno rekurzivna. Pretpostavimo da postoji rekurzivna funkcija g koja je proširenje funkcije f. Neka je e indeks funkcije g. Iz $g(x) \simeq \{e\}(x)$ slijedi da je $\{e\}(e)$ definirano pa je f definirana u točki e te imamo

   $$\{e\}(e) + 1 = f(e) = g(e) = \{e\}(e),$$

   što je kontradikcija.

3. Dokažite da za svaku rekurzivnu funkciju postoji definicija pomoću funkcija koje su sve totalne.

4. Neka je $f : S \subseteq \mathbb{N}^k \to \mathbb{N}$. Dokažite da je funkciju f moguće zapisati u obliku $f(\vec{x}) = \mu y[g(\vec{x}, y) = 0]$, gdje je g primitivno rekurzivna funkcija, ako i samo ako je graf funkcije f primitivno rekurzivan skup.
   Rješenje. Pretpostavimo da postoji primitivno rekurzivna funkcija g takva da je $f(\overrightarrow{x}) = \mu y[g(\overrightarrow{x}, y) = 0]$. Imamo da je $(x_1, ..., x_k, y) \in \Gamma(f)$ ako i samo ako je $g(x_1, ..., x_k, 0) \neq 0$, ..., $g(x_1, ..., x_k, y-1) \neq 0$, $g(x_1, ..., x_k, y) = 0$. Stoga je

$$\chi_{\Gamma(f)}(x_1,...,x_k,y) = \left(sg\left(\prod_{i=0}^{y\dot{-}1} g(x_1,...,x_k,i)\right) sg(y) + \overline{sg}(y)\right) \cdot \overline{sg}(g(x_1,...,x_k,y))$$

iz čega slijedi da je $\Gamma(f)$ primitivno rekurzivan skup.

Obratno, ako je $\Gamma(f)$ primitivno rekurzivan skup, tada je funkcija $g(\overrightarrow{x}, y) = 1 \dot{-} \chi_{\Gamma(f)}(\overrightarrow{x}, y)$ primitivno rekurzivna te vrijedi

$$f(\overrightarrow{x}) = \mu y[(\overrightarrow{x}, y) \in \Gamma(f)] = \mu y[1 \dot{-} \chi_{\Gamma(f)}(\overrightarrow{x}, y) = 0] = \mu y[g(\overline{x}, y) = 0].$$

1.6 Teorem o parametru

U ovoj točki prvo ćemo dokazati važan teorem o parametru, a zatim kao njegovu neposrednu posljedicu dobiti teorem rekurzije, teorem o fiksnoj točki i Riceov teorem.

Ako je funkcija $f : S \subseteq \mathbb{N}^2 \to \mathbb{N}$ parcijalno rekurzivna tada znamo da je za sve $x \in \mathbb{N}$ funkcija $y \mapsto f(x, y)$ također parcijalno rekurzivna. Teorem o parametru govori da prijevod varijable u parametar možemo raditi na rekurzivan način.

Teorem 1.58. *(***Teorem o parametru** *ili* S^m_n**-teorem***)*
Neka su m i n prirodni brojevi različiti od nule. Tada postoji rekurzivna funkcija $S^m_n : \mathbb{N}^{m+1} \to \mathbb{N}$ tako da za sve $e \in \mathbb{N}$, $\vec{x} \in \mathbb{N}^n$ i $\vec{y} \in \mathbb{N}^m$ vrijedi

$$\{S^m_n(e, \vec{y})\}(\vec{x}) \simeq \{e\}(\vec{y}, \vec{x}).$$

Dokaz. Radi kraćeg zapisa promatramo slučaj kada je $m = 1$. Neka je s P_{-1} označen neki fiksirani program za RAM–stroj koji ne staje niti za jedan ulazni podatak. Za svaki $e \in \mathbb{N}$ s P_e označavamo program za RAM–stroj, koji je definiran na sljedeći način: ako je e kod nekog programa s $(n + 1)$–ulaznih podataka, tada je P_e upravo program čiji je kod e. Za sve ostale $e \in \mathbb{N}$ neka je P_e program P_{-1}. Za $e \in \mathbb{N}$ s P^*_e označimo makro za program P_e. Za sve $e \in \mathbb{N}$ i $y \in \mathbb{N}$ s P^e_y označavamo sljedeći program za makro–stroj:

$$\begin{array}{rl} 1. & INC\ \mathcal{R}_{n+1} \\ & \vdots \\ y. & INC\ \mathcal{R}_{n+1} \\ (y+1). & P^*_e \end{array}$$

Očito dani program izračunava funkciju $\{e\}^{n+1}$ za sve $e \in \mathbb{N}$. Za sve $e \in \mathbb{N}$ i $y \in \mathbb{N}$ neka je sa $S^1_n(e, y)$ označen kod programa za RAM–stroj koji je ekvivalentan prethodno definiranom programu P^e_y za makro–stroj. Tada očito vrijedi

$$\{S^1_n(e, y)\}(\vec{x}) \simeq \{e\}^{n+1}(y, \vec{x}),$$

što je i tvrdnja teorema. Preostalo je dokazati da je funkcija S^1_n primitivno rekurzivna. U tu svrhu definiramo funkciju $F : \mathbb{N}^2 \to \mathbb{N}$ na sljedeći način:

$$F(i, y) = \begin{cases} \langle 1, (i)_1, (i)_2 + y\rangle, & \text{ako je } (i)_0 = 1; \\ \langle 2, (i)_1 + y\rangle, & \text{ako je } (i)_0 = 2; \\ i, & \text{inače.} \end{cases}$$

Uočimo: ako je i kod neke instrukcije I oblika DEC $\mathcal{R}_j, q$ ili GO TO q, tada je $F(i,y)$ kod instrukcije dobivene iz I povećanjem q za y, tj. dobivene instrukcije su DEC $\mathcal{R}_j, (q+y)$, odnosno GO TO $(q+y)$. Neka je s G označena funkcija koja je definirana sa:

$$G(y) \simeq \mu z(Seq(z) \ \wedge \ lh(z) = y \ \wedge \ (\forall i < y)((z)_i = \langle 0, n+1 \rangle)).$$

Uočimo da je za svaki $y \in \mathbb{N}$ funkcijska vrijednost $G(y)$ kod sljedećeg programa za RAM–stroj:

$$\begin{array}{ll} 1. & INC\ \mathcal{R}_{k+1} \\ & \vdots \\ y. & INC\ \mathcal{R}_{k+1} \end{array}$$

Iz definicije funkcije G je jasno da je to rekurzivna funkcija.

Neka je $H : \mathbb{N}^2 \to \mathbb{N}$ funkcija definirana s:

$$H(e,y) \simeq \mu z(Seq(z) \ \wedge \ lh(z) = lh(e) \ \wedge \ (\forall i < lh(z))((z)_i = F((e)_i, y))).$$

Uočimo da je za sve $e \in \mathbb{N}$ i $y \in \mathbb{N}$ funkcijska vrijednost $H(e,y)$ kod programa za RAM–stroj koji je dobiven iz programa P_e zamjenom svake instrukcije oblika DEC $\mathcal{R}_j, q$ s instrukcijom DEC $\mathcal{R}_j, (q+y)$, odnosno svake instrukcije oblika GO TO q s instrukcijom GO TO $(q+y)$. Iz definicije funkcije H je jasno da je to rekurzivna funkcija.

Očito je funkcija S^1_n "konkatenacija" funkcija G i H tj. vrijedi $S^1_n(e,y) = G(y) * H(e,y)$. Iz ove posljednje jednakosti slijedi tražena rekurzivnost funkcije S^1_n. □

Navodimo jedan jednostavan primjer kako bi bila jasnija važnost teorema o parametru.

Primjer 1.59. *Tvrdimo da postoji rekurzivna funkcija $pl : \mathbb{N}^2 \to \mathbb{N}$ takva da za sve $m, n \in \mathbb{N}$ vrijedi da je $pl(m,n)$ indeks funkcije $\{m\} + \{n\}$.*

U svrhu dokaza te tvrdnje promotrimo funkciju $(m,n,x) \mapsto \{m\}(x) + \{n\}(x)$. Ona je očito parcijalno rekurzivna funkcija, pa neka je s e označen njen indeks. Iz teorema o parametru slijedi da postoji rekurzivna funkcija S^2_1 tako da vrijedi $\{e\}(m,n,x) \simeq \{S^2_1(e,m,n)\}(x)$. Iz ovog posljednjeg slijedi da traženu funkciju $pl : \mathbb{N}^2 \to \mathbb{N}$ možemo definirati s $pl(m,n) = S^2_1(e,m,n)$. Uočite da tada za sve $x \in \mathbb{N}$ vrijedi:

$$\begin{aligned} (\{m\} + \{n\})(x) &\simeq (\{m\}(x) + \{n\}(x)) \simeq \{e\}(m,n,x) \simeq \{S^2_1(e,m,n)\}(x) \\ &\simeq \{pl(m,n)\}(x) \end{aligned}$$

Ako je $G : S \subseteq \mathbb{N}^{k+1} \to \mathbb{N}$ neka parcijalno rekurzivna funkcija, tada je svaka od sljedećih funkcija također parcijalno rekurzivna:

$$\begin{array}{c} \vec{x} \mapsto G(0, \vec{x}) \\ \vec{x} \mapsto G(1, \vec{x}) \\ \vec{x} \mapsto G(2, \vec{x}) \\ \vdots \end{array}$$

Postavlja se pitanje postoji li $e \in \mathbb{N}$ tako da je e indeks funkcije $\vec{x} \mapsto G(e, \vec{x})$. Pozitivan odgovor na to pitanje daje sljedeći teorem.

Teorem 1.60. (Teorem rekurzije)
Neka je G neka $(k+1)$–mjesna parcijalno rekurzivna funkcija. Tada postoji $e \in \mathbb{N}$ tako da za sve $\vec{x} \in \mathbb{N}^k$ vrijedi

$$\{e\}^k(\vec{x}) \simeq G(e, \vec{x}).$$

Dokaz. Iz Kleenijevog teorema o normalnoj formi slijedi da za sve $y \in \mathbb{N}$ i sve $\vec{x} \in \mathbb{N}^k$ vrijedi

$$\{y\}(y, \vec{x}) \simeq U(\mu z\ T_{k+1}(y, y, \vec{x}, z))$$

Iz toga slijedi da je funkcija $(y, \vec{x}) \mapsto \{y\}(y, \vec{x})$ parcijalno rekurzivna. Iz teorema o parametru slijedi da postoji rekurzivna funkcija S^1_k tako da vrijedi

$$\{S^1_k(y, y)\}(\vec{x}) \simeq \{y\}(y, \vec{x}) \qquad (*)$$

S H označimo parcijalno rekurzivnu funkciju definiranu s

$$H(y, \vec{x}) \simeq G(S^1_k(y, y), \vec{x}) \qquad (**)$$

Označimo s h indeks funkcije H. Neka je $e = S^1_k(h, h)$. Sada nizom jednakosti dobivamo traženu jednakost iz izreke teorema:

$$\begin{aligned} \{e\}^k(\vec{x}) \simeq \quad & \{S^1_k(h, h)\}(\vec{x}) \simeq \text{ (iz } (*)) \simeq \{h\}(h, \vec{x}) \simeq \\ & H(h, \vec{x}) \simeq \text{ (iz } (**)) \simeq G(S^1_k(h, h), \vec{x}) \simeq G(e, \vec{x}) \end{aligned}$$

□

Teorem rekurzije se često koristi prilikom dokaza da je neka funkcija parcijalno rekurzivna. Navodimo jedan primjer.

Primjer 1.61. *Neka je funkcija F definirana s:*

$$\begin{aligned} &F(0,x) \simeq G(x) \\ &F(y+1,x) \simeq H(F(y,2x),y,x) \end{aligned}$$

gdje su G i H neka zadane parcijalno rekurzivne funkcije. Uočimo da rekurzivnost funkcije F ne možemo dokazati na način kako smo to radili u primjerima prije teorema rekurzije. U svrhu dokaza definiramo funkciju L ovako:

$$L(y,x,z) \simeq \begin{cases} G(x), & \text{ako je } \ y=0; \\ H(\{z\}(y \dot{-} 1, 2x), y \dot{-} 1, x), & \text{inače.} \end{cases}$$

Iz teorema 1.56. slijedi da je funkcija L parcijalno rekurzivna. Iz teorema rekurzije slijedi da postoji $e \in \mathbb{N}$ tako da za sve $y, x \in \mathbb{N}$ vrijedi $\{e\}^2(y,x) \simeq L(y,x,e)$. Lako je provjeriti da vrijedi $F \simeq \{e\}^2$.

Iz ovog posljednjeg slijedi tražena tvrdnja da je funkcija F parcijalno rekurzivna.

Sljedeći teorem o fiksnoj točki je direktna posljedica teorema rekurzije.

Teorem 1.62. (Teorem o fiksnoj točki)
Za svaku unarnu parcijalnu rekurzivnu funkciju F postoji $e \in \mathbb{N}$ tako da vrijedi

$$\{e\} \simeq \{F(e)\}$$

Dokaz. Definiramo funkciju G s $G(x,y) \simeq \{F(x)\}(y)$. Očito je G parcijalno rekurzivna funkcija. Iz teorema rekurzije slijedi da postoji $e \in \mathbb{N}$ tako da za sve $y \in \mathbb{N}$ vrijedi $G(e,y) \simeq \{e\}^1(y)$. Tada slijedi da za sve $y \in \mathbb{N}$ vrijedi $\{e\}^1(y) \simeq \{F(e)\}(y)$. □

Riceov teorem, koji sada navodimo, je također posljedica teorema rekurzije. Taj teorem nam govori da neodlučivost nije iznimka, već pravilo. Riceov teorem može biti jako koristan kada želimo dokazati da pojedini skup nije rekurzivan.

Teorem 1.63. (Riceov teorem)
Neka je S rekurzivan podskup od $\mathbb{N}$ koji ima svojstvo da za sve $i, j \in \mathbb{N}$, takve da je $i \in S$ i $\{i\} \simeq \{j\}$ slijedi $j \in S$. Tada je $S = \emptyset$ ili $S = \mathbb{N}$.

Dokaz. Pretpostavimo da je S neprazan rekurzivan pravi podskup od $\mathbb{N}$ koji ima svojstvo da $i \in S$ i $\{i\} \simeq \{j\}$ povlači $j \in S$. Neka su $n \in S$ i $m \in \mathbb{N} \backslash S$ proizvoljni. Definiramo funkciju G ovako:

$$G(i,x) \simeq \begin{cases} \{m\}(x), & \text{ako } i \in S; \\ \{n\}(x), & \text{ako } i \notin S. \end{cases}$$

Funkcija G je parcijalno rekurzivna jer je definirana pomoću parcijalno rekurzivnih funkcija i rekurzivnih uvjeta (vidi teorem 1.56.). Iz teorema rekurzije slijedi da postoji $i \in \mathbb{N}$ tako da vrijedi

$$\{i\}(x) \simeq G(i,x).$$

Ako bi vrijedilo $i \in S$ tada bi imali $\{i\} \simeq \{m\}$. No, tada iz danog svojstva skupa S slijedi $m \in S$, što je u suprotnosti s početnom pretpostavkom. To znači da mora vrijediti $i \notin S$. No, tada je $\{i\} \simeq \{n\}$. No, po pretpostavci je $n \in S$, pa opet zbog danog svojstva skupa S slijedi $i \in S$. To je u suprotnosti s pretpostavkom da $i \notin S$.

