Hilbertov 10. problem

Murtezani, Karlo

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Karlo Murtezani

HILBERTOV 10. PROBLEM

Diplomski rad

Voditelj rada:
prof. dr. sc. Filip Najman

Zagreb, rujan, 2021.

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

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

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

Zahvaljujem svom mentoru prof. dr. sc. Filipu Najmanu
na pomoći i vodstvu diplomskoga rada te
posvećujem rad svima onima koji su mi pomogli da
se i ostvari, a posebno
Helena,
Sarah,
Blaž,
Hvala vam!

Sadržaj

Uvod

Godine 1900. održan je Drugi međunarodni kongres na pariškom sveučilištu Sorbonne u kojem je njemački matematičar David Hilbert, profesor na Sveučilištu u Göttingenu, iznio deset matematičkih problema. Originalnoj listi dodao je još nekoliko problema te je dvije godine poslije iznio ukupno 23 problema koji su utjecali na daljnje razvijanje mnogih grana matematike u 20. stoljeću. U ovom radu analizirat ćemo postupan dolazak do rješenja desetog problema kroz potrebne alate iz teorije izračunljivosti, teorije brojeva te matematičke logike s posebnim naglaskom na rad Yurija Matijaseviča "Hilbertov deseti problem" iz 1993. godine [11].

Hilbertov deseti problem glasi: "Za diofantsku jednadžbu s proizvoljnim brojem nepoznanica i s cjelobrojnim koeficijentima pronađi proces na osnovu kojeg se u konačnom broju koraka može odrediti ima li zadana jednadžba cjelobrojno rješenje" [6, str. 458]. Konačno je dokazan tek 70 godina poslije Matijasevičevim teoremom.

Hilbert ukazuje da se ponekad dogodi da problem rješavamo pod nedovoljnim pretpostavkama ili da tražimo rješenje iz pogrešne perspektive, i iz tog razloga ne uspijemo. Tada se nameće pitanje može li se pokazati da je problem nemoguće riješiti pod danim okolnostima ili iz promatrane perspektive [6, str. 444]. Hilbertov deseti problem bio je osmisliti algoritam takav da odredi ima li jednadžba cjelobrojno rješenje. Nije koristio izraz algoritam nego proces koji u konačnom broju operacija odlučuje rješivost problema. Koristeći izraz "osmisliti" Hilbertov problem pretpostavlja da takav algoritam postoji te ga samo treba pronaći. Dokazano je da takav algoritam ne postoji, ali matematičarima u tom razdoblju i dotadašnjim intuitivnim konceptom algoritma bio je onemogućen dolazak do takvog zaključka [20, str. 183]. Veza između neformalnog pojma algoritma i precizne definicije koje su uveli Alan Turing upotrebom matematičkih strojeva i Alonzo Church upotrebom λ-računa naziva se Church-Turingovom tezom te je omogućeno ustanoviti algoritamsku nerješivost, odnosno nepostojanje algoritma s određenim svojstvima.

Za neke probleme postoje algoritmi koji ih rješavaju, a za neke ne. Dokazivanje da za neki problem ne postoji algoritam koji ga rješava korisno je jer daje naslutiti da je potrebno pojednostavljenje ili izmjena početnoga problema. Sipser kaže da je još jedan razlog za dokazivanje kulturološki te doprinosi važnoj perspektivi u računarstvu [20, str. 193]. Problem odluke zahtijeva pronalazak jedinstvene metode koja će dati odgovor na bilo koji zasebni

potproblem. Mnogi su teoretičari brojeva pronašli rješenja za razne diofantske jednadžbe ili ustanovili nerješivost, ali za mnoge klase jednadžbi ili čak i jedinstvene jednadžbe potrebna je posebna metoda. U Desetom problemu eksplicitno se traži univerzalna metoda koja će odlučiti rješivost diofantske jednadžbe [11, str. 2]. Da bi se ustanovila nerješivost problema odluke potrebno ga je svesti na nerješiv problem koji je već dokazan. Dokazivanje Hilbertovog desetog problema zapravo je uzastopno svođenje na složenije probleme te je cilj doći do problema koji će dati dokaz nerješivosti. Tek nakon što su se ustanovili općeniti pojmovi izračunljivosti omogućene su provjere svih metoda potrebne za takvo svođenje problema.

Sam dokaz zajednički je rad Julije Robinson, Hilary Putnam, Yurija Matijaseviča te Martina Davisa koji su kroz 21 godinu pokušali doći do rješenja, ali temelji se na radovima i ostalih matematičara koji su desetljećima poslije Hilberta proširivali teorije potrebne za dokaz Problema. Emil Leon Post u svom govoru u Američkom matematičkom društvu 1944. propituje postojanje rekurzivnog prebrojivog skupa čija je nerješivost, odnosno Turingov stupanj, manja od problema zaustavljanja, a dao je i naslutiti da Hilbertov deseti problem zahtijeva dokaz da je nerješiv [16, str. 289]. Martin Davis pokazuje da diofantski skupovi nisu zatvoreni na komplement poput rekurzivno prebrojivih skupova te daje slutnju da su te dvije klase jednake, što bi značilo da Hilbertov deseti problem nije rješiv [4, str. 38]. Također je u svojoj doktorskoj disertaciji pokazao da se svaki rekurzivno prebrojiv skup može zapisati u obliku koji danas nazivamo Davisova normalna forma. Davis, Putnam i Robinson dokazuju da je rekurzivno prebrojiv skup ujedno i eksponencijalno diofantski [5, str. 425]. Preostalo je pokazati da je eksponencijalna funkcija diofantska, što je upravo Yuri Matijasevič 1970. uspio dokazati koristeći Fibonaccijeve brojeve.

Diplomski rad napravljen je u sklopu aktivnosti Projekta KK.01.1.1.01.0004 - Znanstveni centar izvrsnosti za kvantne i kompleksne sustave te reprezentacije Liejevih algebri.

Poglavlje 1

Pojmovi iz teorije izračunljivosti

U ovom poglavlju upoznat ćemo se s osnovnim pojmovima iz teorije izračunljivosti koji su nam potrebni za razumijevanje samog Problema. Teorija izračunljivosti grana je teorije računanja i matematičke logike koja proučava probleme koji su računski rješivi koristeći različite modele računanja te nastaje tek 1930-ih.

Problemi odluke općenito se pojavljuju u matematičkim pitanjima odlučivosti, odnosno pitanjima postojanja uspješne metode za određivanje pripadnosti nekom skupu. Problem odluke sastoji se od individualnih problema koji svaki od njih daje odgovor "DA" ili "NE", a svaki taj individualni problem nazivamo potproblem. Hilbertov deseti problem primjer je problema odluke i Hilbert je u njemu zatražio univerzalnu metodu za odlučivanje rješivosti diofantskih jednadžbi. Problemi odluke mogu se riješiti izravno tako da se daje postupak pronalaska odgovora na individualni potproblem ili neizravno tako da se problem svodi na neki drugi za koji je već pokazana rješivost. Dokaz nerješivosti za problem odluke također može biti izravan ili neizravan. Neizravno se također svodi na neki drugi, ali se zahtijeva i svođenje u obrnutom smjeru. Da bismo ustanovili nerješivost problema odluke, potrebno je svesti problem na neki drugi problem čija je nerješivost već pokazana. Cilj nam je postupno svoditi složenije probleme na Hilbertov deseti problem. Taj niz svođenja vodi nas problemu za koji možemo dati dokaz nerješivosti. Navest ćemo osnovne definicije iz teorije izračunljivosti koje su zapisane u [7, str. 3]:

Definicija 1.1. *Za podskup $S \subseteq \mathbb{N}$ kažemo da je rekurzivan ako postoji algoritam koji prihvaća prirodan broj n i nakon konačno mnogo koraka staje i ispisuje istinitu vrijednost tvrdnje $n \in S$.*

Definicija 1.2. *Za podskup $S \subseteq \mathbb{N}$ kažemo da je rekurzivno prebrojiv (poluodlučiv) ako postoji algoritam koji prihvaća prirodan broj n i ako staje nakon konačno koraka i potvrđuje da je $n \in S$. Algoritam ne treba jamčiti da će stati za $n \notin S$, ali ne smije dati netočne odgovore.*

Iz toga također možemo zaključiti da su svi rekurzivni skupovi ujedno i rekurzivno prebrojivi, ali obrnuta implikacija ne vrijedi. Naime, rekurzivno prebrojivi skupovi ne moraju stati ako ulaz nije u rješenju skupa S.

Da bismo definirali funkcije koje su izračunljive, dotaknut ćemo se pojma RAM-stroja. RAM-stroj model je računanja čija je memorija neograničen niz registara takav da svaki može sadržavati cijeli broj. U ovom modelu dopuštene su aritmetičke operacije za računanje adrese registra memorije [1]. RAM-stroj matematički je stroj koji se sastoji od fiksnog konačnog niza instrukcija, registara i programskog brojača. Sadržaj registara mijenja se ovisno o instrukcijama, a programski se brojač povećava za 1 svakom sljedećom instrukcijom, osim ako sama instrukcija ne zahtijeva promjenu. Za funkciju ćemo reći da je računa neki RAM-stroj ako za svaki $(x_1, ..., x_n)$ iz domene funkcije, stroj započinje tako da je u nultom registru zapisana 0, a u ostalim redom vrijednosti $x_1, ..., x_n$, a završava tako da je u nultom registru zapisana vrijednost $f(x_1, ..., x_n)$.

Definicija 1.3. *Funkcija je izračunljiva ako postoji RAM-algoritam koji je računa.*

Definicija 1.4. *Za relaciju kažemo da je rekurzivno prebrojiva ako postoji izračunljiva funkcija čija je domena jednaka toj relaciji.*

U ovom dijelu promatrat ćemo klasu funkcija koje su izračunljive, odnosno opisat ćemo nekoliko osnovnih funkcija koje su intuitivno izračunljive te neke operacije koje čuvaju izračunljivost. Osnovne primitivno rekurzivne funkcije su nulfunkcija C_0, sljedbenik S te funkcije projekcije P_i definirane redom u [14, str. 82]:

$$\begin{aligned} &C_0(x) = 0, \\ &S(x) = x + 1, \\ &P_i(x_1, ..., x_n) = x_i, \text{ za svaki } i \in \{1, ..., n\}. \end{aligned}$$

Preostale primitivno rekurzivne funkcije mogu se dobiti uzastopnom primjenom operacija kompozicije ili primitivne rekurzije. Kompozicija funkcije $f(t_1, ..., t_m)$ s funkcijama $g_1(x_1, ..., x_n), ..., g_m(x_1, ..., x_n))$ dana je funkcijom

$$h(x_1, ..., x_n) = f(g_1(x_1, , , ., x_n), ..., g_m(x_1, ..., x_n)).$$

S druge strane, za dane funkcije $f(x_1, ..., x_n)$ i $g(t_1, ..., t_{n+2})$ primitivna rekurzija daje funkciju $h(x_1, ..., x_n, z)$ koja zadovoljava:

$$\begin{aligned} h(x_1, ..., x_n, 0) &= f(x_1, ..., x_n), \\ h(x_1, ..., x_n, y + 1) &= g(x_1, ..., x_n, t, h(x_1, ..., x_n, y)). \end{aligned}$$

Primjer 1.5. *Pokazat ćemo da je zbrajanje primitivno rekurzivna funkcija [23, str. 4]. Trebamo konstruirati funkciju $f(x, y) = x + y$ pravilima koje smo opisali. Neka je*

$$f(x, 0) = P_1(x, 0) = x.$$

Sada možemo iskoristiti primitivnu rekurziju da bismo izračunali $f(x, y + 1)$:

$$f(x, y + 1) = g(x, y, f(x, y)) = S(f(x, y)).$$

Moguće je pokazati da su sve primitivno rekurzivne funkcije izračunljive, ali obrat ne vrijedi. Protuprimjer je dao Hilbertov učenik Wilhelm Ackermann 1928. godine te glasi

$$Ack(m, n) = \begin{cases} n + 1, & m = 0 \\ Ack(m - 1, 1), & m > 0 \text{ i } n = 0 \\ Ack(m - 1, Ack(m, n - 1)), & m > 0 \text{ i } n > 0 \end{cases}.$$

Iako ova funkcija brzo raste, ona je izračunljiva, ali zbog prebrzog rasta ipak nije primitivno rekurzivna [14, p. 86]. Uvođenjem nove operacije koju je formalizirao Stephen Cole Kleene te uz operacije kompozicije i primitivne rekurzije dobijemo rekurzivne funkcije [9, str. 279]. Za funkciju $f(z, x_1, ..., x_n)$ minimizacija daje parcijalnu funkciju

$$h(x_1, ..., x_n) = \min_z \{f(z, x_1, ..., x_n) = 0\}.$$

Ako ne postoji takav z, tada h nije definirana. Time dolazimo do izjednačavanja izračunljivih funkcija s rekurzivnima te za Ackermannovu funkciju koja je izračunljiva, možemo reći da je i rekurzivna.

Poglavlje 2

Diofantske jednadžbe

Nakon uvoda u teoriju izračunljivosti te opisa problema odluke, u ovom poglavlju definirat ćemo diofantske jednadžbe te proširiti teoriju potrebnu za dokaz Problema.

Diofantske jednadžbe algebarske su jednadžbe s više nepoznanica čiji su koeficijenti cjelobrojni, a rješenja su u skupu $\mathbb{Z}$ ili $\mathbb{Q}$ te su jedno od glavnih područja zanimanja teorije brojeva. Posebnu važnost dajemo Fermatu koji je oko 1637. zaključio da diofantska jednadžba $x^n + y^n = z^n$ za $n \geq 3$ nema netrivijalnih rješenja, odnosno rješenja za koje ne vrijedi $xyz = 0$. S druge strane, za $n = 2$ rješenja iste jednadžbe ima beskonačno mnogo te ih zovemo Pitagorinim trojkama. Taj zaključak nazivamo Velikim Fermatovim teoremom, a dokazao ga je Andrew Wiles tek 1994. godine u [22]. Jednadžbe su dobile ime po Diofantu iz Aleksandrije koji je prvi prihvatio razlomke kao brojeve te je tim dopustio da pozitivni racionalni brojevi budu koeficijenti i rješenja jednadžbi [3, str. 257].

Definicija 2.1. *Diofantska jednadžba je jednadžba oblika* $D(x_1, ..., x_m) = 0$ *gdje* D *predstavlja polinom s cjelobrojnim koeficijentima.*

Primjer 2.2. *Prikazat ćemo jednostavan primjer diofantske jednadžbe*

$$2x + 3y - 7 = 0.$$

Vidimo da je jedno od rješenja jednadžbe sigurno $x = 2$ *i* $y = 1$*, ali budući da tražimo rješenja koja su cjelobrojna možemo ih pronaći beskonačno mnogo. Rješenja možemo zapisati kao*

$$x = 2 + 3t,$$
$$y = 1 - 2t,$$

gdje je $t \in \mathbb{Z}$*.*

2.1 Sustavi Diofantskih jednadžbi

Pozitivno rješenje Hilbertova desetog problema, odnosno da za bilo koju diofantsku jednadžbu možemo odrediti da ima cjelobrojno rješenje, povlačilo bi da to možemo odrediti i za sustav diofantskih jednadžbi. Prikažimo primjer sustava diofantskih jednadžbi:

Primjer 2.3. *Promotrimo sljedeći sustav diofantskih jednadžbi:*

$$\begin{aligned} 6w + 2x^2 - y^3 &= 0, \\ 5xy - z^2 + 6 &= 0, \\ w^2 - w + 2x - y + z - 1 &= 0. \end{aligned}$$

Želimo provjeriti ima li ovaj sustav cjelobrojna rješenja. Iz prve jednadžbe možemo vidjeti da je y paran broj, a iz druge da je z također paran broj. Budući da znamo da je $w^2 - w = w(w-1)$ *paran za bilo koji* $w \in \mathbb{Z}$*, treća jednadžba daje kontradikciju pa možemo reći da taj diofantski sustav nema rješenje.*

Propozicija 2.4. *Sustav koji se sastoji od k jednadžbi*

$$\begin{aligned} D_1(x_1, ..., x_m) &= 0, \\ &\vdots \\ D_k(x_1, ..., x_m) &= 0, \end{aligned}$$

ima rješenje kao niz cijelih brojeva $x_1, ..., x_m$ *ako i samo ako i diofantska jednadžba*

$$D_1^2(x_1, ..., x_m) + \cdots + D_k^2(x_1, ..., x_m) = 0 \tag{2.1}$$

ima rješenje. Štoviše, skup rješenja isti je kod sustava te diofantske jednadžbe.

