Математичка гимназија

МАТУРСКИ РАД

- из математике -

Геделове теореме о непотпуности

Ученик:
Стефан Схрестха IVa

Ментор:
др Зоран Петрић

Београд, јун 2023.

Садржај

1 Увод

Геделове теореме о непотпуности једне су од најважнијих резултата модерне логике и имале су дубок утицај на логику и математику, али и на филозофију математике.

Курт Гедел (1906-1978) је ове резултате објавио у свом револуционарном раду из 1931. године. Теореме о непотпуности нам говоре о границама доказивости унутар формалних система. Угрубо, прва теорема о непотпуности каже да било који формални систем, који задовољава одређене услове, не може бити потпун, то јест не може доказати сва тачна тврђења о природним бројевима. Друга теорема о непотпуности још додаје да овакви формални системи не могу доказати своју конзистентност.

Циљ овог рада је да читаоцу представимо Геделове теореме о непотпуности, али и да прво уведемо и објаснимо сву потребну теорију за њихово разумевање.

Прво ћемо обрадити основне појмове теорије израчунљивости и дефинисати рекурзивне функције и релације. Затим ћемо увести и потребну теорију из логике, конкретније, појмове синтаксе и семантике. У следећем поглављу, прелазимо на Геделову идеју о аритметизацији синтаксе. Затим у поглављу о репрезентабилности, повезаћемо наш рад с рекурзивним функцијама са језиком аритметике, овде уводимо и теорију минималне аритметике. Коначно, у шестом поглављу представићемо Геделове теореме о непотпуности и рећи нешто више о њима, као и о њиховом филозофском значају.

2 Теорија израчунљивости

Када је Гедел објавио свој револуционарни рад 1931. године, још није постојала генерална теорија израчунљивости. Оно што је недостајало је опширна и формална анализа интуитивних појмова, као што су ефективна израчунљивост и ефективна одлучивост. На пример, мора бити ефективно одлучиво да ли је неки низ тврђења доказ неког другог тврђења. Теорија израчунљивости процветала је 1930-тих година, управо са радовима Курта Гедела, Алана Тјуринга, Алонза Черча... Данас уместо појмова ефективно израчунљивих функција и ефективно одлучивих релација имамо појмове рекурзивних функција и рекурзивних релација. Иако су само интуитивни, концепти ефективне израчунљивости и одлучивости могу нам помоћи у разумевању других формалних идеја у теорији израчунљивости.

2.1 Ефективна израчунљивост и одлучивост

Још одавно су нам познате процедуре за множење два броја или налажења њиховог НЗД-а, као и процедура за проверу да ли је неки број прост. Ове процедуре нам омогућавају да ефективно (илити у потпуности механички) израчунамо вредности неких функција.

Шта тачно мислимо под "ефективно израчунамо" је да постоји алгоритам који се завршава после коначно много времена који можемо да пратимо како би дошли до тражене вредности функције. Алгоритам је унапред одређен скуп инструкција, где је свака инструкција до детаља описана, не остављајући простора погрешном тумачењу. Извршавање алгоритма се може посматрати као низ дискретних малих корака које би и врло једноставна машина могла да уради (нпр. Тјурингова машина), где нема никакве потребе за ингениозношћу саме машине или ослањања на спољашње изворе информација.

Дефиниција 2.1. *Функција f је ефективно израчунљива, ако постоји алгоритам којим би, у коначно много корака, могли да израчунамо вредност те* *фунцкије за било који елемент њеног домена.*

Приметимо да под ефективно не мислимо и ефикасно, или уопште извршиво у пракси. Мислимо само на то да би у теорији са довољно времена и простора могли да израчунамо вредност дате фунцкије.

Интересоваће нас и када је нека релација, илити својство природних бројева, ефективно одлучиво, то јест да ли постоји одговарајући алгоритам који би нам, у коначно много корака, дао одговор на питање да ли та релација важи за неки објекат. Обично ће то бити природан број или уређена k-торка.

Дефиниција 2.2. *Карактеристична функција за k-арну релацију R је k-арна функција $c_R : \mathbb{N}^k \to \{0, 1\}$, таква да је $c_R(x_1, \ldots, x_k) = 1$ ако $(x_1, \ldots, x_k) \in R$ и $c_R(x_1, \ldots, x_k) = 0$ у супротном.*

Дефиниција 2.3. *Релација је ефективно одлучива ако је њена карактеристична функција ефективно израчунљива.*

Дефиниција 2.4. *Скуп природних бројева је ефективно одлучив ако је карактеристична функција релације припадања том скупу ефективно израчунљива.*

2.2 Примитивно рекурзивне функције

У овом поглављу дефинисаћемо скуп **примитивно рекурзивних** функција, а затим и показати да су неке нама врло добро познате фунцкије примитивно рекурзивне. Примитивно рекурзивне функције добијају се коришћењем композиције и примитивне рекурзије. Затим ћемо овај скуп надограти операцијом минимизације и тиме добити цео скуп рекурзивних функција.

Почињемо са пар једноставних функција које ћемо звати **основним**, помоћу којих ћемо изградити све рекурзивне функције.

Основне функције су:

1. **Нула функција** која за сваки број узима вредност нула:

$$z(n) = 0$$

2. **Следбеник функција**:

$$s(n) = n + 1$$

3. **Пројекција i-те кординате**:

$$id_i^k(x_1, \ldots, x_k) = x_i \text{ , где је } 1 \leq i \leq k$$

Прва операција која нам омогућава да од основних правимо још рекурзивних функција јесте **композиција**. Тачније, ако је f примитивно рекурзивна функција m аргумената и $g_1, \ldots, g_m$ примитивно рекурзивне функције n аргумената, онда је и:

$$h(x_1, \ldots, x_n) = f(g_1(x_1, \ldots, x_n), \ldots, g_m(x_1, \ldots, x_n))$$

примитивно рекурзивна функција. У скраћеној нотацији ово можемо записати и као:

$$\boxed{h = Cn[f, g_1, \ldots, g_m]}$$

Пример 2.1. *Нека су $m, n \in \mathbb{N}_0$ функција $const_n(m) = n$ је примитивно рекурзивна. Приметимо да је нула функција у ствари $const_0$, а $const_1$ можемо добити композицијом следбеник и нула функције тј. $const_1 = Cn[s, z]$. Сада компоновањем $const_1$ са следбеник функцијом добијамо $const_2$. Оваквим процесом се очигледно може добити $const_n$ за сваки природан број n. На пример, $const_4$ би добили овако:*

$$const_4 = Cn[s, Cn[s, Cn[s, Cn[s, z]]]].$$

Друга операција која нам омогућава да дефинишемо скоро све нама познате функције јесте **примитивна рекурзија**. Нека су f и g примитивно рекурзивне функције онда је примитивно рекурзивна и функција h дефинисана на следећи начин:

$$\begin{aligned} h(x, 0) &= f(x) \\ h(x, s(y)) &= g(x, y, h(x, y)). \end{aligned}$$

У скраћеној нотацији то би изгледало овако $\boxed{h = Pr[f, g]}$.

Напомена. *Ова дефиниција лако се може уопштити на функције више од 2 или само једног аргумента, довољно је у свакој дефиницији заменити x са $x_1, \ldots, x_n$ или га у потпуности избацити (у случају функције једне променљиве $f(x)$ је само константа).*

Формално скуп примитивно рекурзивних функција дефинишемо на следећи начин.

Дефиниција 2.5. *Скуп примитивно рекурзивних функција је најмањи скуп функција који садржи три поменута типа основних функција и затворен је у односу на операције композиције и примитивне рекурзије.*

Пример 2.2 (Сабирање). *Посматрајмо функцију која сабира два броја, правила за израчунавање ове функције могу се концизно записати као:*

$$\begin{aligned} x + 0 &= 0 \\ x + s(y) &= s(x + y). \end{aligned}$$

Овај запис свакако да подсећа на функцију дефинисану помоћу примитивне рекурзије, дефинишимо је сад користећи нашу званичну дефиницију примитивне рекурзије:

$$\begin{aligned} suma(x, 0) &= f(x) = id_1^1(x) \\ suma(x, s(y)) &= g(x, y, suma(x, y)) = s(suma(x, y)). \end{aligned}$$

Илити у нашој скраћеној нотацији $suma = Pr[id_1^1, Cn[s, id_3^3]]$. *Овиме смо показали да је функција која узима два броја и враћа њихов збир примитивно рекурзивна.*

Пример 2.3 (Множење). *Слично сабирању, правила множења се могу записати на следећи начин:*

$$\begin{aligned} x \cdot 0 &= 0 \\ x \cdot s(y) &= x + x \cdot y. \end{aligned}$$

У нашој нотацији то би изгледало овако:

$$proizvod = Pr[z, Cn[suma, id_1^3, id_3^3]].$$

У примитивно рекурзивној дефиницији функције $proizvod$ користили смо функцију $suma$ за коју смо пре тога показали да је примитивно рекурзивна. На сличан начин користићи функцију $proizvod$ можемо дефинисати екпоненцијалну функцију $exp(x, y) = x^y$,
$exp = Pr[Cn[s, z], Cn[proizvod, id_1^3, id_3^3]]$. Онда користећи exp можемо дефинисати такозвану супер-експоненцијалну функцију $supexp(x, y, z) = x^{y^z}$. Ево још неколико примера примитивно рекурзивних функција које ћемо касније користити.

Пример 2.4. *Следеће функције су примитивно рекурзивне:*

1. **Функција претходника** *$pred(x) = x - 1$ за $x \neq 0$ и $pred(x) = 0$ за $x = 0$.*

2. **Измењено одузимање** *које се дефинише $x \dot{-} y = x - y$ за $x \geq y$ и $x \dot{-} y = 0$ за $x < y$.*

3. **Сигнум функције** *$sg(0) = 0$ и $sg(x) = 1$ за $x \neq 0$, $\bar{sg}(x) = 0$ за $x \neq 0$ и $\bar{sg}(0) = 1$.*

4. *Нека је f примитивно рекурзивна функција онда су то и:*

$$g(x, y) = \sum_{i=0}^{y} f(x, i),$$
$$h(x, y) = \prod_{i=0}^{y} f(x, i).$$

Доказ. 1. Видимо да је $pred(0) = 0$, а $pred(s(x)) = x$ илити $pred = Pr[z, id_1^2]$.
2. $x \dot{-} 0 = x$, а $x \dot{-} s(y) = pred(x \dot{-} y)$.
3. $sg(x) = 1 \dot{-} (1 \dot{-} x)$, и $\bar{sg}(x) = 1 \dot{-} x$.
4. $g(x, 0) = f(x, 0)$, $g(x, s(y)) = suma(f(x, s(y)), g(x, y))$, а за другу функцију h важи $h(x, 0) = f(x, 0)$ и $h(x, s(y)) = proizvod(f(x, s(y)), h(x, y))$. □

У будућности се нећемо више трудити да примитивно рекурзивне функције записујемо преко званичне дефиниције, јасно ће бити да се то може урадити.

2.3 Минимизација

У претходном поглављу видели смо да са само три основне функције и две операције над њима можемо добити широк спектар функција. Сада уводимо и трећу операцију *минимизације*, с којом ћемо употпунити нашу дефиницју рекурзивних функција. Помоћу минимизације ћемо такође моћи да дефинишемо и парцијалне функције (до сада смо само говорили о тоталним функцијама). Интуитивно говорећи, постојаће ефекетивна процедура за израчунавање парцијалне функције за сваки елемент њеног домена, међутим за бројеве ван њеног домена можемо узети да наша процедура нема краја.

За дату функцију f са $n + 1$ аргумената **минимизација** нам даје следећу парцијалну функцију h од n аргумената за коју важи:

$Mn[f](x_1, \ldots, x_n) = y$, ако је $f(x_1, \ldots, x_n, y) = 0$ и ако за свако $z < y$ важи да је $f(x_1, \ldots, x_n, z)$ дефинисано и различито од нуле. Ако такво y не постоји, $Mn[f](x_1, \ldots, x_n)$ биће недефинисано.

Напоменимо овде да су све рекурзивне функције ефективно израчунљиве. Обрнуто тврђење зове се *Черчова теза.*

Хипотеза (Черчова теза)**.** *Све ефективно израчунљиве функције су заправо рекурзивне.*

Иако је ово само хипотеза, током година се накупила велика количина посредних доказа који указују на њену тачност. Практично сви резултати у овом поглављу, као и прилично незгодни докази Теорема 4.2 и 4.3 постају скоро тривијални уз њено прихватање. Ми ипак настављамо да радимо само са формалним појмом рекурзивних функција.

Можемо рећи и нешто више, примитивно рекурзивне функције су тачно оне функције које се могу израчунати помоћу коначно много **for** петљи. Ево примера псеудо-кода који рачуна вредност $f(m, n)$, где је $f = Pr[g, h]$.

1. $f = g(m)$
2. **for** $i = 0$ **to** $n - 1$
3. $f = h(m, i, f)$
4. **end do**

У променљивој f на завршетку програма налазиће се вредност $f(m, n)$. Испоставља се, да се не могу све ефективно израчунљиве функције израчунати помоћу коначно много **for** петљи[1], већ нам је потребна и неограничена претрага. У теорији израчунљивости ту улогу врши операција минимизације, док је то у свакодневним програмским језицима **while** петља.

2.4 Рекурзивне релације и скупови

Дефиниција 2.6. *Релација је (примитивно) рекурзивна ако је њена карактеристична функција (примитивно) рекурзивна.*

Посебан случај ове дефиниције који ће нас често интересовати је случај кад је R унарна релација илити само скуп. На пример, скуп простих бројева је примитивно рекурзиван, ово ћемо ускоро и доказати.

[1]За пример рекурзивне функције која није примитивно рекурзивна погледати *Акермանову функцију.*

Пример 2.5 $(=,<,\leq)$**.** *Релација једнакости између два броја је примитвно рекурзивна. Лако се проверава да је њена карактеристична функција заправо:*

$$c_=(x,y) = 1 \dot{-} (sg(x \dot{-} y) + sg(y \dot{-} x)).$$

Карактеристична функција за релацију $x < y$ *само* $sg(y \dot{-} x)$*, а за релацију* $x \leq y$*,* $1 \dot{-} sg(x \dot{-} y)$*. Ово су примитивно рекурзивне функције.*

Сада ћемо навести још један начин прављења нових (примитивно) рекурзивних функција помоћу (примитивно) рекурзивних релација. Ово су заправо две леме у зависности да ли читамо реч примитвно у заградама, исти доказ важи у оба случаја.