Zaključujemo da pretpostavka o egzistenciji nepraznog rekurzivnog pravog podskupa od $\mathbb{N}$, koji ima traženo svojstvo, vodi na kontradikciju. □

Mnoge su primjene Riceovog teorema. Kao malu ilustraciju navodimo nekoliko primjera.

Neka je f proizvoljna k–mjesna parcijalno rekurzivna funkcija. Tada je očito skup $\{e \in \mathbb{N} : \{e\}^k \simeq f\}$ neprazan pravi podskup od $\mathbb{N}$. Iz Riceovog teorema slijedi da taj skup nije rekurzivan. To znači da niti za jednu parcijalno rekurzivnu funkciju skup svih njenih indeksa nije rekurzivan.

Neka je $A = \{e \in \mathbb{N} : \{e\}^1(23) = 33\}$. Lako je vidjeti da skup A nije prazan, a ni jednak $\mathbb{N}$. Ako je $e \in A$, te je $k \in \mathbb{N}$ takav da vrijedi $\{e\}^1 \simeq \{k\}^1$, tada je očito $\{k\}^1(23) = 33$. Iz Riceovog teorema slijedi da skup A nije rekurzivan.

Zatim, neka je $B = \{e \in \mathbb{N} : \{e\}^1 \text{ je totalna funkcija}\}$. Iz Riceovog teorema slijedi da skup B nije rekurzivan.

Zadaci:

1. Dokažite da postoji rekurzivna funkcija f takva da vrijedi:

   a) $f : \mathbb{N}^2 \to \mathbb{N}$, te je $f(m,n)$ indeks funkcije $(m,n,x) \mapsto \{m\}(x) \cdot \{n\}(x)$.

   b) $f : \mathbb{N}^2 \to \mathbb{N}$, te je $f(m,n)$ indeks funkcije $(m,n,x) \mapsto \{m\}^{\{n\}}(x)$.

   c) $f : \mathbb{N}^3 \to \mathbb{N}$, te je $f(m,n,k)$ indeks funkcije:
   $(m,n,k,x,y) \mapsto \{m^2\}(x,y) + 3\{n+k\}(y,y,x)$.

   Uputa. Vidi primjer 1.59.

2. Dokažite da postoji parcijalno rekurzivna funkcija f takva da za sve $e \in \mathbb{N}$ vrijedi da je $Rng(\{f(e)\} = Dom(\{e\})$.
   Rješenje. Definiramo funkciju g ovako:

$$g(e,x) \simeq \begin{cases} x, & \text{ako } \{e\}(x)\downarrow \\ \{3\}(x), & \text{inače} \end{cases}$$

   Primjenom teorema o definiciji funkcije po slučajevima pomoću parcijalno rekurzivnih funkcija i rekurzivnih relacija, slijedi da je funkcija g parcijalno rekurzivna. Za svaki $e \in \mathbb{N}$ sa g_e označimo funkciju koja je definirana sa: $g_e(x) \simeq g(e,x)$. Za svaki $e \in \mathbb{N}$ vrijedi:

$$\begin{aligned} Dom(\{e\}) &= \{x \in \mathbb{N} : \{e\}(x)\downarrow\} = \{g(e,x) : x \in \mathbb{N}, \{e\}(x)\downarrow\} \\ &= \{g_e(x) : x \in \mathbb{N},\ \{e\}(x)\downarrow\} = Rng(g_e) \qquad\qquad (*) \end{aligned}$$

   Iz teorema o parametru slijedi da postoji rekurzivna funkcija S_1^1 tako da vrijedi $\{S_1^1(e)\}(x) \simeq g(e,x)$, za svaki $e, x \in \mathbb{N}$. Definiramo traženu funkciju f sa: $f \simeq S_1^1$. Tada za svaki $e \in \mathbb{N}$ imamo: $Rng(\{f(e)\}) = Rng(\{S_1^1(e)\}) = Rng(g_e) = (*) = Dom(\{e\})$.

3. Neka su G, H i K rekurzivne funkcije. Neka je funkcija F definirana sa:

$$\begin{aligned} F(0,y) &= \quad G(y); \\ F(x+1,y) &= \quad H(F(x, K(F(x,y),x,y)),x,y). \end{aligned}$$

   Dokažite da je funkcija F rekurzivna.
   Rješenje. Neka je funkcija L definirana sa:

$$L(x,y,z) \simeq \begin{cases} G(y), & \text{ako je } x = 0; \\ \\ H(\{z\}(x \dot{-} 1, K(\{z\}(x \dot{-} 1, y), x \dot{-} 1, y))x \dot{-} 1, y), & \text{inače.} \end{cases}$$

   Očito je L parcijalno rekurzivna funkcija. Iz teorema rekurzije slijedi da postoji $e \in \mathbb{N}$ tako da za sve $x, y \in \mathbb{N}$ vrijedi $L(x,y,e) \simeq \{e\}(x,y)$. Provjerite da vrijedi $\{e\} \simeq F$.

4. Neka je funkcija F zadana sa:

$$\begin{aligned} F(0,x_1,x_2) &\simeq \quad x_1 + x_2 \\ F(y+1,x_1,x_2) &\simeq \quad \left\lfloor \log_2(F(y,x_1+1,x_2+2)) \cdot y \dot{-} x_1 \right\rfloor \end{aligned}$$

   Dokažite da je F parcijalno rekurzivna funkcija.

5. Neka je funkcija G zadana sa:

$$G(0,x) \simeq 2x^3 + x^2 \dot{-} x$$

$$G(y+1,x) \simeq 3G^3(y,3x) + 2G^2(y,2x) + G(y,x) + 17$$

Dokažite da je G parcijalno rekurzivna funkcija.

6. Neka je funkcija H zadana sa:

$$H(0,x_1,x_2,x_3) \simeq x_1 \cdot x_2 \cdot x_3$$

$$H(y+1,x_1,x_2,x_3) \simeq \lfloor \sqrt[3]{\frac{H(y,0,0,2x_3) + H(y,0,0,3x_3)}{H(y,x_1,1,1) + H(y,0,0,x_2)+1}} \rfloor$$

Dokažite da je H parcijalno rekurzivna funkcija.

7. Neka je funkcija M zadana sa:

$$M(0,x_1,x_2,\ldots,x_{10}) \simeq x_1^2 + \ldots + x_{10}^2$$

$$\begin{aligned} M(y+1,x_1,\ldots,x_{10}) \simeq\ & (x_1 + 2x_2 + 3x_3 + \ldots + 10x_{10}) \cdot \\ & \cdot M(y,x_1,2x_2,3x_3,\ldots,10x_{10}) \end{aligned}$$

Dokažite da je M parcijalno rekurzivna funkcija.

8. Dokažite da postoji $e \in \mathbb{N}$ tako da je domena funkcije $\{e\}^1$ jednaka upravo skupu $\{e\}$.
Dokaz. Definiramo prvo dvomjesnu relaciju R sa:

$$xRy \text{ ako i samo ako } x = y.$$

Očito je relacija R rekurzivna. Zatim definiramo dvomjesnu funkciju G ovako:

$$G(x,y) \simeq \mu z[\overline{sg}(\chi_R(x,y)) + z \simeq 0]$$

Očito je G parcijalno rekurzivna funkcija pa iz teorema rekurzije slijedi da postoji $e \in \mathbb{N}$ tako da vrijedi $\{e\}^1(y) \simeq G(e,y)$. Lako je vidjeti da je domena funkcije $\{e\}$ jednaka skupu $\{e\}$.

9. Dokažite da postoji $e \in \mathbb{N}$ takav da je domena funkcije $\{e\}$ jednaka $\{e, e+1\}$.
Rješenje. Prvo definiramo dvomjesnu relaciju R sa:

$$xRy \text{ ako i samo ako } x = y \ \vee x + 1 = y.$$

Očito je relacija R rekurzivna. Zatim definiramo dvomjesnu funkciju G ovako:

$$G(x,y) \simeq \mu z[\overline{sg}(\chi_R(x,y)) + z \simeq 0]$$

Očito je G parcijalno rekurzivna funkcija, pa iz teorema rekurzije slijedi da postoji $e \in \mathbb{N}$ tako da za svaki $y \in \mathbb{N}$ vrijedi $\{e\}(y) \simeq G(e,y)$. Pošto je $Dom(G) = \{(y,y),\ (y,y+1) : y \in \mathbb{N}\}$, tada je $Dom(\{e\}) = \{e, e+1\}$.

10. Dokažite da postoji $e \in \mathbb{N}$ tako da je domena funkcije $\{e\}^1$ jednaka upravo skupu $\mathbb{N} \setminus \{e\}$.
    Dokaz. Definiramo prvo dvomjesnu relaciju R sa:

    $$xRy \text{ ako i samo ako } \neg(x = y).$$

    Očito je relacija R rekurzivna. Zatim definiramo dvomjesnu funkciju G ovako:

    $$G(x,y) \simeq \mu z[\overline{sg}(\chi_R(x,y)) + z \simeq 0]$$

    Očito je G parcijalno rekurzivna funkcija pa iz teorema rekurzije slijedi da postoji $e \in \mathbb{N}$ tako da vrijedi $\{e\}^1(y) \simeq G(e,y)$. Lako je vidjeti da je domena funkcije $\{e\}$ jednaka skupu $\mathbb{N} \setminus \{e\}$.

11. Dokažite da postoji $e \in \mathbb{N}$ takav da je domena funkcije $\{e\}$ jednaka:

    a) $\{(e,0)\}$

    b) $\{(e,e)\}$

    c) $\{0,\dots,e\}$

    d) $\{e \cdot k \ :\ k \in \mathbb{N}\}$

    e) $\{1+e, 1+e^2, 1+e^3, \dots\}$

    f) $\{(n,e) \mid n \in \mathbb{N}\}$

    g) $\{(x,y) \in \mathbb{N}^2 \mid x^2 + y^2 \leq e\}$

    Upute. Za svaki od zadataka prvo definiramo relaciju R. Primjerice, za zadatak a) definiramo:

    $$(x_1,x_2,x_3) \in R \text{ ako i samo ako } x_1 = x_2 \ \wedge\ x_3 = 0$$

Za zadatak c) definiramo: $(x_1, x_2) \in R$ ako i samo ako $x_2 \le x_1$.
Za zadatak e) definiramo: $x_1 R x_2$ ako i samo ako $(\exists m > 0) x_2 = 1 + x_1^m$.
Svaka od navedenih relacija je očito rekurzivna. Zatim, definiramo parcijalno rekurzivnu funkciju G čija je mjesnost jednaka mjesnosti relacije R. Ako je R relacija mjesnosti k tada definiramo:

$$G(x_1, \ldots, x_k) \simeq \mu z[\overline{sg}(\chi_R(x_1, \ldots, x_k)) + z \simeq 0].$$

Očito je svaka takva funkcija G parcijalno rekurzivna. Primjenom teorema rekurzije slijedi egzistencija traženog $e \in \mathbb{N}$ za svaki pojedini zadatak.

12. Neka je S rekurzivan podskup od $\mathbb{N}$. Dokažite ili opovrgnite: postoji parcijalno rekurzivna funkcija f takva da je $Dom(f) = S$.

13. Dokažite da postoji $e \in \mathbb{N}$ takav da je slika funkcije $\{e\}^1$ jednaka $\{x \in \mathbb{N} : x \ge e\}$.
Uputa. Definiramo rekurzivnu relaciju R sa:

$$(x_1, x_2) \in R \text{ ako i samo ako } x_2 \ge x_1.$$

Zatim definiramo funkciju G sa:

$$G(x_1, x_2) \simeq \mu z\left(\overline{sg}(\chi_R(x_1, x_2)) \ + \ z \simeq 0\right) + x_2$$

Primjenom teorema rekurzije slijedi da postoji $e \in \mathbb{N}$ tako da vrijedi: $G(e, x_2) \simeq \{e\}(x_2)$, za svaki $x_2 \in \mathbb{N}$. Očito vrijedi $Dom(\{e\}) = Rng(\{e\}) = \{n \in \mathbb{N} : n \ge e\}$.

14. Dokažite da postoji $e \in \mathbb{N}$ takav da je slika funkcije $\{e\}^1$ jednaka $\{e, e+1, e+2, \ldots, e+127\}$.

15. Dokažite da postoji $e \in \mathbb{N}$ tako da je $\{e\}^7$ konstantna funkcija čija je vrijednost e.
Rješenje. Za rekurzivnu funkciju $G(x_0, x_1, \ldots, x_7) = x_0$ postoji $e \in \mathbb{N}$ tako da za sve $\vec{x} \in \mathbb{N}^7$ vrijedi $\{e\}(\vec{x}) \simeq G(e, \vec{x}) = e$ (primjena teorema rekurzije). Pošto je funkcija f totalna tada je i funkcija $\{e\}$ totalna.

16. Dokažite da postoji $e \in \mathbb{N}$ tako da je jednomjesna funkcija $\{e\}$ totalna te tako da je $\{e\}(x) \simeq e \cdot x$, $\forall x \in \mathbb{N}$.
Rješenje. Za rekurzivnu funkciju $G(x, y) = x \cdot y$ postoji $e \in \mathbb{N}$ tako da za svaki $y \in \mathbb{N}$ vrijedi $\{e\}(y) \simeq G(e, y) = e \cdot y$ (primjena teorema rekurzije). Pošto je f totalna funkcija, tada je i funkcija $\{e\}$ totalna.

17. Dokažite da postoji $e \in \mathbb{N}$ tako da je $\{e\}$ totalna funkcija, te za svaki $k \in \mathbb{N}$ vrijedi $\{e\}(k) \simeq e + k$.
Uputa. $G(x, y) \simeq \mu z(x + y \dot{-} z = 0)$. Uočimo da je $Dom(G) = \mathbb{N}^2$. Iz teorema rekurzije slijedi da postoji $e \in \mathbb{N}$ tako da za svaki $y \in \mathbb{N}$ vrijedi: $\{e\}(y) \simeq G(e, y) \simeq e + y$.

18. Postoji li prirodan broj k za koji vrijedi:

    a) $Dom(\{k\}^1) = Rng(\{k\}^1) = \{k\}$?
    b) $Dom(\{k\}^1) = \{k\}$ i $Rng(\{k\}^1) = \mathbb{N} \setminus \{k\}$?

19. Postoji li $k \in \mathbb{N}$ takav da je $Dom(\{k\}^1) = \{1\} \cup \{kn + 2012 \mid n \in \mathbb{N}\}$ i $\{k\}^1(1) = 2012$?

20. Neka je S rekurzivan podskup od $\mathbb{N}$. Dokažite ili opovrgnite: postoji parcijalno rekurzivna funkcija f takva da je $Dom(f) = Rng(f) = S$.

21. Neka je $A = \{e : \{e\}^1$ je totalna funkcija $\}$. Dokažite da ne postoji rekurzivna funkcija f tako da vrijedi $A = Rng(f)$.
Rješenje. Pretpostavimo da takva funkcija f postoji. Neka je funkcija g definirana s $g(x) = \{f(x)\}^1(x) + 1$. Očito je funkcija g rekurzivna. Neka je e indeks od g. Tada je $e \in A$ pa postoji $k \in \mathbb{N}$ tako da je $f(k) = e$. Tada imamo $g(k) = \{f(k)\}^1(k)+1 = \{e\}^1(k)+1 = g(k)+1$, što je kontradikcija.