Zbog toga za sustave diofantskih jednadžbi broj jednadžbi nije bitno svojstvo kao u slučaju linearnih algebarskih ili diferencijalnih jednadžbi. Dalje ćemo iskoristiti transformaciju u obrnutom smjeru, odnosno transformaciju jednadžbe

$$D(x_1, ..., x_m) = 0 \tag{2.2}$$

u sustav diofantskih jednadžbi

$$D_1(x_1, ..., x_m, y_1, ..., y_n) = 0, \tag{2.3}$$

$$\vdots$$

$$D_k(x_1, ..., x_m, y_1, ..., y_n) = 0,$$

koje općenito imaju dodatne nepoznanice $y_1, ..., y_n$. Ako svedemo sustav jednadžbi (2.3) na jednu jednadžbu (2.2) na način koji smo opisali u (2.1), ne bismo dobili početnu jednadžbu. Zanima nas zapravo da sustav ima rješenje ako i samo ako početna jednadžba ima. Ne zahtijevamo da se svako rješenje jednadžbe može proširiti do rješenja sustava kao ni obrnuto.

Primjer 2.5. *Transformirat ćemo diofantsku jednadžbu u ekvivalentni sustav jednadžbi oblika $\alpha = \beta + \gamma$ i $\alpha = \beta\gamma$ i zatim sažeti u jednu jednadžbu. Neka je početna diofantska jednadžba:*

$$3xy + 2x^4z - 5yz + 2y = 0.$$

Uvest ćemo nove nepoznanice i dobiti novi sustav:

$$\begin{aligned} p_1 &= 3x, & p_2 &= p_1y, \\ q_1 &= 2x, & q_2 &= q_1x, \\ q_3 &= q_2x, & q_4 &= q_3x, \\ q_5 &= q_4z, & r_1 &= 5y, \\ r_2 &= r_1z, & s_1 &= 2y, \\ t_1 &= p_2 + q_4 + s_1, & & \\ t_1 &= r_2. & & \end{aligned}$$

Sada iz sustava možemo dobiti jednadžbu koja je opisana u (2.1):

$$\begin{aligned} (p_1 - 3x)^2 + (p_2 - p_1y)^2 + (q_1 - 2x)^2 + (q_2 - q_1x)^2 + (q_3 - q_2x)^2 + \\ (q_4 - q_3x)^2 + (q_5 - q_4z)^2 + (r_1 - 5y)^2 + (r_2 - r_1z)^2 + \\ (s_1 - 2y)^2 + (t_1 - p_2 - q_4 - s_1)^2 + (t_1 - r_2)^2 = 0. \end{aligned}$$

Očito početna jednadžba ima rješenje ako ga i dobivena jednadžba ima, ali posljednja je jednadžba stupnja 4.

Istim postupkom možemo bilo koju diofantsku jednadžbu, uvodeći nove nepoznanice, svesti na diofantsku jednadžbu koja je najviše stupnja 4 te će ona imati rješenja ako i samo ako početna jednadžba ima rješenja.

Propozicija 2.6. *Za pozitivan odgovor na Hilbertov deseti problem dovoljno je pronaći metodu za odlučivanje je li diofantska jednadžba stupnja 4 ima rješenje.*

2.2 Familije diofantskih jednadžbi

Definicija 2.7. *Kažemo da je relacija oblika*

$$D(a_1, ..., a_n, x_1, ..., x_m) = 0$$

familija diofantskih jednadžbi gdje je D polinom s cjelobrojnim koeficijentima i varijablama $a_1, ..., a_n, x_1, ..., x_m$ podijeljenim u parametre $a_1, ..., a_n$ i nepoznanice $x_1, ..., x_m$.

Fiksiranjem vrijednosti parametara dobivamo diofantske jednadžbe koje čine familiju. Familija diofantskih jednadžbi nije beskonačan sustav jednadžbi jer nepoznanice ne trebaju zadovoljiti sve jednadžbe istovremeno kao što bi bio slučaj kod sustava jednadžbi. Familije diofantskih jednadžbi također se nazivaju i parametarskim jednadžbama. Za parametarske diofantske jednadžbe razlikujemo stupanj jednadžbe s obzirom na broj njenih nepoznanica od stupnja jednadžbe s obzirom na sve njene varijable. Za različite vrijednosti parametara mogu se dobiti jednadžbe koje imaju rješenje kao i jednadžbe koje nemaju.

Definicija 2.8. *Parametarska diofantska jednadžba definira skup $\mathfrak{M}$ koji se sastoji od n-torki vrijednosti parametara $a_1, ..., a_n$ za koje postoje vrijednosti nepoznanica $x_1, ..., x_m$ koje zadovoljavaju gornju relaciju:*

$$(a_1, ..., a_n) \in \mathfrak{M} \iff \exists x_1, ..., x_m [D(a_1, ..., a_n, x_1, ..., x_m) = 0].$$

Dimenzija skupa $\mathfrak{M}$ je n, a gornja ekvivalencija zove se diofantska reprezentacija skupa $\mathfrak{M}$. Skupovi koji imaju diofantsku reprezentaciju također se nazivaju diofantskima. Očito svaki diofantski skup ima beskonačno mnogo diofantskih reprezentacija.

Primjer 2.9. *Uzmimo diofantsku jednadžbu s parametrom*

$$x^2 - d(y + 1)^2 = 1$$

gdje su x i y nepoznanice te $d \in \mathbb{N}_0$ parametar. Takva jednadžba ima rješenje za x i y točno kada je $d = 0$ ili d nije potpuni kvadrat. Takva jednadžba daje diofansku definiciju skupa

$$\{0, 2, 3, 5, 6, 7, 8, 10, ...\}.$$

Ustanovimo nekoliko najjednostavnijih svojstava diofantskog skupa.

Propozicija 2.10. *Unija dvaju diofantskih skupova iste dimenzije je također diofantska.*

Dokaz: Neka su

$$D_1(a_1, ..., a_n, x_1, ...x_{m_1}) = 0$$

i

$$D_2(a_1, ..., a_n, x_1, ..., x_{m_2}) = 0$$

diofantske reprezentacije dvaju skupova, tada je jednadžba

$$D_1(a_1, ..., a_n, x_1, ..., x_{m_1}) \cdot D_2(a_1, ..., a_n, x_1, ..., x_{m_2}) = 0$$

diofantska reprezentacija njihove unije. □

Propozicija 2.11. *Presjek dvaju skupova iste dimenzije također je diofantski.*

Presjek je definiran jednadžbom:

$$D_1^2(a_1, ..., a_n, x_1, ..., x_{m_1}) + D_2^2(a_1, ..., a_n, x_1, ..., x_{m_2}) = 0.$$

Propozicija 2.12. *Komplement diofantskog skupa n-torki prirodnih brojeva ne mora nužno biti diofantski.*

Dokaz nije trivijalan te ćemo ga dokazati poslije.

Propozicija 2.13. *Skup prirodnih brojeva je diofantski ako i samo ako je to skup nenegativnih rješenja polinoma s cjelobrojnim koeficijentima.*

Da bismo pojednostavnili korištenje diofantskih skupova i termina, definirat ćemo svojstva, relacije i funkcije vezane za diofantske skupove.

Definicija 2.14. *Kažemo da je svojstvo $\mathcal{P}$ prirodnih brojeva diofantsko svojstvo ako je skup brojeva s tim svojstvom diofantski. Ekvivalencija oblika*

$$\mathcal{P}(a) \iff \exists x_1, ..., x_m[D(a, x_1, ..., x_m) = 0]$$

zove se diofantska reprezentacija svojstva $\mathcal{P}$.

Pogledajmo primjer svojstva parnosti broja za koje možemo napisati diofantsku reprezentaciju kao

$$\text{Paran}(a) \iff \exists x[2x = a].$$

Definicija 2.15. *Relacija $\mathcal{R}$ između n prirodnih brojeva zove se diofantska relacija ako je skup svih n-torki za koje relacija vrijedi diofantski. Ekvivalentnost oblika*

$$\mathcal{R}(a_1, ..., a_n) \iff \exists x_1 ... x_m[D(a_1, ..., a_n, d_1, ..., x_m) = 0]$$

zove se diofantska reprezentacija relacije $\mathcal{R}$.

Možemo pokazati da je relacija djeljivosti također diofantska:

$$a \mid b \iff \exists x[ax = b].$$

Definicija 2.16. *Za funkciju kažemo da je diofantska ako je njen graf diofantski skup. Diofantska reprezentacija funkcije F je ekvivalencija oblika*

$$a = F(b_1, ..., b_n) \iff \exists x_1 ... x_m[D(a, b_1, ..., b_n, x_1, ..., x_m) = 0]$$

gdje je D polinom s cjelobrojnim koeficijentima.

Sada možemo definirati funkciju koja daje ostatak:

$$a = rem(b, c) \iff a < c \wedge c \mid b - a,$$

ali je potrebno još i napisati diofantsku reprezentaciju relacije $<$:

$$a < b \iff \exists x[a + x = b].$$

Pokazat ćemo još da je funkcija $arem(b, c)$ čija je vrijednost najmanja apsolutna vrijednost kongruentna b modulo c. Ta funkcije će biti od važnosti u sljedećem poglavlju te ju možemo prikazati kao

$$a = arem(b, c) \iff 2a \leq c \wedge [c \mid (b - a) \vee c \mid (b + a)].$$

2.3 Prirodni brojevi kao rješenja diofantskih jednadžbi

Ako dopustimo da su rješenja diofantskih jednadžbi cijeli brojevi, možemo vidjeti da postoje diofantske jednadžbe čija su rješenja isključivo negativni brojevi. Restrikcijom rješenja samo na prirodne brojeve za te iste jednadžbe ispostavlja se da nemaju rješenja što čini dva različita problema odluke ovisno o rješenjima koje tražimo. Pokazat ćemo da se problem odluke egzistencije nenegativnih rješenja svodi na problem odluke egzistencije cjelobrojnih rješenja. Dalje, ustanovit ćemo nerješivost analognog Hilbertovog desetog problema s prirodnim brojevima koji uključuju 0, ali prije toga ćemo ustinu pokazati da se ne može dogoditi da ako je analogni problem rješiv, a originalni nerješiv. Neka je

$$D(\chi_1, ..., \chi_m) = 0$$

proizvoljna diofantska jednadžba te tražimo rješenja u u cijelim brojevima $\chi_1, ..., \chi_m$. Provjerimo sada jednadžbu

$$D(x_1 - y_1, ..., x_m - y_m) = 0.$$

Očito svako rješenje jednadžbe generira rješenje $\chi_i = x_i - y_i$ za $i = 1, ..., m$. S druge se strane mogu za svako rješenje prve jednadžbe naći prirodni brojevi $x_1, ..., x_m, y_1, ..., y_m$ koji daju rješenje druge jednadžbe.

Poglavlje 3

Funkcija potenciranja

U ovom poglavlju cilj nam je pokazati da je funkcija potenciranja diofantska. Istraživanje klase diofantskih skupova bilo je povezano s pretpostavkom Alfreda Tarskog da skup svih potencija broja 2 nije diofantski [12, str. 4]. U svom radu [18] Julia Robinson u nemogućnosti dokazivanja pretpostavke Tarskog, uspjela je dati dovoljne uvjete za postojanje diofantske reprezentacije za potenciranje. Da bismo konstruirali takav A dovoljno je imati jednadžbu

$$B(a, b, x_1, ..., x_m) = 0$$

s relacijom $J(a, b)$ koja ima svojstva:

- za svaki a i b, iz $J(a, b)$ slijedi da je $a < b^b$;
- za svaki k postoje a i b takvi da je $J(a, b)$ i $a > b^k$.

Julia Robinson nazvala je relaciju J s ovim svojstvima relacijom eksponencijalnog rasta. Robinson 1969. daje novu ideju povezanu s posebnim oblikom Pellove jednadžbe

$$x^2 - (a^2 - 1)y^2 = 1.$$

Rješenja $(x_0, y_0), (x_1, y_1), ...$ ove jednadžbe zapisani redom od najmanjeg zadovoljavaju rekurzivne relacije [12, str. 4]:

$$x_{n+1} = 2ax_n - x_{n-1},$$
$$y_{n+1} = 2ay_n - y_{n-1}.$$

Možemo vidjeti da je za bilo koji m niz $x_0, x_1, ..., y_0, y_1, ...$ periodičan modulo m pa su onda i njihove linearne kombinacije. Provjerit ćemo indukcijom po a da vrijedi sustav:

$$\begin{aligned} y_0 &\equiv 0 \pmod{a-1}, \\ y_1 &\equiv 1 \pmod{a-1}, \\ y_2 &\equiv 2 \pmod{a-1}, \\ &\vdots \end{aligned}$$

Neka je $a = 3$ baza indukcije. Tada je $y_{n+1} = 6y_n - y_{n-1}$. Provjerimo vrijednosti:

$$\begin{aligned} y_0 &= 0, \\ y_1 &= 1, \\ y_2 &= 6y_1 - y_0 = 6 \cdot 1 - 0 = 6, \\ y_3 &= 6y_2 - y_1 = 6 \cdot 6 - 1 = 35, \\ y_4 &= 6y_3 - y_2 = 6 \cdot 35 - 6 = 204, \\ &\vdots \end{aligned}$$

Vidimo da za sve $k \in \mathbb{N}$ vrijedi

$$\begin{aligned} y_{2k} &\equiv 0 \pmod{2}, \\ y_{2k+1} &\equiv 1 \pmod{2}. \end{aligned}$$

Pretpostavimo da za neki a vrijedi početni sustav i promotrimo slučaj $b = a + 1$. Vrijedi:

$$\begin{aligned} y_{n+1} &= 2by_n - y_{n-1}, \\ y_{n+1} &\equiv 2by_n - y_{n-1} \pmod{b-1}, \\ y_{n+1} &\equiv 2(a+1)y_n - y_{n-1} \pmod{a}, \\ y_{n+1} &\equiv 2ay_n + 2y_n - y_{n-1} \pmod{a}, \\ y_{n+1} &\equiv 2y_n - y_{n-1} \pmod{a}, \end{aligned}$$