Лема 2.1 (Дефиниција по случајевима)**.** *Нека је* f *функција дефинисана на следећи начин:*

$$f(x,y) = \begin{cases} g_1(x,y) & \textit{ако } R_1(x,y) \\ \vdots & \quad \vdots \\ g_n(x,y) & \textit{ако } R_n(x,y) \end{cases}$$

где су релације $R_1, \ldots, R_n$ *(примитивно) рекурзивне и за свако* (x,y) *важи тачно једна од њих и где су* $g_1, \ldots, g_n$ *(примитивно) рекурзивне функције. Онда је* f *(примитивно) рекурзивна.*

Доказ. Нека је c_i карактеристична функција за релацију R_i. Функција f је заправо онда:

$$f(x,y) = \sum_{i=1}^{n} g_i(x,y)c_i(x,y).$$

Ова функција је (примитивно) рекурзивна. □

Пример овакве дефиниције су функције минимум и максимум:

$$min(x,y) = \begin{cases} x & \text{ако } x \leq y \\ y & \text{ако } y < x \end{cases} \qquad max(x,y) = \begin{cases} x & \text{ако } y \leq x \\ y & \text{ако } x < y \end{cases}$$

Дефиниција 2.7. *Ограничена егзистеницјална, односно универзална квантификација релације* $R(x_1, \ldots, x_n, y)$ *је релација* S *дефинисана на следећи начин:*

$$S(x_1, \ldots, x_n, z) \iff \exists y < z \, R(x_1, \ldots, x_n, y) \textit{ односно,}$$
$$S(x_1, \ldots, x_n, z) \iff \forall y < z \, R(x_1, \ldots, x_n, y)$$

у случају универзалне квантификације.

Дефиниција 2.8. *Под субституцијом тоталних функција* $f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n)$ *у релацију* $R(x_1, \dots, x_m)$ *мислимо на релацију* $R'(x_1, \dots, x_n)$ *дефинисану на следећи начин:*

$$R'(x_1, \dots, x_n) \iff R(f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n)).$$

Следећи скуп тврђења даће нам још начина за прављење нових (примитивно) рекурзивних релација. У исказу и доказу ове теореме писаћемо само реч рекурзивна, али ће она једнако важити ако испред сваког њеног појављивања додамо реч примитивно.

Теорема 2.1.

(а) Релација добијена супституцијом рекурзивних функција у рекурзивне релације је рекукрзивна.

(б) Ако је $f(x_1, \dots, x_n)$ *рекурзивна функција онда је рекурзивна и релација* G *(граф функције* f*) која је дефинисана као:*

$$G(x_1, \dots, x_n, y) \iff f(x_1, \dots, x_n) = y.$$

(ц) Негација рекурзвине релације је рекурзивна релација

(д) Конјункција две рекурзивне релације је рекурзивна релација.

(е) Дисјункција две рекурзивне релације је рекурзивна релација.

(ф) Релација добијена ограниченом егзистенцијалном квантификацијом рекурзивне релације је рекурзивна.

(г) Релација добијена ограниченом универзалном квантификацијом рекурзивне релације је рекурзивна.

Доказ. (а) Нека је R' релација добијена супституцијом рекурзивних функција n аргумената $f_1, \dots, f_m$ у рекурзивну релацију $R(x_1, \dots, x_m)$ односно:

$$R'(x_1, \dots, x_n) \iff R(f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n))$$

Карактеристична функције релације R' је онда:

$$c'(x_1, \dots, x_n) = c_R(f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n)),$$

Како је c' композиција рекурзивних функција то је и она рекурзивна, па самим тим је и релација R'.

(б) Карактеристична функција релације G је:

$$c_G(x_1,\ldots,x_n,y) = c_=(f(x_1,\ldots,x_n),y).$$

(ц) Ако је $R(x_1,\ldots,x_n)$ рекурзивна релација карактеристична функција њене негације је $c_{neg} = 1 \dot{-} c_R$.
(д),(е) Карактеристична функција коњункције релација R_1, R_2 је $c_\wedge = min(c_{R_1}, c_{R_2})$, а у случају дисјункције $c_\vee = max(c_{R_1}, c_{R_2})$.
(ф),(г) Ради прегледности пишемо $\vec{x}$ уместо $x_1,\ldots,x_n$.
Карактеристична фунцкија релације $\exists y < z\, R(\vec{x},y)$ је:

$$c(\vec{x},z) = sg\big(\sum_{i=0}^{z} c_R(\vec{x},i)\big) \dot{-} sg(c_R(\vec{x},z)).$$

Док је за релацију $\forall y < z\, R(\vec{x},y)$ то:

$$c(\vec{x},z) = c_R(\vec{x},z)\prod_{i=0}^{z} c_R(\vec{x},i) + (1 \dot{-} c_R(\vec{x},z))\prod_{i=0}^{z} c_R(\vec{x},i).$$

$\square$

Пример 2.6. *Скуп простих бројева P је примитивно рекурзиван. Ако је $P(x)$ релација која важи акко је x прост онда је она еквивалентна са:*

$$P(x) \iff 1 < x \ \wedge\ \forall u < x\ \forall v < x(v \cdot u \neq x).$$

Десна стране ове еквиваленције добијена је применом неколико различитих ставки претходне теореме. Како су све коришетене релације примитивно рекурзивне, то је и $P(x)$. Напоменимо да је $v \cdot u \neq x$ негација релације графа за функцију proizvod.

Теорема 2.2 (Ограничена минимизација и максимизација)**.** *За дату (примитивно) рекурзивну релацију R функције дефинисане на следећи начин:*

$$Min[R](x_1,\ldots,x_n,z) = \begin{cases} \textit{најмањем } y \leq z \textit{ за које важи } R(x_1,\ldots,x_n,y) \\ z+1 \quad \textit{ако такво } y \textit{ не постоји} \end{cases}$$

$$Max[R](x_1,\ldots,x_n,z) = \begin{cases} \textit{највећем } y \leq z \textit{ за које важи } R(x_1,\ldots,x_n,y) \\ 0 \quad \textit{ако такво } y \textit{ не постоји} \end{cases}$$

су (примитивно) рекурзивне.

Доказ. Ради прегледности пишемо $\vec{x}$ уместо $x_1, \dots, x_n$.

Дајемо доказ за функцију $Min[R]$, случај $Max[R]$ је сличан. Посматрајмо (примитивно) рекурзивну релацију $\forall t \leq y \neg R(\vec{x}, t)$. Ако постоји најмање y тако да је $R(\vec{x}, y)$ за њену карактеристичну функцију важиће:

$$c(\vec{x}, 0) = c(\vec{x}, 1) = \dots = c(\vec{x}, y-1) = 1 \text{ и } c(\vec{x}, y) = \dots = c(\vec{x}, z) = 0,$$

ако такво y не постоји све вредности $c(\vec{x}, i)$, $0 \leq i \leq z$ биће једнаке 1. У сваком случају је:

$$Min[R](\vec{x}, z) = \sum_{i=0}^{z} c(\vec{x}, i).$$

□

Коначно смо у позицији да докажемо да су неке функције, које ће нам бити неопходне у даљем раду, (примитивно) рекурзивне.

Пример 2.7. *Помоћу претходне теореме можемо и дефинисати функције које израчунавају* **количник** *и* **остатак** *при дељењу нека два броја. Ако је* $n = k \cdot m + r$, *где је* $r < m$, *тражене функције треба да узимају редом вредности* k *и* r. *Оне се могу дефинисати овако:*

$$quo(n, m) = \begin{cases} \text{највеће } \ k \text{ такво да је } k \cdot m \leq n \\ 0 \quad \text{ако је } \ m = 0 \end{cases}$$

за количник, док ће остатак онда само бити $rem(n, m) = n - quo(n, m) \cdot m$.

Као последицу претходног примера лако дефинишемо и релацију "|" (дели).

$$m|n \iff rem(n, m) = 0 \land m \neq 0.$$

Следеће функције се односе на представљање (кодирање) коначног низа природних бројева само једним бројем. Кодирање које користимимо је следеће:

$$\text{низ } (a_0, a_1, \dots, a_{n-1}) \text{ кодирамо бројем } 2^n \cdot 3^{a_0} \cdot \ldots \cdot \pi_n^{a_{n-1}},$$

где је π_{n-1}, n-ти прост број.

Теорема 2.3.

(a) *Функција* $\pi(n-1) = \pi_{n-1}$, *где је* π_{n-1}, n*-ти прост број је примитивно рекурзивна* ($\pi(0) = 2, \pi(1) = 3 \dots$).

(б) *Нека је* $ent(n, i)$ *експонент простог броја* π_{i+1} *у канонској факторизацији* n*. Функција* $ent(n, i)$ *је примитивно рекурзивна. Ова функција нам заправо даје* i*-ти члан оригиналног низа бројева,* $ent(n, i) = a_i$*.*

(ц) *Функција* $len(n)$ *која враћа експонент двојке у канонској факторизацији броја* n *је примитивно рекурзивна. Ова функција нам заправо даје дужину оригиналног низа бројева.*

Доказ. (а) Позивајући се на Теорему 2.2 дефинишимо функцију $h(n) = Min[R](n, 2n)$ где је $R(n, x) \Leftrightarrow n < x \wedge P(x)$ и где нам $P(x)$ говори да ли је број x прост. Функција $Min[R](n, 2n)$ онда узима вредност најмањег простог броја већег од n, а мањег од $2n$. Чињеница да између n и $2n$ увек постоји бар један прост број, зове се *Бертранд - Чебишевљева* теорема и може се доказати елементарном теоријом бројева. Тражена функција $\pi(n)$ се добија примитивно рекурзијом на следећи начин:

$$\begin{aligned} \pi(0) &= 2 \\ \pi(s(n)) &= h(\pi(n)). \end{aligned}$$

Како је h примитивно рекурзивна функција, то је и $\pi(n)$.
(б) Тражена функција биће само:

$$ent(n, i) = Min[R](i, n, n),$$

где је $R(i, n, x) \Leftrightarrow \pi^x(i + 1)|n \;\wedge\; \pi^{x+1}(i + 1) \nmid n$.
(ц) Слично као под *(б)*, тражена функција биће:

$$len(n) = Min[R](n, n)$$

где је овог пута $R(n, x) \Leftrightarrow 2^x|n \wedge 2^{x+1} \nmid n$. □

На пример, низ $(3, 2, 0, 1)$ кодирамо бројем $n = 2^4 \cdot 3^3 \cdot 5^2 \cdot 7^0 \cdot 11^1$ и важи $len(n) = 4$, $ent(n, 0) = 3$, $ent(n, 1) = 2$.

2.5 Рекурзивно набројиве релације

Интуитивно говорећи, скуп бројева је ефективно набројив, ако постоји алгоритам који ће нам при убацивању броја из тог скупа вратити 1 (или-ти 'да'), а ако број није из тог скупа, алгоритам се никад не завршава.

Конкретније после t малих корака алгоритма можемо видети да ли смо добили одговор 1 или још нисмо добили ништа. Зато можемо записати ефективно набројив скуп S као:

$$S(x) \iff \exists t\, R(x,t) \tag{1}$$

где је R ефективно одлучива релација, после t корака алгоритма добили смо одговор 1. Обрнуто, ако је $R(x,y)$ ефективно одлучива релација и S као у (1) онда је S ефективно набројив скуп. Можемо проверити редом да ли важи $R(x,0)$, $R(x,1)$, $R(x,2)$... Дефиниција рекурзивно набројивих релација биће слична овој за ефективно набројиве скупове, само што ефективно одлучива релација R сада рекуризвна.

Дефиниција 2.9. *Релација S је рекурзивно набројива, ако и само ако је она облика:*

$$S(x_1,\ldots,x_n) \iff \exists y\, R(x_1,\ldots,x_n,y),$$

где је R рекурзивна релација. Број y зовемо сведоком да релација S важи за $x_1,\ldots,x_n$.

Сада слично Теореми 2.1 имамо следећи низ тврђења.

Теорема 2.4.

(a) Свака рекрузивна релација је и рекурзивно набројива.

(б) Релација добијена супституцијом тоталних рекрузивних функција у рекурзивно набројиву релацију је рекурзивно набројива.

(ц) Конјункција и дисјункција две рекурзивно набројиве релације је рекурзивно набројива релација.

(д) Релација добијена **неограниченом** *егзистенцијалном квантификацијом или* **ограниченом** *универзалном квантификацијом рекурзивно набројиве релације је рекурзивно набројива релација.*

Доказ. Скраћено пишемо $\vec{x}$ за $x_1,\ldots,x_n$.

(a) Ако је $R(\vec{x})$ рекурзивна релација онда је то и $S(\vec{x},y) \Leftrightarrow R(\vec{x}) \wedge y = y$, а онда имамо и $R(\vec{x}) \Leftrightarrow \exists y\, S(\vec{x},y)$.

(б) Ако је R рекурзивно набројива релација $R(\vec{x}) \Leftrightarrow \exists y\, S(\vec{x},y)$, ми желимо да покажемо да је $R(f(\vec{x}))$ рекурзивно набројива. Пошто је S рекурзивна релација онда је то и S' дефинисана као $S'(\vec{x},y) \Leftrightarrow S(f(\vec{x}),y)$. Па је $R(f(\vec{x})) \Leftrightarrow \exists y\, S'(\vec{x},y)$, из чега следи да је $R(f(\vec{x}))$ рекурзивно набројива релација.

(ц) Нека је $R(\vec{x}) \Leftrightarrow \exists y\, S_1(\vec{x}, y)$ и $Q(\vec{x}) \Leftrightarrow \exists y\, S_2(\vec{x}, y)$, уз то што су S_1, S_2 рекурзивне релације. Онда важи:

$$(R(\vec{x}) \wedge Q(\vec{x})) \iff \exists w\, (\exists y_1 < w\, \exists y_2 < w(S_1(\vec{x}, y_1)) \wedge S_2(\vec{x}, y_2)),$$

где је десна страна, занемарујући $\exists w$, рекурзивна. Доказ за дисјункцију је још лакши.

(д) Ако је R рекурзивно набројива релација $R(\vec{x}, y) \Leftrightarrow \exists z S(\vec{x}, y, z)$, ако је $R'(\vec{x}) \Leftrightarrow \exists y R(\vec{x}, y)$ онда је релација $S'(\vec{x}, w) \Leftrightarrow \exists y < w \exists z < w S(\vec{x}, y, z)$ рекурзивна, а такође имамо и $R'(\vec{x}) \Leftrightarrow \exists w S(\vec{x}, w)$, што је и требало доказати. Случај ограничене универзалне кванитификације је сличан. $\square$

Замислимо сада да имамо алгоритам који нам у случају да је $m \in S$ на питање "Да ли је $m \in S$?" после коначно много времена даје одговор. Као и други алгоритам који нам у случају $m \notin S$ после коначно много времена даје одговор на питање "Да ли је $m \in \overline{S}$?" ($\overline{S}$ је комплемент скупа S). Ми бисмо комбиновањем ова два алгоритма могли да одредимо за произвољан број да ли је он елемент скупа S. Концизније ако су скуп и његов комплемент ефективно набројиви, онда је тај скуп заправо одлучив.

Следећа теорема нам ово и формално казује.

Теорема 2.5 (**Принцип комплементарности**). *Ако су скуп R као и његов комплемент $\overline{R}$ рекурзивно набројиви онда је скуп R (а због тога и $\overline{R}$) рекурзиван.*

Доказ. По претпоставци важи $R(x) \Leftrightarrow \exists y\, S^+(x, y)$ и $\neg R(x) \Leftrightarrow \exists y\, S^-(x, y)$, где су S^+ и S^- рекурзивне релације. Дефинишимо $S'(x, y) \Leftrightarrow (S^+(x, y) \vee S^-(x, y))$. И нека је $f(x)$ једнако најмањем y за које важи $S'(x, y)$.

Овако y увек постоји, да би ово видели размотримо следећа два случаја: ако би $x \in R$ (илити $R(x)$) по дефиницји важи $\exists y\, S^+(x, y)$, слично ако $x \in \overline{R}$ важи $\exists y\, S^-(x, y)$, у сваком случају $\exists y\, S'(x, y)$. Из овога следи да је f рекурзивна функција, која за домен има цео $\mathbb{N}_0$.