22. Neka je $f : \mathbb{N} \to \mathbb{N}$ zadana sa $f(x) = 2x^3 + 3x^2 + 5x + 7$. Dokažite da postoji $x_0 \in \mathbb{N}$ tako da vrijedi $\{6f(x_0) \dot{-} 7\} \simeq \{x_0\}$.

23. Neka je $S = \{3k + 2 : k \in \mathbb{N}\}$, te $f : S \to \mathbb{N}$ funkcija definirana sa $f(x) = \lfloor \log_3(4x + x^2) \rfloor$. Dokažite da postoji $e \in \mathbb{N}$ tako da vrijedi:
$$\{3^{f(2e+3)} + 2^{f(e+7)}\} \simeq \{e\}.$$

24. Neka je funkcija F zadana sa:
$$\begin{aligned} F(0, x, y) &\simeq x + y + 1 \\ F(z + 1, x, y) &\simeq \mu t\Big(F(z, x + 10, y \dot{-} 2)) \cdot z \simeq 2^x + 3^y + 5^t \cdot t\Big) \end{aligned}$$
Zatim, definiramo jednosmjesnu funkciju f sa $f(x) \simeq F(2x, 3x + 1, 7x + 2x)$. Dokažite da postoji $e \in \mathbb{N}$ tako da vrijedi $\{3f^2(e+3)+2^5(e+5)\} \simeq \{e\}$.

25. Dokažite da sljedeći skupovi nisu rekurzivni:

    a) $\{e : \text{funkcija } \{e\}^2 \text{ ima beskonačnu domenu}\}$
    b) $\{e : \text{funkcija } \{e\}^3 \text{ ima praznu domenu}\}$
    c) $\{e : \text{funkcija } \{e\}^7 \text{ ima beskonačnu sliku}\}$
    d) $\{e : \text{funkcija } \{e\}^1 \text{ ima praznu sliku}\}$
    e) $\{e : \text{funkcija } \{e\}^1 \text{ je totalna }\}$
    f) $\{e : \text{funkcija } \{e\}^4 \text{ je konstantna funkcija}\}$

    Rješenje a). Označimo dani skup sa S. Očito je indeks dvomjesne nul–funkcije element skupa S, pa je $S \neq \emptyset$. Primjerice, broj 3 nije kod niti jednog RAM–programa, pa $3 \notin S$, tj. $S \neq \mathbb{N}$. Neka je $i \in S$, te $j \in \mathbb{N}$ tako da vrijedi $\{i\} \simeq \{j\}$. Tada očito funkcija $\{j\}$ ima beskonačnu domenu, pa vrijedi $j \in S$. Iz Riceovog teorema slijedi da skup S nije rekurzivan.

26. Dokažite da sljedeći skupovi nisu rekurzivni:

    a) $\{(i, j, k) : (i, i + k) \text{ je u domeni funkcije } \{j\}\}$
    b) $\{(i, j) \mid (j, j + 1) \text{ je u domeni od } \{i\}\}$
    c) $\{(i, j) : \text{funkcije } \{i + j\} \text{ i } \{j\} \text{ imaju istu domenu }\}$

    Rješenje a). Označimo dani skup sa S. Definiramo skup $T = \{j : (0, j, 0) \in S\}$, tj. $T = \{j : (0, 0) \text{ je u domeni funkcije } \{j\}\}$. Očito je indeks dvomjesne nul-funkcije element skupa T, pa $T \neq \emptyset$. Zatim, pošto primjerice $3 \notin T$, tada je $T \neq \mathbb{N}$. Neka je $i \in T$, te $j \in \mathbb{N}$ takvi da je $\{i\} \simeq \{j\}$. Tada $(0, 0)$ nije u domeni funkcije $\{i\}$, pa iz $\{i\} \simeq \{j\}$ slijedi da $(0, 0)$ nije u domeni funkcije $\{j\}$, tj. vrijedi $j \in T$. Iz Riceovog teorema slijedi da skup T nije rekurzivan. Pošto očito vrijedi $\chi_S(0, j, 0) = \chi_T(j)$, tada ni skup S ne može biti rekurzivan.

27. Neka je $S = \{\langle a, b, c\rangle : \{a\}(b) \simeq \{b\}(c)\ \}$. Dokažite da skup S nije rekurzivan.
    Rješenje. Definiramo skup $T = \{a \in \mathbb{N} : \langle a, 0, 0\rangle \in S\}$, tj. $T = \{a \in \mathbb{N} : \{a\}(0) \simeq \{0\}(0)\} = \{a \in \mathbb{N} : \{a\}(0) \text{ nije definirano }\}$. Uočimo da je $T \neq \emptyset$, jer primjerice očito vrijedi $0 \in T$. Zatim, uočimo da je $T \neq \mathbb{N}$, jer primjerice indeks nul–funkcije nije element skupa T. Neka je $i \in T$, te $j \in \mathbb{N}$ tako da vrijedi $\{i\} \simeq \{j\}$. Tada $\{i\}(0)$ nije definirano. No, pošto je $\{i\} \simeq \{j\}$, tada ni $\{j\}(0)$ nije definirano. To znači da vrijedi $j \in T$. Time smo dokazali da su ispunjeni uvjeti Riceovog teorema, pa skupo T nije rekurzivan. Pošto očito vrijedi $\chi_T(x) = \chi_S(2^{x+1} \cdot 3^1 \cdot 5^1)$, tada ni skup S ne može biti rekurzivan.

28. Dokažite da sljedeći skupovi nisu rekurzivni:

   a) $\{\langle a, b\rangle : \text{funkcije } \{a\}^5 \text{ i } \{b\}^5 \text{ imaju istu domenu}\}$
   b) $\{\langle a, b\rangle : \text{funkcije } \{a\}^9 \text{ i } \{b\}^9 \text{ imaju istu sliku}\}$;
   c) $\{\langle a, b\rangle : b \in Rng(\{a\}^2)\}$;
   d) $\{\langle a, b\rangle : \text{funkcije } \{a \cdot b\} \text{ i } \{b\} \text{ imaju istu domenu}\}$
   e) $\{\langle a, b\rangle : \text{funkcije } \{a\} \text{ i } \{b\} \text{ imaju istu sliku}\}$
   f) $\{\langle a, b\rangle : \ \{b\}(a) \simeq 1\}$
   g) $\{\langle a, b\rangle \ : \ \{a\}(b) \simeq \{b\}(a)\}$
   h) $\{\langle a, b\rangle \ : \ \{a\}(b) \simeq b\}$
   i) $\{\langle a, b, c\rangle \ : \ \{a\}(b) \simeq \{b\}(c)\}$
   j) $\{\langle a, b, c\rangle \mid a + c \text{ je u domeni funkcije } \{b\} \ \}$

1.7 Churchova teza

Bili smo već naveli da smatramo da je svaka parcijalno rekurzivna funkcija izračunljiva (u intuitivnom smislu koji smo opisali na samom početku). Alonso Church (1903.–1995.) je 1936. godine postavio tezu da vrijedi i obrat. Zbog važnosti sada je posebno ističemo.

Churchova teza: svaka izračunljiva funkcija je parcijalno rekurzivna.

Pošto je pojam izračunljive funkcije intuitivan pojam, tj. nije strogo definiran, nemoguće je dati dokaz Churchove teze. Oboriti pak Churchovu tezu značilo bi odrediti funkciju za koju bi se svi složili da je izračunljiva, a istovremeno bi dokazali da nije parcijalno rekurzivna. No, to do sada nije učinjeno. Ovdje navodimo dvije važne činjenice zbog kojih Churchovu tezu smatramo istinitu.

1. Razni načini definiranja novih funkcija pomoću već danih parcijalno rekurzivnih funkcija (npr. simultana rekurzija, povratna rekurzija, definicija funkcija po slučajevima, ...) daju ponovno parcijalno rekurzivne funkcije.
2. Sve do sada poznate definicije koje imaju za cilj opisati klasu izračunljivih funkcija (parcijalno rekurzivne funkcije, RAM-izračunljive funkcije, Turing izračunljive, ABAK-izračunljive, ...) definiraju istu klasu funkcija.

Važnost Churchove teze je vrlo velika. Ona se primjenjuje uvijek prilikom dokaza nepostojanja algoritma za rješavanje nekog problema (tj. nerješivosti problema). Sada dajemo dva primjera takvih problema.

Primjer 1.64. Postoji funkcija koja nije izračunljiva.
U svrhu dokaza gornje tvrdnje definiramo funkciju F na sljedeći način:

$$F(x) \simeq \begin{cases} \{x\}(x)+1, & \textit{ako je } \{x\}(x)\downarrow; \\ 0, & \textit{inače.} \end{cases}$$

Lako je vidjeti da niti za jedan $e \in \mathbb{N}$ ne vrijedi $F \simeq \{e\}$. To znači da za funkciju F ne postoji indeks, a tada iz teorema 1.53. slijedi da funkcija F nije parcijalno rekurzivna. Primjenom Churchove teze slijedi da funkcija F nije izračunljiva.

Primjer 1.65. Halting problem nije rješiv.
Halting problem glasi:

> *odrediti postoji li algoritam koji će za proizvoljan program P za RAM-stroj i ulazne podatke $\vec{x}$ odrediti hoće li P-izračunavanje sa $\vec{x}$ stati.*

Dokazat ćemo da takav algoritam ne postoji. Štoviše, definirat ćemo jedan program P za RAM-stroj i za njega pokazati da ne postoji algoritam koji bi za svaki $x \in \mathbb{N}$ ispitao hoće li P-izračunavanje sa x stati. Iz Churchove teze će tada slijediti da je halting problem nerješiv. U svrhu dokaza definiramo skup S sa:

$$x \in S \quad \text{ako i samo ako} \quad \{x\}(x)\downarrow .$$

Napišimo definiciju funkcije F iz prethodnog primjera 1.64. pomoću skupa S :

$$F(x) \simeq \begin{cases} \{x\}(x) + 1, & \text{ako je } \ x \in S; \\ 0, & \text{inače.} \end{cases}$$

Ako bi skup S bio rekurzivan tada bi funkcija F bila definirana po slučajevima pomoću rekurzivnih uvjeta i parcijalno rekurzivnih funkcija. Iz teorema 1.56. tada bi slijedilo da je funkcija F parcijalno rekurzivna. No, u primjeru 1.64. dokazali smo da funkcija F nije parcijalno rekurzivna. Dakle, skup S nije rekurzivan. Primjenom Churchove teze slijedi da ne postoji algoritam koji će za svaki $x \in \mathbb{N}$ ispitati je li izraz $\{x\}(x)$ definiran.

Neka je funkcija G definirana sa $G(x) \simeq \{x\}(x)$. Iz Kleenijevog teorema o normalnoj formi slijedi da je funkcija G parcijalno rekurzivna. Neka je P program za RAM-stroj koji izračunava funkciju G. Očito vrijedi:

> *RAM-stroj će stati prilikom P-izračunavanja sa x ako i samo ako je izraz $\{x\}(x)$ definiran.*

No, prije smo bili dokazali da ne postoji algoritam koji bi za svaki $x \in \mathbb{N}$ ispitivao je li izraz $\{x\}(x)$ definiran. Dakle, za program P ne postoji algoritam koji bi za svaki $x \in \mathbb{N}$ ispitao hoće li P-izračunavanje sa x stati.

1.8 Aritmetička hijerahija

Sada ćemo proučavati što se događa s relacijom kada je kvantificiramo s neograničenim kvantifikatorima. Prisjetimo se: ako je relacija R (primitivno) rekurzivna relacija tada su i relacije $(\forall z < y)R(\vec{x}, z)$ i $(\exists z < y)R(\vec{x}, z)$ (primitivno) rekurzivne.

Definicija 1.66. *Kažemo da je relacija $R \subseteq \mathbb{N}^k$* **aritmetička** *ako postoji rekurzivna relacija P tako da vrijedi:*

$$R(\vec{x}) \;\; \textit{ako i samo ako} \;\; Q_1 y_1 \ldots Q_n y_n P(\vec{x}, y_1, \ldots, y_n),$$

gdje je Q_i simbol $\forall$ ili $\exists$. Kažemo da je $Q_1 y_1 \ldots Q_n y_n$ **prefiks**.

Sada nam je cilj pokazati da svaka aritmetička relacija može biti prikazana u vrlo jednostavnom obliku, tj. da njen prefiks možemo zapisati u ekvivalentnom "standardnom" obliku. U tu svrhu prvo dokazujemo sljedeću propoziciju.

Propozicija 1.67. *Neka je R rekurzivna relacija. Tada postoje rekurzivne relacije P i Q tako da vrijedi:*

$$\forall y \forall z R(\vec{x}, y, z) \;\; \textit{ako i samo ako} \;\; \forall u P(\vec{x}, u), \;\; \textit{i}$$

$$\exists y \exists z R(\vec{x}, y, z) \;\; \textit{ako i samo ako} \;\; \exists u Q(\vec{x}, u).$$

Dokaz. Očito vrijedi

$$\forall y \forall z R(\vec{x}, y, z) \;\; \text{ako i samo ako} \;\; \forall u R(\vec{x}, (u)_0, (u)_1), \;\; \text{i}$$

$$\exists y \exists z R(\vec{x}, y, z) \;\; \text{ako i samo ako} \;\; \exists u R(\vec{x}, (u)_0, (u)_1).$$

Na strani 51 smo dokazali da su funkcije $x \mapsto (x)_1$ i $x \mapsto (x)_0$ rekurzivne, pa iz rekurzivnosti relacije R slijedi da je i relacija $R(\cdot, (\cdot)_0, (\cdot)_1)$ također rekurzivna. □

Primjenom gornje propozicije slijedi da uvijek možemo vršiti **kontrakciju** istovrsnih kvantifikatora. Kažemo da je prefiks **alternirajući** ako ne sadrži dva uzastopna egzistencijalna ili univerzalna kvantifikatora.

Definicija 1.68. *Neka je $n > 0$. Kažemo da je prefiks Π^0_n ako je alternirajući, sadrži n kvantifikatora i prvi kvantifikator slijeva je $\forall$. Kažemo da je prefiks Σ^0_n ako je alternirajući, sadrži n kvantifikatora i prvi kvantifikator slijeva je $\exists$.*

Kažemo da je relacija R jedna Π^0_n relacija ako postoji rekurzivna relacija P i prefiks $Q_1 y_1 \ldots Q_n y_n$, koji je Π^0_n, tako da vrijedi

$$R(\vec{x}) \;\; \textit{ako i samo ako} \;\; Q_1 y_1 \ldots Q_n y_n P(\vec{x}, y_1, \ldots, y_n).$$

Ponekad ćemo pisati $R \in \Pi^0_n$, te govoriti da je Π^0_n oznaka klase svih Π^0_n relacija. Slično definiramo pojam Σ^0_n relacije. Kažemo da je relacija Δ^0_n ako je istovremeno Π^0_n i Σ^0_n.

Uočite da bilo koji od simbola Π^0_0, Σ^0_0 i Δ^0_0 nam označava klasu svih rekurzivnih relacija.

Jasna je uloga donjeg indeksa u oznakama Π^0_n, Σ^0_n i Δ^0_n. Gornji indeks, tj. nula, označava da se radi o relacijama "na brojevima". Relacija koja bi bila npr. Π^1_n "djelovala" bi na skupovima brojeva.

Očito je svaka rekurzivna relacija Δ^0_n, za sve $n \in \mathbb{N}$ (kao prefiks možemo staviti irelevantne kvantifikatore). To znači da su npr. relacije $=$, $\leq$ i $>$ primjeri Δ^0_7 relacija. Relacija $\exists x \forall y (x = y \land x < z)$ je jedna Σ^0_2 relacija, dok je $\forall x \exists z \forall y (x \cdot y < z)$ jedna Π^0_3 relacija.