Pokazat ćemo da za niz $y_{n+1} = 2y_n - y_{n-1}$ kojem su početni uvjeti $y_0 = 0$ i $y_1 = 1$ vrijedi

$$y_{n+1} = n + 1.$$

Karakteristična jednadžba za rekurziju $y_{n+1} - 2y_n + y_{n-1} = 0$ je

$$x^2 - 2x + 1 = 0$$

koja ima dvostruko rješenje $x_{1,2} = 1$. Sada je opće rješenje rekurzije

$$y_{n+1} = A \cdot 1^{n+1} + B \cdot (n+1) \cdot 1^{n+1}.$$

Uvrštavanjem početnih vrijednosti dobijemo da su $A = 0$ i $B = 1$ pa slijedi

$$y_{n+1} = n + 1.$$

Povratkom u korak indukcije možemo napraviti pokazanu zamjenu.

$$\begin{aligned} y_{n+1} &\equiv 2y_n - y_{n-1} \pmod{a}, \\ y_{n+1} &\equiv n + 1 \pmod{a}, \\ y_{n+1} &\equiv n + 1 \pmod{b-1}. \end{aligned}$$

Zadnjom kongruencijom pokazali smo da početni sustav vrijedi za svaki a. Može se također pokazati i da vrijedi [19, str. 536]:

$$\begin{aligned} x_0 - (a-2)y_0 &\equiv 2^0 \pmod{4a-5}, \\ x_1 - (a-2)y_1 &\equiv 2^1 \pmod{4a-5}, \\ x_2 - (a-2)y_2 &\equiv 2^2 \pmod{4a-5}, \\ &\vdots \end{aligned}$$

Glavna ideja Julije Robinson bila je uskladiti dva niza uvjetom $G(a)$ koji bi zahtijevao da duljina perioda prvog niza bude višekratnik duljine perioda drugog niza. Kad bi takav uvjet bio diofantski i vrijedio za beskonačno mnogo vrijednosti a, tada bi se moglo pokazati i da je relacija $a = 2^c$ diofantska. Robinson nije mogla pronaći takav uvjet G, ali je takvo usklađivanje usmjerilo Yurija Matijaseviča na sličnu ideju te ju je pokušao implementirati malo drugačiji slučaj [12, str. 6]. Promatrao je jednadžbu

$$x^2 - xy - y^2 = \pm 1$$

koja ima ulogu sličnu gornjoj Pellovoj jednadžbi, ali su rješenja samo Fibonaccijevi brojevi. Niz

$$0, 1, 3, 8, 12, ...$$

Fibonaccijevih brojeva s parnim indeksima zadovoljava rekurzivnu relaciju

$$\phi_{n+1} = 3\phi_n - \phi_{n-1}.$$

Takav niz raste kao $\left[\frac{3+\sqrt{5}}{2}\right]^n$ te se može iskoristiti za konstrukciju relacije eksponencijalnog rasta. Za $a = \phi_{2k} + \phi_{2k+2}$ vrijedi

$$\begin{aligned}
y_0 &\equiv 0 \pmod{a-3},\\
y_1 &\equiv 1 \pmod{a-3},\\
y_2 &\equiv 3 \pmod{a-3},\\
&\vdots\\
y_l &\equiv \phi_{2k} \pmod{a-3},\\
y_{l+1} &\equiv -\phi_{2k} \pmod{a-3},\\
&\vdots\\
y_{2l-1} &\equiv -3 \pmod{a-3},\\
y_{2l} &\equiv -1 \pmod{a-3}
\end{aligned}$$

te sada imamo diofantski uvjet $H(a)$ koji kaže da je duljina perioda drugog niza višekratnik duljine prvog niza. Konstrukcija uvjeta H činila se jednostavnijom od konstrukcije uvjeta G. U tu svrhu Matijasevič je iskoristio lemu koja tvrdi

$$\phi_n^2 \mid \phi_m \Rightarrow \phi_n \mid m.$$

Diofantska definicija relacije eksponencijalnog rasta u imala je 14 nepoznanica, ali je Matijasevič kasnije uspio smanjiti broj nepoznanica na 5 [12, str. 9].

Dokazat ćemo općenitiji oblik spomenute leme. Pod α_b podrazumijevamo rekurzivni niz drugog reda oblika

$$\begin{aligned}
\alpha_b(0) &= 0,\\
\alpha_b(1) &= 1,\\
\alpha_b(n+2) &= b\alpha_b(n+1) - \alpha_b(n).
\end{aligned}$$

Taj niz pomoću matrice možemo zapisati u obliku relacije prvog reda

$$A_b(n) = \begin{pmatrix} \alpha_b(n+1) & -\alpha_b(n) \\ \alpha_b(n) & -\alpha_b(n-1) \end{pmatrix},$$

gdje je $\alpha_b(-1) = -1$. Također je i

$$A_b(0) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad A_b(n+1) = A_b(n)\begin{pmatrix} b & -1 \\ 1 & 0 \end{pmatrix}.$$

Iz čega slijedi zapravo da je

$$A_b(n) = \begin{pmatrix} b & -1 \\ 1 & 0 \end{pmatrix}^n$$

te je determinanta za $A_b(n)$ jednaka 1 za svaki $n \in \mathbb{N}$.

Lema 3.1. $\alpha_b^2(k) \mid \alpha_b(m) \Rightarrow \alpha_b(k) \mid m$.

Dokaz. Neka su b, k i m takvi da zadovoljavaju

$$\alpha_b^2(k) \mid \alpha_b(m)$$

te neka je za $k > n \geq 0$

$$m = n + kl.$$

Imamo

$$\begin{aligned}\begin{pmatrix} \alpha_b(m+1) & -\alpha_b(m) \\ \alpha_b(m) & -\alpha_b(m-1) \end{pmatrix} = A_b(m) = \begin{pmatrix} b & -1 \\ 1 & 0 \end{pmatrix}^m &= \begin{pmatrix} b & -1 \\ 1 & 0 \end{pmatrix}^{n+kl} \\ &= \begin{pmatrix} b & -1 \\ 1 & 0 \end{pmatrix}^n \begin{pmatrix} b & -1 \\ 1 & 0 \end{pmatrix}^{kl} = A_b(n)A_b^l(k) \\ &= \begin{pmatrix} \alpha_b(n+1) & -\alpha_b(n) \\ \alpha_b(n) & -\alpha_b(n-1) \end{pmatrix} \begin{pmatrix} \alpha_b(k+1) & 0 \\ 0 & -\alpha_b(k-1) \end{pmatrix}^l.\end{aligned}$$

Relacija kongruencije modulo $\alpha_b(k)$ posebno iz jednakosti daje

$$\alpha_b(m) \equiv \alpha_b(n)\alpha_b^l(k+1) \pmod{\alpha_b(k)},$$

pa uz početni uvjet $\alpha_b^2(k) \mid \alpha_b(m)$ dobijemo

$$\alpha_b(k) \mid \alpha_b(n) \tag{3.1}$$

jer su $\alpha_b(k)$ i $\alpha_b(k+1)$ relativno prosti.

Slijedi da je $\alpha_b(n) < \alpha_b(k)$ jer je $m = n + kl$ i jer je niz α_b rastući pa je (3.1) moguće samo ako je $n = 0$, odnosno $m = kl$. Dalje slijedi da je

$$\begin{aligned}A_b(m) &= A_b^l(k) \\ &= \begin{pmatrix} b\alpha_b(k) - \alpha_b(k-1) & -\alpha_b(k) \\ \alpha_b(k) & -\alpha_b(k-1) \end{pmatrix}^l \\ &= \left[\begin{pmatrix} b\alpha_b(k) & -\alpha_b(k) \\ \alpha_b(k) & 0 \end{pmatrix} - \begin{pmatrix} \alpha_b(k-1) & 0 \\ 0 & \alpha_b(k-1) \end{pmatrix} \right]^l \\ &= \sum_{i=0}^{l} (-1)^{l-i} \binom{l}{i} \alpha_b^i(k)\alpha_b^{l-i}(k-1) \begin{pmatrix} b & -1 \\ 1 & 0 \end{pmatrix}.\end{aligned}$$

Relacijom kongruencije modulo $\alpha_b^2(k)$ na jednakost dobijemo

$$\alpha_b(m) \equiv (-1)^{l-1} l\alpha_b(k)\alpha_b^{l-1}(k-1) \pmod{\alpha_b^2(k)}$$

pa slijedi da

$$\alpha_b(k) \mid l\alpha_b^{l-1}(k-1),$$

a jer su $\alpha_b(k)$ i $\alpha_b(k-1)$ relativno prosti slijedi da je

$$\alpha_b(k) \mid l.$$

□

Propozicija 3.2. *Skup* $\{ (a,b) \mid b \geq 2 \wedge \exists n[a = \alpha_b(n)] \}$ *je diofantski.*

Dokaz. Ako pogledamo početnu matricu $A_b(n)$ vidimo da je njena determinanta

$$\alpha_b^2(n+1) - b\alpha_b(n+1) + \alpha_b^2(n) = 1.$$

Sada možemo uzeti jednadžbu

$$x^2 - bxy + y^2 = 1$$

i vidimo da je za neki m ili

$$x = \alpha_b(m+1), \qquad y = \alpha_b(m) \tag{3.2}$$

ili

$$x = \alpha_b(m), \qquad y = \alpha_b(m+1). \tag{3.3}$$

Jer je α_b rastuća, uzimamo u obzir i nejednakost $y < x$, slijedi da je postoji neki m tako da vrijedi (3.2), što se može pokazati indukcijom i time $\{ (a,b) \mid b \geq 2 \ \ \& \ \ \exists n[a = \alpha_b(n)] \}$ možemo definirati formulom

$$b \geq 2 \ \ \& \ \ \exists x[x^2 - abx + a^2 = 1].$$

□

Propozicija 3.3. *Sljedeći sustav diofantskih uvjeta rješiv je ako i samo ako* (a,b,c) *pripada skupu* $\{ (a,b,c) \mid b \geq 4 \ \ \& \ \ a = \alpha_b(c) \}$*:*

$$
\begin{aligned}
&b \geq 4,\\
&u^2 - but + t^2 = 1,\\
&s^2 - bsr + r^2 = 1,\\
&r < s,\\
&u^2 \mid s,\\
&v = bs - 2r,\\
&v \mid w - b,\\
&u \mid w - 2,\\
&w > 2,\\
&x^2 - wxy + y^2 = 1,\\
&2a < u,\\
&a = arem(x, v),\\
&c = arem(x, u).
\end{aligned}
$$

Dokaz.

$\Rightarrow$ Prvo ćemo pokazati da ako su uvjeti zadovoljeni da slijedi $a = \alpha_b(c)$. Već smo pokazali da iz

$$
\begin{aligned}
b &\geq 4,\\
u^2 - but + t^2 &= 1,
\end{aligned}
$$

za neki k vrijedi

$$u = \alpha_b(k).$$

Isto tako iz

$$
\begin{aligned}
b &\geq 4,\\
s^2 - bsr + r^2 &= 1,\\
r &< s,
\end{aligned}
$$

slijedi da je

$$
\begin{aligned}
s &= \alpha_b(m),\\
r &= \alpha_b(m-1).
\end{aligned}
$$

Dalje, koristeći lemu 3.1 uvjeti

$$u^2 \mid s,$$
$$u = \alpha_b(k),$$

povlače $u \mid m$. Jer je $\alpha_b(n+2) = b\alpha_b(n+1) - \alpha_b(n)$ iz uvjeta $v = bs - 2r$ slijedi da je

$$v = \alpha_b(m+1) - \alpha_b(m-1).$$

Jer je $w > 2$ i $x^2 - wxy + y^2 = 1$ slijedi da je za neke n

$$x = \alpha_w(n).$$

Iz uvjeta $u \mid w - b$ i $u \mid w - 2$ i iz

$$\alpha_{b_1}(n) \equiv \alpha_{b_2}(n) \pmod{q}$$

slijede

$$x \equiv \alpha_b(n) \pmod{v},$$
$$x \equiv n \pmod{u}.$$

Neka je $n = 2lm \pm j$ takav da je $j \leq m$, tada imamo

$$\begin{aligned} A_b(n) &= \begin{pmatrix} b & -1 \\ 1 & 0 \end{pmatrix}^n = \begin{pmatrix} b & -1 \\ 1 & 0 \end{pmatrix}^{2lm \pm j} = \begin{pmatrix} b & -1 \\ 1 & 0 \end{pmatrix}^{2lm} \begin{pmatrix} b & -1 \\ 1 & 0 \end{pmatrix}^{\pm j} \\ &= [(A_b(m))^2]^l [A_b(j)]^{\pm 1}, \end{aligned}$$

$$\begin{aligned} A_b(m) &= \begin{pmatrix} \alpha_b(m+1) & -\alpha_b(m) \\ \alpha_b(m) & -\alpha_b(m-1) \end{pmatrix} \\ &\equiv -\begin{pmatrix} -\alpha_b(m-1) & \alpha_b(m) \\ -\alpha_b(m) & \alpha_b(m+1) \end{pmatrix} \pmod{v} \\ &= -[A_b(m)]^{-1}, \end{aligned}$$

$$[A_b(m)]^2 \equiv \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \pmod{v}$$
$$A_b(n) \equiv \pm [A_b(j)]^{\pm 1} \pmod{v}$$

Relacija kongruencije daje

$$x \equiv \alpha_b(n) \equiv \pm\alpha_b(j) \pmod{v}.$$

Jer je α_b rastuća i $j \leq m$ također vrijedi

$$2\alpha_b(j) \leq 2\alpha_b(m) \leq (b-2)\alpha_b(m) < b\alpha_b(m) - 2\alpha_b(m-1) = v,$$

te stoga

$$a = arem(x, v) = arem(\alpha_b(n), v) = \alpha_b(j).$$

Jer je $2a < u$ i $n \leq \alpha_b(n)$ slijedi i

$$2j \leq 2\alpha_b(j) = 2a < u.$$

Na kraju, zbog $u \mid m$, $x \equiv \alpha_b(n) \pmod{v}$, $u = 2lm \pm j$ i $2j \leq u$ slijedi da je

$$c = arem(x, u) = arem(n, u) = j,$$

što s $a = \alpha_b(j)$ daju željenu jednakost $a = \alpha_b(c)$.

$\Leftarrow$ Pokazat ćemo da ako a, b i c zadovoljavaju $b \geq 4$ i $a = \alpha_b(c)$, onda postoje s, r, u, t, v i w takvi da zadovoljavaju uvjete iz propozicije. Odaberimo u takav da vrijedi $u = \alpha_b(k)$ gdje za a i k vrijedi nejednakost $2a < u$, a u je neparan. α_b raste monotono i barem je jedan od dva uzastopna elementa niza neparan. Neka je

$$t = \alpha_b(k+1),$$

tada uvrštavanjem u $\alpha_b^2(n+1) - b\alpha_b(n+1)\alpha_b(n) + \alpha_b^2(n) = 1$ slijedi

$$u^2 - but + t^2 = 1.$$

Neka su

$$\begin{aligned} s &= \alpha_b(m), \\ r &= \alpha_b(m-1), \\ m &= uk. \end{aligned}$$

Time su zadovoljeni uvjeti $s^2 - bsr + r^2 = 1$ i $r < s$.