Али је онда $R(x) \iff S^+(x, f(x))$, то јест R се добија супституцијом рекурзивне функције f у рекурзивну релацију S^+, па је самим тим R рекурзиван скуп. $\square$

3 Логика

У овом поглављу обрадићемо два кључна појма логике првог реда која ће нас највише интересовати, то су *синтакса* и *семантика*. Затим ћемо поменути и синтактички појам, *доказне процедуре*, која нам омогућава да од неког скупа тврђења (аксиома) изводимо теореме (дедукције).

3.1 Синтакса

Синтакса се бави правилима писања и трансформисања израза формалног језика, без обзира да ли ти изрази имају неко значење и да ли им је дата нека интерпретација. Синтакса је у суштини граматика нашег језика. Правила синтаксе ће нам на пример рећи да је "$(A(x, y, z) \vee B(x, y))$" формула нашег језика, за разлику од "$A)(x, z(y)$" што није формула. Наш циљ у овом поглављу је да за појмове формуле, реченице и језика дамо строге дефиниције.

Логички симболи које ћемо користити биће класични логички везници: $\neg$ негација, $\vee, \wedge$ дисјункција и конјункција, $\Rightarrow$ импликација, $\iff$ еквиваленција, квантификатори "за сваки" $\forall$ и "постоји" $\exists$, као и промењиве $x, y, z \ldots$ које иду уз квантификаторе. Међу логичке симболе сврстаћемо и бинарни предикат једнакости $=$, мада ће ово бити једини предикат којег ћемо тако сврстати (остале предикате третирамо као нелогичке симболе). Притом, уз ове ћемо у логичке симболе сврставати леву "(" и десну ")" заграду као и зарезе ",".

Нелогичке симболе делимо на константе, предикате или релационе симболе, и функцијске симболе.

Узећемо да реч *језик* означава пребројив скуп нелогичких симбола.

Пример 3.1 (Језик аритметике). *Језик који ћемо ми све време користити зове се језик аритметике L_A. Његови нелогички симболи су константа нула* $\mathbf{0}$*, бинарни предикат "мање од" $<$, унарни функцијски симбол следбеник* $\boldsymbol{S}$ *и бинарни функцијски симболи сабирање $+$ и множење $\cdot$.*

Званично, ми ћемо рећи да за свако $k > 0$ радимо са фиксираним бесконачим пребројивим скупом симбола за k-арне предикате:

$$\begin{array}{lllll} A_0^1 & A_1^1 & A_2^1 & A_3^1 & \ldots \\ A_0^2 & A_1^2 & A_2^2 & A_3^1 & \ldots \\ A_0^3 & A_1^3 & A_2^3 & A_3^3 & \ldots \\ & & \vdots & & \end{array}$$

као и фиксираним бесконачим пребројивм скупом симбола за константе:

$$f_0^0,\ f_1^0,\ f_2^0,\ f_3^0 \ldots$$

Слично као за предикате, рећи ћемо да за свако $k > 0$ имамо фиксирани бесконачан скуп k-арних функцијских симбола:

$$\begin{array}{lllll} f_0^1 & f_1^1 & f_2^1 & f_3^1 & \ldots \\ f_0^2 & f_1^2 & f_2^2 & f_3^1 & \ldots \\ f_0^3 & f_1^3 & f_2^3 & f_3^1 & \ldots \\ & & \vdots & & \end{array}$$

као и фиксиран бесконачан скуп симбола за променљиве:

$$v_0,\ v_1,\ v_2,\ v_3 \ldots$$

Званичан језик ће опет онда бити пребројив подскуп ових симбола. У том смислу су симболи $\mathbf{0}$, $<$, $\boldsymbol{S}$ $+$, $\cdot$ које смо користили у дефинисању језика аритметике и које ћемо наставити да користимо, само колоквијализми, који заправо представљу редом f_0^0, A_0^2, f_0^1 f_0^2, f_1^2, док би у принципу и променљиве x, y, z требало писати у облику v_i, v_j, v_k.

Сада ћемо дефинисати појам формуле, мада нам пре тога треба још неколико дефиниција.

Променљиве и константе су **атомски терми**. Ако је f n-арни функцијски симбол и $t_1, \ldots, t_n$ терми, онда је и $f(t_1, \ldots, t_n)$ терм. **Терми** су онда тачно оно што се може добити узастопним додавањем функцијских симбола на једноставније терме. На пример, $f_1^2(f_0^2(f_0^0, f_0^0), v_0)$ илити $(\mathbf{0} + \mathbf{0}) \cdot x$ је терм. Терми који садрже променљиве су *отворени*, а терми који их не садрже су *затворени*.

Атомска формула је формула облика $R(t_1, \ldots, t_n)$ (или $= (t_1, t_2)$, овај изузетак наводимо јер је знак једнакости званично логички симбол), где је R, n-арни предикат, а $t_1, \ldots, t_n$ терми. Ако је F формула, онда је формула и њена негација $\neg F$. Ако су F и G формуле, онда су и њихове дисјункције и конјункције $(F \vee G)$, $(F \wedge G)$ формуле. Ако је F формула а x променљива онда су $\forall x F$ и $\exists x F$ формуле. Све што спада у формуле се може добити примењивањем коначно много негација, дисјункција, конјункција и квантификација над једноставнијим формулама. На пример, $\forall v_0 (A^2_0(f^0_0, v_0) \vee = (v_0, 0))$ илити $\forall x(\mathbf{0} < x \vee x = \mathbf{0})$ је формула.

Напоменимо, да би званично предикати као $<$ требало да се пишу испред терма $<(x, y)$ и да је $x < y$ још једно одступање од званичних правила синтаксе. Наводимо још нека таква одступања, писаћемо:

$$(A \Rightarrow B) \text{ уместо } (\neg A \vee B),$$
$$(A \iff B) \text{ уместо } (\neg A \vee B) \wedge (\neg B \vee A),$$
$$\forall x < y(...) \text{ уместо } \forall (x < y \Rightarrow (...)) \text{ и } \exists x < y(...) \text{ уместо } \exists x(x < y \wedge (...))$$
$$x \neq y \text{ уместо } \neg = (x, y).$$

Такође ћемо занемаривати непотребне заграде, најчешће $\boldsymbol{S}(\mathbf{0})$ пишемо $\boldsymbol{S}\mathbf{0}$. На крају још, уместо $\boldsymbol{S}\mathbf{0}$, $\boldsymbol{SS}\mathbf{0}$, $\boldsymbol{SSS}\mathbf{0}\ldots$ ћемо стандардно писати $\mathbf{1}, \mathbf{2}, \mathbf{3}\ldots$ Болдирана слова у формулама (попут $\boldsymbol{a}$ и $\boldsymbol{b}$) означавају нумерале. Односно, нумерал $\boldsymbol{a}$ представљају скраћеницу за запис $\boldsymbol{S}\ldots\boldsymbol{S}\mathbf{0}$, где се симбол $\boldsymbol{S}$ појављује a пута.

Природно се поставља питање, зашто не бисмо све ове скраћенице додали у званичну дефиницију језика. Испоставља се да је лакше доказивати тврђења о термима и формулама неког језика, ако је тај језик врло ригидан и нефлексибилан, међутим, то има своју цену јер су формуле званичног језика непрактичне за писање и тешке за читање. Стандардни приступ логичара је да званични језик о коме доказујемо тврђења оставимо нефлексибилним, док у незваничном језику заправо записујемо све формуле. Наравно, да би тврђења доказана о званичном језику била применљива на незванични језик мора бити могуће да се све скраћенице врате у своје формалне облике, мада то у пракси неће бити потребно.

Главна метода за доказивање теорема о формулама неког језика је **индукција по комплексности**. Она изгледа овако:
База индукције: Атомске формуле задовољавају тражени услов (овде обично морамо напоменути и да атомска формула са знаком = задовољава тражени услов, то радимо зато што смо знак = додали у логичке симболе)
Индуктивни корак: Ако се формула веће комплексности формира додавањем логичких оператора ($\neg$,$\wedge$, $\vee$, $\forall$, $\exists$) на једноставнију формулу онда, претпостављајући да све једноставније формуле задоваљавју тражени

услов, и формула веће комплексности задовољава тај услов. Индуктивни корак се обично дели на случајеве у зависности од тога који логички оператор смо искористили.

Следећа лема илуструје овај метод.

Лема 3.1. *За формуле записане у званичном језику важе следећа тврђења:*

(а) Свака формула се завршава десном заградом.

(б) Свака формула има једнако много десних и левих заграда

(ц) Ако поделимо формулу на леви и десни део и при том су оба дела непразна, онда леви део формуле садржи или више левих него десних заграда или не садржи заграде уопште.

Доказ. (а) База, формуле облика $R(t_1, \ldots, t_n)$ и $= (t_1, t_2)$ се наравно завршавају десном заградом. Ако се формуле F и G завршавају десном заградом, онда се и $\neg F$, $\forall x F$, $\exists x F$ завршавају десном заградом, јер су једини нови симболи на почетку израза. Такође, $(F \wedge G)$ и $(F \vee G)$ се очигледно завршавају десном заградом.

(б) Да би доказали ово тврђење за формуле прво ћемо доказати помоћно тврђење да сви терми имају једнако много левих и десних заграда. Ово такође радимо индукцијом по комплексности. Атомски терми немају заграде, па за њих тврђење важи. Претпоставимо да тврђење важи за терме t_1 и t_2 и да они имају редом по m и n левих (односно десних) заграда. Онда и терм $f(t_1, t_2)$ има исто левих и десних заграда, тачније $m + n + 1$ обе врсте. Слично и за $f(t_1, \ldots, t_k)$ за $k \neq 2$.

Нека терми $t_1, \ldots, t_k$ редом имају $n_1, \ldots, n_k$ левих и десних заграда, за атомску формулу облика $R(t_1, \ldots, t_k)$, важи да има $(\sum_{i=1}^{k} n_i) + 1$ левих и десних заграда (слично за специјални случај $= (t_1, t_2)$). Ако формуле F и G имају једнако много левих и десних заграда, лако се види да имају и формуле $\neg F$, $\forall x F$, $\exists x F$, $(F \wedge G)$ и $(F \vee G)$, чиме је доказ завршен.

(ц) И у овом случају нам треба прелиминарни резултат да одговарајуће тврђење важи за терме, мада га ми нећемо доказати. За атомску формулу $R(t_1, \ldots, t_k)$ се тврђење лако показује. Претпоставимо да тврђење важи за формуле F и G и погледајмо формулу $(F \wedge G)$, имамо неколико случајева како леви део ове формуле може изгледати:

<u>Сл. 1:</u>	<u>Сл. 2:</u>	<u>Сл. 3:</u>	<u>Сл. 4:</u>	<u>Сл. 5:</u>	<u>Сл. 6:</u>
$($	$(f_l$	$(F$	$(F \wedge$	$(F \wedge g_l$	$(F \wedge G$

где су f_l и g_l леви делови формула F и G. Примера ради, урадимо случај три, како F има једнако много левих и десних заграда по *(б)* онда $(F$ има једну леву заграду више него десних, што је и требало доказати. Остали случајеви се слично раде. $\square$

Посматрајмо низ узастопних симбола неке формуле F. Ако је овај низ и сам формула, зваћемо га **потформулом** формуле F. На пример $F \vee G$ је потформула формуле $\exists x(\neg(F \vee G) \wedge (F \wedge \neg G))$. Следећа лема, коју дајемо без доказа, нам говори нешто више о потформулама.

Лема 3.2.

(а) *Једина потформула атомске формуле $R(t_1, \ldots, t_k)$ или $= (t_1, t_2)$ је та сама формула.*

(б) *Једине потформуле формуле $\neg F$ су све потформуле F и само $\neg F$.*

(ц) *Једине потформуле формуле $(F \wedge G)$ су све потфорумле F, све потформуле G и само $(F \wedge G)$. Слично за $(F \vee G)$.*

(д) *Једине потформуле формуле $\forall x F$ су све потформуле F и само $\forall x F$. Слично за $\exists x F$.*

Мада ово тврђење делује тривијално, оно је једино тачно зато што користимо довољно заграда. У горе наведеном примеру $\exists x(\neg(F \vee G) \wedge (F \wedge \neg G))$ могли би да помислимо и да је $(F \vee G) \wedge (F \wedge \neg G)$ потформула оригиналне формуле, међутим ово уопште није формула. Шта по званичној дефиницији јесте формула је $((F \vee G) \wedge (F \wedge \neg G))$.

Појављивање променљиве x која је у формули F је **везано**, ако је део потформуле F која почиње са $\forall x$ или $\exists x$, а у супротном је **слободно**. На пример, у формули $(\forall x \exists y R(x, y) \vee \forall y P(x, y))$, прво појављивање променљиве x је везано, друго слободно, а оба појављивања променљиве y су везана.

У наставку ћемо када кажемо нека је $F(x)$ формула, мислити нека је F формула у којој се ниједна променљива осим x не појављује слободна.

Инстанца $F(t)$ формуле $F(x)$ се добија супституисањем затвореног терма t за свако слободно појављивање x.

Реченица је формула без слободних променљивих. Формуле, при валуацији слободних променљивих, ће заправо имати истинитосне вредности, тачно или нетачно. Специфично, реченице ће имати истинитосну вредност. Мада, да би говорили о истинитосној вредности неке реченице прво морамо дати *интерпретацију* за језик у коме су написане.

Напоменимо, да исте реченице могу имати различите истинитосне вредности у две различите интерпретације. Појам интерпретације и истине над интерпретацијом дефинишемо у следећем одељку.

3.2 Семантика

Прецизним дефинисањем синтактичког појма реченице осигурали смо се да имамо посла са смисленим изразима. Природно се поставља питање када је нека реченица **тачна** илити **истинита**. Имамо за циљ да у дефиницији истине имамо исти ниво прецизности као када смо дефинисали реченицу. Сада ћемо дефинисати појам интерпретације, који нам омогућује да причамо о истинитосној вредности неке реченице.

Интерпретација $\mathcal{I}$ неког језика L садржи две ствари.

Прво, непразан скуп $|\mathcal{I}|$ који зовемо **домен** интерпретације, то јест скуп објеката (најчешће скуп бројева $\mathbb{N}$, $\mathbb{Q}$,...) о коме говори језик L по интерпретацији $\mathcal{I}$. Када кажемо "за свако x" или "за неко x" шта ми по интерпретацији $\mathcal{I}$ мислимо је "за свако $x \in |\mathcal{I}|$" и "постоји $x \in |\mathcal{I}|$".