Iz propozicije 1.67. slijedi da prefiks svake aritmetičke relacije možemo napisati u alternirajućem obliku iz čega odmah slijedi tvrdnja sljedeće propozicije.

Propozicija 1.69. *Svaka aritmetička relacija je Π^0_n ili Σ^0_n, za neki $n \in \mathbb{N}$.*

U sljedećoj propoziciji naglašavamo da za sve $k \in \mathbb{N}$ vrijedi $\Pi^0_k \subseteq \Pi^0_{k+1}$, odnosno $\Sigma^0_k \subseteq \Sigma^0_{k+1}$.

Propozicija 1.70. *Ako je $R \in \Pi^0_n$ ili $R \in \Sigma^0_n$, za neki $n \in \mathbb{N}$, tada je $R \in \Delta^0_k$ za sve $k > n$.*

Dokaz. Primijetimo da svakoj relaciji možemo dodati irelevantne kvantifikatore. Npr. neka $R \in \Pi^0_2$ tj. vrijedi $R(x) \Leftrightarrow \forall y \exists z P(x, y, z)$. No, vrijedi i $R(x) \Leftrightarrow \exists u \forall y \exists z R(x, y, z) \Leftrightarrow \forall y \exists z \forall u R(x, y, z)$. $\square$

Sada nam je cilj dokazati da za upravo definiranu hijerahiju aritmetičkih relacija niti u jednom trenutku ne nastupa "kolaps", tj. da ne postoji $n \in \mathbb{N}$ tako da bi vrijedilo $\Pi^0_n = \Pi^0_{n+1}$, odnosno $\Sigma^0_n = \Sigma^0_{n+1}$. U tu svrhu prvo definiramo sljedeći pojam.

Definicija 1.71. *Kažemo da se k–mjesna relacija P može* **reducirati** *na n–mjesnu relaciju Q ako postoje rekurzivne funkcije $f_1, \ldots, f_n$ tako da za sve $\vec{x} \in \mathbb{N}^k$ vrijedi:*

$$P(\vec{x}) \text{ ako i samo ako } Q(f_1(\vec{x}), \ldots, f_n(\vec{x})).$$

Ako se relacija P može reducirati na rekurzivnu relaciju Q tada je očito i P rekurzivna. Iz te činjenice odmah slijedi tvrdnja sljedeće propozicije.

Propozicija 1.72. *Neka se relacija P može reducirati na relaciju Q. Ako je $Q \in \Pi^0_n$ (odnosno $Q \in \Sigma^0_n$, ili $Q \in \Delta^0_n$) tada je i $P \in \Pi^0_n$ (odnosno $P \in \Sigma^0_n$, ili $P \in \Delta^0_n$).*

Sada promatramo djelovanje kvantifikatora na Π^0_n i Σ^0_n relacije. Prisjetimo se prvo **pravila prijelaza** za kvantifikatore (vidi [18]). Neka su P i R relacije (proizvoljne mjesnosti), pri čemu se u sljedećim tvrdnjama varijabla y ne pojavljuje kao varijabla kod relacije P. Tada vrijede sljedeće ekvivalencije:

$$\begin{array}{rcl}
\neg\forall y\ R(y,\vec{x}) & \Leftrightarrow & \exists y\ \neg R(y\vec{x}) \\
\neg\exists y\ R(y,\vec{x}) & \Leftrightarrow & \forall y\ \neg R(y,\vec{x}) \\
Qy\ R(y,\vec{x}) \vee P & \Leftrightarrow & Qy\ (R(y,\vec{x}) \vee P) \\
P \vee Qy\ R(y,\vec{x}) & \Leftrightarrow & Qy\ (P \vee R(y,\vec{x})) \\
Qy\ R(y,\vec{x}) \wedge P & \Leftrightarrow & Qy\ (R(y,\vec{x}) \wedge P) \\
P \wedge Qy\ R(y,\vec{x}) & \Leftrightarrow & Qy\ (P \wedge R(y,\vec{x})),
\end{array}$$

gdje je Q simbol $\forall$ ili $\exists$.

Primjenom prva dva pravila prijelaza slijedi da je negacija neke Π^0_n relacije nužno neka Σ^0_n relacija, a negacija Σ^0_n relacije je Π^0_n relacija. Preostala četiri pravila govore da su klase Π^0_n i Σ^0_n zatvorene za veznike $\wedge$ i $\vee$. Za ilustraciju promotrimo sljedeći primjer:

$$\forall x \exists y P(x,y)\ \vee\ \forall z \exists w Q(z,w) \Leftrightarrow$$

$$\forall x \forall z \exists y \exists w (P(x,y) \vee Q(z,w)) \Leftrightarrow$$

$$\forall v \exists u (P((v)_0,(u)_0)\ \vee\ Q((v)_1,(u)_1)).$$

Iz toga slijedi da je disjunkcija Π^0_2 relacija ponovo Π^0_2 relacija.

Promotrimo sada djelovanje kvantifikatora na Π^0_n i Σ^0_n relacije. Neka su R i P relacije za koje vrijedi $R(\vec{x}) \Leftrightarrow \forall y P(\vec{x},y)$. Ako je $P \in \Pi^0_n$ tada primjenom kontrakcije kvantifikatora slijedi da je tada i $R \in \Pi^0_n$. Ako pak je $P \in \Sigma^0_n$ tada je $R \in \Pi^0_{n+1}$.

Neka su R i P relacije za koje vrijedi $R(\vec{x}) \Leftrightarrow \exists y P(\vec{x},y)$. Ako je $P \in \Pi^0_n$ tada vrijedi $R \in \Sigma^0_{n+1}$. Ako pak je $P \in \Sigma^0_n$ tada primjenom kontrakcije kvantifikatora slijedi da je relacija R također Σ^0_n.

Promotrimo sada djelovanje ograničenih kvantifikatora na Π^0_n i Σ^0_n relacije. U tu svrhu primijetimo da vrijede sljedeće četiri ekvivalencije:

$$\begin{array}{rcl}
(\forall y < x)\forall z R(x,y,z) & \Leftrightarrow & \forall z(\forall y < x)R(x,y,z) \\
(\exists y < x)\exists z R(x,y,z) & \Leftrightarrow & \exists z(\exists y < x)R(x,y,z) \\
(\forall y < x)\exists z R(x,y,z) & \Leftrightarrow & \exists z(\forall y < x)R(x,y,(z)_y) \\
(\exists y < x)\forall z R(x,y,z) & \Leftrightarrow & \forall z(\exists y < x)R(x,y,(z)_y)
\end{array}$$

Navedene prve dvije ekvivalencije očito vrijede. Obje strane u trećoj ekvivalenciji tvrde da postoji konačan niz $z_0,\ldots,z_{x-1}$ tako da vrijedi $R(x,y,z_y)$, za sve $y < x$. Četvrta ekvivalencija se lako dobiva iz treće uvrštavanjem relacije $\neg R$ umjesto R, te "dovođenjem" negacije na početak.

Primjenom prethodnih četiri ekvivalencija možemo neograničene kvantifikatore uvijek dovesti na početak prefiksa. Ako je relacija R rekurzivna tada iz propozicije 1.43. slijedi da su i relacije $(\forall y < x)R(x, y, z)$ i $(\exists y < x)R(x, y, z)$ rekurzivne. Iz svega navedenog slijedi da su klase Π^0_n i Σ^0_n zatvorene za ograničene kvantifikatore.

Sumirajmo sve do sada navedeno u sljedećoj tablici. Neka su P i R aritmetičke relacije proizvoljne mjesnosti, a Q neka je simbol $\forall$ ili $\exists$. Tada iz sljedeće tablice čitamo djelovanje logičkih veznika i kvantifikatore na dane relacije.

P, R	$\neg P$	$P \vee R$	$P \wedge R$	$\forall x P$	$\exists x P$	$(Qx < y)P$
Π^0_n	Σ^0_n	Π^0_n	Π^0_n	Π^0_n	Σ^0_{n+1}	Π^0_n
Σ^0_n	Π^0_n	Σ^0_n	Σ^0_n	Π^0_{n+1}	Σ^0_n	Σ^0_n
Δ^0_n	Δ^0_n	Δ^0_n	Δ^0_n	Π^0_n	Σ^0_n	Δ^0_n

Kada relacije P i R nisu iz iste klase tada primjenjujemo propoziciju 1.70. Npr. neka je $P \in \Pi^0_2$, a $R \in \Sigma^0_2$. Iz propozicije 1.70. slijedi da je tada $P \in \Delta^0_3$ i $R \in \Delta^0_3$. Sada možemo dalje zaključivati o relacijama $P \wedge R$ i $P \vee R$.

Primijetite da ne moramo promatrati posebno veznike $\rightarrow$ i $\leftrightarrow$, jer se oni mogu izraziti pomoću veznika $\neg$, $\wedge$ i $\vee$.

Klasifikaciju aritmetičkih relacija na Π^0_n i Σ^0_n relacije nazivamo **aritmetička hijerarhija.** Primijetite da još nismo dokazali da su klase Π^0_n i Σ^0_n u toj hijerarhiji različite. U svrhu tog dokaza uvodimo sljedeći pojam.

Definicija 1.73. *Neka je $\mathcal{S}$ neka klasa k–mjesnih relacija. Kažemo da $(k+1)$–mjesna relacija Q* **prebraja klasu** $\mathcal{S}$ *ako za svaku relaciju $R \in \mathcal{S}$ postoji $e \in \mathbb{N}$ tako da za sve $\vec{x} \in \mathbb{N}^k$ vrijedi:*

$$R(\vec{x}) \ \text{ ako i samo ako } \ Q(\vec{x}, e).$$

Kako bismo mogli dokazati teorem o aritmetičkom prebrajanju definiramo pojam s–te aproksimacije funkcije $\{e\}^k$. Za sve $e, s, k \in \mathbb{N}$ definiramo funkciju $\{e\}^k_s$ na sljedeći način:

$$\{e\}^k_s(\vec{x}) \simeq U(\mu y(y \leq s \wedge T_k(e, \vec{x}, y))).$$

Očito za sve $e, z, k \in \mathbb{N}$ i $\vec{x} \in \mathbb{N}^k$ vrijedi:

$$\{e\}^k(\vec{x}) \simeq z \ \text{ ako i samo ako } \ \text{postoji } \ s \in \mathbb{N} \ \text{ tako da } \{e\}^k_s(\vec{x}) \simeq z.$$

Po definiciji $\{e\}^k(\vec{x})$ je definirano ako postoji $y \in \mathbb{N}$ tako da vrijedi $T_k(e, \vec{x}, y)$. Ako takav y postoji tada vrijedi $U(y) = \{e\}(\vec{x})$. Pošto je y veći od svakog broja koji se pojavljuje u registrima u toku P-izračunavanja sa $\vec{x}$ tada je $y > x_i$, za sve $i = 0, \ldots, k-1$ i $y > \{e\}^k(\vec{x})$. Ako je $\{e\}^k(\vec{x}) = z$ tada je $\{e\}^k_s(\vec{x}) = z$, za sve $s \geq y$, a inače je za sve $s \in \mathbb{N}$ izraz $\{e\}^k_s(\vec{x})$ nedefiniran.

Za dane e i s funkcija $\{e\}^k_s$ je konačna funkcija, tj. njena domena je podskup konačnog skupa $\{0, 1, \ldots, s-1\}^k$ (jer vrijedi $s \geq y \geq x_i$, za sve $i = 1, \ldots, k$). To znači da funkcija $\{e\}^k_s$ može biti shvaćena kao s–ta aproksimacija funkcije $\{e\}^k$. Sljedeća lema ističe važnost funkcija $\{e\}^k_s$.

Lema 1.74. *Neka su relacije P i Q definirane s:*

$$P(e, s, \vec{x}, z) \quad \textit{ako i samo ako} \quad \{e\}^k_s(\vec{x}) \simeq z,$$

$$Q(e, s, \vec{x}) \quad \textit{ako i samo ako} \quad \{e\}^k_s(\vec{x}) \downarrow .$$

Tada su relacije P i Q rekurzivne.

Dokaz. Očito vrijedi

$$P(e, s, \vec{x}, z) \quad \text{ako i samo ako} \quad (\exists y \leq s)(T_k(e, \vec{x}, y) \wedge U(y) = z),$$

$$Q(e, s, \vec{x}) \quad \text{ako i samo ako} \quad (\exists y \leq s) T_k(e, \vec{x}, y).$$

Znamo da je funkcija U primitivno rekurzivna (vidi stranu 61). Iz propozicije 1.36. slijedi da je relacija $U(y) = z$ rekurzivna. Znamo da je relacija T_k primitivno rekurzivna. Iz propozicije 1.34. slijedi da je tada i relacija $T_k(e, \vec{x}, y) \wedge U(y) = z$ također rekurzivna. Sada primjenom propozicije 1.43. slijedi rekurzivnost relacije P. Sasvim analogno bi dokazali rekurzivnost relacije Q. □

Važno je spomenuti da relacija $\{e\}^{k+2}(\vec{x}, y, z) \simeq 0$ općenito nije rekurzivna što ćemo dokazati u sljedećem poglavlju, pa je jasnija važnost prethodne propozicije, odnosno uvođenja funkcije $\{e\}^k_s$.

Sada dokazujemo teorem o aritmetičkom prebrajanju koji će nam biti ključan prilikom dokaza teorema o aritmetičkoj hijerarhiji.

Teorem 1.75. (Teorem o aritmetičkom prebrajanju)
Neka su $n > 0$ i $k > 0$ proizvoljni prirodni brojevi. Za klasu svih k–mjesnih Π^0_n relacija postoji $(k+1)$–mjesna Π^0_n relacija koja je prebraja. Analogno, za klasu svih k–mjesnih Σ^0_n relacija postoji $(k+1)$–mjesna Σ^0_n relacija koja je prebraja.

Dokaz. Radi kraćeg zapisa promatramo slučaj kada je $n = 2$. Neka je R k–mjesna Π^0_2 relacija, tj. postoji rekurzivna relacija P tako da vrijedi:

$$R(\vec{x}) \text{ ako i samo ako } \forall y \exists z P(\vec{x}, y, z).$$

Pošto je P rekurzivna relacija tada je po definiciji njena karakteristična funkcija χ_P rekurzivna. Iz Kleenijevog teorema o normalnoj formi slijedi da postoji indeks za funkciju χ_P. Neka je e neki indeks za χ_P. Tada iz definicije funkcije $\{e\}^{k+2}_s$ slijedi da vrijede sljedeće ekvivalencije:

$$R(\vec{x}) \Leftrightarrow \forall y \exists z (\{e\}^{k+2}(\vec{x}, y, z) \simeq 1) \Leftrightarrow \forall y \exists z \exists s (\{e\}^{k+2}_s(\vec{x}, y, z) \simeq 1).$$

Označimo s Q relaciju definiranu s:

$$Q(\vec{x}, e) \text{ ako i samo ako } \forall y \exists z \exists s (\{e\}^{k+2}_s(\vec{x}, y, z)) \simeq 1).$$

Iz leme 1.74. slijedi da je relacija $\{e\}^{k+2}_s(\vec{x}, y, z) \simeq 1$ rekurzivna, a onda je $Q \in \Pi^0_2$.