Jer je

$$s = \alpha_b(uk) \equiv (-1)^{u-1} u\alpha_b(k)\alpha_b(k)\alpha_b^{u-1}(k-1) \pmod{u^2},$$

tada je i uvjet $u^2 \mid s$ ispunjen. Vidimo da v zadovoljava $v = bs - 2r$ jer je

$$bs - 2r \geq 4\alpha_b(m) - 2\alpha_b(m-1) > 2\alpha_b(m).$$

Trebamo pokazati da su u i v relativno prosti. Ako je $d \mid u$ i $d \mid v$, tada zbog $u^2 | s$ vrijedi $d \mid s$ i zbog $v = bs - 2r$ vrijedi $d \mid 2r$. Zbog odabira u, d je neparan pa vrijedi $d \mid r$ i zbog $s^2 - bsr + r^2 = 1$ vrijedi $d \mid l$. Primjenom Kineskog teorema o ostacima možemo pronaći w koji zadovoljava

$$\begin{aligned} v &\mid w - b, \\ u &\mid w - 2, \\ w &> 2. \end{aligned}$$

Neka su

$$\begin{aligned} x &= \alpha_w(c), \\ y &= \alpha_w(c+1), \end{aligned}$$

tada i uvjet $x^2 - wxy + y^2 = 1$ vrijedi. Zbog $a = \alpha_b(c)$ i $v \mid w - b$ slijedi da je

$$x = \alpha_w(c) \equiv \alpha_b(c) = a \pmod{v}.$$

Možemo proširiti nejednakost

$$v = bs - 2r \geq 2\alpha_b(c) = a$$

pa vidimo da je $v > 2a$ i s tim je ispunjen i uvjet $a = arem(x, v)$. Iz $x = \alpha_w(c)$ slijedi

$$x \equiv c \pmod{w - 2}$$

što zajedno s $u \mid w - 2$ daje

$$x \equiv c \pmod{u}.$$

Imamo

$$2c \leq 2\alpha_b(c) = 2a < u,$$

što nam povlači i uvjet $c = arem(x, u)$. Svi uvjeti su diofantski pa je zato također i skup $\{ (a, b, c) \mid b \geq 4 \ \ \& \ \ a = \alpha_b(c) \}$ diofantski. □

3.1 Funkcija potenciranja je diofantska

Preostaje nam pokazati da je funkcija potenciranja uistinu diofantska. Indukcijom se može pokazati da je

$$(b-1)^n \leq \alpha_b(n+1) \leq b^n.$$

Uvodimo novu varijablu x s velikom vrijednosti. Poslije ćemo utvrditi da je

$$b^c = \lim_{x\to\infty} \frac{\alpha_{bx+4}(c+1)}{\alpha_x(c+1)}.$$

Ova relacija vrijedi za sve vrijednosti b i c, ali jezik diofantskih jednadžbi za sad ne sadrži operaciju lim. U ovom slučaju zamijenit ćemo ga operacijom div. Gornja nejednakost povlači

$$\frac{\alpha_{bx+4}(c+1)}{\alpha_x(c+1)} \geq \frac{(bx+3)^c}{x^c} \geq b^c$$

za veliki x pa je onda

$$b^c = \alpha_{bx+4}(c+1) \text{ div } \alpha_x(c+1).$$

Trebamo odrediti kad je x dovoljno velik pa pretpostavimo lijevu stranu gornje nejednadžbe. Razvojit ćemo na slučaj ako je $b = 0$ i $b > 0$. Za slučaj da su i $b = 0$ i $c = 0$ vrijedi

$$\frac{\alpha_{bx+4}(c+1)}{\alpha_x(c+1)} = 1,$$

a za $b = 0$, $c > 0$ i $x > 4$

$$\frac{\alpha_{bx+4}(c+1)}{\alpha_x(c+1)} < \frac{4^c}{(x-1)^c} \leq 1,$$

za $b = 0$ i $x > 16c$

$$\begin{aligned}\frac{\alpha_{bx+4}(c+1)}{\alpha_x(c+1)} \leq \frac{(bx+4)^c}{(x-1)^c} \leq \frac{(1+\frac{4}{x})^c}{(1-\frac{1}{x})^c} b^c \leq \frac{b^c}{(1-\frac{1}{x})^c(1-\frac{4}{x})^c} \\ \leq \frac{b^c}{(1-\frac{4}{x})^{2c}} \leq \frac{b^c}{1-\frac{8c}{x}} \leq b^c(1+\frac{16c}{x}).\end{aligned}$$

Tada $b^c = \alpha_{bx+4}(c+1)$ div $\alpha_x(c+1)$ vrijedi za sve x

$$x > 16(c+1)(b+1)^c$$

pa možemo uzeti da je

$$x = 16(c+1)\alpha_{b+4}(c+1).$$

Da bismo dobili diofantsku reprezentaciju za $a = b^c$, trebamo zamijeniti α_b iz $b^c = \alpha_{bx+4}(c+1)$ div $\alpha_x(c+1)$ i $x = 16(c+1)\alpha_{b+4}(c+1)$, a to možemo postići zamjenom uvjetima iz propozicije 3.3.

Poglavlje 4

Kodiranje konačnih nizova

Radovi s ciljem dokazivanja nerješivosti Hilbertovog desetog problema počeli su se pojavljivati 1950-ih. Tada već nije bilo prepreka u dokazivanju da su svi diofantski skupovi također i poluodlučivi, odnosno rekurzivno prebrojivi. Odvažnu obrnutu implikaciju dao je Martin Davis u [4] pokazujući da su svi rekurzivno prebrojivi skupovi ujedno i diofantski. Pokazao je da se za poluodlučiv skup prirodnih brojeva može dati reprezentacija

$$a \in \mathfrak{M} \iff \exists z \forall y \leq z \exists x_1, ..., x_m [D(a, x_1, ..., x_m, y, z) = 0].$$

Dana reprezentacija naziva se Davisova normalna forma te dopušta prikaz rekurzivno prebrojivog skupa aritmetičkom formulom koja sadrži više univerzalnih kvantifikatora. Ako su svi kvantifikatori ograničeni, odnosno imaju restrikciju nad varijablama, tada aritmetička formula definira rekurzivno prebrojiv skup i može se iskoristiti za njegovu definiciju [15, str. 39]. Martin Davis i Hilary Putnam uspjeli su eliminirati univerzalni kvantifikator iz Davisove normalne forme te su time provjeravali klasu eksponencijalnih diofantskih funkcija, ali je dokaz imao uvjet koji tada nisu uspjeli dokazati: Za svaki k postoji aritmetički red duljine k koji se sastoji od različitih prostih brojeva. Upotrebu dugih aritmetičkih redova koji se sastoje od prostih brojeva pripisujemo primjeni Gödelovog kodiranja proizvoljno dugih nizova prirodnih brojeva. Julia Robinson uspjela je zamijeniti takve redove aritmetičkim redovima koji se sastoje od relativno prostih brojeva čiji su prosti faktori proizvoljno veliki [15, str. 42]. Hilary Putnam predložio je upotrebu Gödelovog kodiranja da bi omogućili uklanjanje ograničenog univerzalnog kvantifikatora [15, str. 97]. U ovom poglavlju obradit ćemo nekoliko vrsta kodiranja koje su korištene za dokazivanje Problema, ali prvo ćemo definirati što je kodiranje.

Definicija 4.1. *Neka je $\mathcal{K}$ neki skup. Kodiranje skupa $\mathcal{K}$ je izračunljiva totalna injekcija $\mathbb{N}\mathcal{K} : \mathcal{K} \to \mathbb{N}$ kojoj je slika $\mathcal{I}_{\mathbb{N}\mathcal{K}}$ rekurzivna, a parcijalni inverz $\mathbb{N}\mathcal{K}^{-1} : \mathbb{N} \rightharpoonup \mathcal{K}$ s domenom $\mathcal{D}_{\mathbb{N}\mathcal{K}^{-1}} = \mathcal{I}_{\mathbb{N}\mathcal{K}}$ je također izračunljiva funkcija.*

4.1 Cantorovo kodiranje

Georg Cantor utemeljio je teoriju skupova uvođenjem koncepta beskonačnih brojeva i razlike među njima [21]. Dijagonalizacijom je pokazao korespondenciju između skupova $\mathbb{N} \times \mathbb{N}$ i $\mathbb{N}$ tako što je grupirao parove prirodnih brojeva: $(0,0), (0,1), (1,0), (0,2), (1,1), (0,2), \ldots$ te vidio da postoji injektivna funkcija sa skupa $\mathbb{N} \times \mathbb{N}$ u $\mathbb{N}$ [14, str. 7]. Prikazat ćemo funkciju koju nazivamo Cantorovim kodiranjem.

Definicija 4.2. *Za parove prirodnih brojeva* $(a, b) \in \mathbb{N} \times \mathbb{N}$ *definiramo Cantorovo kodiranje kao injektivnu funkciju Cantor* : $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *s*

$$\text{Cantor}(a, b) = \frac{(a+b)^2 + 3a + b}{2}.$$

Tako možemo dobiti diofantske funkcije Elema(c) i Elemb(c) koji za redni broj para u nizu daju prvi i drugi element.

$$a = \text{Elema}(c) \iff \exists y[(a+y)^2 + 3a + y = 2c],$$

$$b = \text{Elemb}(c) \iff \exists y[(x+b)^2 + 3x + b = 2c].$$

Budući da se radi o kodiranju, a i b moraju biti jedinstveni i treba biti omogućen njihov izračun. Formule za njihovo računanje su

$$\begin{aligned} w &= \left\lfloor \frac{\sqrt{8\text{Cantor}(a,b)+1} - 1}{2} \right\rfloor, \\ t &= \frac{w^2 + 2}{2}, \\ a &= \text{Cantor(a,b)} - t, \\ b &= w - a. \end{aligned}$$

Primjer 4.3. *Kodirajmo par* $(18, 41)$. *Uvrštavanjem u formulu za Cantorovo kodiranje dobijemo da je Cantor*$(18, 41) = 1788$. *Sada ćemo pokušati iz* 1788 *dobiti početne vrijednosti a i b. Uvrštavanjem u formule dobijemo*

$$\begin{aligned} w &= \left\lfloor \frac{\sqrt{8 \cdot 1788 + 1} - 1}{2} \right\rfloor = 59, \\ t &= \frac{59^2 + 59}{2} = 1770, \\ a &= 1788 - 1770 = 18, \\ b &= 59 - 18 = 41. \end{aligned}$$

Numeriranje parova može se generalizirati na numeriranje trojki, četvorki i tako dalje. Na primjer može se definirati

$$\text{Cantor}_1(a_1) = a_1,$$
$$\text{Cantor}_{n+1}(a_1, ..., a_{n+1}) = \text{Cantor}_n(a_1, ..., a_{n-1}, \text{Cantor}(a_n, a_{n+1})).$$

Time definiramo Cantorov broj kao $\text{Cantor}_n(a_1, ..., a_n)$ za neku n-torku $(a_1, ..., a_n)$. Analogno imamo i diofantsku funkciju $Elem_{n,m}(c)$ koja izlučuje m-ti element n-torke s Cantorovim brojem c:

$$a = Elem_{n,m}(c) \iff$$
$$\exists x_1, ..., x_{m-1}, x_{m+1}, ..., x_n[2^{2^n}\text{Cantor}_n(x_1, ..., x_{m-1}, a, x_{m+1}, ..., x_n) = 2^{2^n}c].$$

4.2 Gödelovo kodiranje

Hilbert je još krajem 19. stoljeća počeo potpuno formalizirati matematiku tako da bi se svaka istinita tvrdnja mogla dokazati, a danas taj prijedlog nazivamo Hilbertovim programom [24]. Istraživao je pojam dokaza te svojim radom uvelike doprinio teoriji dokaza. Najavom teorema o nepotpunosti 1931. Kurt Gödel onemogućio je daljni razvoj Hilbertovog programa te potaknuo istraživanja pojmova izračunljivosti i neodlučivosti. Gödel je pri dokazivanju značajnih teorema o nepotpunosti upotrijebio posebnu vrstu kodiranja koju Turingovi strojevi mogu pročitati [13, str. 6].

Neka je $(a_1, ..., a_n)$ konačan niz. Htjeli bismo ga kodirati, ali za razliku od Cantorovog kodiranja, Gödelov kod neće biti jedinstven. Neka su $b_1, ..., b_n$ u parovima relativno prosti brojevi takvi da za svaki $i \in \{1, ..., n\}$ vrijedi $a_i < b_i$. Koristeći Kineski teorem o ostacima možemo pronaći a takav da za svaki $i \in \{1, ..., n\}$ vrijede

$$a_i = \text{rem}(a, b_i),$$

$$b_i = bi + 1,$$

gdje je b višekratnik broja $n!$ i dovoljno je velik da vrijede sve nejednakosti $a_i < b_i$. Par (a, b) sadrži sve informacije o elementima niza osim o duljini pa možemo dodati dodatnu informaciju o duljini.

Definicija 4.4. *Za trojku $\langle a, b, c\rangle$ kažemo da je Gödelov kod niza $(a_1, ..., a_n)$ ako je $c = n$ te za svaki $i = \{1, ..., n\}$*

$$a_i = \text{GElem}(a, b, i),$$

gdje je GElem diofantska funkcija takva da

$$e = GElem(a, b, i) \iff e = rem(a, bi + 1).$$

4.3 Pozicijsko kodiranje

Uvođenjem novog kodiranja moći ćemo ustanoviti da su mnoge druge funkcije također diofantske kao što je npr. konkatenacija.

Definicija 4.5. *Za trojku $\langle a, b, c\rangle$ kažemo da je pozicijski kod konačnog niza $(a_1, ..., a_n)$ ako je $c = n$, za svaki $i \in \{1, ..., n\}$ vrijedi $b > a_i$ te*

$$a = a_n b^{n-1} + a_{n-1} b^{n-2} + \cdots + a_1 b^0.$$

Vrijednost a nazivamo šifrom, b bazom i c duljinom koda.

Kod nije jedinstven, ali možemo ustanoviti da je diofantski, odnosno $\langle a, b, c\rangle$ je pozicijski kod ako i samo ako vrijedi

$$b \geq 2 \wedge a < b^c.$$

Uvest ćemo relaciju $\mathrm{Kod}(a, b, c)$ koja će biti istinita ako a, b i c čine pozicijski kod. Možemo vidjeti da je funkcija $Elem(a, b, d)$, koja izlučuje d-ti po redu element, također diofantska:

$$e = \mathrm{Elem}(a, b, d) \Longleftrightarrow \exists x, y, z[d = z + 1 \wedge a = xb^d + eb^x + y \wedge y < b^x].$$

Pokazat ćemo da je i konkatenacija dvaju nizova diofantska funkcija. Definirat ćemo relaciju $\mathrm{Konkat}(a, b, c, a_1, b_1, c_1, a_2, b_2, c_2)$. Kod $\langle a, b, c\rangle$ bit će kod konkatenacije nizova s kodovima $\langle a_1, b_1, c_1\rangle$ i $\langle a_2, b_2, c_2\rangle$, odnosno za fiksiranu bazu konkatenaciju možemo prikazati kao

$$\begin{aligned}&\mathrm{Konkat}(a, b, c, a_1, b, c_1, a_2, b, c_2)\\ &\Longleftrightarrow \mathrm{Kod}(a_1, b, c_1) \wedge \mathrm{Kod}(a_2, b, c_2) \wedge a = a_2 b^{c_1} + a_1 \wedge c = c_1 + c_2.\end{aligned}$$

Propozicija 4.6. *Svojstvo „biti prost" je diofantsko.*

Dokaz. Svojstvo možemo prikazati kao:

$$\mathrm{Prost}(a) \Longleftrightarrow a > 1 \wedge \mathrm{nzd}(a, (a-1)!) = 1.$$

Tada trebamo pokazati da su funkcije faktorijel i najveći zajednički djelitelj također diofantske. Započet ćemo s nizom

$$\left(\binom{n}{0}, \binom{n}{1}, \ldots, \binom{n}{n}\right).$$

Ako uzmemo dovoljno veliki b, kod ovog niza dan je s $\langle (b+1)^n, b, n+1\rangle$. Za $b = 2^n + 1$ vidimo da je

$$c = \binom{n}{m} \iff c = Elem((2^n+2)^n, 2^n+1, m+1).$$

Prikazat ćemo faktorijel broja m inverzom definicije binomnog koeficijenta

$$\begin{aligned} m! &= \frac{n!}{\binom{n}{m}(n-m)!} \\ &= \frac{n(n-1)\cdots(n-m+1)}{\binom{n}{m}} \\ &= \frac{n^m}{\binom{n}{m}}\left(1-\frac{1}{n}\right)\ldots\left(1-\frac{m-1}{n}\right)n \\ &= \lim_{n\to\infty}\frac{n^m}{\binom{n}{m}}\left(1-\frac{1}{n}\right)\ldots\left(1-\frac{m-1}{n}\right)n \\ &= \lim_{n\to\infty}\frac{n^m}{\binom{n}{m}}. \end{aligned}$$

Ponovo ćemo lim zamijeniti operacijom div. Za dovoljno velike n vrijedi

$$m! = n^m \operatorname{div} \binom{n}{m}.$$

Provjerom vrijedi za $n \geq (m+1)^{m+2}$. Još preostaje pokazati i da je najveći zajednički djelitelj također diofantska funkcija:

$$a = nzd(b,c) \iff bc > 0 \wedge a \mid b \wedge a \mid c \wedge \exists x, y[a = bx - cy].$$

□

Navest ćemo sada nekoliko relacija koje su diofantske;

$$\text{NijeVeći}(a_1, b_1, a_2, b_2) \iff \forall k[\text{Elem}(a_1, b_1, k) \leq \text{Elem}(a_2, b_2, k)],$$

koja redom uspoređuje elemente dvaju nizova i vrijedi ako vrijede i sve usporedbe.

$$\text{Manji}(a, b, c, e) \iff \text{Kod}(a, b, c) \wedge \forall k[\text{Elem}(a, b, k) \leq e],$$

koji uspoređuje sve elemente niza s određenim brojem.