Друго, сваком нелогичком симболу језика L придодајемо неко **значење**. За константу c њено значење $c^{\mathcal{I}}$ је само неки елемент скупа $|\mathcal{I}|$. За нелогички n-арни предикат R његово значење $R^{\mathcal{I}}$ је само подскуп свих уређених n-торки елемената $|\mathcal{I}|$ (Подсетимо се да се нека релација стандардно дефинише као скуп уређених n-торки). За n-арни функцијски симбол f његово значење $f^{\mathcal{I}}$ је само функција n аргумената из $|\mathcal{I}|$ у $|\mathcal{I}|$. Треба још само да придодамо значење затвореним термима. За атомске затворене терме, то јест константе, већ имамо њихово значење. Ако су нам већ позната значења $t_1^{\mathcal{I}}, \ldots, t_n^{\mathcal{I}}$ терма $t_1, \ldots, t_n$, онда је значење сложенијег терма $f(t_1, \ldots, t_n)$ дефинисано овако:

$$(f(t_1, \ldots, t_n))^{\mathcal{I}} = f^{\mathcal{I}}(t_1^{\mathcal{I}}, \ldots, t_n^{\mathcal{I}}).$$

Пример 3.2 (Стандардна интерпретација језика аритметике). *Интерпретација која ће нам бити од највећег значаја зове се стандардна интерпретација језика аритметике (или скраћено само* стандардна интерпретација*), коју означавамо $\mathcal{I}_{\mathcal{A}}$. Њен домен $|\mathcal{I}_{\mathcal{A}}|$ је скуп природних бројева (укључујући и нулу), значење $\mathbf{0}^{\mathcal{I}_{\mathcal{A}}}$ симбола $\mathbf{0}$ је само број $\mathbf{0}$, значење $<^{\mathcal{I}_{\mathcal{A}}}$ симбола $<$ је уобичајена "мање од" релација, значење $\boldsymbol{S}^{\mathcal{I}_{\mathcal{A}}}$ симбола $\boldsymbol{S}$ је само функција следбеника, која за природан број враћа следећи природан број, значење $+^{\mathcal{I}_{\mathcal{A}}}$ и $\cdot^{\mathcal{I}_{\mathcal{A}}}$ знакова $+$ и $\cdot$ су уобичајене функције за сабирање и множење.*

Под овом интерпретацијом реченица: $\forall x \forall y (x \cdot y = \boldsymbol{SS}\mathbf{0} \Rightarrow (x = \boldsymbol{SS}\mathbf{0} \vee$

$y = \boldsymbol{SS}\mathbf{0}$)), означава: "за свака два природна броја x и y ако је њихов производ два онда је бар један од бројева x и y једнак два". Ова реченица је *тачна* у стандардној интерпретацији.

Дефиниција 3.1. *Ако је реченица F тачна у интерпретацији $\mathcal{I}$ писаћемо $\mathcal{I} \models F$, а у супротном $\mathcal{I} \not\models F$.*

Посматрајмо реченице:

(1) $\forall x \exists y(x < y \wedge \neg \exists z(x < z \wedge z < y))$,

(2) $\forall x(x < \boldsymbol{S}x \wedge \neg \exists z(x < z \wedge z < \boldsymbol{S}x))$

за обе важи да су тачне у стандрадној интерпретацији језика аритметике. Ако би сада узели другачију интерпретацију језика аритметике $\mathcal{Q}$ где је домен скуп позитивних рационалних бројева, али је значење $\mathbf{0}^{\mathcal{Q}}$ симбола $\mathbf{0}$ и даље број 0, значење $\boldsymbol{S}^{\mathcal{Q}}$ симбола $\boldsymbol{S}$ функција која на број додаје један, значење симбола $+, \cdot$ и $<$ су и даље уобичајене функције за сабирање, множење и уобичајена релација "мање од" на скупу позитивних рационалих бројева. Реченице (1) и (2) су сада нетачне у интерпретацији $\mathcal{Q}$, зато што између свака два рационална броја постоји бесконачно много других рационалних бројева. Размотримо још једну интерпретацију језика аритметике $\mathcal{P}$ и нека је домен ове интерпретације скуп $|\mathcal{P}| = \{0, \frac{1}{2}, 1, \frac{3}{2}, 2, \frac{5}{2}, 3, \frac{7}{2}, 4 \ldots\}$, значења симбола $\boldsymbol{S}, +, <$ су редом и даље, функција која на број додаје 1, и уобичајена функција сабирања бројева, уобичајена релација "мање од" (Наравно на нашем скупу $|\mathcal{P}|$). Множење се не може интерпретирати на стандардни начин, јер производ $\frac{1}{2} \cdot \frac{3}{2} = \frac{3}{4}$ даје број који није у скупу $|\mathcal{P}|$, мада нам за овај пример интерпретација множења није битна. У интерпретацији $\mathcal{P}$ је сада реченица (1) тачна, а реченица (2) нетачна. Шта нећемо наћи је интерпретацију где је (1) нетачно, а (2) тачно. Реченица (1) је заправо *логичка последица* реченице (2).

Мада смо у последњем пасусу рекли за неке реченице да су тачне и даље нисмо дали прецизну дефиницију шта мислимо под овим. Сада ћемо дати дефиницију истине, то јест дефиницију шта значи да је реченица F тачна у интерпретацији $\mathcal{I}$.

Први корак је да дефинишемо истинитост за атомске реченице, то јест реченице облика $R(t_1, \ldots, t_k)$ где су $t_1, \ldots, t_k$ *затворени* терми. Рећи ћемо да је:

$$(1a) \qquad \mathcal{I} \models R(t_1, \ldots, t_k) \text{ ако и само ако } \quad R^{\mathcal{I}}(t_1^{\mathcal{I}}, \ldots, t_k^{\mathcal{I}}).$$

Када је знак једнакости = присутан као логички симбол постоји још једна врста атомске реченице:

$$(1b) \qquad \mathcal{I} \models \,=(t_1, t_2) \text{ ако и само ако } t_1^{\mathcal{I}} = t_2^{\mathcal{I}}.$$

На пример у стандардној интерпретацији језика аритметике значење терма $\boldsymbol{SSS}\mathbf{0}$ је број 3 и значење терма $\boldsymbol{SS}\mathbf{0}+\boldsymbol{S}\mathbf{0}$ је такође број 3, па је тачна атомска реченица $\boldsymbol{SSS}\mathbf{0} = \boldsymbol{SS}\mathbf{0} + \boldsymbol{S}\mathbf{0}$. Док је на пример значење терма $\boldsymbol{SS}\mathbf{0}$ број 2, па је нетачна реченица $\boldsymbol{SS}\mathbf{0} + \boldsymbol{S}\mathbf{0} = \boldsymbol{SS}\mathbf{0}$.

За логичке везнике $\neg, \vee$ и $\wedge$ дефиниције су следеће:

$$(2a) \qquad \mathcal{I} \models \neg F \text{ ако и само ако } \mathcal{I} \not\models F$$

$$(2b) \qquad \mathcal{I} \models (F \vee G) \text{ ако и само ако } \mathcal{I} \models F \text{ или } \mathcal{I} \models G$$

$$(2c) \qquad \mathcal{I} \models (F \wedge G) \text{ ако и само ако } \mathcal{I} \models F \text{ и } \mathcal{I} \models G$$

На пример, у стандарној интерпретацији језика аритметике тачна је реченица $\mathbf{0} = \mathbf{0}$, а нетачна реченица $\mathbf{0} < \mathbf{0}$ па је тачна и дисјункција $(\mathbf{0} = \mathbf{0} \vee \mathbf{0} < \mathbf{0})$, док је конјункција $(\mathbf{0} = \mathbf{0} \wedge \mathbf{0} < \mathbf{0})$ нетачна.

Још једна последица ове дефиниције је да је $(F \wedge G)$ тачно ако и само ако је $\neg(\neg F \vee \neg G)$ тачно. Тако да смо могли, као што смо $\Rightarrow$ и $\iff$, да избацимо $\wedge$ (или $\vee$) из нашег званичног језика и да останемо само са $\neg$ и $\vee$ ($\neg$ и $\wedge$).

Још нам само преостаје да дефинишемо тачност у случају универзалне и егзистенцијалне квантификације, следећа дефиниција би могла на први поглед изгледати добро:

$$(3\text{а}^*) \qquad \mathcal{I} \models \forall x F(x) \text{ акко за сваки затворени терм } t,\ \mathcal{I} \models F(t)$$

$$(3\text{б}^*) \qquad \mathcal{I} \models \exists x F(x) \text{ акко за неки затворени терм } t,\ \mathcal{I} \models F(t).$$

Оваква дефиниција у општем случају не би била задовољавајућа. Посматрајмо интерпретацију језика аритметике чији је домен $|\mathcal{I}|$ непребројив. Онда није могуће сваки елемент домена записати као затворени терм. Подсетимо се, да смо за дефиницију језика рекли да је то *пребројив* скуп нелогичких симбола, лако се онда може видети да коришћењем пребројиво много функцијских симбола и пребројиво много константи можемо добити само пребројиво много затворених термова. На пример, замислимо да је домен наше интерпретације заправо скуп реалних бројева $\mathbb{R}$ и да је значење симбола $\cdot$ стандардна функција за множење два реална броја. По дефиницији (3б*) реченица $\exists x\ x \cdot x = 2$ би била нетачна, овакав резултат није сагласан са интуицијом. Проблем настаје, јер се број $\sqrt{2}$ не може представити као затворен терм.

Исправна дефиниција је следећа:

(3а) $\mathcal{I} \models \forall x F(x)$ акко за свако $m \in \mathcal{I}$, $\mathcal{I}_m^c \models F(c)$

(3б) $\mathcal{I} \models \exists x F(x)$ акко за неко $m \in \mathcal{I}$, $\mathcal{I}_m^c \models F(c)$.

Под $\mathcal{I}_m^c$ мислимо на интерпретацију која проширује интерпретацију $\mathcal{I}$ тако што на њен језик дода нову константу c која има значење m. У примеру горе, реченица $\exists x\ x \cdot x = 2$, би сада била тачна јер би у језик аритметике могли да додамо нову константу c која означава број $\sqrt{2}$.

Напоменимо да се у стандардној интерпретацији језика аритметике лако могу сви елементи њеног домена представити као затворени терми, па би у том случају дефиниције (3а*) и (3б*) такође биле исправне.

У наредном одељку требаће нам и следећа дефиниција.

Дефиниција 3.2. *Нека је S реченица, а Γ скуп реченица језика L. Рећи ћемо да је S* **логичка последица** *од Γ ако и само ако не постоји интерпретација $\mathcal{I}$ језика L таква да су све реченице скупа Γ тачне, а да је реченица S нетачна у интерпретацији $\mathcal{I}$.*

3.3 Доказна процедура

Када касније будемо формулисали Геделове теореме о непотпуности, видећемо да оне говоре о границама доказивости унутар формалних система. Међутим, наше интуитивно разумевање шта конституише математички доказ није довољно прецизно за овакву анализу.

Оно што нам је потребно је *доказна процедура*, која се састоји из скупа логичких аксиома и правила извођења. Користећи ова правила и аксиоме ћемо, полазећи од неког скупа тврђења (премиса), моћи да у малим, дисректним корацима формално докажемо нека друга тврђења.

Формални систем се управо и задаје формалним језиком (у нашем случају најчешће језиком аритметике), скупом аксиома и правилима извођења.

Ипак, нећемо излагати конкретан скуп правила извођења, пошто их у даљем раду нећемо ни помињати. За нас ће пак важнија бити нека својства заједничка за све познатије доказне процедуре.

Формалан доказ формуле S, полазећи од скупа Γ, је коначан низ формула који се завршава формулом S, такав да за сваку формулу тог низа важи да је аксиома или припада скупу Γ или се добија примењивањем неког правила извођења на претходне формуле низа. Постоји прецизно дефинисана процедура која нам говори да ли је дати низ симбола доказ или не. Наводимо још два својства, која су познатија као теорема о сагласности и Геделова теорема о потпуности.

Теорема 3.1 (Теорема о сагласности)**.** *Ако постоји доказ реченице S полазећи од скупа реченица Γ, онда је S логичка последица од Γ.*

Теорема 3.2 (Геделова теорема о потпуности)**.** *Ако је S логичка последица од скупа реченица Γ, онда постоји доказ реченице S полазећи од Γ.*

Напомена. *Да разјаснимо, Геделова теорема о потпуности и Геделове теореме о непотпуности нису супротна тврђења. Ове теореме говоре о различитим врстама (не)потпуности.*

Докази ових теорема зависе од детаља изабране доказне процедуре. Нама ови детаљи неће бити од пресудне важности докле год доказна процедура има претходних неколико својстава.

Наводимо још појмова које ћемо користити касније у раду.

Дефиниција 3.3. *Ако је полазећи од скупа реченица T доказива реченица S писаћемо $\vdash_T S$.*

Дефиниција 3.4. *Под речи* **теорија** *мислимо на скуп реченица неког језика, који је затворен у односу на доказивање. Реченице које припадају теорији зовемо теоремама те теорије.*

Дакле исто значење имају, "S је теорема теорије T", $\vdash_T S$ и $S \in T$.

Дефиниција 3.5. *Ако постоји рекурзиван скуп реченица Γ, такав да се теорија T састоји из оних и само оних реченица доказивих полазећи од премиса Γ, рећи ћемо да је T* **аксиоматизабилна** *теорија.*

Дефиниција 3.6. *Теорија T је* **конзистентна** *ако и само ако не доказује све реченице њеног језика.*

Дефиниција 3.7. *Теорија T је* **потпуна** *ако и само ако за сваку реченицу S њеног језика, $\vdash_T S$ или $\vdash_T \neg S$.*

У наставку ћемо, ако није другачије наведено, под речи теорија подразумевати да се ради о теорији језика аритметике.

4 Аритметизација синтаксе

Како би доказали Геделове теореме о непотпуности, треба нам начин да теорије аритметике "причају саме о себи". Пошто језик аритметике говори само о природним бројевима, мораћемо синтактичке објекте логике (формуле, реченице, доказе) да такође претворимо (кодирамо) у природне бројеве. Постоје многи начини да се ово уради, оно што је најважније за било које кодирање је да се од објекта на *у потпуности механчки* начин може добити његов код и обрнуто од кода назад добити објекат. Идеја о аритметизацији синтаксе потиче од самог Гедела, а кодирање које ћемо ми користити, данас познато као *Геделово кодирање*, долази још од његовог славног рада из 1931. године.

4.1 Геделово кодирање

Пре него што кренемо фиксирајмо још неке дефиниције.

Дефиниција 4.1. *Скуп симбола, формула, реченица, доказа или компликованијих објеката је рекурзиван ако и само ако је скуп кодова тих објеката рекурзиван.*

Подсетимо се да смо дефинисали језик као пребројив скуп не-логичких симбола.

Дефиниција 4.2. *За неки језик ћемо рећи да је (примитивно) рекурзиван ако и само ако је скуп кодова за симболе тог језика (примитивно) рекурзиван. Језик аритметике L_A је примитивно рекурзиван.*

Пређимо сада на дефиницију Геделовог кодирања. Сваки појединачни симбол представљамо једним бројем и то на следећи начин:

Симбол	(	)	,	$\neg$	$\vee$	$\exists$	$\forall$	$=$	v_i	A_i^n	f_i^n
Код	1	3	5	7	9	11	13	17	$2 \cdot 5^i$	$2^2 \cdot 3^n \cdot 5^i$	$2^3 \cdot 3^n \cdot 5^i$

Притом је битно да напоменемо да никоја два различита симбола немају исти код. Како би разликовали предикатске од функцијских симбола једни су облика $2^2 \cdot x$ а други $2^3 \cdot x$. На пример, у језику аритметике симбол $\mathbf{0}$ илити f_0^0 представљамо бројем $2^3 \cdot 3^0 \cdot 5^0 = 8$, симбол $\boldsymbol{S}$ илити f_0^1 бројем $2^3 \cdot 3^1 \cdot 5^0 = 24$, симбол $<$ илити A_0^2 бројем $2^2 \cdot 3^2 \cdot 5^0 = 36$ итд.