Dakle, Q je Π^0_2 relacija koja prebraja klasu svih k–mjesnih Π^0_2 relacija. Lako je vidjeti da je $\neg Q$ jedna Σ^0_2 relacija koja prebraja klasu svih k–mjesnih Σ^0_2 relacija. □

Teorem 1.76. (Teorem o aritmetičkoj hijerarhiji)
Za svaki $n > 0$ postoji Π^0_n relacija koja nije Σ^0_n, te postoji Σ^0_n relacija koja nije Π^0_n.

Dokaz. Iz teorema o aritmetičkom prebrajanju slijedi da za klasu svih unarnih Σ^0_n relacija postoji binarna Σ^0_n relacija Q koja je prebraja, tj. za sve unarne relacije R iz klase Σ^0_n postoji $e \in \mathbb{N}$ tako da vrijedi:

$$R(x) \text{ ako i samo ako } Q(x, e).$$

Definiramo relaciju D s:

$$D(y) \text{ ako i samo ako } Q(y, y).$$

Očito vrijedi:

$$D(y) \text{ ako i samo ako } Q(I^1_1(y), I^1_1(y)).$$

To znači da se relacija D može reducirati na relaciju Q. No, Q je Σ^0_n relacija, pa iz propozicije 1.72. slijedi da je i relacija D također Σ^0_n. Tada vrijedi $\neg D \in \Pi^0_n$. Tvrdimo da relacija $\neg D$ nije Σ^0_n. Pretpostavimo suprotno, tj. da $\neg D \in \Sigma^0_n$.

Pošto relacija Q prebraja klasu unarnih Σ^0_n relacija tada posebno za relaciju $\neg D$ postoji $e \in \mathbb{N}$ tako da za sve $y \in \mathbb{N}$ vrijedi

$$\neg D(y) \text{ ako i samo ako } Q(y, e).$$

Posebno, za $y = e$ vrijedi: $\neg D(e)$ ako i samo ako $Q(e, e)$. No, iz definicije relacije D slijedi: $D(e)$ ako i samo ako $Q(e, e)$. Time smo dobili da vrijedi: $D(e)$ ako i samo ako $\neg D(e)$. To znači da iz pretpostavke $\neg D \in \Sigma^0_n$ slijedi kontradikcija. Zaključimo: unarna relacija $\neg D$ je Π^0_n relacija, ali nije Σ^0_n relacija. □

Primijetite da teorem o aritmetičkom prebrajanju ne vrijedi za klase Δ^0_n relacija. Posebno ne vrijedi za klasu svih rekurzivnih relacija, jer to je zapravo klasa svih Δ^0_0 relacija. Kada bi teorem o aritmetičkom prebrajanju vrijedio za Δ^0_n relacije tada bi mogli dokazati i teorem o aritmetičkoj hijerarhiji za Δ^0_n relacije. No, teorem o aritmetičkoj hijerarhiji za Δ^0_n relacije izricao bi da postoji Δ^0_n relacija koja nije Δ^0_n, što očito nema smisla.

Sumirajmo na kraju rezultate o aritmetičkoj hijerahiji u sljedećem korolaru.

Korolar 1.77. *a) Za sve $i < j$ vrijedi:* $\Pi^0_i \subset \Sigma^0_j$, $\Pi^0_i \subset \Pi^0_j$, $\Sigma^0_i \subset \Pi^0_j$ *i* $\Sigma^0_i \subset \Sigma^0_j$.

b) Za sve $i \in \mathbb{N}$ vrijedi: $\Pi^0_i \cup \Sigma^0_i \subset \Pi^0_{i+1} \cap \Sigma^0_{i+1}$.

1.9 Rekurzivno prebrojivi skupovi

Prisjetimo se definicije rekurzivnog skupa: za $R \subseteq \mathbb{N}^k$ kažemo da je rekurzivan ako je njegova karakteristična funkcija χ_R rekurzivna. Sada ćemo proučavati skupove koji su "skoro" rekurzivni.

Skup smatramo odlučivim (odnosno rekurzivnim) ako postoji algoritam koji za svaki prirodan broj može odrediti pripada li skupu ili ne. Slično, skup A ćemo smatrati rekurzivno prebrojivim ako postoji algoritam koji kao izlazne podatke daje upravo sve elemente skupa A. Možemo zapravo reći da je rekurzivno prebrojiv skup slika neke parcijalno rekurzivne funkcije. No, stroga definicija rekurzivno prebrojivog skupa će se činiti u prvi tren različita od intuitivnog opisa koji smo naveli. Kasnije ćemo dokazati (propozicija 1.89.) da je to ekvivalentno.

Definicija 1.78. *Kažemo da je skup (odnosno relacija) $A \subseteq \mathbb{N}^k$* **rekurzivno prebrojiv** *ako je A domena neke parcijalno rekurzivne funkcije. Kratko ćemo reći da je to RE–skup (ili RE–relacija) (eng. recursively enumerable).*

Skupovi $\mathbb{N}$ i $\emptyset$ su rekurzivno prebrojivi, jer je $\mathbb{N}$ domena npr. rekurzivne funkcije Sc, a prazan skup je domena npr. funkcije $\{3\}$. Svaki rekurzivan skup A je RE–skup, jer je A domena sljedeće parcijalno rekurzivne funkcije

$$x \mapsto \mu y\big(y + 1 = \chi_A(x)\big).$$

Kasnije ćemo pokazati da obrat ne vrijedi, tj. svaki RE–skup nije nužno rekurzivan. Sada želimo proučiti svojstva rekurzivno prebrojivih skupova. U tu svrhu prvo uvodimo sljedeći pojam.

Definicija 1.79. *Za $e, k \in \mathbb{N}$ s W_e^k označavamo RE–skup koji je domena parcijalno rekurzivne funkcije $\{e\}^k$. Neka je R rekurzivno prebrojiva k–mjesna relacija.* **Indeks relacije** *R je najmanji $e \in \mathbb{N}$ takav da je $R = W_e^k$.*

U daljnjim razmatranjima pisat ćemo i W_e, odnosno $\{e\}$, kada nije nužno istaknuti mjesnost.

Primijetite da se ovako definirani indeks (rekurzivno prebrojive) relacije R ne mora nužno poklapati s indeksom funkcije χ_R. Zatim, za neku relaciju R postoji indeks ako i samo ako je relacija R rekurzivno prebrojiva.

Sljedeću propoziciju ćemo često koristiti.

Propozicija 1.80. *Relacija R je rekurzivno prebrojiva ako i samo ako je $R \in \Sigma_1^0$.*

Dokaz. Pretpostavimo prvo da je R rekurzivno prebrojiva relacija. Tada vrijedi $W_e = R$ za neki $e \in \mathbb{N}$. No, pošto vrijedi

$$\vec{x} \in W_e \text{ ako i samo ako } \exists y T_k(e, \vec{x}, y),$$

te je T_k primitivno rekurzivna relacija, tada je $W_e \in \Sigma_1^0$, a onda je i $R \in \Sigma_1^0$.

Pretpostavimo sada da je $R \in \Sigma_1^0$. Neka je P rekurzivna relacija tako da vrijedi: $R(\vec{x})$ ako i samo ako $\exists y P(\vec{x}, y)$. Neka je f funkcija definirana sa $f(\vec{x}) \simeq \mu y P(\vec{x}, y)$. Očito je f parcijalno rekurzivna funkcija, te vrijedi $Dom(f) = R$. $\square$

Uočite da iz prethodne propozicije posebno slijedi da je unija i presjek konačno mnogo RE–skupova ponovo RE–skup.

Bili smo prije već napomenuli da kvantifikacijom rekurzivne relacije ne moramo ponovo dobiti rekurzivnu relaciju. Sljedeći teorem je jako značajan, jer upravo to pokazuje.

Teorem 1.81. *Postoji RE–skup koji nije rekurzivan.*

Dokaz. Iz teorema o aritmetičkoj hijerahiji, tj. iz teorema 1.76., slijedi da postoji RE–skup A (tj. unarna Σ_1^0 relacija) koji nije Π_1^0. Pretpostavimo da je A rekurzivan skup. Iz propozicije 1.34. znamo da je tada i skup A^c rekurzivan, a onda je taj skup i rekurzivno prebrojiv. Tada je komplement skupa A^c, tj. skup A, Π_1^0 skup, što je kontradikcija. $\square$

U Uvodu smo bili opisali deseti Hilbertov problem. Sada spominjemo još jedan detalj u vezi s tim problemom. Promotrimo diofantsku jednadžbu

$$p(\vec{x}, y) = q(\vec{x}, y),$$

gdje su p i q polinomi s varijablama $\vec{x}$ i y, te s koeficijentima iz skupa cijelih brojeva. Neka je D skup definiran sa:

$$y \in D \text{ ako i samo ako } \exists \vec{x}(p(\vec{x}, y) = q(\vec{x}, y)).$$

Lako je vidjeti da je D rekurzivno prebrojiv skup. Prilikom rješavanja desetog Hilbertovog problema dokazano je da vrijedi i obrat, tj. svaki RE–skup je skup rješenja neke diofantske jednadžbe.

Sljedeći teorem je analogon teorema o parametru koji smo bili razmatrali.

Teorem 1.82. (Teorem o RE-parametrizaciji)
Neka je R $(k+m)-$mjesna RE–relacija. Tada postoji rekurzivna funkcija S tako da za sve $\vec{x}$, $y_1, \ldots, y_m$ vrijedi:

$$\vec{x} \in W_{S(y_1, \ldots, y_m)} \textit{ ako i samo ako } R(\vec{x}, y_1, \ldots, y_m).$$

Dokaz. Neka je $e \in \mathbb{N}$ tako da vrijedi $R = W_e$. Iz teorema 1.58. slijedi da postoji rekurzivna funkcija S tako da vrijedi

$$\{e\}(\vec{x}, y_1, \ldots, y_m) \simeq \{S(y_1, \ldots, y_m)\}(\vec{x}).$$

Tada vrijede redom sljedeće ekvivalencije:

$$\vec{x} \in W_{S(y_1,\ldots,y_m)} \text{ ako i samo ako } \{e\}(\vec{x}, y_1, \ldots, y_m)\downarrow \text{ ako i samo ako}$$

$$(\vec{x}, y_1, \ldots, y_m) \in W_e \text{ ako i samo ako } R(\vec{x}, y_1, \ldots, y_m).$$

□

Sada promatramo problem "odvajanja" (selektiranja) funkcije iz neke zadane relacije.

Definicija 1.83. *Neka je R neka $(k+1)$-mjesna relacija. Kažemo da je k–mjesna funkcija f* **selektor** *za relaciju R ako vrijedi:*

$$f(\vec{x})\downarrow \text{ ako i samo ako postoji } y \text{ tako da } R(\vec{x}, y), \text{ te je tada } f(\vec{x}) = y.$$

Egzistencija selektora za svaku RE–relaciju iskazana je u sljedećem teoremu.

Teorem 1.84. (Teorem o selektoru)
Za svaku $(k+1)$–mjesnu RE–relaciju postoji selektor koji je parcijalno rekurzivna funkcija.

Dokaz. Neka je R rekurzivno prebrojiva relacija. Iz propozicije 1.80. slijedi da je $R \in \Sigma_1^0$. Tada po definiciji postoji rekurzivna relacija P tako da vrijedi:

$$R(\vec{x}, y) \text{ ako i samo ako } \exists z P(\vec{x}, y, z).$$

Definiramo funkciju f s $f(\vec{x}) \simeq \mu w\ P\big(\vec{x}, (w)_0, (w)_1\big)$. Očito je f parcijalno rekurzivna funkcija. Tvrdimo da je f selektor za relaciju R. Pretpostavimo prvo da je $\vec{x} \in \mathbb{N}^k$ tako da je $\vec{x}$ iz domene funkcije f. Tada postoji $w \in \mathbb{N}$ tako da vrijedi $P(\vec{x}, (w)_0, (w)_1)$, a tada vrijedi i $R(\vec{x}, (w)_0)$. Uočimo još da iz definicije funkcije f slijedi da je tada i $f(\vec{x}) = (w)_0$.

Pretpostavimo sada da za neke $\vec{x} \in \mathbb{N}^k$ i $y \in \mathbb{N}$ vrijedi $R(\vec{x}, y)$. Tada postoji $z \in \mathbb{N}$ takav da vrijedi $P(\vec{x}, y, z)$. Označimo s u kod uređenog para (y, z), tj. neka je $u = \langle y, z\rangle$. Tada očito vrijedi $P(\vec{x}, (u)_0, (u)_1)$. Označimo s w najmanji prirodan broj koji ima svojstvo $P(\vec{x}, (w)_0, (w)_1)$. Tada iz definicije funkcije f slijedi $f(\vec{x}) = (w)_0$, tj. funkcija f je definirana za $\vec{x}$. □

Sada razmatramo vezu između rekurzivnosti funkcije i rekurzivnosti njenog grafa. Prvo ponavljamo definiciju grafa funkcije, te uvodimo oznaku za graf.

Definicija 1.85. *Neka je f neka k–mjesna funkcija.* **Graf** *od f je $(k+1)$–mjesna relacija G_f definirana sa:*

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

Sljedeći teorem pokazuje kako se parcijalno rekurzivne funkcije mogu karakterizirati pomoću grafa.

Teorem 1.86. (Teorem o grafu)
Neka je $f : S \subseteq \mathbb{N}^k \to \mathbb{N}$ funkcija. Tada vrijede sljedeće tvrdnje:

a) funkcija f je parcijalno rekurzivna ako i samo ako je graf od f RE–relacija;

b) funkcija f je rekurzivna ako i samo ako je graf od f rekurzivna relacija.

Dokaz. Dokažimo prvo tvrdnju a). Neka je e indeks za funkciju f. Tada vrijedi:

$$G_f(\vec{x}, y) \text{ ako i samo ako } \{e\}^k(\vec{x}) \simeq y \text{ ako i samo ako } \exists s(\{e\}^k_s(\vec{x}) \simeq y).$$

Iz leme 1.74. znamo da je relacija $\{e\}^k_s(\vec{x}) \simeq y$ rekurzivna. Iz toga slijedi da je graf funkcije f RE–relacija.

Dokažimo sada obrat u tvrdnji a). Pretpostavimo da je relacija G_f rekurzivno prebrojiva. Iz teorema o selektoru slijedi da postoji parcijalno rekurzivna funkcija g tako da vrijedi:

$$g(\vec{x}) \downarrow \text{ ako i samo ako } \exists y R(\vec{x}, y), \text{ te je tada } g(\vec{x}) = y.$$

No, po definiciji grafa jedini selektor za relaciju G_f je upravo funkcija f. To znači da vrijedi $f \simeq g$, a iz toga direktno slijedi da je funkcija f parcijalno rekurzivna.

Dokažimo sada tvrdnju b). Pretpostavimo da je f rekurzivna funkcija. Tada iz propozicije 1.36. (jednakost je rekurzivna relacija) slijedi da je relacija $f(\vec{x}) = y$ rekurzivna. Iz definicije grafa slijedi da je tada i relacija G_f rekurzivna. Analogno slijedi obrat tvrdnje. $\square$

Kao jednu primjenu teorema o grafu dokazujemo sljedeću propoziciju koja govori o rekurzivnosti funkcija koje su definirane po slučajevima. Prisjetimo se da smo u propoziciji 1.37. dokazali da je funkcija definirana po slučajevima pomoću rekurzivnih funkcija i relacija, također rekurzivna. Zatim, u teoremu 1.56. smo dokazali da je funkcija definirana po slučajevima pomoću parcijalno rekurzivnih funkcija i rekurzivnih relacija, također parcijalno rekurzivna. Sada promatramo parcijalno rekurzivne funkcije i RE–relacije.