Iskazat ćemo Kummerov teorem koji je potreban za dokaz sljedeće propozicije.

Teorem 4.7. *(Kummer [10, str. 115]) Ako je p prost broj, onda je njegov eksponent u kanonskom proširenju binomnog koeficijenta* $\binom{m+n}{m}$ *u proste faktore jednak broju prenošenja pri zbrajanju brojeva m i n u bazi p.*

Propozicija 4.8. *Relacija Jednaki*$(a_1, b_1, c_1, a_2, b_2, c_2)$ *je istina ako i samo ako su* $\langle a_1, b_1, c_1\rangle$ *i* $\langle a_2, b_2, c_2\rangle$ *kodovi istog niza.*

Dokaz. Treba nam pomoćna relacija Je koja će biti jača od relacije Jednaki za koju će vrijediti

$$\begin{aligned}\text{Jednaki}(a_1, b_1, c_1, a_2, b_2, c_2) \iff \\ \exists x, y, z[\text{Je}(a_1, b_1, c_1, x, y, z) \wedge \text{Je}(a_2, b_2, c_2, x, y, z)].\end{aligned}$$

Da bismo pokazali da je pomoćna relacija diofantska, uvest ćemo još nekoliko diofantskih relacija:

$$\text{PNijeVeći}(a_1, a_2, b) \iff \text{Prost}(b) \wedge \text{NijeVeći}(a_1, b, a_2, b).$$

Kummerovim teoremom slijedi da je

$$\text{PNijeVeći}(a_1, a_2, b) \iff \text{Prost}(b) \wedge b \nmid \binom{a_2}{a_1}.$$

Koristeći PNijeVeći možemo pokazati i da je sljedeća relacija diofantska:

$$\text{PManji}(a, b, c, e) \iff \text{Prost}(b) \wedge \text{Manji}(a, b, c, e),$$

$$\text{PManji}(a, b, c, e) \iff \text{Prost}(b) \wedge [e \geq b \vee \text{PNijeVeći}(a, \text{Ponovi}(e, b, c), b)],$$

gdje je $\text{Ponovi}(p, q, r) = \frac{p(q^r-1)}{q-1}$ šifra niza $(p, ..., p)$ duljine r u bazi q. Neka su b_1 i b_2 takvi da vrijedi $b_1 < b_2$ i $\langle a_2, b_2, c\rangle$ je kod nekog niza čiji su elementi svi manji od b_1. Očito šifra a_1 istog niza u bazi b_1 zadovoljava kongruenciju

$$a_1 \equiv a_2 \pmod{b_2 - b_1}$$

i nejednakost $a_1 < b_1^c$ iz koje za dovoljno velike b_2 vrijedi

$$b_1^c < b_2 - b_1.$$

Tada je a_1 jedinstveno određen gornjim uvjetima. Sada možemo definirati relaciju Je:

$$\begin{aligned}\text{Je}(a_1, b_1, c_1, a_2, b_2, c_2) \Longleftrightarrow &\text{Kod}(a_1, b_1, c_1) \wedge c_1 = c_2 \\ &\wedge \text{Pmanji}(a_2, b_2, c_2, b_1 - 1) \\ &\wedge b_1^{c_1} + b_1 < b_2 \\ &\wedge a_1 \equiv a_2 \pmod{b_2 - b_1}.\end{aligned}$$

□

Pokazat ćemo da su i relacije NijeVeći, Manji i Konkat za nizove različite duljine također diofantske:

$$\begin{aligned}\text{NijeVeći}(a_1, b_1, a_2, b_2) \Longleftrightarrow \exists x_1, x_2, y, z[&\text{Jednaki}(a_1, b_1, z, x_1, y, z) \\ &\wedge\text{Jednaki}(a_2, b_2, z, x_2, y, z) \\ &\wedge\text{PNijeVeći}(x_1, x_1, y)],\end{aligned}$$

$$\text{Manji}(a, b, c, e) \Longleftrightarrow \exists x, y[\text{Jednaki}(a, b, c, x, y, c) \wedge \text{PManji}(x, y, c, e)],$$

$$\begin{aligned}\text{Konkat}(a, b, c, a_1, b_1, c_1, a_2, b_2, c_2) \Longleftrightarrow \exists x_1, x_2[&\text{Jednaki}(a_1, b_1, c_1, x_1, b, c_1) \\ &\wedge\text{Jednaki}(a_2, b_2, c_2, x_2, b, c_2) \\ &\wedge a = x_2 b^{c_1} + x_1 \\ &\wedge c = c_1 + c_2].\end{aligned}$$

Poglavlje 5

Univerzalna diofantska jednadžba

Martin Davis, Hilary Putnam i Julia Robinson dokazali su 1961. da je svaki rekurzivni skup S eksponencijalno diofantski, odnosno da se može prikazati u obliku

$$x \in S \iff \exists x_1, x_2, ..., x_n[D(x, x_1, ...x_n, 2^{x_1}, ..., 2^{x_n}) = 0],$$

gdje je D polinom s cjelobrojnim koeficijentima i pozitivnim cjelobrojnim rješenjima. Matijasevič je proširio ekvivalenciju pokazujući da je eksponencijalna relacija $y = 2^x$ diofantska. Formalno možemo prikazati rekurzivno prebrojiv skup S kao

$$x \in S \iff \exists x_1, ..., x_n[D(x, x_1, ..., x_n) = 0].$$

Iz toga slijedi da ne postoji algoritam koji odlučuje rješivost diofantskih jednadžbi [8, str. 549]. Nepostojanje takvog algoritma slijedi direktno iz postojanja skupova koji nisu rekurzivni, ali jesu rekurzivno prebrojivi. Rekurzivno prebrojivi skupovi $S_1, S_2, ...$ mogu se enumerirati tako da je binarna relacija $x \in S_\nu$ također rekurzivno prebrojiva. Matijasevičev teorem tada kaže da postoji diofantska jednadžba U takva da za svaki x i ν vrijedi

$$x \in S_\nu \iff \exists x_1, ..., x_\nu[U(x, \nu, x_1, ..., x_\nu) = 0].$$

Diofantska jednadžba U fiksirani je polinom s cjelobrojnim koeficijentima. Promjenom vrijednosti parametra ν polinom U definira svaki rekurzivno prebrojiv skup te je U time polinomski analogon univerzalnom Turingovom stroju te ga nazivamo univerzalnom diofantskom jednadžbom.

Pokušat ćemo konstruirati univerzalnu diofantsku jednadžbu. Odabirom odgovarajućih vrijednosti parametara rješavanje bilo koje diofantske jednadžbe svodi se na rješavanje univerzalne diofantske jednadžbe koja nam dopušta konstruiranje diofantskog skupa čiji je komplement nediofantski.

Univerzalna diofantska jednadžba ima oblik familije diofantskih jednadžbi

$$U(a_1, ..., a_n, k_1, ..., k_l, y_1, ..., y_w) = 0$$

čiji su parametri podijeljeni u parametre elemenata $a_1, ..., a_n$ i parametre koda $k_1, ..., k_l$.

Definicija 5.1. *Kažemo da je jednadžba*

$$U(a_1, ..., a_n, k_1, ..., k_l, y_1, ..., y_w) = 0$$

univerzalna ako za bilo koju diofantsku jednadžbu s n parametara $D(a_1, ..., a_n, x_1, ..., x_m) = 0$ *postoje brojevi* $k_1, ..., k_l$ *takvi da diofantska jednadžba ima rješenje u* $x_1, ..., x_m$ *za točno one vrijednosti parametara* $a_1, ..., a_n$ *za koje jednadžba U ima rješenja u* $y_1, ..., y_w$.

Diofantska jednadžba time daje još jednu reprezentaciju diofantskog skupa koji je definiran univerzalnom diofantskom jedndadžbom. Svaka univerzalna jednadžba dopušta kodiranje diofantskog skupa određene dimenzije pa $\langle k_1, ..., k_l \rangle$ možemo gledati kao kod skupa definiran diofantskom jednadžbom.

Svaku univerzalnu diofantsku jednadžbu možemo zamijeniti drugom dodavanjem još jednog elementa k koji će sam predstavljati kod, a ostali će parametri biti nepoznanice. Zamjenu možemo napraviti na sljedeći način:

$$U^2(a_1, ..., a_n, k_1, ..., k_l, y_1, ..., y_w) + (k - 2^{2^l}\text{Cantor}_l(k_1, ..., k_l))^2 = 0 \tag{5.1}$$

gdje je kod $k = 2^{2^l}\text{Cantor}_l(k_1, ..., k_l)$.

Propozicija 5.2. *Postoji konstanta m takva da za svaki n postoji univerzalna diofantska jednadžba* $U(a_1, ..., a_n, k_1, ..., k_l, y_1, ..., y_w) = 0$ *takva da su* $l = 1$ *i* $w = m$.

Dokaz. Pomoću Cantorovog kodiranja možemo ograničiti broj nepoznanica u univerzalnoj jednadžbi. Neka je m broj nepoznanica u danoj univerzalnoj diofantskoj jednadžbi $U_1(a, k, y_1, ..., y_m) = 0$ koja kodira jednodimenzionalni diofantski skup. Za $n > 1$ definiramo polinom

$$U_n(a_1, ..., a_n, k, y_1, ..., y_m) = U_1(2^{2^n}\text{Cantor}_n(a_1, ..., a_n), k, y_1, ..., y_m).$$

Zamjenom (5.1) možemo dobiti da je

$$U_n(a_1, ..., a_n, k, y_1, ..., y_m) = 0$$

također univerzalna diofantska jednadžba.

□

5.1 Kodiranje jednadžbi i rješenja

Započinjemo konstruiranjem univerzalne jednadžbe sa šest parametara koda b, c_L, c_R, d, e, f sa samo jednim parametrom a, tj., prikazat ćemo polinom U tako da za svaku diofantsku jednadžbu

$$D(a, x_1, ..., x_m) = 0,$$

postoje brojevi b, c_L, c_R, d, e, f takvi da je dana diofantska jednadžba rješiva za iste vrijednosti parametra a kao i jednadžba

$$U(a, b, c_L, c_R, d, e, f, y_7, ..., y_m) = 0.$$

Definicija univerzalne jednadžbe zahtijeva da niz (b, c_L, c_R, d, e, f) određuje skup koji definira početna diofantska jednadžba. Kod $\langle b, c_L, c_R, d, e, f\rangle$ mora sadržavati informacije o polinomu pa je e jednak broju nepoznanica, d je broj veći od stupnja polinoma D te je

$$f = 2^{d^1} + \cdots + 2^{d^e}.$$

Uvodimo relaciju Format(d, e, f) koju definira gornja jednadžba. U prošlom smo poglavlju definirali kodiranje samo za prirodne brojeve, a kako u diofantskim jednadžbama za koeficijente dopuštamo cijele brojeve, morat ćemo rastaviti početni polinom na razliku C_L i C_R:

$$\begin{aligned} D(x_0, ..., x_m) &= C_L(x_0, ..., x_m) - C_R(x_0, ..., x_m), \\ C_L(x_0, ..., x_m) &= \sum_{i_0+\cdots+i_m<d} c_{L,i_0,...,i_m} x_0^{i_0} \cdots x_m^{i_m}, \\ C_R(x_0, ..., x_m) &= \sum_{i_0+\cdots+i_m<d} c_{R,i_0,...,i_m} x_0^{i_0} \cdots x_m^{i_m}. \end{aligned}$$

Brojevi c_L i c_R su šifre niza u bazi b koje sadrže koeficijente polinoma C_L i C_R. Koristit ćemo c_L, c_R, kao i polinome C_L i C_R na isti način pa ih možemo dalje zamijeniti s šifrom c i polinomom C. Definiramo šifru c polinoma C u bazi b:

$$c = \sum_{i_0+\cdots+i_m<d} i_0!...i_m!(d - 1 - i_0 - \cdots - i_m)!c_{i_0,...,i_m} b^{d^{m+1}-i_0 d^0-\cdots-i_m d^m}.$$

Niz $\langle b, c, d, e, f\rangle$ nazvat ćemo kod polinoma C ako još vrijedi i

$$b > d!\max\{c_{i_0,...,i_m}\}.$$

Želimo konstruirati univerzalnu jednadžbu

$$U(a, b, c_L, c_R, d, e, f, y_7, ..., y_m) = 0$$

takvu da ako je $\langle b, c_L, c_R, d, e, f\rangle$ kod, tada vrijedi:

$$\forall a[\exists y_7, ..., y_m[U(a, b, c_L, c_R, d, e, f, y_7, ..., y_m) = 0] \\ \iff \exists x_1, ..., x_m[D_{b,c_L,c_R,d,e,f}(a, x_1, ..., x_m) = 0]],$$

gdje je $D_{b,c_L,c_R,d,e,f}(a, x_1, ..., x_m)$ jednadžba s kodom $\langle b, c_L, c_R, d, e, f\rangle$.