Желимо да проширимо кодирање на коначне низове симбола, то радимо на следећи начин. Нека је I израз од n симбола и нека су $(c_1, \ldots, c_n)$ редом њихови кодови, код за израз I је онда број $2^n \cdot 3^{c_1} \cdot 5^{c_2} \cdot ... \cdot \pi_n^{c_n}$. На пример код за реченицу $\mathbf{0} = \mathbf{0}$, коју званично пишемо $= (f_0^0, f_0^0)$ је $2^6 \cdot 3^{17} \cdot 5^1 \cdot 7^8 \cdot 11^5 \cdot 13^8 \cdot 17^3$ што је број са 36 цифара. Срећом, у пракси никад нећемо сами морати да кодирамо или декодирамо велике изразе, једино што је битно је да је то у теорији могуће учинити. Слично као за низ симбола, можемо дефинисати и код за низ формула. Код за скуп формула ће нам бити исти као код за низ формула, само што ћемо прво захтевати да су кодови у низу поређани у растућем редоследу.

Пре него што пређемо на важније резултате, морамо да докажемо да је функција *конкатенације* примитивно рекурзивна.

Лема 4.1. *Ако је a код за низ $(a_0, \ldots, a_{n-1})$ а b код за низ $(b_0, \ldots, b_{m-1})$ онда је функција $conc(a, b)$ која враћа код за низ $(a_0, \ldots, a_{n-1}, b_0, \ldots, b_{m-1})$ примитивно рекурзивна.*

Доказ. Докажимо прво да је помоћна функција $ext(a, e)$ која за код a низа $(a_0, \ldots, a_{n-1})$ и број e враћа код за проширени низ $(a_0, \ldots, a_{n-1}, e)$ примитивно рекурзивна. Лако се види да заправо важи:

$$ext(a, e) = 2 \cdot a \cdot (\pi(len(a) + 1))^e$$

и да је ext примитинво рекурзивна функција. Са функцијом ext дефинишемо помоћну, примитивно рекурзивну, фукцију g:

$$\begin{aligned} g(a, b, 0) &= a \\ g(a, b, s(i)) &= ext(g(a, b, i), ent(b, i)) \end{aligned}$$

Коначно добијамо $conc(a, b) = g(a, b, len(b))$, из чега следи да је $conc$ примитивно рекурзивна функција. □

Скраћено ћемо писати $a * b$ уместо $conc(a, b)$.

Пример 4.1. *Функција $num(n)$ која за број n узима вредност кода за нумерал $\boldsymbol{n}$ је примитивно рекурзивна.*

Доказ. Довољно је приметити да је:

$$\begin{aligned} num(0) &= 8 \\ num(s(n)) &= 24 * 1 * num(n) * 3 \end{aligned}$$

Јер су 8, 24, 1, 3 редом кодови за **0**, ***S***, леву заграду и десну заграду. □

Теорема 4.1. *Логичке операције негирања, дисјункције, егзистенцијалне и универзалне квантификције и супституисања терма уместо слободне променљиве су примитивно рекурзивне.*

Доказ. Нека је x код за неку формулу, код за негацију ове формуле добија се из $neg(x) = 7 * x$, зато што је број 7 код за симбол $\neg$.

За дисјункцију две формуле са кодовима x и y редом важи $disj(x, y) = 1 * x * 9 * y * 3$, зато што су бројеви 1,9,3 редом кодови за леву заграду, дисјункцију и десну заграду. Одавде можемо лако и дефинисати конјункцију две формуле са кодовима x и y:

$$conj(x, y) = neg(disj(neg(x), neg(y)))$$

Ако је v код променљиве у односу на коју вршимо егзистенцијалну квантификацију формуле са кодом x важи $exquant(v, x) = 11*v*x$ јер је број 11 код за симбол $\exists$. Слично за универзалну квантификацију $uquant(v, x) = 13 * v * x$.

Доказ за супституцију је нешто компликованији и идејно је сличан доказу Теореме 4.2. □

Од скупова израза за нас ће најзначајнији бити скупови формула и реченица. Интуитивно видимо да је ефективно одлучиво да ли је неки низ симбола заправо формула (или реченица). Следећа теорема ово и формално тврди.

Теорема 4.2. *Скупови формула и реченица су примитивно рекурзивни.*

Напомена. *Ако је језик у коме радимо само рекурзиван, а не примитивно рекурзиван као L_A, у тврђењу горе треба обрисати реч примитивно.*

Доказ. Прво, показаћемо да су унарна релација "a је код за предикат" и бинарна релација "a је код за n-арни предикат" примитивно рекурзивне. Функција $f(n, i) = 2^2 \cdot 3^n \cdot 5^i$ је примитивно рекурзивна, а самим тим и њена релација графа $a = f(n, i)$. Одавде се ограниченом егзистеницјалном квантификацијом добијају тражене релације:

$$\exists n < a \exists i < a(a = 2^2 \cdot 3^n \cdot 5^i) \text{ и } \exists i < a(a = 2^2 \cdot 3^n \cdot 5^i).$$

Слично се може показати да су релације "a је код за променљиву", "a је код за функцијски симбол", "a је код за n-арни функцијски симбол", "a је код за константу" (односно функцију 0 места) и "a је код за атомски терм" (односно константу или променљиву) примитивно рекурзивне.

Сада показујемо и да је релација "s је код за атомску формулу" примитивно рекурзивна (додуше у специјалном случају када нису присутни функцијски симболи нити знак једнакости). Због разумљивости пишемо на следећи, мање формалан начин, s је код за атомску формулу ако и само ако постоји $n < len(s)$ тако да важи следеће:

$len(s) = 2n + 2 \ \ \wedge$

$ent(s, 0)$ је код за n-арни предикат $\wedge$

$ent(s, 1) = 1$ (код за леву заграду) $\wedge$

за свако i, $\ 1 < i < len(s) - 1:$

ако је i паран, $ent(s, i)$ је код за атомски терм $\wedge$

ако је i непаран, $ent(s, i) = 5$ (код за зарез) $\wedge$

$ent(s, len(s) - 1) = 3$ (код за десну заграду).

При дефинисању када је s код за произвољну формулу, не можемо бити толико директни. Прво дефинишемо *низ формирања* фомуле F као низ формула у којем је свака формула или атомска или је добијена негацијом, дисјункцијом или егзистенцијалном квантификацијом формуле/ла које се појављују раније у низу, и притом је последња формула низа баш F. Нека је низ формирања *редукован* ако је сваки члан тог низа потформула од F и ако се свака потформула F у низу појављује тачно једанпут. На пример, редуковани низ формирања за формулу $(\neg F \vee G) \wedge (F \vee \neg G)$, уз претпоставку да су F и G атомске формуле, би могао бити низ:

$$(F, G, \neg F, \neg G, \neg F \vee G, F \vee \neg G, (\neg F \vee G) \wedge (F \vee \neg G)) .$$

Настављајући наш доказ, s је код за формулу ако и само ако постоји неко r које је код за низ формирања те формуле. Релација "r је код за низ формирања формуле са кодом s" је примитивно рекурзивна јер је еквивалентна са:

за свако $\ i < len(r)$ важи:

$\big(ent(r, i)$ је код за атомску формулу $\vee$

за неко $k < i$, $\ \ ent(r, i) = neg(ent(r, k)) \ \vee$

за неко $k < i$ и неко $l < i \ \ \ ent(r, i) = disj(ent(r, k), ent(r, l)) \ \vee$

за неко $k < i$ и неко $e < r$, $ent(r,i) = exquant(2 \cdot 5^e, ent(r,k) \vee$
за неко $k < i$ и неко $e < r$, $ent(r,i) = uquant(2 \cdot 5^e, ent(r,k))\big) \wedge$
$ent(r, len(r) - 1) = s.$

Није тешко показати да ће ако је s код за формулу увек постојати код r за редуковани низ формирања, такав да је $r < \pi(len(s))^{s \cdot (len(s)+1)} = f(s)$. Приметимо да је $f(s)$ примитивно рекурзивна функција. Због тога се у последњем пасусу "ако постоји неко r" може заменити "ако постоји неко $r < f(s)$", из чега следи да је релација "s је код за формулу" примитивно рекурзивна.

Када су функцијски симболи и симбол једнакости присутни, морали бисмо прво успоставити прелиминарне резултате о низу формирања за терме и сходно томе променити дефиницију за атомску формулу.

Да бисмо доказали да је скуп реченица примитивно рекурзиван, морали бисмо још да дефинишемо релацију која проверава да ли је неко појављивање променљиве везано или не, а затим да проверимо да ли су сва појављивања променљивих везана. Изостављамо детаље. $\square$

Следи још једна битна теорема, чији ће доказ зависити од тога коју смо доказну процедуру изабрали.

Теорема 4.3. *Ако је Γ рекурзиван скуп реченица онда је релација "Σ је доказ реченице D од премиса Γ" рекурзивна.*

Обично се под аритметизацијом синтаксе мисли на претходне 3 теореме и њихове последице.

4.2 Корисни резултати

Овде ћемо показати пар резултата који ће нам касније бити корисни.

Теорема 4.4. *Скуп реченица који је доказив полазећи од датог рекурзивног скупа реченица Γ је рекурзивно набројив.*

Доказ. Теорема 4.3 нам заправо говори да је релација:

$$\begin{aligned} R(r,d) \iff & r \text{ је код за реченицу}, \\ & d \text{ је код за дедукцију те реченице из скупа } \Gamma, \end{aligned}$$

рекурзивна. Онда је скуп кодова за реченице доказиве из Γ рекурзивно набројив, јер је он уствари $S(r) \Leftrightarrow \exists d\ R(r,d)$ $\square$

За теорију T кажемо да је рекурзивна ако је скуп кодова њених теорема рекурзиван.

Теорема 4.5. *Нека је T аксиоматизабилна теорија. Ако је T потпуна онда је и рекурзивна.*

Доказ. То што је T аксиоматизабилна теорија значи да постоји рекурзиван скуп реченица Γ из којег су доказиве све реченице у T. Нека је T^* скуп кодова теорема од T. По прошлој теореми је T^* рекурзивно набројив скуп. Треба да покажемо да је скуп T^* рекурзиван. Ако би се за неку реченицу R десило да су R и $\neg R$ теореме теорије T, онда би T био скуп свих реченица, који је рекурзиван по Теореми 4.2.

То што је T потпуна теорија значи да је за сваку реченицу R или $\neg R$ теорема ове теорије. Посматрајмо комплемент од T^* скуп $\overline{T^*}$. Овај скуп је заправо унија скупа X бројева који нису кодови за реченице и скупа Y реченица чија је негација теорема T. Како је рекурзиван комплемент од скупа X, односно скуп свих реченица, то је по Теореми 2.1(*ц*) и X рекурзиван. Нека је $Thm_T(y)$ рекурзивно набројива релација која нам говори да ли је y код теореме теорије T. Скуп Y је онда скуп свих y за које је $Thm_T(neg(y))$, то јест скуп кодова чија је негација теорема од T (користимо то да је T потпуна теорија), приметимо и да је ова релација добијена супституцијом рекурзивне релације neg у рекурзивно набројиву релацију Thm_T. Одавде следи да је скуп Y рекурзивно набројив, самим тим је и унија X и Y рекурзивно набројива.

Одавде су онда T^* и $\overline{T^*}$ рекурзивно набројиви скупови, па је по принципу комплементарности (Теорема 2.5) скуп T^* и рекурзиван, што је требало доказати.

□

5 Репрезентабилност

У прошлом поглављу повезали смо наш рад о рекурзивним функцијама са појмовима формуле, реченице и доказа. Сада ћемо ове области повезати у другом смеру. Показаћемо како можемо да причамо о рекурзивним функцијама користећи формуле језика аритметике.

5.1 Аритметичка дефинабилност

Циљ нам је да покажемо да за било коју рекурзивну функцију f постоји формула φ_f, таква да ако је $f(a) = b$ онда је $\forall y(\varphi_f(\boldsymbol{a}, y) \Leftrightarrow y = \boldsymbol{b})$ тачно у стандардној интерпретацији језика аритемтике.

Скраћено ћемо уместо тачно у стандардној интерпретацији језика аритметике писати само тачно.

Формула $F(x)$ **аритметички дефинише** скуп S ако за свако $a \in \mathbb{N}_0$ важи: $a \in S$ ако и само ако је $F(\boldsymbol{a})$ тачно. Природно се овај појам прошируне на n-арне релације, формула $F(x_1, \ldots, x_n)$ аритметички дефинише n-арну релацију R ако важи:

$$R(a_1, \ldots, a_n) \text{ ако и само је } F(\boldsymbol{a_1}, \ldots, \boldsymbol{a_n}) \text{ тачно.}$$

Ако постоји формула која аритметички дефинише релацију кажемо да је та релација **аритметички дефинабилна** или скраћено **аритметичка**.

Функција f је аритметичка ако и само ако је њена релација графа аритметичка. На пример, унарна функција f је аритметичка ако постоји формула F таква да је за све $a, b \in \mathbb{N}_0$, $f(a) = b$ ако и само ако је $F(\boldsymbol{a}, \boldsymbol{b})$.

Пример 5.1. *Основне функције су аритметичке.*

Нула функцију $z(x) = 0$ аритметички дефинише формула:

$$\varphi_z(x, y) \equiv x = x \wedge y = 0.$$

Функцију следбеника $s(x)$ аритметички дефинише следећа формула :

$$\varphi_{\boldsymbol{S}}(x, y) \equiv \boldsymbol{S}x = y.$$

Пројекцију i-те кординате аритметички дефинише формула:

$$\varphi_{id}(x_1, \ldots, x_k, y) \equiv x_1 = x_1 \wedge \cdots \wedge x_n = x_n \wedge y = x_i.$$

Пример 5.2. *Сабирање и множење су аритметичке функције.*

Сабирање и множење аритметички дефинишу редом формуле:

$$\varphi_{+}(x_1, x_2, y) \equiv x_1 + x_2 = y \text{ и } \varphi_{\cdot}(x_1, x_2, y) \equiv x_1 \cdot x_2 = y.$$

Пример 5.3. *Функције количника и остатка су аритметичке.*

Функције quo и rem аритметички дефинишу редом формуле:

$$\varphi_{quo}(x_1, x_2, y) \equiv (x_2 = 0 \wedge y = 0) \vee \exists u < x_2 (x_1 = x_2 \cdot y + u),$$
$$\varphi_{rem}(x_1, x_2, y) \equiv (x_2 = 0 \wedge y = x_1) \vee \exists u \leq x_1 (y < x_2 \wedge x_1 = u \cdot x_2 + y).$$

Желимо да докажемо да су све рекурзивне функције аритметичке. Пошто смо већ доказали да су основне функције аритметичке, довољно је сад показати да су композиција, примитивна рекурзија и минимизација неколико аритметичких функција такође аритметичка функција.