Propozicija 1.87. *Neka su $R_1, \ldots, R_n$ neke RE–relacije koje imaju svojstvo da za svaki $\vec{x} \in \mathbb{N}^k$ postoji najviše jedan $i \in \{1, \ldots, n\}$ tako da vrijedi $R_i(\vec{x})$. Neka su $f_1, \ldots, f_n$ parcijalno rekurzivne funkcije. Definiramo funkciju f na sljedeći način:*

$$f(\vec{x}) \simeq \begin{cases} f_1(\vec{x}), & \textit{ako vrijedi } R_1(\vec{x}); \\ \qquad \vdots & \\ f_n(\vec{x}), & \textit{ako vrijedi } R_n(\vec{x}), \end{cases}$$

gdje se podrazumijeva da $f(\vec{x})$ nije definirano ako niti za jedan $i \in \{1, \ldots, n\}$ nije ispunjeno $R_i(\vec{x})$. Tada je funkcija f parcijalno rekurzivna.

Dokaz. Iz teorema o grafu slijedi da je za svaki $i \in \{1, \ldots, n\}$ graf G_{f_i} rekurzivno prebrojiva relacija. Iz propozicije 1.80. slijedi da je tada $G_{f_i} \in \Sigma_1^0$. No, tada je za svaki $i \in \{1, \ldots, n\}$ relacija $G_{f_i} \wedge R_i \in \Sigma_1^0$ (vidi stranu 84). Iz toga pak slijedi da je relacija

$$\Big(G_{f_1}(\vec{x}, y) \wedge R_1(\vec{x})\Big) \ \vee \ \ldots \ \vee \Big(G_{f_n}(\vec{x}, y) \wedge R_n(\vec{x})\Big)$$

Σ_1^0 relacija. Iz propozicije 1.80. tada slijedi da je ta relacija rekurzivno prebrojiva. Pošto očito vrijedi:

$$G_f(\vec{x}, y) \ \text{ ako i samo ako } \ \big(G_{f_1}(\vec{x}, y) \wedge R_1(\vec{x})\big) \ \vee \ \ldots \ \vee \big(G_{f_n}(\vec{x}, y) \wedge R_n(\vec{x})\big),$$

tada je i relacija G_f rekurzivno prebrojiva. Primjenom teorema o grafu slijedi da je funkcija f parcijalno rekurzivna. □

Sljedeći teorem otkriva do kraja povezanost rekurzivnih i *RE*–relacija.

Teorem 1.88. *(E. Post, 1897.–1954.)*
Relacija R je rekurzivna ako i samo ako su relacije R i $\neg R$ rekurzivno prebrojive.

Dokaz. Ako je R rekurzivna tada iz propozicije 1.34. slijedi da je i relacija $\neg R$ rekurzivna. Na samom početku ove točke bili smo primijetili da je svaka rekurzivna relacija rekurzivno prebrojiva. Iz toga slijedi da su relacije R i $\neg R$ rekurzivno prebrojive.

Pretpostavimo sada da su R i $\neg R$ RE–relacije. Iz propozicije 1.80. slijedi da su to Σ_1^0 relacije. Očito vrijedi:

$$G_{\chi_R}(\vec{x}, y) \ \text{ ako i samo ako } \ \Big(R(\vec{x}) \wedge y = 1\Big) \ \vee \ \Big(\neg R(\vec{x}) \wedge y = 0\Big).$$

Iz ovog posljednjeg slijedi da je $G_{\chi_R} \in \Sigma^0_1$, a onda iz propozicije 1.80. slijedi da je to RE–relacija. Iz teorema o grafu slijedi da je funkcija χ_R parcijalno rekurzivna. No, svaka karakteristična funkcija je totalna, pa iz toga slijedi da je χ_R rekurzivna funkcija, a onda je i R rekurzivna relacija. $\square$

Sljedeća propozicija na neki način povezuje intuitivni opis rekurzivno prebrojivog skupa i formalnu definiciju.

Propozicija 1.89. *Neka je A podskup od $\mathbb{N}$. Tada vrijedi: skup A je rekurzivno prebrojiv ako i samo ako je skup A slika neke parcijalno rekurzivne funkcije.*

Dokaz. Pretpostavimo prvo da je $f : A \subseteq \mathbb{N}^k \to \mathbb{N}$ parcijalno rekurzivna funkcija. Iz teorema o grafu slijedi da je skup $G_f = \{(x_1, \ldots, x_k, f(\vec{x})) \ : \ \vec{x} \in A\}$ rekurzivno prebrojiv. Iz propozicije 1.80. slijedi da postoji rekurzivna relacija R tako da za sve $(\vec{x}, y) \in \mathbb{N}^{k+1}$ vrijedi:

$$(\vec{x}, y) \in G_f \ \text{ ako i samo ako } \ \exists z R(\vec{x}, y, z).$$

Označimo s $Rng(f)$ sliku funkcije f. Pošto očito redom vrijedi:

$$\begin{aligned} y \in Rng(f) \quad &\Leftrightarrow \ \exists x_1 \ldots \exists x_k [(\vec{x}, y) \in G_f] \ \Leftrightarrow \ \exists x_1 \ldots \exists x_k \exists z R(\vec{x}, y, z) \\ &\Leftrightarrow \ \exists u R((u)_0, \ldots, (u)_k, y, (u)_{k+1}), \end{aligned}$$

tada je $Im(f) \in \Sigma^0_1$. Iz propozicije 1.80. slijedi da je $Rng(f)$ rekurzivno prebrojiv skup.

Dokažimo sada obrat. Pretpostavimo da je A neki RE–skup. Ako je A prazan skup tada je A slika parcijalno rekurzivne funkcije $\{3\}$. Promotrimo slučaj kada je $A \neq \emptyset$. Neka je a proizvoljan element od A. Iz propozicije 1.80. slijedi da postoji rekurzivna relacija R tako da za sve $x \in \mathbb{N}$ vrijedi:

$$x \in S \ \text{ ako i samo ako } \ \exists y R(x, y).$$

Definiramo funkciju $f : \mathbb{N} \to \mathbb{N}$ sa:

$$f(x) = \begin{cases} (x)_0, & \text{ako vrijedi } \ R((x)_0, (x)_1); \\ a, & \text{inače.} \end{cases}$$

Iz propozicije 1.87. slijedi da je funkcija f parcijalno rekurzivna. Uočimo da za sve $x \in \mathbb{N}$ redom vrijedi:

$$\begin{aligned}
x \in A \quad &\Leftrightarrow \exists y R(x,y) \;\Leftrightarrow\; \Big(\exists y R(a,y) \;\text{ ili }\; \exists z R(x,(z)_1)\Big) \\
&\Leftrightarrow\; \Big(x = a \;\text{ ili }\; \exists z (f(z) = (z)_0)\Big) \;\Leftrightarrow\; \exists z \in \mathbb{N} (f(z) = x) \\
&\Leftrightarrow\; x \in Rng(f),
\end{aligned}$$

tj. $A = Rng(f)$.

□

Detaljnijem raspisivanjem dokaza prethodne propozicije može se vidjeti da za svaki neprazan RE–skup A postoji primitivno rekurzivna funkcija f tako da vrijedi $A = Rng(f)$.

Napomena 1.90. *U točki 1.3 definirali smo μ–operator i operator M. Prisjetimo se definicije operatora M. Ako je φ funkcija tada sa $M(\varphi)$ označavamo funkciju koja je definirana s*

$$M(f)(\vec{x}) \simeq \Big\{ \;\textit{najmanji } \; z \textit{ takav da je } \; f(\vec{x}, z) = 0, \;\textit{ ako takav } \; z \; \textit{ postoji.}$$

Već smo tamo bili istaknuli da klasa RAM–izračunljivih funkcija nije zatvorena za operator M. Primjenom rekurzivno prebrojivih skupova sada to možemo i dokazati.

Znamo da se klase RAM-izračunljivih funkcija i parcijalno rekurzivnih funkcija poklapaju. Dokažimo da klasa parcijalno rekurzivnih funkcija nije zatvorena za operator M. Neka je A neki rekurzivno prebrojiv skup koji nije rekurzivan (dokazali smo u teoremu 1.81. da takav skup postoji). Definiramo funkciju φ ovako:

$$\varphi(x, y) \simeq 0, \quad \textit{ako je } (y = 0 \;\; \textit{i} \;\; x \notin A) \;\; \textit{ili} \;\; y = 1.$$

Iz propozicije 1.87. slijedi da je funkcija φ parcijalno rekurzivna. Definiramo funkciju f sa $f(x) = M(\varphi)(x)$.

Uočimo da je f totalna funkcija: ako je $x \in A$ tada je $\varphi(x, 0) \uparrow$ i $\varphi(x, 1) = 0$, tj. $f(x) = 1$. Ako $x \notin A$ tada je $\varphi(x, 0) = 0$, tj. $f(x) = 0$. Posebno, vidimo da vrijedi $f = \chi_A$.

(Uočimo da za sve $x \in A^c$ vrijedi da je $\varphi(x, 0)$ nedefinirano, a $\varphi(x, 1)$ je definirano. To znači da ne vrijedi $f(x) = \mu\, y[\varphi(x, y) \simeq 0]$).

Pretpostavimo da je f parcijalno rekurzivna funkcija. Pošto smo prije bili primijetili da je f totalna funkcija, tada slijedi da je f rekurzivna funkcija. No, pošto je $f = \chi_A$, tada slijedi da je A rekurzivan skup. To je kontradikcija s početnom pretpostavkom.

Zadaci:

1. Neka je A kofinitan podskup od $\mathbb{N}$ (tj. komplement od A je konačan). Mora li skup A biti rekurzivno prebrojiv?
Rješenje. Neka je $B = \{b_1, \ldots, b_n\}$ komplement od A. Skup B je rekurzivan jer je njegova karakteristična funkcija jednaka

$$\chi_B(x) = sg(\prod_{i=1}^{n} \mid x - b_i \mid).$$

Karakteristična funkcija skupa A je dana s

$$\chi_A(x) = 1 \dot{-} \chi_B(x).$$

To znači da je i skup A rekurzivan, a onda je i RE–skup.

2. Neka je A rekurzivno prebrojiv skup. Dokažite da je tada i skup $\bigcup_{x \in A} Im(\{e\})$ također RE–skup.
Rješenje. Očito za sve $y \in \mathbb{N}$ vrijedi sljedeća ekvivalencija:

$$y \in \bigcup_{x \in A} Im(\{x\}) \ \text{ ako i samo ako } \ (\exists x \in A)(y \in Im(\{x\})).$$

Pošto su skupovi A i $Im(\{x\})$ Σ_1^0 skupovi tada iz navedene ekvivalencije lako slijedi da je skup $\bigcup_{x \in A} Im(\{x\})$ Σ_1^0 skup.

3. Neka su A i B rekurzivno prebrojivi skupovi. Dokažite da postoje rekurzivno prebrojivi skupovi C i D tako da vrijedi: $C \subseteq A$, $D \subseteq B$, $C \cup D = A \cup B$ i $C \cap B = \emptyset$.
Rješenje. Postoje rekurzivne relacije R i Q tako da vrijedi

$$x \in A \Leftrightarrow \exists y R(x, y) \ \text{ i } \ x \in B \Leftrightarrow \exists y Q(x, y)$$

Tada tražene skupove C i D definiramo ovako:

$$x \in C \quad \Leftrightarrow \quad \exists y R(x, y) \land (\forall z \leq y)(\neg Q(x, z));$$

$$x \in D \quad \Leftrightarrow \quad \exists y Q(x, y) \land (\forall z \leq y)(\neg R(x, z)).$$

Očito su skupovi C i D rekurzivno prebrojivi, te vrijedi $C \subseteq A$ i $D \subseteq B$. Provjerite da vrijedi $C \cup D = A \cup B$ i $C \cap S = \emptyset$.

4. Neka je funkcija f definirana sa:

$$f(x) = \left\lfloor \sqrt[7]{\log_2 \tfrac{2x+1}{2} + 3} \right\rfloor$$

Dokažite da je slika funkcije f, tj. $Im(f)$, skup koji pripada klasi Π^0_{17}.
Rješenje. Iz zadatka 10 sa strane 42 znamo da je funkcija f primitivno rekurzivna. Iz propozicije 1.89. slijedi da je $Im(f)$ rekurzivno prebrojiv skup. Iz propozicije 1.80. slijedi da je $Im(f) \in \Sigma^0_1$. Iz definicije aritmetičke hijerahije vrijedi $\Sigma^0_1 \subseteq \Pi^0_{17}$, pa je $Im(f) \in \Pi^0_{17}$.

5. Neka je funkcija f definirana sa:

$$f(x) = \left\lfloor \frac{\sqrt[3]{x} + 1}{x+1} \right\rfloor.$$

Vrijedi li $Im(f) \in \Sigma^0_3 \cap \Pi^0_7$?

6. Neka je P $(k+1)$–mjesna RE–relacija. Dokažite da postoji $e \in \mathbb{N}$ i k–mjesna relacija R tako da vrijedi:

$$R(\vec{x}) \text{ ako i samo ako } P(\vec{x}, e),$$

pri čemu je R neka RE–relacija i e je njen indeks.
Rješenje. Pošto je P rekurzivno prebrojiva relacija tada postoji parcijalno rekurzivna funkcija f tako da je $Dom(f) = P$. Iz teoremu o rekurziji slijedi da postoji parcijalno rekurzivna funkcija F s indeksom e tako da vrijedi

$$F(\vec{x}) \simeq f(\vec{x}, e).$$

Neka je $R = W_e$. Po definiciji tada vrijedi da je R rekurzivno prebrojiva relacija, a e je njezin indeks. Uočimo još:

$$R(\vec{x}) \Leftrightarrow \vec{x} \in Dom(F) \Leftrightarrow (\vec{x}, e) \in Dom(f) \Leftrightarrow P(\vec{x}, e).$$

7. Neka je $A \subseteq \mathbb{N}^{n+m}$. Kažemo da je skup $B \subseteq \mathbb{N}^n$ **projekcija skupa** A na $\mathbb{N}^n$ ako za sve $\vec{x} \in \mathbb{N}^n$ vrijedi

$$\vec{x} \in B \text{ ako i samo ako } \exists(\vec{y} \in \mathbb{N}^m)(\vec{x}, \vec{y}) \in A.$$

Projekcija nivo skupa primitivno rekurzivne funkcije naziva se **primitivno prebrojiv skup**. Dokažite da je klasa primitivno prebrojivih skupova zatvorena na:

a) konačne produkte;

b) konačne presjeke;

c) konačne unije;

d) projekcije.

8. Neka je $A \subseteq \mathbb{N}^k$. Dokažite da su sljedeće tvrdnje ekvivalentne:

   a) skup A je rekurzivno prebrojiv;

   b) skup A je projekcija nekog rekurzivnog skupa, tj. postoji rekurzivan skup $R \subseteq \mathbb{N}^{k+1}$ tako da za sve $\vec{x} \in \mathbb{N}^k$ vrijedi:

   $$\vec{x} \in S \text{ ako i samo ako } (\exists y)\big((\vec{x}, y) \in R\big);$$

   c) skup A je projekcija nekog primitivno rekurzivnog skupa;

   d) postoji $e \in \mathbb{N}$ tako da za sve $\vec{x} \in \mathbb{N}^k$ vrijedi

   $$\vec{x} \in S \text{ ako i samo ako } (\exists y)T_k(e, \vec{x}, y).$$

9. Dokažite: skup A je rekurzivno prebrojiv ako i samo ako postoji parcijalno rekurzivna funkcija f tako da vrijedi $A = \{\vec{x} : f(\vec{x}) = 0\}$.