Uvest ćemo novo kodiranje nizova prirodnih brojeva koji će biti potencijalna rješenja diofantske jednadžbe. Kodiranje će se sastojati od brojeva d, e, f, g i h. Prva tri broja čine diofantsku jednadžbu, g je veći od brojeva $1, x_1, ..., x_m$, a

$$h = x_1 g^{d^1} + x_2 g^{d^2} + \cdots + x_m g^{d^m}.$$

Tada je $\langle h, g, d^m + 1\rangle$ pozicijski kod niza

$$(0, ..., 0, x_1, 0, ..., 0, x_2, ..., 0, ..., 0, x_m).$$

Kod mogućeg rješenja zapisat ćemo kao RKod(d, e, f, g, h). Prvo ćemo pokazati da je nova relacija RK diofantska koja će se podudarati s RKod ako je (d, e, f) format jednadžbe

$$\text{Format}(d, e, f) \Rightarrow [\text{RK}(d, e, f, g, h) \iff \text{RKod}(d, e, f, g, h)]. \tag{5.2}$$

Za Relaciju RK vrijedi ako je (d, e, f) format jednadžbe, tada je $\langle f, 2, d^e + 1\rangle$ pozicijski kod niza

$$(0, ..., 0, 1, 0, ..., 0, 1, ..., 0, ..., 0, 1)$$

gdje se jedinice pojavljuju točno na mjestima gdje su bili $x_1, ..., x_m$. Koristeći relaciju Jednaki možemo staviti da je t šifra za niz nula i jedinica u bazi g. Tada je $(g-1)t$ šifra niza

$$(0, ..., 0, g-1, 0, ..., 0, g-1, ..., 0, ..., 0, g-1)$$

u bazi g i dovoljno je primijeniti relaciju NijeVeći. Sada možemo definirati relaciju RK

$$\text{RK}(d, e, f, g, h) \iff \exists t[\text{Jednaki}(f, 2, d^2 + 1, t, g, d^e + 1) \wedge \text{NijeVeći}(h, (g-1)t, g)].$$

Vidimo da svojstvo (5.1) vrijedi za ovu definiciju relacije RK.

5.2 Računanje vrijednosti polinoma

Propozicija 5.3. *Neka je $\langle b, c_L, c_R, d, e, f\rangle$ kod rješive diofantske jednadžbe*

$$D(a, x_1, ..., x_m) = 0.$$

Tada postoji kod $\langle d, e, f, g, h\rangle$ koji predstavlja jedno od rješenja diofantske jednadžbe D za dani parametar a.

Dokaz. Vrijednost polinoma C možemo izračunati izravno iz koda jednadžbe $\langle b, c, d, e, f\rangle$, koda mogućeg rješenja $\langle d, e, f, g, h\rangle$ i vrijednosti parametra a.

Neka je w dovoljno velik broj za koji ćemo poslije naći donju ogradu. Koristeći relaciju Jednaki kodove iz baza b i g možemo prebaciti u bazu w. Promotrimo broj

$$\begin{aligned}(1 + aw + t)^{d-1} &= (1 + aw^{d^0} + x_1 w^{d^1} + \cdots + x_m w^{d^m})^{d-1} \\ &= \sum_{i_0+\cdots+i_m<d} \binom{d-1}{i_0 \ldots i_m} a^{i_0} x_1^{i_1} \ldots x_m^{i_1} \ldots x_m^{i_m} w^{i_0 d^0 + \cdots + i_m d^m}.\end{aligned}$$

U sumi su svi eksponenti od w različiti pa će za w koji je dovoljno velik, broj $(1+aw+t)^{d-1}$ biti šifra u bazi w nekog niza koji sadrži sve članove koji čine polinom C, ali s drugačijim koeficijentima. Da bismo dobili ispravne koeficijente, pomnožit ćemo $(1 + aw + t)^{d-1}$ sa

$$s = \sum_{i_0+\cdots+i_m<d} i_0! \ldots i_m! (d - 1 - i_0 - \cdots i_m)! c_{i_0 \ldots i_m} w^{d^{m+1} - i_0 d^0 - \cdots i_m d^m}$$

i kombinirati članove u kojima w ima isti eksponent:

$$(1 + aw + t)^{d-1} s = \sum_{k=0}^{2d^{m+1}-1} C_k w^k.$$

Ovdje su C_k izrazi koji sadrže $c_{i_0 \ldots i_m}$, $a, x_1, \ldots, x_m$. Možemo vidjeti da je

$$\begin{aligned}C_{d^{e+1}} &= \sum_{i_0+\cdots+i_m<d} \binom{d-1}{i_0 \ldots i_m} i_0! \ldots i_m! (d - 1 - i_0 - \cdots - i_m)! c_{i_0 \ldots i_m} a^{i_0} x_1^{i_1} \ldots x_m^{i_m} \\ &= (d-1)! C(a, x_1, \ldots, x_m).\end{aligned}$$

Ako je w veći od $C_0, \ldots, C_{2d^{m+1}-1}$, tada

$$C(a, x_1, \ldots, x_m) = \frac{\mathrm{Elem}((1 + aw + t)^{d-1} s, w, d^{e+1} + 1)}{(d-1)!}.$$

Preostaje pronaći donju ogradu za w koja će garantirati gornju jednadžbu. Sljedeća će nejednakost to zadovoljavati

$$w > (1 + a + h)^{d-1} c.$$

Možemo definirati sljedeću relaciju:

$$\begin{aligned}\text{Rješenje}(a,b,c_L,c_R,d,e,f,g,h) \iff \\ \text{RK}(d,e,f,g,h) \ \& \ \exists s_L s_R t w[w > (1+a+h)^{d-1}(c_L+c_R) \\ \wedge\text{Jednaki}(c_L,b,d^{e+1}+1,s_L,w,d^{e+1}+1) \\ \wedge\text{Jednaki}(c_R,b,d^{e+1}+1,s_R,w,d^{e+1}+1) \\ \wedge\text{Jednaki}(h,g,d^e+1,t,w,d^e+1) \\ \wedge Elem((1+aw+t)^{d-1}s_L,w,d^{e+1}+1) \\ = Elem((1+aw+t)^{d-1}s_R,w,d^{e+1}s_R,w,d^{e+1}+1)].\end{aligned}$$

Ako je $\langle b, c_L, c_R, d, e, f\rangle$ kod diofantske jednadžbe, tada slijedi i

$$\begin{aligned}\exists g,h[\text{RKod}(d,e,f,g,h) \wedge \text{Rješenje}(a,b,c_L,c_R,d,e,f,g,h)] \\ \iff \exists x_1 ... x_m [D_{b,c_L,c_R,d,e,f}(a,x_1,...,x_m) = 0].\end{aligned}$$

□

5.3 Univerzalna diofantska jednadžba

Relacija Rješenje(a,b,c_L,c_R,d,e,f,g,h) diofantska je te možemo konstruirati diofantsku jednadžbu

$$U(a,b,c_L,c_R,d,e,f,g,h,y_9,...,y_m) = 0$$

koja definira ovu relaciju. Ako uzmemo da su g i h nepoznanice, dobijemo potrebnu univerzalnu jednadžbu. Možemo konstruirati za svaki n univerzalni polinom U_n s jednim kodom za sve parametre i m nepoznanica. Definirajmo polinom

$$U_1(a,k,y_1,...,y_m) = U^2(a,y_1,...,y_m) + (k - 2^{2^6} Cantor_6(y_1,...,y_6))^2.$$

Tada ako je $\langle b, c_l, c_r, d, e, f\rangle$ kod jednadžbe $D(a,x_1,...,x_m) = 0$, broj

$$2^{2^6}\text{Cantor}_6(b,c_L,c_R,d,e,f)$$

bit će kod te diofantske jednadžbe u novom kodiranju.

S ovom definicijom nisu svi prirodni brojevi kodovi neke jednadžbe. Za neki broj k možemo odrediti može li se prikazati u obliku gornjeg koda gdje je $\langle b, c_L, c_R, d, e, f\rangle$ kod neke jednadžbe. Ako k nije moguće prikazati u tom obliku, onda smatramo da je k po definiciji kod jednadžbe

$$U_1(a,k,x_1,...,x_m) = 0$$

s jednim parametrom a i m nepoznanica $x_1,...,x_m$ te iz toga slijedi sljedeća propozicija.

Propozicija 5.4. *Očito je za svaku vrijednost a i k jednadžba rješiva ako i samo ako je jednadžba s kodom k rješiva, bez obzira je li k kod D ili U_1.*

Za svaki $n > 1$ univerzalni polinom U_n se može definirati kao

$$U_n(a_1, ..., a_n, k, y_1, ..., y_m) = U_1(2^{2^n}\text{Cantor}_n(a_1, ..., a_n), k, y_1, ..., y_m).$$

Sada možemo definirati univerzalni polinom U_0 kao

$$U_0(k, y_1, ..., y_m) = U_1(0, k, y_1, ..., y_m)$$

i promatramo bilo koji kod diofantske jednaždbe kodom jednadžbe bez parametara

$$D(0, x_1, ..., x_m) = 0.$$

5.4 Diofantski skupovi s nediofantskim komplementima

Sada možemo konstruirati primjer diofantskog skupa kojem komplement nije diofantski. Logički alati za konstrukciju diofantskih skupova sastoje se od $\exists$, $\wedge$ i $\vee$. Postojanje diofantskih skupova kojima komplement nije diofantski onemogućuje proširenje logičkih alata dodavanjem ili negacije $\neg$ ili univerzalnim kvantifikatorom $\forall$ jer je komplement diofantskog skupa definiran jednadžbom

$$D(a, x_1, ..., x_m) = 0$$

definiran je i s

$$\neg\exists x_1...x_m[D(a, x_1, ..., x_m) = 0]$$

i s

$$\forall x_1...x_m[D(a, x_1, ..., x_m) \neq 0].$$

Konstrukcija se temelji na klasičnoj metodi dijagonalizacije.

Primjer 5.5. *Neka je*

$$U_1(p, q, y_1, ..., y_m) = 0$$

te zamijenimo oba parametra jednim a:

$$U_1(a, a, y_1, ..., y_m) = 0.$$

Dobivena jednadžba definira odgovarajući diofantski skup $\mathfrak{H}_1$ prirodnih brojeva. Pokažimo da $\overline{\mathfrak{H}}_1$, koji je komplement skupa $\mathfrak{H}_1$, nije diofantski. Pretpostavimo suprotno; Tada $\overline{\mathfrak{H}}_1$ ima neki kod k. Pokušat ćemo odlučiti ima li

$$U_1(k, k, y_1, ..., y_m) = 0$$

rješenje. Ako ima, po definiciji je onda i $k \in \mathfrak{H}_1$. S druge strane je U_1 univerzalna pa slijedi da je $k \in \overline{\mathfrak{H}}_1$. Ako U_1 nema rješenje, onda po definiciji $\mathfrak{H}_1$, $k \notin \mathfrak{H}_1$, dok univerzalnost povlači da $k \notin \overline{\mathfrak{H}}_1$. Kontradikcija pokazuje da $\overline{\mathfrak{H}}_1$ ne može biti diofantski.

Poglavlje 6

Turingovi strojevi

Hilbert je u opisu svog desetog problema govorio o procesu koji u konačnom broju operacija određuje ima li jednadžba cjelobrojna rješenja. Kad bi postojao takav proces, kojeg danas promatramo kao algoritam, tada bi bez ikakve intervencije, odnosno automatski, bilo moguće doći do postojanja rješenja jednadžbe. Turingovi strojevi apstraktna su računala te za razliku od pravih fizičkih računala koriste beskonačnu traku. Ne može doći do problema nedostatka memorije, ali ipak da bi smo došli do rješenja nekog problema potrebno je iskoristiti konačan broj ćelija na traci. Svaka će ćelija biti ili prazna ili popunjena simbolom iz konačnog skupa koji se naziva alfabet. Glava čita i piše simbole pomičući se lijevo ili desno. U svakom trenutku stroj se nalazi u jednom od konačno mnogo stanja te dodatno razlikujemo početno stanje, kao i završna stanja. Na početku su na nekom dijelu trake upisani simboli iz alfabeta bez razmaka, ostatak trake je prazan i stroj je u početnom stanju q_1. Rad stroja odvija se korak po korak po instrukcijama. Stroj prestaje s radom nakon što se izvrši instrukcija u završnom stanju. Postoji mogućnost da stroj nikad ne dođe do završnog stanja i da će nastaviti raditi beskonačno.

Alan Turing, Alonzo Church i Kurt Gödel predložili su i razvili model Turingovog stroja 1930. Izložili su definicije koje su već do tad kao pojmovi bili intuitivni i time konstruirali temelje na kojima će se riješiti Hilbertov deseti problem. Razvijanje teorije Turingovih strojeva bila je istovremena s Gödelovim razvojem pojma primitivno rekurzivne funkcije [2, str. 1]. Važnost Turingovih strojeva je i postojanje univerzalnog Turingovog stroja, odnosno stroj koji može simulirati Turingov stroj, može simulirati i univerzalni Turing stroj te je pokazano da Turingov stroj može biti simuliran raznim tipovima strojeva, kao što je npr. RAM-stroj [17, str. 513]. Definirat ćemo Turingov stroj:

Definicija 6.1. *Turingov stroj uređena je sedmorka* $\mathcal{T} = (Q, \Sigma, \Gamma, \delta, q_0, q_{DA}, q_{NE})$ *gdje su:*

- Q *konačan skup čije elemente nazivamo* ***stanja****;*

- Σ *konačan skup čije elemente nazivamo* ***ulazni simboli****. Pretpostavljamo da* Σ *ne sadrži prazan simbol kojeg označujemo s* Λ*;*
- Γ *konačan skup kojeg nazivamo* ***alfabet Turingovog stroja****. Pretpostavljamo da je prazan simbol* Λ *element od* Γ *te* $\Sigma \subseteq \Gamma$*;*
- $\delta : Q \times \Gamma \to \Gamma \times \{L, D, S\} \times Q$ *proizvoljna funkcija koju nazivamo* ***funkcija prijelaza****;*
- $q_1 \in Q$ *i nazivamo ga* ***početno stanje***;
- $q_{DA} \in Q$ *i nazivamo ga* ***početno stanje****;*
- $q_{NE} \in Q$ *i nazivamo ga* ***stanje odbijanja****.*

Alfabet našeg Turingovog stroja bit će konačan skup elemenata $\{\alpha_1, ..., \alpha_w\}$. Jer je traka beskonačna, označavat ćemo ćeliju koju smo koristili, a nalazi se najviše lijevo s $\star$.

6.1 Kompozicija strojeva

Trebamo ustanoviti egzistenciju strojeva s određenim svojstvima. Eksplicitno ćemo dati instrukcije samo za neke najjednostavnije strojeve i opisati dvije metode za konstrukciju kompleksnijih strojeva iz danih strojeva. To će nam omogućiti pristup strojevima s traženim svojstvima. Svi strojevi koje ćemo konstruirati imat će isti alfabet

$$\{\star, 0, 1, 2, 3, \lambda\}.$$

Niz $(a_1, ..., a_n)$ na traci možemo prikazati unarno tako da simbol 0 razdvaja dva elementa, a broj uzastopnih simbola 1 označava broj a_k za svaki $k \in \{1, ..., n\}$. Na primjer možemo prikazati niz $(2, 0, 0, 3, 1)$ kao

$$(..., \star, 1, 1, 0, 0, 1, 1, 1, 0, 1, \lambda, ...)$$

Bit će dva završna stanja q_{DA} i q_{NE} koje interpretiraju dolazak stroja do q_{DA} kao odgovor "DA", a q_{NE} kao "NE". Prva metoda konstrukcije novog Turingovog stroja M iz dva dana stroja M_1 i M_2:

- U svim instrukcijama stroja M_1 završno stanje q_{DA} zamijenjeno je s q_{v+1} gdje je v broj stanja stroja M_1,
- U svim instrukcijama stroja M_2 svako nezavršno stanje q_i zamijenjeno je stanjem q_{v+i},

- Skup instrukcija novog stroja M sastoji se od instrukcija oba stroja izmijenjeno na jednak način kao i prethodno.