Нека су f и g унарне функције и нека их редом аритметички дефинишу формуле φ_f и φ_g. Њихову **композицију** $h(a) = g(f(a))$ аритметички дефинише следећа формула:

$$\varphi_h(x, z) \equiv \exists y (\varphi_f(x, y) \wedge \varphi_g(y, z)).$$

Слично се може аритметички дефинисати композиција за функције било које арности.

При дефинисању примитивне рекурзије имамо мало више проблема. Шта би нам било корисно је да имамо начин да квантификујемо преко низова произвољне дужине. На пример, нека је f унарна функција дефинисана примитивном рекурзијом на следећи начин $f(0) = c$ и $f(s(x)) = g(x, f(x))$. Да би изразили $f(n) = y$ желели бисмо да можемо да кажемо: постоји низ $a_0, a_1, \ldots, a_n$ такав да је:

$$\begin{aligned} & a_0 = c \\ \text{за свако } i < n \quad & g(i, a_i) = a_{i+1} \\ & a_n = y. \end{aligned}$$

Међутим, логика првог реда нема уграђену овакву могућност. Овај проблем решио је опет сам Гедел дефинисањем такозване β функције.

Лема 5.1 (Лема β функције)**.** *За свако k и сваки низ бројева $a_0, \dots, a_k$, постоје бројеви s и t такви да за свако i, $0 \leq i \leq k$ важи $\beta(s,t,i) = a_i$.*

Доказ. Функцију β заправо дефинишемо на следећи начин:

$$\beta(s,t,i) = rem(s, t(i+1)+1).$$

Сада треба доказати да постоје бројеви s и t такви да је:

$$\begin{aligned} s &\equiv a_0 \pmod{t+1} \\ s &\equiv a_1 \pmod{2t+1} \\ &\vdots \\ s &\equiv a_k \pmod{(k+1)t+1} \end{aligned}$$

Ово тврђење ће одмах следити, из *Кинеске теореме о остацима*, ако нађемо t тако да су за свако i, j $1 \leq i, j \leq k+1$ бројеви $t \cdot i+1$ и $t \cdot j+1$ узајмно прости. Притом t мора и бити довољно велико, тј. мора важити $a_i < t(i+1)+1$. Нека је $a_m = max\{a_0, \dots, a_k\}$, довољно је узети $t = (a_m+1)! \cdot (k+1)!$. Ово t је свакако довољно велико, докажимо да задовољава и први услов. Претпоставимо супротно, да $t \cdot i + 1$ и $t \cdot j + 1$ нису узајамно прости и нека је $d > 1$ њихов НЗД. Одавде закључујемо да $d \mid t(j-i)$, лако се види да d и t морају бити узајамно прости. Следи да $d \mid j - i$ међутим како је $j - i < k + 1$ добијамо $d \mid j - i$, $d \mid (k+1)!$ из последње дељивости следи и $d \mid t = (a_m+1)(k+1)!$ контрадикција. □

Формула која аритметички дефинише β функцију је:

$$\varphi_\beta(x_1, x_2, x_3, y) \equiv \varphi_{rem}(x_1, (x_3 + \mathbf{1}) \cdot x_2 + \mathbf{1}, y).$$

Сада можемо да наставимо са аритметичким дефинисанњем **примитивне рекурзије**. Нека су f и g редом унарна и тернарна функција које су аритметички дефинисане формулама φ_f и φ_g, и нека се фунцкија h добија од њих примитивном рекурзијом. Формула која аритметички дефинише h је $\varphi_h(x,y,z) = \exists s \exists t \varphi$ где је φ конјункција следеће три формуле:

$$\begin{aligned} &\exists u(\varphi_\beta(s,t,\mathbf{0},u) \wedge \varphi_f(x,u)), \\ &\forall w < y \; \exists u \exists v(\varphi_\beta(s,t,w,u) \wedge \varphi_\beta(s,t,\boldsymbol{S}w,v) \wedge \varphi_g(x,w,u,v)), \\ &\varphi_\beta(s,t,y,z). \end{aligned}$$

Конструкција је врло слична за функције било које арности.

Остала нам је још само операција **минимизације**. Нека је функција g добијена од бинарне функције f минимизацијом. Нека је f аритметички дефинисана формулом φ_f онда је функција g аритметички дефинисана формулом:

$$\varphi_g(x, y) \equiv \varphi_f(x, y, \mathbf{0}) \wedge \forall z < y \, \exists u(\varphi_f(x, z, u) \wedge u \neq \mathbf{0}).$$

Опет, конструкција је слична за функције било које арности.

Овиме смо одрадили велики део посла потребан за доказивање следеће важне теореме.

Теорема 5.1.

(а) Све рекурзивне функције су аритметичке.

(б) Све рекурзивне и рекурзивно набројиве релације су аритметичке.

Доказ. (а) Како смо доказали да су основне функције аритметичке и да су композиција, примитивна рекурзија и минимизација неколико аритметичких функција аритметичка, можемо закључити да су све рекурзивне функције аритметичке.

(б) Нека је R n-арна релација и нека је f њена карактеристична функција. Из *(а)* закључујемо да постоји формула $\varphi_f(x_1, \ldots, x_n, y)$ која је аритметички дефинише. Онда $\varphi_R(x_1, \ldots, x_n) \equiv \varphi_f(x_1, \ldots, x_n, \mathbf{1})$ аритметички дефинише релацију R.

По дефиницији, рекурзивно набројиве релације се добијају егзистенцијалном квантификацијом рекурзивних релација. Нека је S рекурзивно набројива релација облика

$$S(x_1, \ldots, x_n) \Leftrightarrow \exists z Q(x_1, \ldots, x_n, z),$$

ако $\varphi_Q(x_1, \ldots, x_n, z)$ аритметички дефинише релацију Q формула:

$$\exists z \varphi_Q(x_1, \ldots, x_n, z),$$

аритметички дефинише релацију S. □

Овај резултат можемо и да ојачамо, тако што ћемо да дефинишемо различите врсте формула. Рећи ћемо да је формула **елементарна** ако је изграђена од атомских формула користећи само негацију, дисјункцију, конјункцију и ограничене квантификације $\forall x < t$ и $\exists x < t$. Формула је **$\exists$-елементарна** ако је облика $\exists x F$ где је F елементарна формула, слично се дефинишу $\forall$-елементарне формуле.

Дефиниција 5.1. *Две формуле φ и ψ (са на пример две слободне промењиве) су аритметички еквивалентне ако је за све бројеве $a, b \in \mathbb{N}_0$ $\psi(\boldsymbol{a}, \boldsymbol{b})$ тачно ако и само ако је $\varphi(\boldsymbol{a}, \boldsymbol{b})$ тачно.*

Теорема 5.2.

(а) Свака елементарна формула је аритметички еквивалентна некој $\exists$-елементарној формули.

(б) Дисјункција (конјункција) две $\exists$-елементарне формуле је аритметички еквивалента $\exists$-елементарној формули.

(ц) Формула добијена ограниченом егзистенцијалном (универзалном) квантификацијом $\exists$-елементарне формуле је аритметички еквивалентна $\exists$-елементарној формули.

(д) Формула добијена неограниченом егзистенцијалном квантификацијом $\exists$-елементарне формуле је аритметички еквивалента са $\exists$-елементарном формулом.

Доказ. (а) Елементарна формула φ логички је еквивалентна $\exists$-елементарној формули $\exists t(t = t \wedge \varphi)$.

(б) Формула $\exists x\, \varphi(x) \wedge \exists y\, \psi(y)$ аритметички је еквивалентна $\exists$-елементарној формули $\exists t \exists x < t \exists y < t(\varphi(x) \wedge \psi(y))$. Док је $\exists x\, \varphi(x) \vee \exists y\, \psi(y)$ логички еквивалентно $\exists$-елементарној формули $\exists t(\varphi(t) \vee \psi(t))$.

(ц) Формула $\exists y < z \exists x \varphi(x, y)$ је логички еквивалентна $\exists$-елементарној $\exists x \exists y < z \varphi(x, y)$. Док је $\forall y < z \exists x\, \varphi(x, y)$ аритметички еквивалентно формули $\exists t \forall y < z \exists x < t\, \varphi(x, y)$. У једном смеру импликација је логичка, а у другом користимо чињеницу да за сваки коначни низ бројева $x_1, \dots, x_z$ постоји број t већи од свих њих.

(д) Формула $\exists x \exists y \varphi(x, y)$ је аритметички еквивалентна $\exists$-елементарној формули $\exists t \exists x < t \exists y < t \varphi(x, y)$. □

Приметимо сада да су све формуле коришћене у доказу Теореме 5.1. заправо аритметички еквивалентне $\exists$-елементарним формулама. Из овога добијамо следећу лему, која је побољшање Теореме 5.1.

Лема 5.2. *Свака рекурзивна функција или рекурзивно набројива релација може се аритметички дефинисати $\exists$-елементарном формулом.*

Нека је функција која се може аритметички дефинисати елементарном формулом *елементарна функција.*

Следећа лема, коју наводимо без доказа, ће нам знатно олакшати доказ да су све рекурзивне функције *репрезентабилне* у одређеној теорији аритметике, $\boldsymbol{Q}$.

Лема 5.3. *Свака рекурзивна функција се може добити композицијом од елементарних функција.*

Напоменимо још само да се не може свака рекурзивна функција аритметички дефинисати елементарном формулом.

5.2 Репрезентабилност у Q

Пре него што дефинишемо *теорију минималне аритметике*, коју ћемо означавати са $\boldsymbol{Q}$[1], морамо дефинисати појмове **дефинабилности** и **репрезентабилности** у теорији T.

Нека је T конзистентна теорија, рећи ћемо да је скуп S дефинабилан у теорији T ако постоји формула φ таква да је:

$$T \vdash \varphi(\boldsymbol{n}) \text{ ако је } n \in S \text{ и}$$
$$T \vdash \neg\varphi(\boldsymbol{n}) \text{ ако је } n \notin S.$$

За формулу φ кажемо да дефинише овај скуп у теорији T. Ова дефиниција лако се генерализује на произвољне релације. Али се испоставља да је *дефинабилност функције* мање корисна од мало другачијег појма *репрезентабилности функције.* Унарна функција f је репрезентабилна у теорији T ако и само ако постоји формула $\varphi(x, y)$ за коју важи:

$$\text{ако је } f(a) = b \text{ онда је } T \vdash \forall y(\varphi(\boldsymbol{a}, y) \Leftrightarrow y = \boldsymbol{b}).$$

Кажемо да формула φ за коју овај услов важи репрезентује функцију f у теорији T. Поменути услов је логички еквивалентан са $\varphi(\boldsymbol{a}, \boldsymbol{b}) \wedge \forall y(y \neq b \Rightarrow \neg\varphi(\boldsymbol{a}, y))$. Док би дефинабилност функције захтевала само да можемо доказати $\varphi(\boldsymbol{a}, \boldsymbol{b})$, и да за произвољно $c \neq b$ можемо да докажемо $\neg\varphi(\boldsymbol{a}, \boldsymbol{c})$. У теорији $\boldsymbol{Q}$ постојаће реченице чија се свака појединачна инстанца може доказати, док генерално тврђење неће бити доказиво. Пример за то је проста реченица $\forall x(\mathbf{1} + x = x + \mathbf{1})$, која се не може доказати из аксиома $\boldsymbol{Q}$, док се за било који број n може доказати $\mathbf{1} + \boldsymbol{n} = \boldsymbol{n} + \mathbf{1}$.

[1] У литератури $\boldsymbol{Q}$ често означава Робинсонову аритметику. Робинсонова аритметика је у неким погледима јача, а у неким слабија од теорије минималне аритметике.

Напоменимо још само да ако је T^* слабија теорија од T (скуп теорема T^* је подскуп теорема T) репрезентабилност у T^* имплицира репрезентабилност у T.

Коначно наводимо аксиоме **минималне аритметике $\boldsymbol{Q}$**.

(Q1)	$\forall x(\mathbf{0} \neq \boldsymbol{S}x)$
(Q2)	$\forall x \forall y(\boldsymbol{S}x = \boldsymbol{S}y \Rightarrow x = y)$
(Q3)	$\forall x(x + \mathbf{0} = x)$
(Q4)	$\forall x \forall y(x + \boldsymbol{S}y = \boldsymbol{S}(x + y))$
(Q5)	$\forall x(x \cdot \mathbf{0} = \mathbf{0})$
(Q6)	$\forall x \forall y(x \cdot \boldsymbol{S}y = x \cdot y + x)$
(Q7)	$\forall x(\neg x < \mathbf{0})$
(Q8)	$\forall x \forall y(x < \boldsymbol{S}y \Leftrightarrow (x < y \vee x = y))$
(Q9)	$\forall x(\mathbf{0} < x \Leftrightarrow x \neq \mathbf{0})$
(Q10)	$\forall x \forall y(\boldsymbol{S}x < y \Leftrightarrow (x < y \wedge \boldsymbol{S}x \neq y))$

Теорија $\boldsymbol{Q}$ је онда скуп свих реченица доказивих полазећи од ових аксиома. Аксиоме минималне аритметике нису довољно јаке да докажу већину резултата теорије бројева, мада би сваки скуп аксиома који је "адекватан" за теорију бројева морао да их докаже (а ако их доказује може и да их има као аксиоме). Поставља се питање зашто би уопште посматрали овако слабу теорију (која не може да докаже ни $\forall x(x + \mathbf{1} = \mathbf{1} + x)$), испоставља се ипак да $\boldsymbol{Q}$ може да докаже све $\exists$-елементарне реченице језика аритметике које су тачне у стандардној интерпретацији. Шта је још интересантније је да се прва Геделова теорема о непотпуности може доказати за сваку теорију која садржи $\boldsymbol{Q}$, пошто је $\boldsymbol{Q}$ слаба теорија наш резултат непотпуности ће бити утом снажнији.(Осим да задрже $\boldsymbol{Q}$, теорије на које се односи прва Геделова теорема морају да буду конзистентне и аксиоматизабилне)

Сада прелазимо на доказе главних теорема везаних за теорију $\boldsymbol{Q}$.

Теорема 5.3. *Било која $\exists$-елементарна реченица је тачна ако и само ако је теорема од $\boldsymbol{Q}$.*

Доказ. Пошто су све аксиоме теорије $\boldsymbol{Q}$ тачне, из теореме о сагласности добијамо да су и све теореме од $\boldsymbol{Q}$ тачне. Друга страна еквиваленције захтева више посла.

Чистом логиком је доказиво $\boldsymbol{m} = \boldsymbol{m}$. Из аксиоме $(Q1)$ је доказиво $\mathbf{0} \neq \mathbf{1}, \mathbf{0} \neq \mathbf{2}, \mathbf{0} \neq \mathbf{3} \ldots$ Из аксиоме $(Q2)$ се доказује $\mathbf{1} = \mathbf{2} \Rightarrow \mathbf{0} = \mathbf{1}$, $\mathbf{1} = \mathbf{3} \Rightarrow$

$\mathbf{0} = \mathbf{2}\ldots$ Из претходна два запажања само користећи логику следи да је доказиво $\mathbf{1} \neq \mathbf{2}, \mathbf{1} \neq \mathbf{3}\ldots$ Опет користећи $(Q2)$ добијамо $\mathbf{2} = \mathbf{3} \Rightarrow \mathbf{1} = \mathbf{2}$, $\mathbf{2} = \mathbf{4} \Rightarrow \mathbf{1} = \mathbf{3}\ldots$ користећи и малопре доказано $\mathbf{1} \neq \mathbf{2}, \mathbf{1} \neq \mathbf{3}\ldots$, добијамо да је $\mathbf{2} \neq \mathbf{3}, \mathbf{2} \neq \mathbf{4}\ldots$ доказиво. Настављајући на исти може се доказати $\boldsymbol{m} \neq \boldsymbol{n}$ кад год је $m < n$. Користећи симетрију једнакости и чињеницу да ако је $m \neq n$ важи $m < n$ или $m > n$, може се доказати да је $\boldsymbol{m} \neq \boldsymbol{n}$ кад год је $m \neq n$.