10. Neka je $f : S \subseteq \mathbb{N}^n \to \mathbb{N}$ i $m \in \mathbb{N}$. Tada skup $E_m = \{\vec{x} \in S : f(\vec{x}) = m\}$ nazivao m–**nivo skup** funkcije f. Dokažite da su sljedeće klase skupova jednake:

    a) klasa svih rekurzivno prebrojivih skupova;

    b) klasa svih m–nivo skupova parcijalno rekurzivnih skupova, za sve $m \in \mathbb{N}$;

    c) klas svih 1–nivo skupova parcijalno rekurzivnih funkcija.

    Rješenje. Neka je E neki RE–skup. Tada postoji parcijalno rekurzivna funkcija f tako da vrijedi $Dom(f) = E$. Neka je $g : \mathbb{N} \to \mathbb{N}$ definirana sa $g(x) = 1$. Očito je E 1–nivo skup parcijalno rekurzivne funkcije $g \circ f$.

    Ako je E m–nivo skup parcijalno rekurzivne funkcije f tada je E 1–nivo skup parcijalno rekurzivne funkcije $(f - m)^1 + 1$.

    Ako je E 1–nivo skup parcijalno rekurzivne funkcije f tada je skup E domena parcijalno rekurzivne funkcije g koja je definirana sa:

    $$g(x_1, \ldots, x_n) = \mu y\Big[\Big(f(x_1, \ldots, x_n) - 1\Big)^2 + y\Big] = 1.$$

11. Dokažite da je klasa svih RE–skupova jednaka klasi svih primitivno prebrojivih skupova.

12. Neka su $A_1, \ldots, A_n$ RE–skupovi. Dokažite da je $A_1 \times \ldots \times A_n$ Σ_3^0-skup.
Rješenje. Iz zadataka 11 slijedi da je svaki skup A_i primitivno prebrojiv. Primjenom zadatka 7 slijedi da je skup $A_1 \times \ldots \times A_n$ primitivno prebrojiv, a onda iz zadatka 11 slijedi da je to RE–skup. Iz propozicije 1.80. slijedi da skup $A_1 \times \ldots \times A_n$ pripada klasi Σ_0^1.

    (Naravno, rješenje ovog zadatka može se napisati i elementarnije.)

13. Neka je $(A_n)_{n\in\mathbb{N}}$ niz RE–skupova. Dokažite da je tada i skup $\cup_{n\in\mathbb{N}} A_n$ rekurzivno prebrojiv. Vrijedi li analogna tvrdnja i za rekurzivne skupove? Vrijedi li analogna tvrdnja za presjek RE–skupova, odnosno rekurzivnih skupova?

14. Dokažite da su sljedeće tvrdnje ekvivalentne:

    a) skup A je rekurzivan;

    b) $A = \emptyset$ ili je A slika neke rastuće rekurzivne funkcije.

    Rješenje. Neka je $A \neq \emptyset$ rekurzivan, te neka je $a \in A$ najmanji. Definiramo funkciju f sa:

$$\begin{aligned} f(0) &= a \\ f(n+1) &= \begin{cases} n+1, & \text{ako je } \ n+1 \in S; \\ f(n), & \text{inače.} \end{cases} \end{aligned}$$

    Rekurzivnost funkcije f slijedi iz propozicije 1.37. Lako je provjeriti da je $Im(f) = A$, te da je funkcija f rastuća.

15. Dokažite da svaki beskonačan RE–skup A sadrži beskonačan rekurzivan podskup.
Rješenje. Iz propozicije 1.89. slijedi da postoji rekurzivna (totalna!) funkcija f tako da vrijedi $Im(f) = A$. Definiramo funkciju g na sljedeći način:

$$\begin{aligned} g(0) &= f(0) \\ g(n+1) &= f(\mu y[f(y) > g(n)]) \end{aligned}$$

    Očito je g rekurzivna i rastuća funkcija. Očito je $Im(g) \subseteq A$ i $Im(g)$ je beskonačan skup. Iz prethodnog zadatka slijedi da je $Im(g)$ rekurzivan skup.

16. Neka je $A = \{e \in \mathbb{N} : \text{skup } W_e \text{ sadrži barem dva elementa}\}$. Dokažite da $A \in \Sigma_1^0$, te $A \notin \Pi_1^0$.

17. Dokažite da skup $K = \{e : \ e \notin W_e\}$ nije rekurzivan.
Rješenje. Pretpostavimo da je skup $\mathbb{N} \setminus K$ rekurzivno prebrojiv. Tada iz definicije slijedi da postoji $e \in \mathbb{N}$ tako da vrijedi $W_e = \mathbb{N} \setminus K$. Iz definicije skupa K slijedi da za sve $x \in \mathbb{N}$ vrijedi:

$$x \in W_e \ \text{ ako i samo ako } \ x \notin K \ \text{ ako i samo ako } \ x \notin W_x.$$

Primjenom posljednje ekvivalencije na $x = e$ dobivamo kontradikciju. To znači da skup $\mathbb{N} \setminus K$ nije RE–skup. Iz Postovog teorema slijedi da skup K nije rekurzivan.

18. Dokažite da skup $\{e : \ \text{skup } \ W_e \ \text{ je rekurzivan}\}$ nije rekurzivno prebrojiv.

19. Dokažite da skup $\{e : \ \{e\} \ \text{ je totalna funkcija}\}$ nije RE–skup.

20. Dokažite da postoji prebrojivo mnogo RE–skupova koji nisu rekurzivni.

21. Dokažite da postoji rekurzivan skup A tako da skup $\cap_{x \in A} Dom(\{x\})$ nije rekurzivno prebrojiv.

22. Dokažite da je beskonačan skup A rekurzivno prebrojiv ako i samo ako je skup A slika neke parcijalno rekurzivne funkcije koja je injekcija.
Rješenje. Ako je f parcijalno rekurzivna funkcija, koja je injekcija, tada iz propozicije 1.89. slijedi da je $Im(f)$ rekurzivno prebrojiv skup.

Dokažimo obrat. Neka je A beskonačan RE–skup. Neka je f funkcija kao u dokazu propozicije 1.89. Definiramo funkciju h s:

$$\begin{aligned} h(0) &= 0 \\ h(x+1) &\simeq \mu y\Big((\forall z \le x) f(y) \le f(h(z)) \Big) \end{aligned}$$

Uočite da je funkcija h definirana pomoću povratne rekurzije, pa je parcijalno rekurzivna zbog propozicije 1.49. (Uočite da pomoću funkcije h izdvajamo sve brojeve x_1 i x_2 za koje vrijedi $f(x_1) = f(x_2)$. Točnije: ako za $n \in \mathbb{N}$ označimo $A_n = \{x : f(x) = n\}$, tada je $\min A_n \in Im(h)$.) Uočite, zatim, da ako je f konstantna funkcija tada je $Dom(h) = \{0, 1\}$, tj. općenito funkcija h ne mora biti totalna).

Sada definiramo funkciju g s: $g(x) \simeq f(h(x))$. Očito je funkcija g parcijalno rekurzivna. Provjerite da je g injekcija, te da je $Im(g) = A$.

23. Dokažite ili nađite protuprimjer za sljedeće tvrdnje.

    a) Podskup rekurzivnog skupa je rekurzivan.
    b) Podskup RE–skupa je RE–skup.
    c) Beskonačan RE–skup sadrži beskonačan rekurzivan podskup.
    d) Podskup rekurzivnog skupa je RE–skup.
    e) Ako je A RE–skup, tada je i A^c RE–skup.
    f) Ako je A rekurzivan skup, tada je i A^c rekurzivan.
    g) Ako A nije RE–skup tada A^c može biti konačan.
    h) Neka je I RE–skup, te $\{A_i : i \in I\}$ familija RE–skupova. Tada je $\cup_{i \in I} A_i$ također RE–skup.

Dodatak 1.
Ackermannova funkcija

Neka je funkcija $A : \mathbb{N}^2 \to \mathbb{N}$ definirana s:

$$A(0, y) = y + 1$$

$$A(x + 1, 0) = A(x, 1)$$

$$A(x + 1, y + 1) = A(x, A(x + 1, y))$$

Funkcija A se naziva Ackermannova funkcija. U ovoj točki ćemo dokazati da funkcija A nije primitivno rekurzivna, ali je rekurzivna.

Cilj nam je pokazati da za svaku k-mjesnu primitivno rekurzivnu funkciju F postoji broj C takav da za sve prirodne brojeve $x_1, \ldots, x_k$ vrijedi

$$F(x_1, \ldots, x_k) < A(C, \sum_{i=1}^{k} x_i)$$

To dokazujemo nizom lema i propozicija koje slijede.

Lema 1.91. *Za sve prirodne brojeve x i y vrijedi*

$$y < A(x, y).$$

Dokaz. Dokaz provodimo indukcijom po x. Za $x = 0$ imamo $A(0, y) = y+1 > y$.

Pretpostavimo da tvrdnja vrijedi za neki $x \in \mathbb{N}$ i sve $y \in \mathbb{N}$. Kako bi pokazali da tvrdnja vrijedi za $x + 1$ provodimo indukciju po y. Za $y = 0$ imamo

$$A(x + 1, 0) = A(x, 1) > 1 > 0.$$

Pretpostavimo da za neki y vrijedi $A(x + 1, y) > y$. Iz definicije Ackermannove funkcije slijedi $A(x+1, y+1) = A(x, A(x+1, y))$, a iz pretpostavke indukcije (po x!) imamo $A(x, A(x+1, y)) > A(x+1, y)$, a iz pretpostavke indukcije (po y!) slijedi $A(x+1, y) > y$. Time imamo da je $A(x+1, y+1) > y+1$. $\square$

Lema 1.92. *Za sve prirodne brojeve x i y vrijedi*

$$A(x, y) < A(x, y+1).$$

Dokaz. Ako je $x = 0$ tada po definiciji funkcije A imamo

$$A(0, y+1) = y+2 > y+1 = A(0, y).$$

Ako pak je $x \neq 0$ tada je $A(x, y+1) = A(x-1, A(x, y))$, što je strogo veće od $A(x, y)$ po lemi 1.91. $\square$

Korolar 1.93. *Za sve prirodne brojeve x, y i z vrijedi*

$$A(x, y) < A(x, y+z),$$

tj. funkcija A je strogo rastuća po drugom argumentu.

Lema 1.94. *Za sve prirodne brojeve x i y vrijedi*

$$A(x, y+1) \leq A(x+1, y).$$

Dokaz. Dokaz provodimo indukcijom po y. Za $y = 0$ po definiciji funkcije A imamo $A(x, 1) = A(x+1, 0)$.

Pretpostavimo da tvrdnja vrijedi za neki prirodan broj y, tj. za sve $x \in \mathbb{N}$ imamo $A(x, y+1) \leq A(x+1, y)$. Iz leme 1.91. znamo da vrijedi $y+1 < A(x, y+1)$, a onda iz pretpostavke indukcije slijedi $y+1 < A(x+1, y)$. Iz ovog posljednjeg slijedi $y+2 \leq A(x+1, y)$. Sada iz korolara 1.93. slijedi $A(x, y+2) \leq A(x, A(x+1, y))$. No, iz definicije funkcije A slijedi $A(x, A(x+1, y)) = A(x+1, y+1)$, a onda i tražena tvrdnja $A(x, y+2) \leq A(x+1, y+1)$. $\square$

Lema 1.95. *Za sve prirodne brojeve x i y vrijedi*

$$A(x, y) < A(x+1, y).$$

Dokaz. Iz leme 1.94. slijedi $A(x+1, y) \geq A(x, y+1)$, a iz leme 1.92. znamo da vrijedi $A(x, y+1) > A(x, y)$. $\square$

Lema 1.96. *Za sve prirodne brojeve y vrijedi*

$$A(1, y) = y+2.$$

Dokaz.

$$\begin{aligned} A(1,y) = \quad & A(0, A(1, y-1)) = 1 + A(1, y-1) = \ldots = \\ & y \cdot 1 + A(1,0) = y + A(0,1) = y + 2 \end{aligned}$$

□

Lema 1.97. *Za sve prirodne brojeve y vrijedi*

$$A(2, y) = 2y + 3.$$

Dokaz. Dokaz provodimo indukcijom po y. Za $y = 0$ imamo: $A(2,0) = A(1,1)$, a po prethodnoj lemi 1.96. to je jednako 3 ($3 = 2 \cdot 0 + 3$).

Pretpostavimo da tvrdnja vrijedi za neki prirodan broj y. Tada redom imamo:

$$A(2, y+1) = A(1, A(2, y)) = A(1, 2y + 3),$$

a to je po lemi 1.96. jednako $2y + 3 + 2$, tj. $2(y + 1) + 3$. □

Lema 1.98. *Za svaki prirodan broj r i sve prirodne brojeve $x_1, \ldots, x_r$ postoji prirodan broj x^* takav da za sve prirodne brojeve y vrijedi:*

$$\sum_{i=1}^{r} A(x_i, y) \le A(x^*, y).$$

Dokaz. Dokaz provodimo indukcijom po r. Kada je $r = 1$ tada za traženi broj x^* možemo uzeti x_1.