Radnja stroja M sastoji se od uzastopnih izvršenja strojeva M_1 i M_2 s tim da stroj M_1 staje u stanju q_{DA}. Da bismo označili stroj M koristimo

$$M_1; M_2,$$

$$M_1 \text{ i } M_2,$$

ili

$$\text{ako } M_1, \text{ onda } M_2,$$

ovisno o danom kontekstu. Kompozicija Turingovih strojeva je asocijativna operacija, odnosno $M_1; M_2; M_3$ jednoznačno je određeno.

Druga metoda za konstrukciju novog Turingovog stroja M iz dva dana stroja M_1 i M_2 je:

- U svim instrukcijama stroja M_1 završno stanje q_{DA} zamijenjeno je stanjem q_{v+1} gdje je v broj stanja stroja M_1 i završno stanje q_{NE} zamijenjeno je stanjem q_{DA},
- U svim instrukcijama stroja M_2 svako nezavršno stanje q_i zamijenjeno je stanjem q_{v+i} te je završno stanje q_{DA} zamijenjeno s q_1,
- Skup instrukcija novog stroja M sastoji se od instrukcija oba stroja izmijenjeno na jednak način kao i prethodno.

Turingov stroj konstruiran na ovaj način označava se s

$$\text{dok } M_1 \text{ radi } [M_2].$$

Radnja ovog stroja sastoji se od radnji stroja M_1 i M_2 dok jedan od njih ne dođe u završno stanje q_{NE}.

6.2 Osnovni Turingovi strojevi

Prije nego što pokažemo što su Turing-poluodlučivi skupovi i njihovu poveznicu s diofantskim skupovima, navest ćemo osnovne Turingove strojeve i njihove kompozicije koje će nam biti potrebne:

- LIJEVO
  Pomiče glavu za jednu ćeliju ulijevo, osim ako je označena simbolom $\star$.

- DESNO
  Pomiče glavu za jednu ćeliju udesno, osim ako je ćelija prazna.

- ZAPIŠI(k)
  Zapisuje u ćeliju simbol $k \in \Gamma \setminus \{\star\}$, osim ako je ćelija označena sa $\star$.

- PROČITAJ(k)
  Čita simbol u ćeliji te ako odgovara simbolu k, odlazi u stanje q_{DA}, a inače q_{NE}.

- ZAUSTAVI
  Odlazi u stanje q_{NE}.

- NIKAD-NE-ZAUSTAVI
  Ostaje na istom mjestu i ne mijenja stanje pa nikad neće stati.

- NE-PROČITAJ(k) = dok PROČITAJ(k) radi [STOP]
  Radi suprotno od PROČITAJ(k).

- ZVJEZDICA = dok NE-PROČITAJ($\star$) radi [LIJEVO]
  Postavlja glavu na $\star$.

- PRAZAN = ZVJEZDICA; dok NE-PROČITAJ(λ) radi [DESNO]
  Postavlja glavu na prvi prazni element slijeva.

- PRESKOČI = dok NE-PROČITAJ(0) radi [DESNO]
  Glava se pomiče udesno dok ne pročita simbol 0, ako ne postoji, stroj nikad neće stati.

- PRONAĐI(k)
  PRONAĐI(1) = ZVJEZDICA; PRESKOČI
  PRONAĐI($k+1$) = PRONAĐI(k); DESNO; PRESKOČI:
  Stroj PRONAĐI(k) zadan je rekurzivno i pomiče se do početka elementa a_k iz niza $(a_1, ..., a_n)$.

- POSLJEDNJI = PRAZAN; dok NE-PROČITAJ(0) radi [LIJEVO]
  Dolazi do početka reprezentacija posljednjeg elementa iz niza $(a_1, ..., a_n)$.

- NOVI = PRAZAN; ZAPIŠI(0)
  Pretvara niz $(a_1, ..., a_n)$ u $(a_1, ..., a_n, 0)$.

- INKREMENT = PRAZAN; ZAPIŠI(1)
  Pretvara niz $(a_1, ..., a_n)$ u $(a_1, ..., a_n + 1)$.

- DEKREMENT = PRAZAN; LIJEVO; if PROČITAJ(1) then ZAPIŠI(λ)
  Pretvara niz $(a_1, ..., a_n + 1)$ u $(a_1, ..., a_n)$.

- IZBRIŠI = PRAZAN; dok NE-PROČITAJ(0) radi [ZAPIŠI(λ); LIJEVO]; ZAPIŠI(λ)
  Pretvara niz $(a_1, ..., a_{n-1}, a_n)$ u $(a_1, ..., a_{n-1})$.

- OZNAČI(k) = dok DESNO; PROČITAJ(1) radi [ZAPIŠI(k)]
  Zamjenjuje uzastopna ponavljanja simbola 1 sa simbolom $k \in \{2, 3\}$.

- POSTOJI(k) = ZVJEZDICA; dok NE-PROČITAJ(k) radi [ako NE-PROČITAJ(λ) onda DESNO]
  Ukoliko naiđe na simbol $k \in \{2, 3\}$, stroj staje u stanje q_{DA}, a inače q_{NE}.

- POSTOJAO-JE(k) = ako POSTOJI(k) onda ZAPIŠI(1)
  Ukoliko naiđe na simbol $k \in \{2, 3\}$, stroj zamjenjuje simbol k simbolom 1.

- OBNOVI = dok POSTOJI(2) radi [POSTOJAO-JE(2)]; dok POSTOJI(3) radi [POSTOJAO-JE(3)]
  Zamjenjuje sve simbole 2 ili 3 na traci simbolom 1.

- PRIDODAJ(k) = PRONAĐI(k); označi(2); dok POSTOJAO-JE(2) radi [INKREMENT]
  Pretvara niz $(a_1, ..., a_n)$ u $(a_1, ..., a_n + a_k)$.

- KOPIRAJ(k) = NOVI; PRIDODAJ(k)
  Pretvara niz $(a_1, ..., a_n)$ u $(a_1, ..., a_n, a_k)$.

- ZBROJI(k, l) = KOPIRAJ(k); PRIDODAJ(l)
  Pretvara niz $(a_1, ..., a_n)$ u $(a_1, ..., a_n, a_k + a_l)$.

- POMNOŽI(k, l) = NOVI; PRONAĐI(k); OZNAČI(3); dok POSTOJAO-JE(3) radi [PRIDODAJ(l)]
  Vrijedi za $k \neq l$ i pretvara niz $(a_1, ..., a_n)$ u $(a_1, ..., a_n, a_k a_l)$.

- POMNOŽI(k, k) =
  KOPIRAJ(k); POSLJEDNJI; OZNAČI(3);
  dok POSTOJAO-JE(3) radi [dok POSTOJAO-JE(3) radi [PRIDODAJ(k)]]
  Pretvara niz $(a_1, ..., a_k)$ u $(a_1, ..., a_k^2)$.

- NIJE-VEĆI(k, l) =
  PRONAĐI(k); OZNAČI(2); PRONAĐI(l); OZNAČI(3);
  dok POSTOJI(2) i POSTOJI(3) radi [POSTOJAO-JE(2); POSTOJAO-JE(3)];
  dok POSTOJ(2) radi [OBNOVI; ZAUSTAVI];
  OBNOVI
  Uspoređuje a_k i a_l i staje u stanju q_{DA} ako $a_k \leq a_l$, a inače u q_{NE}.

- JEDNAKI(k, l) = NIJE-VEĆI(k, l) i NIJE-VEĆI(l, k)
  Određuje jesu li a_k i a_l jednaki.

- NISU-JEDNAKI(k, l) = dok JEDNAKI(k, l) radi [STOP]
  Radi suprotno od JEDNAKI(k, l).

- SLJEDEĆI = POSLJEDNJI; ZAPIŠI(1); DESNO;
  dok PROČITAJ(λ) radi [ZAPIŠI(1); POSLJEDNJI; DESNO]; ZAPIŠI(0)
  Pretvara niz $(a_1, ..., a_n)$ u $(a_1, ..., a_{n-2}, b, c)$ gdje je (b, c) par koji slijedi nakon (a_{n-1}, a_n) u Cantorovoj listi parova dijagonalizacije.

- DEKODIRAJ = POSLJEDNJI; OZNAČI(2); NOVI; NOVI; dok POSTOJAO-JE(2) radi [SLJEDEĆI]
  Pretvara niz $(a_1, ..., a_n)$ u $(a_1, ..., a_n, b, c)$ gdje je (b, c) par koji daje Cantorov broj a_n.

6.3 Turingovi strojevi prepoznaju Diofantske skupove

Definicija 6.2. *Kažemo da* ***Turingov stroj*** $\mathcal{T} = (Q, \Sigma, \Gamma, \delta, q_0, q_{DA}, q_{NE})$ ***prepoznaje*** *neku riječ* $w \in \Gamma*$ *ako postoji konačan niz parova* $(r_1, s_1), ..., (r_m, s_m) \in Q \times \Gamma$ *te konačan niz simbola* $I_2, ..., I_m \in \{L, D, S\}$ *tako da vrijedi:*

- $r_1 = q_1$ *i* s_1 *je prvi lijevi simbol riječi* w*;*
- *za svaki* $j \in \{1, ..., m-1\}$ *imamo* $\delta(r_j, s_j) = (r_{j+1}, s_{j+1}, I_{j+1})$ *i* $r_j \notin \{q_{DA}, q_{NE}\}$;
- $r_m = q_{DA}$.

Propozicija 6.3. *Neka je* $D(a_1, ..., a_n, x_1, ..., x_{m+1}) = 0$ *parametarska diofantska jednadžba. Postoji Turingov stroj koji počinje s reprezentacijom niza* $(a_1, ..., a_n)$ *i u jednom trenutku će stati ako i samo ako je* D *rješiva u* $x_1, ..., x_{m+1}$.

Dokaz. Prvo ćemo konstruirati pomoćni stroj M_1 koji za danu niz $(a_1, ..., a_n, y_0)$ odlučuje je li y_0 Cantorov broj niza $(x_1, ..., x_{m+1})$ koji ne zadovoljava jednadžbu D. Taj stroj M_1 konstruiran je konkatenacijama nekoliko drugih strojeva koristeći operaciju ";". Koristimo m puta stroj DEKODIRAJ da bismo pretvorili $(a_1, ..., a_n, y_0)$ u

$$(a_1, ..., a_n, y_0, x_1, y_1, ..., x_m, y_m)$$

gdje je $y_{k-1} = \text{Cantor}(x_k, y_k)$. Iz toga slijedi da je

$$y_0 = \text{Cantor}_{m+1}(x_1, ..., x_m, y_m).$$

Početnu diofantsku jednadžbu možemo zapisati u obliku

$$C_L(a_1, ..., a_n, x_1, ..., x_m, y_m) = C_R(a_1, ..., a_n, x_1, ..., x_m, y_m),$$

gdje su C_L i C_R polinomi čiji su koeficijenti prirodni brojevi i nepoznanica x_{m+1} zamijenjena je s y_m. Računanje vrijednosti C_L i C_R može se prikazati kao niz elementarnih operacija

$$z_1 = \alpha_1 \circ_1 \beta_1,$$

$$\vdots$$

$$z_k = \alpha_k \circ_k \beta_k,$$

gdje su $\alpha_i, \beta_i \in \{1, a_1, ..., a_n, x_1, ..., x_m, y_m, z_1, ..., z_{k-1}\}$ i gdje je svaki $\circ_i$ ili + ili $\cdot$, a vrijednosti C_L i C_R pojavljuju se među $z_1, ..., z_k$. Kombinacijom strojeva NOVI, INKREMENT, ZBROJI i POMNOŽI $(a_1, ..., a_n, y_0, x_1, y_1, ..., x_m, y_m)$ može se pretvoriti u

$$(a_1, ..., a_n, y_0, x_1, y_1, ..., x_m, y_m, 1, z_1, z_k).$$

Da bismo dovršili konstrukciju stroja M_1, dovoljno je iskoristiti stroj NISU-JEDNAKI s odgovarajućim ulaznim argumentima. Tim će se stroj M_1 zaustaviti u stanju q_{DA} ako y_0 iz niza $(a_1, ..., a_n)$ nije Cantorov broj rješenja diofantske jednadžbe D, a u stanje q_{NE} ako je.

Neka je M_2 stroj koji se sastoji od $2m + k + 1$ strojeva IZBRIŠI. Očito M_2 transformira

$$(a_1, ..., a_n, y_0, x_1, y_1, ..., x_m, y_m, 1, z_1, ..., z_k)$$

u $(a_1, ..., a_n, y_0)$. Sada možemo definirati stroj M kao

$$M = \text{NOVI; dok } M_1 \text{ radi } [M_2; \text{INKREMENT}].$$

Stroj M započinje transformiranjem niza

$$(a_1, ..., a_n) \rightarrow (a_1, ..., a_n, 0).$$

Ako M_1 odluči da je 0 Cantorov broj rješenja jednadžbe D, tada M odmah staje s radom. Inače, stroj M_2 i INKREMENT konstruiraju niz

$$(a_1, ..., a_n, 1)$$

i stroj M_1 provjerava je li 1 Cantorov broj rješenja i tako dalje. Ako D ima rješenje, stroj M jednom će stati, a ako nema, stroj nastavlja s radom zauvijek.

□

6.4 Turing-poluodlučiv skup je diofantski

Poluodlučivost diofantskih jednadžbi intuitivno je svojstvo te dokazivanje potvrđuje da su Turingovi strojevi dovoljno snažni unatoč njihovim primitivnim funkcijama.

Definicija 6.4. *Kažemo da je skup $\mathfrak{M}$ nizova prirodnih brojeva duljine n Turing-poluodlučiv ako postoji Turingov stroj M takav da započinje u stanju q_1, s trakom koja sadrži prikaz niza $(a_1, ..., a_n)$, kojem glava čita najljeviju ćeliju na traci i koji će stati ako i samo ako je $(a_1, ..., a_n) \in \mathfrak{M}$. U tom slučaju M poluodlučuje $\mathfrak{M}$.*

U prošlom smo poglavlju pokazali da je svaki diofantski skup također i Turing-poluodlučiv, a u ovom poglavlju želimo pokazati obrnutu implikaciju.

Propozicija 6.5. *Svaki Turing-poluodlučiv skup je diofantski.*

Neka je M Turingov stroj takav da poluodlučuje skup $\mathfrak{M}$ koji se sastoji samo od nizova prirodnih brojeva duljine n te neka je $\{\alpha_1, ..., \alpha_w\}$ alfabet stroja M. U svakom koraku prolaska stroja M kroz operacije, simboli iz alfabeta zauzimaju konačno mnogo početnog segmenta trake duljine l pa stoga možemo prikazati traku kao $(s_1, s_2, ..., s_m, ..., s_{l-1}, s_l)$ koji se sastoji samo od indeksa čiji se simboli pojavljuju u ćelijama. Trenutno stanje q_i i položaj glave može se prikazati nizom jednake duljine $(0, ..., i, ..., 0)$. Samo je jedan element različit od 0 te se nalazi na poziciji glave. Trojka koja se sastoji od trenutnog sadržaja trake, stanja i položaja zove se konfiguracija. Očito navedeni nizovi jedinstveno određuju konfiguraciju.

Da bismo prikazali ove nizove, koristit ćemo pozicijsko kodiranje s fiksnom bazom β koja ne smije biti manja od 3, veća od broja stanja stroja M (v) i veća od broja simbola alfabeta (w). Par $\langle p, t\rangle$ kod je konfiguracije ako su p i t šifre nizova duljine l u bazi β. Stoga je konfiguracija jedinstveno određena kodom, a naša upotreba šifri nizova odgovara potencijalnoj beskonačnosti trake.