Сада желимо да покажемо да кад год је $m < n$ да је $\boldsymbol{m} < \boldsymbol{n}$ доказиво, а кад год је $m \geq n$ да је $\neg\boldsymbol{m} < \boldsymbol{n}$ доказиво. Користећи $(Q8)$ добијамо $x < \mathbf{1} \Leftrightarrow (x < \mathbf{0} \vee x \neq \mathbf{0})$, како је $(Q7)$ $\neg x < \mathbf{0}$ добијамо $x < \mathbf{1} \Leftrightarrow x = \mathbf{0}$, из чега следи да је $\mathbf{0} < \mathbf{1}$ доказиво. Како је $\mathbf{1} \neq \mathbf{0}, \mathbf{2} \neq \mathbf{0}\ldots$ доказиво чистом логиком из тога и $x < \mathbf{1} \Leftrightarrow x = \mathbf{0}$ добијамо да је $\neg\mathbf{1} < \mathbf{1}, \neg\mathbf{2} < \mathbf{1}, \neg\mathbf{3} < \mathbf{1}$ доказиво. Користећи $(Q8)$ опет добијамо $x < \mathbf{2} \Leftrightarrow (x < \mathbf{1} \vee x = \mathbf{1})$ користећи шта смо претходно доказали добијамо $x < \mathbf{2} \Leftrightarrow (x = \mathbf{0} \vee x = \mathbf{1})$, одавде се добија да је $\mathbf{0} < \mathbf{2}, \mathbf{1} < \mathbf{2}$ и $\neg\mathbf{2} < \mathbf{2}, \neg\mathbf{3} < \mathbf{2}\ldots$ доказиво. Настављајући на овај начин добијамо да је за било које m доказиво:

$$x < \boldsymbol{m} \iff (x = \mathbf{0} \vee x = \mathbf{1} \vee \cdots \vee x < \boldsymbol{m} - \mathbf{1}). \tag{1}$$

Из овога следи да је $\boldsymbol{m} < \boldsymbol{n}$ доказиво кад год је $m < n$ и да је $\neg\boldsymbol{m} < \boldsymbol{n}$ доказиво кад год је $m \geq n$.

Прелазимо сада на сабирање и множење, циљ нам је да докажемо да кад год је $a+b = c$ да је $\boldsymbol{a}+\boldsymbol{b} = \boldsymbol{c}$ доказиво. Показаћемо да је $\mathbf{2}+\mathbf{3} = \mathbf{5}$ или $\boldsymbol{SS}\mathbf{0} + \boldsymbol{SSS}\mathbf{0} = \boldsymbol{SSSSS}\mathbf{0}$ доказиво. Користећи $(Q4)$ доказиво је редом:

$$\begin{aligned}
\boldsymbol{SS}\mathbf{0} + \boldsymbol{SSS}\mathbf{0} &= \boldsymbol{S}(\boldsymbol{SS}\mathbf{0} + \boldsymbol{SS}\mathbf{0})\\
\boldsymbol{SS}\mathbf{0} + \boldsymbol{SS}\mathbf{0} &= \boldsymbol{S}(\boldsymbol{SS}\mathbf{0} + \boldsymbol{S}\mathbf{0})\\
\boldsymbol{SS}\mathbf{0} + \boldsymbol{S}\mathbf{0} &= \boldsymbol{S}(\boldsymbol{SS}\mathbf{0} + \mathbf{0}).
\end{aligned}$$

Користећи $(Q3)$ је $\boldsymbol{SS}\mathbf{0} + \mathbf{0} = \boldsymbol{SS}\mathbf{0}$ доказиво, користећи ово и враћајући се уназад кроз претходне једнакости добијамо да је доказиво:

$$\begin{aligned}
\boldsymbol{SS}\mathbf{0} + \boldsymbol{S}\mathbf{0} &= \boldsymbol{SSS}\mathbf{0}\\
\boldsymbol{SS}\mathbf{0} + \boldsymbol{SS}\mathbf{0} &= \boldsymbol{SSSS}\mathbf{0}\\
\boldsymbol{SS}\mathbf{0} + \boldsymbol{SSS}\mathbf{0} &= \boldsymbol{SSSSS}\mathbf{0}.
\end{aligned}$$

Овај метод се може применити у општем случају, па добијамо $\boldsymbol{a} + \boldsymbol{b} = \boldsymbol{c}$ кад год је $a + b = c$. На сличан начин се и у случају множења показује да је $\boldsymbol{a} \cdot \boldsymbol{b} = \boldsymbol{c}$ доказиво кад год је $a \cdot b = c$.

Сада посматрајмо сложеније терме. На пример, желимо да је $(\mathbf{1}+\mathbf{2}) \cdot (\mathbf{3}+\mathbf{4}) = \mathbf{21}$ доказиво. Из претходних разматрања је $\mathbf{1}+\mathbf{2} = \mathbf{3}$, $\mathbf{3}+\mathbf{4} = \mathbf{7}$ и

$\mathbf{3}\cdot\mathbf{7} = \mathbf{21}$ доказиво. Одавде само логиком добијамо да је $(\mathbf{1}+\mathbf{2})\cdot(\mathbf{3}+\mathbf{4}) = \mathbf{21}$ доказиво. Слично је за било који затворени терм изграђен од $\mathbf{0}, \boldsymbol{S}, +, \cdot$ доказиво која му је тачна вредност. Претпоставимо да два терма s и t имају исту вредност m. Доказиво је $s = \boldsymbol{m}$ и $t = \boldsymbol{m}$ одакле је и $s = t$ доказиво. Ако два терма s и t имају различите вредности m и n, доказиво је $\boldsymbol{m} \neq \boldsymbol{n}$ одакле је и $s \neq t$ доказиво. Слично су доказиве и све таче реченице облика $s < t$ и $\neg s < t$. Овиме смо показали да су све тачне атомске и негиране атомске реченице доказиве.

Сада прелазимо на сложеније реченице од атомских. Прво, дупла негација реченице доказива је ако је реченица доказива. Конјункција две реченице је доказива ако су оба конјукта доказива, дисјункција две реченице је доказива ако је бар један дисјункт доказив. Негација конјункције је доказива ако је негација бар једног конјукта доказива, негација дисјункције је доказива ако су негације оба дисјункта доказиве. Како су све тачне атомске и негиране атомске реченице доказиве, доказиве су и све тачне реченице облика:

$$\neg S_1,\ \neg\neg S_1,\ S_1 \wedge S_2,\ S_1 \vee S_2,\ \neg(S_1 \wedge S_2),\ \neg(S_1 \vee S_2)$$

где су S_1 и S_2 атомске или негиране атомске реченице. Понављањем оваквог разматрања на реченице са више негација, конјункција и дисјункција добија се да су све тачне реченице без квантификатора доказиве.

У случају ограничене квантификације, користећи (1), имамо да је за било коју формулу $\varphi(x)$ доказиво:

$$\begin{aligned}\forall x < \boldsymbol{m}\, \varphi(x) &\iff (\varphi(\mathbf{0}) \wedge \varphi(\mathbf{1}) \wedge \cdots \wedge \varphi(\boldsymbol{m} - \mathbf{1})),\\ \exists x < \boldsymbol{m}\, \varphi(x) &\iff (\varphi(\mathbf{0}) \vee \varphi(\mathbf{1}) \vee \cdots \vee \varphi(\boldsymbol{m} - \mathbf{1})).\end{aligned}$$

Овако је свака ограничена квантификација формуле без квантификатора доказиво еквивалентна реченици без квантификатора, а ова реченица је по прошлом параграфу доказива ако је тачна. Сличним аргументовањем је и свака тачна реченица добијена негацијом, дисјункцијом, конјукцијом и ограниченом квантификацијом атомских формула доказива. Другим речима свака тачна *елементарна формула* је доказива.

Коначно посматрајмо тачну $\exists$-елементарну реченицу $\exists x\, \varphi(x)$. Како је она тачна постоји неко a за које је $\varphi(\boldsymbol{a})$ тачно. Како је $\varphi(\boldsymbol{a})$ тачна, елементарна реченица она је доказива, а како је доказиво $\varphi(\boldsymbol{a})$ доказиво је и $\exists x\, \varphi(x)$. $\square$

Како би доказали да су све рекурзивне функције репрезентабилне у $\boldsymbol{Q}$ потребне су нам следеће две теореме.

Теорема 5.4. *Свака елементарна функција је репрезентабилна у* $\boldsymbol{Q}$ *и то елементарном формулом.*

Доказ. Из аксиома $(Q7)$ и $(Q8)$ претходно смо доказали:

$$x < \boldsymbol{m} \Leftrightarrow (x = \boldsymbol{0} \vee x = \boldsymbol{1} \vee \cdots \vee x = \boldsymbol{m-1}), \tag{1}$$

слично томе се из аксиома $(Q9)$ и $(Q10)$ се може показати:

$$\boldsymbol{m} < x \Leftrightarrow (x \neq \boldsymbol{0} \wedge x \neq \boldsymbol{1} \wedge \cdots \wedge x \neq \boldsymbol{m}). \tag{2}$$

Као последицу (1) и (2) имамо $x < \boldsymbol{m} \vee x = \boldsymbol{m} \vee x > \boldsymbol{m}$.

Сада нека је f унарна елементарна функција (доказ за функције друге арности је исти) и нека елементарна формула $\varphi(x, y)$ аритметички дефинише функцију f. Користимо φ како би направили нову елементарну формулу ψ која репрезентује f у теорији $\boldsymbol{Q}$. За формулу $\psi(x, y)$ узећемо:

$$\varphi(x, y) \wedge \forall z < y \neg\varphi(x, z).$$

Прво, морамо да покажемо да ако је $f(a) = b$ онда је $\psi(\boldsymbol{a}, \boldsymbol{b})$ теорема од $\boldsymbol{Q}$. Како је $\varphi(\boldsymbol{a}, \boldsymbol{b})$ тачно и како је $\neg\varphi(\boldsymbol{a}, \boldsymbol{c})$ тачно за свако $c \neq b$ добијамо да је и $\varphi(\boldsymbol{a}, \boldsymbol{b}) \wedge \forall z < \boldsymbol{b} \neg\varphi(\boldsymbol{a}, z)$ тачно, то јест $\psi(\boldsymbol{a}, \boldsymbol{b})$ је тачно. Користећи чињеницу да је $\psi(x, y)$ елементарна формула и Теорему 5.3 добијамо да је $\psi(\boldsymbol{a}, \boldsymbol{b})$ доказиво, тј. да је теорема теорије $\boldsymbol{Q}$.

Друго, морамо да покажемо да је $\forall y (y \neq \boldsymbol{b} \Rightarrow \neg\psi(\boldsymbol{a}, y))$ теорема од $\boldsymbol{Q}$. Расписујући ψ треба да докажемо:

$$\forall y (y \neq \boldsymbol{b} \Rightarrow \neg(\varphi(\boldsymbol{a}, y) \wedge \forall z < y \neg\varphi(\boldsymbol{a}, z))). \tag{3}$$

Формула (3) је логички еквивалентна са:

$$\forall y (\varphi(\boldsymbol{a}, y) \Rightarrow (y = \boldsymbol{b} \vee \exists z < y \, \varphi(\boldsymbol{a}, z)). \tag{4}$$

Заправо, довољно би било да докажемо:

$$\forall y (\varphi(\boldsymbol{a}, y) \Rightarrow (y = \boldsymbol{b} \vee \boldsymbol{b} < y)) \tag{5}$$

Јер (5) заједно са $\varphi(\boldsymbol{a}, \boldsymbol{b})$ логички имплицира (4). Приметимо да

$$\forall y (y < \boldsymbol{m} \vee y = \boldsymbol{m} \vee \boldsymbol{m} < y) \;\text{ и }\; \forall y < \boldsymbol{b} \neg\varphi(\boldsymbol{a}, y),$$

логички имплицирају (5).

Овиме је доказано да су $\psi(\boldsymbol{a}, \boldsymbol{b})$ и $\forall y (y \neq \boldsymbol{b} \Rightarrow \neg\psi(\boldsymbol{a}, y))$ теореме $\boldsymbol{Q}$, из чега следи да ψ репрезентује f у $\boldsymbol{Q}$. □

Теорема 5.5. *Композиција две елементарне функције је репрезентабилна у* $\boldsymbol{Q}$ *и то* $\exists$*-елементарном формулом.*

Доказ. Нека су f и g две унарне елементарне функције (доказ за функције друге арности је сличан) и нека их у $\boldsymbol{Q}$ репрезентују редом формуле φ_f и φ_g. Нека је $h(x) = g(f(x))$, тврдимо да следећа формула φ_h репрезентује h у $\boldsymbol{Q}$:

$$\exists y(\varphi_f(x, y) \wedge \varphi_g(y, z)).$$

Нека је $f(a) = b$ и $c = h(a) = g(f(a)) = g(b)$. Како је $f(a) = b$ и како φ_f репрезентује f следећа формула је теорема $\boldsymbol{Q}$:

$$\forall y\,(\varphi_f(\boldsymbol{a}, y) \iff y = \boldsymbol{b}). \tag{1}$$

Како је $g(b) = c$ и како φ_g репрезентује g следећа формула је теорема $\boldsymbol{Q}$:

$$\forall z\,(\varphi_g(\boldsymbol{b}, z) \iff z = \boldsymbol{c}). \tag{2}$$

Да би показали да φ_h репрезентује h треба да докажемо да је:

$$\forall z(\exists y(\varphi_f(\boldsymbol{a}, y) \wedge \varphi_g(y, z)) \iff z = \boldsymbol{c}), \tag{3}$$

теорема теорије $\boldsymbol{Q}$. Међутим, (1) и (2) логички имплицирају (3), чиме је доказ завршен. □

Сада смо у позицији и да докажемо следећу важну теорему.

Теорема 5.6.

(а) Све рекурзивне функције су репрезентабилне у $\boldsymbol{Q}$ *и то* $\exists$*-елементарним формулама*

(б) Свака рекурзивна релација је дефинабилна у $\boldsymbol{Q}$ *и то* $\exists$*-елементарном формулом.*

Доказ. Део под *(а)* одмах следи из Леме 5.3 и Теорема 5.4 и 5.5.
(б) Нека је R рекурзиван скуп и f његова карактеристична функција. Нека $\exists$-елементарна формула $\exists t\,\varphi(x, y, t)$ репрезентује f у $\boldsymbol{Q}$. Ако је број n у скупу R онда је $f(n) = 1$ и $\boldsymbol{Q}$ доказује $\exists t\varphi(\boldsymbol{n}, \mathbf{1}, t)$. Ако n није у скупу R онда је $f(n) = 0$ и $\boldsymbol{Q}$ доказује:

$$\forall y(y \neq \mathbf{0} \Rightarrow \neg\exists t\,\varphi(\boldsymbol{n}, y, t)),$$

посебно за $y = 1$, $\boldsymbol{Q}$ доказује $\neg\exists t\,\varphi(\boldsymbol{n}, \mathbf{1}, t)$. Следи да формула $\exists t\,\varphi(x, \mathbf{1}, t)$ дефинише скуп R у теорији $\boldsymbol{Q}$. Доказ за рекурзивне релације било које арности је сличан. □

Овиме смо доказали све потребне резултате за анализу прве Геделове теореме о непотпуности, међутим за другу теорему о непотпуности ће нам бити потребна теорија јача од $\boldsymbol{Q}$.