Pretpostavimo da tvrdnja vrijedi za neki $r \in \mathbb{N}$, tj. za sve $x_1, \ldots, x_r \in \mathbb{N}$ postoji $x^* \in \mathbb{N}$ takav da za sve $y \in \mathbb{N}$ vrijedi

$$\sum_{i=1}^{r} A(x_i, y) \le A(x^*, y).$$

Neka je $x_1, \ldots, x_r, x_{r+1}$ proizvoljan niz prirodnih brojeva. Želimo dokazati da postoji x^{**} takav da za sve $y \in \mathbb{N}$ vrijedi

$$\sum_{i=1}^{r+1} A(x_i, y) \le A(x^{**}, y).$$

Označimo s x veći od brojeva x^* i x_{r+1}. Očito vrijedi

$$\sum_{i=1}^{r+1} A(x_i, y) = \sum_{i=1}^{r} A(x_i, y) + A(x_{r+1}, y),$$

a po pretpostavci indukcije to je manje od $A(x^*, y) + A(x_{r+1}, y)$, tj.

$$\sum_{i=1}^{r+1} A(x_i, y) \leq A(x, y) + A(x, y) = 2A(x, y).$$

Ovo posljednje je očito strogo manje od $2A(x, y)+3$, što je po lemi 1.97. jednako $A(2, A(x, y))$. Iz leme 1.95. znamo da je $A(2, A(x, y)) < A(x+2, A(x, y))$, a onda iz lema 1.92. i 1.95. slijedi da je ovo posljednje strogo manje od $A(x+2, A(x+3, y))$. Pošto je $A(x + 2, A(x + 3, y)) = A(x + 3, y + 1)$, te je po lemi 1.94. $A(x + 3, y + 1)$ manje od $A(x + 4, y)$, konačno imamo

$$\sum_{i=1}^{r+1} A(x_i, y) \leq A(x + 4, y).$$

Dakle, za traženi x^{**} možemo uzeti $x + 4$. □

Propozicija 1.99. *Za svaku inicijalnu funkciju $F \in \{Z, Sc, I_k^n\}$ postoji $C \in \mathbb{N}$ tako da za sve $\vec{x} = (x_1, \ldots, x_n)$ vrijedi*

$$F(\vec{x}) < A(C, \sum_{i=1}^{n} x_i).$$

Dokaz. Za svaku pojedinu vrstu inicijalne funkcije provjeravamo traženu nejednakost.

$$Sc(x) = x + 1 = A(0, x) < A(1, x) \quad \text{(lema 1.95.)}$$

$$Z(x) = 0 < 1 \leq A(0, x)$$

$$I_k^n(x_1, \ldots, x_n) = x_k < \sum_{i=1}^{n} x_i + 1 = A(0, \sum_{i=1}^{n} x_i)$$

□

Propozicija 1.100. *Neka su $G_1, \ldots, G_r$ i H primitivno rekurzivne funkcije, te $C_1, \ldots, C_r$ i C_{r+1} prirodni brojevi tako da za sve $j \in \{1, \ldots, r\}$, te $\vec{x}$ i $\vec{y}$ vrijedi*

$$G_j(\vec{x}) < A(C_j, \sum_{i=1}^{n} x_i) \qquad i \qquad H(\vec{y}) < A(C_{r+1}, \sum_{i=1}^{r} y_i).$$

Zatim, neka je s F označena funkcija koja je definirana pomoću kompozicije funkcija $G_1, \ldots, G_r$ i H, tj. vrijedi $F(\vec{x}) = H(G_1(\vec{x}), \ldots, G_r(\vec{x}))$. Tada postoji $C \in \mathbb{N}$ tako da za sve $\vec{x}$ vrijedi

$$F(\vec{x}) < A(C, \sum_{i=1}^{n} x_i).$$

Dokaz. Iz pretpostavke propozicije i leme 1.92. slijede nejednakosti

$$\begin{aligned} F(\vec{x}) = \quad & H(G_1(\vec{x}), \ldots, G_r(\vec{x})) < A(C_{r+1}, \sum_{j=1}^{r} G_j(\vec{x})) \\ & < A(C_{r+1}, \sum_{j=1}^{r} A(C_j, \textstyle\sum_{i=1}^{n} x_i)) \end{aligned}$$

Iz leme 1.98. slijedi da postoji $x^* \in \mathbb{N}$ tako da vrijedi

$$F(\vec{x}) < A(C_{r+1}, A(x^*, \sum_{i=1}^{n} x_i))$$

Sada imamo (prvo iz lema 1.92. i 1.95.)

$$F(\vec{x}) \leq A(C_{r+1} + x^*, A(C_{r+1} + x^* + 1, \sum_{i=1}^{n} x_i)) = A(C_{r+1} + x^* + 1, \sum_{i=1}^{n} x_i + 1) \leq$$

$$\leq A(C_{r+1} + x^* + 2, \sum_{i=1}^{n} x_i).$$

To znači da za traženi broj C možemo uzeti $C_{r+1} + x^* + 2$. □

Propozicija 1.101. *Neka su G i H primitivno rekurzivne funkcije za koje postoje brojevi C_1 i C_2 takvi da za sve $\vec{x} = (x_1, \ldots, x_n)$ i sve $\vec{y} = (y_1, \ldots, y_{n+2})$ vrijedi*

$$G(\vec{x}) < A(C_1, \sum_{i=1}^{n} x_i) \qquad i \qquad H(\vec{y}) < A(C_2, \sum_{i=1}^{n+2} y_i).$$

Neka je funkcija F definirana primitivnom rekurzijom pomoću funkcija G i H, tj.

$$\begin{aligned} F(0, \vec{x}) &= G(\vec{x}) \\ F(y+1, \vec{x}) &= H(F(y, \vec{x}), y, \vec{x}). \end{aligned}$$

Tada postoji $C \in \mathbb{N}$ takav da za sve $\vec{x} = (x_1, \ldots, x_n)$ i sve $y \in \mathbb{N}$ vrijedi:

$$F(y, \vec{x}) < A(C, \sum_{i=1}^{n} x_i + y).$$

Dokaz. Pokažimo prvo da postoji $C_3 \in \mathbb{N}$ takav da za sve $\vec{x}$ vrijedi

$$G(\vec{x}) + \sum_{i=1}^{n} x_i < A(C_3, \sum_{i=1}^{n} x_i).$$

Primjenom pretpostavke propozicije za funkciju G i propozicije 1.99. na inicijalne funkcije $I_1^n, \ldots, I_n^n$ slijedi

$$G(\vec{x}) + \sum_{i=1}^{n} x_i = G(\vec{x}) + \sum_{i=1}^{n} I_i^n(\vec{x}) < A(C_1, \sum_{i=1}^{n} x_i) + \sum_{i=1}^{n} A(0, \sum_{i=1}^{n} x_i).$$

Sada iz leme 1.98. slijedi egzistencija $C_3 \in \mathbb{N}$ tako da vrijedi

$$A(C_1, \sum_{i=1}^{n} x_i) + \sum_{i=1}^{n} A(0, \sum_{i=1}^{n} x_i) < A(C_3, \sum_{i=1}^{n} x_i).$$

Time imamo

$$G(\vec{x}) + \sum_{i=1}^{n} x_i < A(C_3, \sum_{i=1}^{n} x_i).$$

Analogno, kao što smo upravo dokazali prethodnu tvrdnju, dokazali bi i da postoji $C_4 \in \mathbb{N}$ tako da za sve $\vec{y}$ vrijedi

$$H(\vec{y}) + \sum_{i=1}^{n+2} y_i < A(C_4, \sum_{i=1}^{n+2} y_i).$$

Sada definiramo traženi broj C kao $\max\{C_3, C_4\} + 1$. Indukcijom po y dokazujemo da vrijedi

$$F(y, \vec{x}) + \sum_{i=1}^{n} x_i + y < A(C, \sum_{i=1}^{n} x_i + y).$$

Za $y = 0$ imamo:

$$F(0, \vec{x}) + \sum_{i=1}^{n} x_i + 0 = G(\vec{x}) + \sum_{i=1}^{n} x_i < A(C_3, \sum_{i=1}^{n} x_i) < A(C, \sum_{i=1}^{n} x_i + y)$$

(Posljednje nejednakosti slijede iz prve dokazane pomoćne tvrdnje, odnosno lema 1.92. i 1.95.)

Pretpostavimo da za neki $y \in \mathbb{N}$ i sve $\vec{x}$ vrijedi:

$$F(y, \vec{x}) + \sum_{i=1}^{n} x_i + y < A(C, \sum_{i=1}^{n} x_i + y).$$

Tada vrijedi:

$$F(y+1,\vec{x}) + \sum_{i=1}^{n} x_i + y + 1 = H(F(y,\vec{x}), y, \vec{x}) + \sum_{i=1}^{n} x_i + y + 1 \leq$$

$$H(F(y,\vec{x}), y, \vec{x}) + F(y,\vec{x}) + \sum_{i=1}^{n} x_i + y + 1 <$$

$$A(C_4, F(y,\vec{x}) + \sum_{i=1}^{n} x_i + y) + 1 <$$

$$A(C_4, A(C, \sum_{i=1}^{n} x_i + y)) + 1 \leq A(C-1, A(C, \sum_{i=1}^{n} x_i + y)) + 1 \leq$$

$$A(C, \sum_{i=1}^{n} x_i + y + 1) + 1,$$

pa je očito

$$F(y+1,\vec{x}) + \sum_{i=1}^{n} x_i + y + 1 < A(C, \sum_{i=1}^{n} x_i + y + 1).$$

Iz upravo dokazane tvrdnje slijedi odmah tražena tvrdnja propozicije. □

Teorem 1.102. *Za svaku primitivno rekurzivnu funkciju F postoji $C \in \mathbb{N}$ tako da za sve $\vec{x} = (x_1, \ldots, x_n)$ vrijedi*

$$F(\vec{x}) < A(C, \sum_{i=1}^{n} x_i).$$

Dokaz. Za niz funkcija $f_1, \ldots, f_k$ kažemo da je definicioni ako je svaka funkcija f_i ili inicijalna ili je nastala iz prethodnih pomoću primitivne rekurzije, odnosno kompozicije. (Za svaku primitivnu rekurzivnu funkciju postoji definicioni niz). Za definicioni niz $f_1, \ldots, f_k$ prirodan broj k nazivamo duljina niza. Indukcijom po k dokazujemo da za svaki definicioni niz $f_1, \ldots, f_k$ postoji broj C_k takav da za sve $\vec{x}$ vrijedi $f_k(\vec{x}) < A(C_k, \sum_{i=1}^{n} n_i)$. Uočite da iz toga odmah slijedi tražena tvrdnja teorema.

Ako je duljina definicionog niza jednaka jedan, tada taj niz sadrži samo neku inicijalnu funkciju. No, tada tražena tvrdnja slijedi iz propozicije 1.99.

Pretpostavimo da tvrdnja vrijedi za neki $k \in \mathbb{N}$. Neka je $f_1, \dots, f_k, f_{k+1}$ neki definicioni niz. Promatramo tri slučaja obzirom na način pojavljivanja funkcije f_{k+1} u nizu.

a) Funkcija f_{k+1} je inicijalna. Tada tražena tvrdnja slijedi iz propozicije 1.99.

b) Funkcija f_{k+1} je definirana pomoću kompozicije iz funkcija $f_{i_1}, \dots, f_{i_m}$, $f_{i_{m+1}}$, tj. vrijedi

$$f_{k+1}(\vec{x}) = f_{i_{m+1}}(f_{i_1}(\vec{x}), \dots, f_{i_m}(\vec{x}))$$

(gdje su $i_1, \dots, i_m, i_{m+1} \in \{1, \dots, k\}$). Primjenom pretpostavke indukcije na funkcije $f_{i_1}, \dots, f_{i_m}$, $f_{i_{m+1}}$ i propozicije 1.100. slijedi tražena tvrdnja.

c) Funkcija f_{k+1} je definirana pomoću primitivne rekurzije iz nekih funkcija f_i i f_j, gdje su $i, j \leq k$. Tada za sve $\vec{x}$ vrijedi

$$\begin{aligned} f_{k+1}(0, \vec{x}) &= f_i(\vec{x}) \\ f_{k+1}(y+1, \vec{x}) &= f_j(f_{k+1}(y, \vec{x}), y, \vec{x}). \end{aligned}$$

Primjenom prepostavke indukcije na funkcije f_i i f_j, te propozicije 1.101. slijedi tražena tvrdnja.

□

Korolar 1.103. *Ackermannova funkcija nije primitivno rekurzivna.*

Dokaz. Pretpostavimo suprotno, tj. da je funkcija A primitivno rekurzivna. Neka je funkcija $A' : \mathbb{N} \to \mathbb{N}$ definirana s $A'(x) = A(x, x)$. Pošto smo pretpostavili da je funkcija A primitivno rekurzivna, tada je očito i funkcija A' primitivno rekurzivna. Iz prethodnog teorema slijedi da postoji $C \in \mathbb{N}$ tako da za sve $x \in \mathbb{N}$ vrijedi $A'(x) < A(C, x)$. No, tada posebno za $x = C$ imamo

$$A(C, C) = A'(C) < A(C, C),$$

što je nemoguće. □

Teorem 1.104. *Ackermannova funkcija je rekurzivna.*

Dokaz. Definicije i dokazi rekurzivnosti relacije Seq i funkcija lh i $()_i$ su dani u točki 1.4

U svrhu dokaza teorema definiramo jednomjesnu relaciju Adv (relacija adekvatnosti) koja "prepoznaje" brojeve koji kodiraju konačne trojke $(x, y, z) \in \mathbb{N}^3$ za koje vrijedi $z = A(x, y)$. Kako bi pokazali da je relacija Adv rekurzivna pišemo sljedeću ekvivalenciju:

$$
\begin{aligned}
&Adv(v) \Leftrightarrow \\
&(\forall i < lh(v)) \Bigg[\bigg((\exists y < v)\ (\exists z < v)\ \Big((v)_i = \langle 0, y, z\rangle \ \to\ z = y + 1\Big)\bigg) \vee \\
&\bigg((\exists x < v)\ (\exists z < v)\ \Big((v)_i = \langle x+1, 0, z\rangle \ \to\ \Big((\exists j < lh(v))\ \langle x, 1, z\rangle = (v)_j\Big)\Big)\bigg) \vee \\
&\bigg((\exists x < v)\ (\exists y < v)\ (\exists z < v)\ \Big((v)_i = \langle x+1, y+1, z\rangle \ \to \\
&\qquad (\exists w < v)\ \Big(\Big((\exists j < lh(v))\ \langle x+1, y, w\rangle = (v)_j\Big) \wedge \\
&\qquad (\exists k < lh(v))\Big(\langle x, w, z\rangle = (v)_k\Big)\Big)\Big)\bigg)\Bigg] \ \wedge\ Seq(v)
\end{aligned}
$$

Iz dane ekvivalencije očito slijedi da je relacija Adv rekurzivna. Primijetimo da vrijedi:

$$\forall x \forall y \forall z \Bigg[\forall v \Bigg(\bigg((\exists i < lh(v))\langle x, y, z\rangle = (v)_i\bigg) \ \wedge\ Adv(v)\Bigg) \ \to\ z = A(x, y)\Bigg].$$

Neka je funkcija f definirana sa:

$$f(x, y) = \mu v \Bigg(Adv(v) \ \wedge\ \bigg((\exists z < v)(\exists i < lh(v))\langle x, y, z\rangle = (v)_i\bigg)\Bigg)$$

Očito je funkcija f rekurzivna, te vrijedi

$$A(x, y) = \mu z \Bigg((\exists i < lh(f(x, y))\ \langle x, y, z\rangle = \Big(f(x, y)\Big)_i\Bigg),$$

iz čega slijedi da je Ackermannova funkcija A rekurzivna. $\square$

Indeks

Bibliografija

[1] K. J. Barwise (ed.), *Handbook of Mathematical Logic, III,* North-Holland, Amsterdam, 1977.

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

[3] M. Davis, *Computability and Unsolvability*, Dover Publications, Inc., New York, 1982.

[4] M. Davis, *Hilbert's Tenth Problem is Unsolvable*, The American Mathematical Monthly, 80 (1973), 233-269

[5] S. Homer, A. L. Selman, *Computability and Complexity Theory*, Springer–Verlag, 2001.

[6] Yu. I. Manin, *A Course in Mathematical Logic*, Springer–Verlag, 1977.

[7] A. B. Manaster, *Completeness, compactness and undecidability: an introduction to mathematical logic*, Prentice–Hall, Inc., New Jersey, 1975.

[8] E. Mendelson, *Introduction to Mathematical Logic*, D. van Nostrand Company, Inc. Princeton, 1997.

[9] Ž. Mijajlović, Z. Marković, K. Došen, *Hilbertovi problemi i logika*, Beograd, 1986.

[10] P. Odifreddi, *Classical Recursion Theory*, North-Holland, 1987.

[11] P. G. Odifreddi, *Classical Recursion Theory, Volume II*, Elsevier, 1999.

[12] C. H. Papadimitriou, *Computational Complexity*, Addison–Wesley, 1994.

[13] R. Péter, *Recursive functions*, Akadémiai Kiadó, Budapest, 1967.

[14] H. Rogers Jr., *Theory of Recursive Functions and Effective Computability*, McGraw-Hill Book Company, 1967.

[15] J. R. Shoenfield, *Recursion Theory,* Springer-Verlag, 1993.

[16] M. Sipser, *Introduction to the Theory of Computation*, PWS Publishing Company, 1996.

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

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

[19] A. Yasuhara, *Recursive function theory and logic*, Academic Press, New York, 1971.