Naš je cilj konstruirati diofantsku jednadžbu

$$D(p, t, x_1, ..., x_m) = 0$$

takvu da ako je $\langle p, t\rangle$ kod konfiguracije, onda je diofantska jednadžba D rješiva u $x_1, ..., x_m$ ako i samo ako stroj M, koji započinje u ovoj konfiguraciji jednom stane. Zanemarit ćemo rješivost diofantskih jednadžbi rješive ako $\langle p, t\rangle$ nije kod konfiguracije.

Započinjemo simuliranjem jednog koraka Turingovog stroja. Zatim stroj M nastavlja iz konfiguracije s kodom $\langle p, t\rangle$ u konfiguraciju s kodom $\langle \text{SljedećiP}(p, t), \text{SljedećiT}(p, t)\rangle$. Trebamo provjeriti da su SljedećiP i SljedećiT diofantske funkcije. Do sada smo definirali funkcije SljedećiP i SljedećiT samo kad je $\langle p, t\rangle$ kod konfiguracije sa stanjem koje nije

završno. Postavimo

$$\text{SljedećiP}(p,t) = 0,$$
$$\text{SljedećiT}(p,t) = t$$

ako je $\langle p,t\rangle$ konfiguracijski kod s završnim stanjem. Podrazumijevamo da su funkcije SljedećiP i SljedećiT diofantske ako postoje diofantske funkcije koje su jednake funkcijama SljedećiP i SljedećiT ako je $\langle p,t\rangle$ kod konfiguracije, ali mogu biti bilo koje vrijednosti ili nedefinirane ako $\langle p,t\rangle$ nije kod konfiguracije.

Funkcije SljedećiP i SljedećiT određene su funkcijama A, D i Q dobivene iz funkcija prijelaza stroja M. Funkcija D za određeno stanje i simbol koji se nalazi u njemu predstavlja sljedeći korak Turingovom stroju iz skupa $\{L,S,D\}$, A indeks znaka iz alfabeta koji će se zapisati i Q indeks sljedećeg novog stanja. Proširujemo funkcije SljedećiP i SljedećiT za kod konfiguracije sa završnim stanjem postavljajući $A(i,j) = j$, $D(i,j) = S$ i $Q(i,j) = 0$ kad je q_i završno stanje.

Svaki je element niza sa šifrom $\text{SljedećiT}(p,t)$ jedinstveno određen elementima na istom mjestu u nizovima sa šiframa p i t. Definiramo funkciju A

$$A(i,j) = \begin{cases} A(i,j) & \text{ako } 0 < i \le v, 0 \le j \le w, \\ j & \text{inače.} \end{cases}$$

Sada možemo definirati SljedećiT kao

$$t' = \text{SljedećiT}(p,t) \iff \exists w[t' = A[\beta](p,t,w)]$$

gdje je $A[\beta]$ proširenje funkcije A.

Neka su

$$p^R = p\beta,$$
$$p^L = p \operatorname{div} \beta,$$
$$t^R = t\beta,$$
$$t^L = t \operatorname{div} \beta,$$

odnosno L i R pomiču niz za jedno mjesto ulijevo ili udesno pritom se za L briše prvi element i dodaje 0 na kraj, a za R obrnuto. Za SljedećiP uvest ćemo funkciju DQ:

$$DQ(i^L,i,i^R,j^l,j,j^R) = \begin{cases} Q(i^L,j^L) & \text{ako } i^L > 0, i = i^R \text{ i } D(i^L,j^L) = L, \\ Q(i,j) & \text{ako } i^L = 0, i > 0, i^R = 0 \text{ i } D(i,j) = S, \\ Q(i^R,j^R) & \text{ako } i^L = i = 0, i^R > 0 \text{ i } D(i^R,j^R) = R, \\ 0 & \text{inače.} \end{cases}$$

Sada možemo dati diofantsku reprezentaciju za SljedećiP:

$$p' = \text{SljedećiP}(p,t) \Longleftrightarrow \exists w[p' = DQ[\beta](p\beta, p, p \text{ div } \beta, t\beta, t, t \text{ div } \beta, w)].$$

Da bismo dobili više koraka Turingovog stroja, definirat ćemo i funkcije NakonP i NakonT koje će primati tri argumenta od kojih je prvi broj koraka koje želimo napraviti:

$$\begin{aligned}
\text{NakonP}(0,p,t) &= p,\\
\text{NakonT}(0,p,t) &= t,\\
\text{NakonP}(k+1,p,t) &= \text{SljedećiP}(\text{NakonP}(k,p,t), \text{NakonT}(k,p,t)),\\
\text{NakonT}(k+1,p,t) &= \text{SljedećiT}(\text{NakonP}(k,p,t), \text{NakonT}(k,p,t)).
\end{aligned}$$

Potreban nam je još jedan korak da bismo mogli konstruirati diofantsku jednadžbu. Neka su $\omega_1, ..., \omega_z$ indeksi završnih stanja stroja M. Sljedeći uvjet

$$\exists k, r[\text{Elem}(\text{NakonT}(k,p,t),\beta,r) = \omega_1 \vee \cdots \vee \text{Elem}(\text{NakonT}(k,p,t),\beta,r) = \omega_z]$$

vrijedi za kod konfiguracija $\langle p,t\rangle$ ako i samo ako stroj koji započinje tom konfiguracijom u nekom trenutku stane. Uvjet je diofantski pa se može transformirati u diofantsku jednadžbu $D(p,t,x_1,...,x_m) = 0$. Da bismo dokazali da je $\mathfrak{M}$ poluodlučiv strojem M, trebamo zamijeniti p i t parametrima $a_1, ..., a_n$. Neka je $p = 1$ i konkatenacija

$$\langle t,\beta,a\rangle = \langle\kappa,\beta,1\rangle{+}\langle\mu,\beta,1\rangle{+}\langle\text{Ponovi}(\nu,\beta,a_1),\beta,a_1\rangle{+}\cdots{+}\langle\mu,\beta,1\rangle{+}\langle\text{Ponovi}(\nu,\beta,a_n),\beta,a_n\rangle$$

gdje je $a = a_1 + \cdots + a_n + n + 1$ broj zauzetih ćelija, a κ, μ i ν indeksi simbola $\star$, 0 i 1. Time smo dobili potrebnu diofantsku reprezentaciju skupa $\mathfrak{M}$.

6.5 Neodlučivost Hilbertovog desetog problema Turingovim strojevima

Definicija 6.6. *Kažemo da je skup $\mathfrak{M} \in \mathbb{N}^n$ Turing-odlučiv ako postoji Turingov stroj M takav da za ulaz $(a_1,,,,.a_n)$ stroj staje u stanju q_{DA} ako je iz skupa $\mathfrak{M}$, a inače staje u stanje q_{NE}.*

Ako je skup Turing-odlučiv, tada je i Turing-poluodlučiv. Također ako je skup odlučiv, tada je i njegov komplement poluodlučiv. Ako su skup i njegov komplement poluodlučivi, tada je skup odlučiv. Konstrukcijom para diofantski jednadžbi

$$D_2(a_1, ..., a_n, x_1, ..., x_m) = 0$$

i

$$D_3(a_1, ..., a_n, x_1, ..., x_m) = 0,$$

definiramo skup $\mathfrak{M}$ i njegov komplement. Kombiniramo dvije jednadžbe u jednu

$$(D_2^2(a_1, .., a_n, x_1, ..., x_m) + (1 - y_m)^2) \cdot (D_3^2(a_1, ..., a_n, x_1, ..., x_m) + y_m) = 0. \tag{6.1}$$

Očito jednadžba ima rješenje ako i samo ako je $y_m = 1$. Neka je M stroj

$$M = \text{NOVI; dok } M_1 \text{ radi } [M_2; \text{INKREMENT}].$$

konstruiran s jednadžbom (6.1). Kada M stane, traka će sadržavati prikaz niza

$$(a_1, ..., a_n, y_0, x_1, y_1, ..., x_m, y_m, 1, z_1, ..., z_k).$$

Stroj koji odlučuje skup $\mathfrak{M}$ može biti definiran kao

$$M; \text{JEDNAKI}(l, l + 1)$$

gdje je $l = n + 1 + 2m$. Taj stroj određuje je li $y_m = 1$ vrijedi jer su 1 i y_m l. i $(l + 1)$. elementi niza. Sada možemo preoblikovati Hilbertov deseti problem tako da se pitamo je li skup kodova svih rješivih diofantskih jednadžbi Turing-odlučiv. Za taj skup već smo utvrdili da mu komplement nije diofantski pa onda slijedi da takav skup ne može biti Turing-odlučiv. Nemoguće je konstruirati Turingov stroj koji započinje s reprezentacijom broja k na traci takav da će se zaustaviti nakon konačnog broja koraka u stanju q_{DA} ili q_{NE} ovisno je li jednadžba s kodom k rješiva ili ne. Sam taj skup je diofantski. Zbog toga Turingovi strojevi nisu u mogućnosti odlučiti je li jednadžba koja pripada nekoj familiji diofantskih jednadžbi ima rješenja.

Bibliografija

[1] P. E. Black. Algorithms and Theory of Computation Handbook. *CRC Press LLC*, 1999.

[2] L. Cabusora. *Diophantine Sets, Primes, and the Resolution of Hilbert's 10th Problem*. PhD thesis, Harvard University, 2004.

[3] W. Conradie and V. Goranko. *Logic and Discrete Mathematics: a Concise Introduction*. John Wiley & Sons, 2015.

[4] M. Davis. Arithmetical Problems and Recursively Enumerable Predicates. *The journal of symbolic logic*, 18(1):33–41, 1953.

[5] M. Davis, H. Putnam, and J. Robinson. The Decision Problem for Exponential Diophantine Equations. *Annals of Mathematics*, pages 425–436, 1961.

[6] D. Hilbert. Mathematical Problems. *Bulletin of the American Mathematical Society*, 8(10):437–479, 1902.

[7] A. J. Ho. Hilbert's Tenth Problem. `https://sites.math.washington.edu/~morrow/336_15/papers/andrew.pdf`.

[8] J. P. Jones. Universal Diophantine Equation. *The journal of symbolic logic*, 47(3):549–571, 1982.

[9] S. C. Kleene. Introduction to Metamathematics. 1952.

[10] E. E. Kummer. Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen. 1852.

[11] Y. Matijasevič. *Hilbert's Tenth Problem*. MIT press, 1993.

[12] Y. Matijasevič. My Collaboration with Julia Robinson. In *Mathematical Conversations*, pages 49–60. Springer, 2001.

[13] A. J. Misner and T. Bay. Hilbert's Tenth Problem. https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.1052.5077&rep=rep1&type=pdf, 2013.

[14] M. R. Murty and B. Fodden. *Hilbert's Tenth Problem: An Introduction to Logic, Number Theory, and Computability*, volume 88. American Mathematical Soc., 2019.

[15] E. Omodeo and A. Policriti. Martin Davis on Computability, Computational Logic, and Mathematical Foundations. *The Mathematical Intelligencer*, 10(2), 2016.

[16] E. L. Post. Recursively enumerable sets of positive integers and their decision problems. *Bulletin of the American Mathematical Society*, 50(5):284–316, 1944.

[17] P. Rendell. Turing universality of the game of life. In *Collision-based computing*, pages 513–539. Springer, 2002.

[18] J. Robinson. Existential Definability in Arithmetic. *Transactions of the American Mathematical Society*, 72(3):437–449, 1952.

[19] J. Robinson. Unsolvable diophantine problems. *Proceedings of the American Mathematical Society*, 22(2):534–538, 1969.

[20] M. Sipser. *Introduction to the Theory of Computation*. Cengage Learning, 3rd edition, 2013.

[21] The Editors of Encyclopaedia Britannica. Georg cantor. https://www.britannica.com/biography/Georg-Ferdinand-Ludwig-Philipp-Cantor.

[22] A. Wiles. Modular Elliptic Curves and Fermat's Last Theorem. *Annals of mathematics*, 141(3):443–551, 1995.

[23] C. Xu. Computable Functions. https://sites.math.washington.edu/~morrow/336_20/papers20/chen.pdf, 2020.

[24] R. Zach. Hilbert's program. https://plato.stanford.edu/entries/hilbert-program/, 2003.

Sažetak

David Hilbert objavio je 23 problema koji su doprinijeli razvoju matematike u 20. stoljeću. U Hilbertovom desetom problemu cilj je bio pronaći proces koji u konačnom broju operacija može odrediti ima li bilo koja jednadžba cjelobrojno rješenje. Yuri Matijasevič 1970. godine dokazao je posljednju tvrdnju koja je nedostajala da bi se pokazalo da takav proces, koji danas promatramo kao algoritam, ipak ne postoji.

Rad sadrži dokaz nerješivosti Desetog problema. Na početku smo istaknuli i objasnili pojmove iz teorije izračunljivosti te uveli pojam diofantskog skupa za koji želimo dokazati da je ekvivalentan poluodlučivom skupu iz teorije izračunljivosti. Diofantske jednadžbe, odnosno jednadžbe čiji su koeficijenti i rješenja cjelobrojni, definiraju diofantske skupove pa kad bismo dokazali da nisu odlučivi, mogli bismo zaključiti da Hilbertov deseti problem nema rješenje. Dalje smo dokazali da su eksponencijalne funkcije diofantske koristeći Fibonaccijeve nizove, što je predstavljalo prepreku pri dokazu navedene ekvivalencije. Samu ekvivalenciju dokazali smo uvođenjem univerzalne diofantske jednadžbe i Turingovih strojeva. Prije samog dokaza uveli smo vrste kodiranja poput Cantorovog te Gödelovog te diofantske relacije.

Summary

David Hilbert published twenty-three problems that contributed to the development of mathematics in the 20th century. Hilbert's tenth problem asked to devise a process according to which it can be determined by a finite number of operations whether the equation is solvable in rational integers. In 1970, Yuri Matijasevich finally proved the missing link in decades-long proof research to show that such a process, today regarded as an algorithm, does not exist.

This work contains proof of unsolvability to the Tenth problem. In the beginning, we indicate and clarify the basic notions in the theory of computability. We introduce the diophantine set for which we want to demonstrate the equivalence to the semidecidable set established in the theory of computability. Diophantine equations, i.e., equations composed with integer coefficients and solutions, define diophantine sets. Proving that the diophantine sets are also semi-decidable implies the unsolvability of Hilbert's tenth problem. Furthermore, we also show that the exponential functions are diophantine using Fibonacci's sequences, which was the last obstacle of the mentioned equivalence. Introducing the universal diophantine equation, as well as the Turing machines makes it possible to conclude the equivalence. For the proof, we also introduce different types of coding, e.g., Cantor's and Gödel's coding, and necessary diophantine relations.

Životopis

Rođen sam 25. srpnja 1994. godine u Metkoviću. Osnovnu školu Stjepana Radića završavam 2009. godine nakon koje upisujem Gimnaziju Metković prirodoslovno-matematičkog usmjerenja. Nakon završetka gimnazije 2013. godine upisujem preddiplomski sveučilišni studij Matematike na Prirodoslovno-matematičkom fakultetu u Zagrebu. Preddiplomski studij završavam 2018. te iste godine upisujem diplomski studij Računarstva i matematike na istom fakultetu. U ljetnom semestru akademske godine 2018./2019. sudjelujem u studentskoj razmjeni na Sveučilištu u Dortmundu.