5.3 Пеанова аритметика

У претходном одељку дефинисали смо теорију минималне аритметике $\boldsymbol{Q}$, напоменули смо и да $\boldsymbol{Q}$ не може да докаже неке врло једноставне $\forall$-елементарне реченице. Најочигледнији начин да се овај недостатак исправи је да на неки начин додамо *индукцију* у нашу теорију $\boldsymbol{Q}$. С тим у виду дефинисаћемо нови бесконачан (али примитивно рекурзиван) скуп аксиома. Узимамо да су све реченице следећег облика аксиоме:

$$\forall y_1 \cdots \forall y_k((A(0) \wedge \forall x(A(x) \implies A(\boldsymbol{S}x))) \implies \forall x A(x)),$$

где је $A(x)$ формула која нема друге слободне променљиве осим $x, y_1, \ldots, y_k$.

Пеанова аритметика **PA** је теорија која се добија додавањем горе наведеног бесконачног скупа аксиома на аксиоме минималне аритметике $\boldsymbol{Q}$. На пример следеће две реченице су аксиоме **PA**:

$$((\mathbf{0}+\mathbf{0}=\mathbf{0}+\mathbf{0} \wedge$$
$$\forall x(\mathbf{0}+x=x+\mathbf{0} \implies \mathbf{0}+\boldsymbol{S}x=\boldsymbol{S}x+\mathbf{0})) \implies \forall x(\mathbf{0}+x=x+\mathbf{0}))$$

и

$$((\mathbf{1}+\mathbf{0}=\mathbf{0}+\mathbf{1} \wedge$$
$$\forall x(\mathbf{1}+x=x+\mathbf{1} \implies \mathbf{1}+\boldsymbol{S}x=\boldsymbol{S}x+\mathbf{1})) \implies \forall x(\mathbf{1}+x=x+\mathbf{1})).$$

Теорија **PA** је знатно јача од минималне аритметике $\boldsymbol{Q}$. Сада је из аксиома **PA** доказива реченица $\forall x \forall y(x+y=y+x)$. Заправо, теорија **PA** је довољна јака да докаже све класичне резултате теорије бројева, укључујући и тврђења попут *теореме о простим бројевима*, чији стандардни докази користе комплексну анализу.

6 Теореме о непотпуности

У претходним поглављима увели смо практично сву теорију потребну за разумевање Геделових теорема о непотпуности, тако да сада можемо прећи на њихову анализу.

Прво доказујемо *дијагоналну лему*, која игра кључну улогу у доказу прве теореме о непотпуности. Затим, прелазимо на саме теореме о непотпуности и говоримо нешто више о њима и њиховим последицама на математику и филозофију математике.

6.1 Дијагонална лема

Из резултата поглавља о репрезентабилности рекурзивних функција закључујемо да можемо да "причамо" о рекурзивним функцијама унутар формалних теорија аритметике. Из резултата поглавља о аритметизацији синтаксе закључујемо да можемо да "причамо" о реченицама и доказима формалне теорије користећи рекурзивне функције. Спајајући ова два запажања, можемо да "причамо" о реченицама и доказима унутар формалне теорије аритметике.

Кључна лема потребна за доказивање теорема о непотпуности јесте *дијагонална лема*. У свом раду из 1931. године Курт Гедел је доказао само њен специјални случај, док је *Рудолф Карнап* био први који је доказао њен општи облик.

У поглављу о аритметизацији синтаксе дефинисали смо код за сваки израз A језика аритметике, овај код зваћемо *Геделовим бројем* за израз A. Ако је a Геделов број израза A онда нумерал $\boldsymbol{a}$ ($\boldsymbol{S}\ldots\boldsymbol{S}\mathbf{0}$ где се $\boldsymbol{S}$ појављује a пута) зовемо *Геделовим нумералом* израза A и обележавамо га са $\ulcorner A \urcorner$.

Дефиниција 6.1. *Дијагонализација произвољног израза A је израз:*

$$\exists x(x = \ulcorner A \urcorner \wedge A).$$

Иако ова дефиниција има смисла за произвољне изразе нас ће највише занимати случај када је A заправо формула $A(x)$, са само једном слободном променљивом x. У случају да је A таква формула, њена дијагонализација ће бити логички еквивалентна реченици $A(\ulcorner A \urcorner)$.

Лема 6.1 (**Дијагонална лема**). *Нека је T теорија која садржи теорију минималне аритметике $\boldsymbol{Q}$, онда за сваку формулу $B(y)$ постоји реченица G таква да је $\vdash_T G \Leftrightarrow B(\ulcorner G \urcorner)$.*

Доказ. Докажимо прво да постоји примитивно рекурзивна функција $diag$ која за Геделов број израза A узима вредност Геделовог броја дијагонализације од A. Лако се види да важи:

$$diag(a) = exquant(v, conj(j * l * v * z * num(a) * r, a)),$$

где је v код за променљиву x, а слова j, l, z, r редом кодови за знак једнакости, леву заграду, зарез и десну заграду.

Ако теорија T садржи $\boldsymbol{Q}$, онда је по Теореми 5.6 функција $diag$ репрезентабилна у T. Нека формула $Diag(x, y)$ репрезентује $diag(x)$ у теорији T, то јест ако је $diag(m) = n$ онда је и $\vdash_T \forall y(Diag(\boldsymbol{m}, y) \Leftrightarrow y = \boldsymbol{n})$.

Нека је $A(x)$ формула $\exists y(Diag(x, y) \wedge B(y))$ и нека је a Геделов број формуле $A(x)$ и $\boldsymbol{a}$ њен Геделов нумерал. Дефинишимо још G као реченицу:

$$\exists x(x = \boldsymbol{a} \wedge \exists y(Diag(x, y) \wedge B(y))).$$

Заправо G је $\exists x(x = \boldsymbol{a} \wedge A(x))$, што је управо дијагонализација од $A(x)$ и логички је еквивалентна са $A(\boldsymbol{a})$. Расписујући реченицу $A(\boldsymbol{a})$ добијамо $\exists y(Diag(\boldsymbol{a}, y) \wedge B(y))$. Одавде је еквиваленција $G \Leftrightarrow \exists y(Diag(\boldsymbol{a}, y) \wedge B(y))$ логичка (то јест тачна у свакој интерпретацији) и самим тим је по Геделовој теореми о потпуности доказива у свакој теорији. Дакле имамо:

$$\vdash_T G \Leftrightarrow \exists y(Diag(\boldsymbol{a}, y) \wedge B(y)). \tag{1}$$

Нека је сад g Геделов број реченице G и нека је $\boldsymbol{g}$ њен Геделов нумерал. Због тога што је G дијагонализација од $A(x)$ имамо $diag(a) = g$, из чега следи:

$$\vdash_T \forall y(Diag(\boldsymbol{a}, y) \Leftrightarrow y = \boldsymbol{g}). \tag{2}$$

Даље из (1) и (2) добијамо:

$$\vdash_T G \Leftrightarrow \exists y(y = \boldsymbol{g} \wedge B(y)).$$

Пошто је $\exists y(y = \boldsymbol{g} \wedge B(y))$ логички еквивалентно са $B(\boldsymbol{g})$ добијамо:

$$\vdash_T B(\boldsymbol{g}) \Leftrightarrow \exists y(y = \boldsymbol{g} \wedge B(y)).$$

Коначно имамо:

$$\vdash_T G \Leftrightarrow B(\boldsymbol{g})$$

или другим речима $\vdash_T G \Leftrightarrow B(\ulcorner G \urcorner)$, што је и требало доказати. $\square$

Лема 6.2. *Нека је T конзистентна теорија која садржи $\boldsymbol{Q}$. Скуп Геделових бројева свих теорема теорије T није дефинабилан у T.*

Доказ. Претпоставимо супротно, да формула $\tau(x)$ дефинише скуп G_T Геделових бројева теорема теорије T. По дијагоналној леми постоји реченица G за коју важи:

$$\vdash_T G \Leftrightarrow \neg\tau(\ulcorner G \urcorner).$$

Нека је g Геделов број реченице G. Докажимо прво да G мора бити теорема од T. Претпоставимо да G није теорема теорије T то јест $g \notin G_T$, како $\tau(x)$ дефинише скуп G_T у теорији T имамо $\vdash_T \neg\tau(\ulcorner G \urcorner)$. Али како је $\vdash_T G \Leftrightarrow \neg\tau(\ulcorner G \urcorner)$ добијамо да је $\vdash_T G$.

Како је G теорема од T имамо $g \in G_T$, а опет из тога што $\tau(x)$ дефинише скуп G_T имамо и $\vdash_T \tau(\ulcorner G \urcorner)$. Али онда из $\vdash_T G \Leftrightarrow \neg\tau(\ulcorner G \urcorner)$ добијамо $\vdash_T \neg G$. Како смо доказали да је $\vdash_T G$ и $\vdash_T \neg G$ добијамо да је T неконзистентна теорија, контрадикција. $\square$

6.2 Прва теорема о непотпуности

6.2.1 Егзистенцијални доказ

Први доказ који дајемо је чисто егзистенцијалне природе. Сва његова тежина налази се у резултатима које смо већ показали.

Теорема 6.1 (**Геделова прва теорема о непотпуности**).
Ако је T конзистентна, аксиоматизабилна теорија која садржи теорију минималне аритметике $\boldsymbol{Q}$, онда је T непотпуна теорија.

Доказ. Како T садржи $\boldsymbol{Q}$ из Леме 6.2 добијамо да скуп теорема T није дефинабилан у T. Међутим, по Теореми 5.6*(б)* су сви рекурзивни скупови дефинабилни у T, из чега следи да скуп теорема од T није рекурзиван. Сада из контрапозиције Теореме 4.5 одмах добијамо да је T непотпуна теорија. $\square$

Често се среће и овај мање прецизан облик теореме: Било који формални систем који је "довољно јак" је непотпун ако је конзистентан. Под "формалан систем" мисли се на теорију (не нужно аритметике) чије се теореме могу доказати полазећи од ефективно одлучивог скупа аксиома (или само рекурзивног скупа уз прихватање Черчове тезе). Из наше формулације теореме видимо да је довољно да теорија садржи $\boldsymbol{Q}$ да би била "довољна јака". Како је $\boldsymbol{Q}$ "слаба" теорија овај резултат о непотпуности је утом снажнији.

Природно се поставља питање да ли се ова теорема може применити на формалне системе који нису дефинисани у језику аритметике. На пример, да ли је непотпуна Зермело-Фраенкелова теорија скупова са аксиомом избора, позната као **ZFC**, у којој се скоро сва модерна математика може формализовати. Генерално, шта треба да важи да би се резултати ове теореме применили на друге конзистентне формалне системе је да се аксиоме теорије $\boldsymbol{Q}$ могу "превести" у посматрану теорију. На пример аксиома $(Q8)$, $\forall x \forall y (x < \boldsymbol{S}y \Leftrightarrow (x < y \vee x = y))$ би превођењем у језик те теорије требало да изражава исто својство природних бројева, и могла би изгледати овако:

$$\forall x \forall y (N(x) \wedge N(y) \wedge (L(x, S(y)) \Leftrightarrow (L(x, y) \vee x = y))),$$

где унарна релација $N(x)$ изражава "x је природан број", бинарна релација $L(x, y)$ изражава "x је мање од y" и функција $S(y)$ изражава функцију следбеника. Уз строго дефинисање појма "превођења" (у које ми не улазимо) Геделову прву теорему о непотпуности можемо применити и на све "довољно јаке" формалне системе, а не само на теорије језика аритметике. Конкретно, теорија **ZFC** јесте **непотпуна**.

6.2.2 Геделов доказ

Дефиниција 6.2. *Реченица S је неодлучива у теорији T ако ни S ни негација од S нису доказиве у теорији T тј. ако $\nvdash_T S$ и $\nvdash_T \neg S$.*

Ако није другачије наведено подразумевамо да је T конзистентна аксиоматизабилна теорија која садржи $\boldsymbol{Q}$.

Наш први доказ нам међутим не даје ниједан конкретан пример неодлучиве реченице за теорију T, већ само тврди да таква реченица постоји. Гедел је 1931. године у овом погледу отишао корак даље и експлицитно конструисао једну неодлучиву реченицу (за формални систем Principia Mathematica). Данас ову и друге њој сличне неодлучиве реченице зовемо *Геделове реченице*.

Прво, рећи ћемо да је реченица *оспорива* у теорији T ако је њена негација доказива у T. Даље, позивајући се на Теорему 4.4 добијамо да је скуп реченица који је доказив (оспорив) полазећи од датог рекурзивног скупа аксиома рекурзивно набројив. Одавде користећи чињеницу да су сви рекурзивни скупови дефинабилни $\exists$-елементарним формулама у T добијамо да постоје формуле $Prv_T(x)$ и $Disprv_T(x)$ редом облика $\exists y Prf_T(x, y)$ и $\exists y Disprf_T(x, y)$, где су $Prf_T(x, y)$ и $Disprf_T(x, y)$ елементарне формуле, и за које је $\vdash_T A$ ако и само ако је $Prv_T(\ulcorner A \urcorner)$ тачно у стандардној интерпретацији. Одавде је и $\vdash_T A$ ако и само ако је за неки број b, $Prf_T(\ulcorner A \urcorner, \boldsymbol{b})$ тачно, или шта је за елементарне реченице еквивалентно, доказива у $\boldsymbol{Q}$, то јест у T. Слично за $Disprv_T(x)$ и $Disprf_T(x, y)$. Ако је $Prf_T(\ulcorner A \urcorner, \boldsymbol{b})$ тачно може се рећи да "број b сведочи доказивости од A".

По дијагоналној леми постоји реченица G_T за коју важи:

$$\vdash_T G_T \Leftrightarrow \neg \exists y Prf_T(\ulcorner G_T \urcorner, y).$$

Ово је **Геделова реченица** за теорију T. Њена неодлучивост почива на *самореференцији* и може се повући паралела са *парадоксом лажљивца.* Овај наводни парадокс произилази из следеће реченице: "Ова реченица је нетачна". Резонујући добијамо да је ова реченица тачна само ако је нетачна и да је нетачна само ако је тачна. Ми у нашој дефиницији истине међутим нисмо давали истинитосне вредности произвољним реченицама природног језика, већ само ваљано формираним формулама без слободних промењљивих. Тако да претходни "парадокс" нама не представља никакав проблем. Гедел је међутим успео да на један индиректан начин убаци самореференцију у нашу формалну теорију.

Често се може чути да Геделова реченица "каже за саму себе да је недоказива", мада овакав опис може бити користан за разумевање Геделове реченице треба му прићи са дозом резервисаности. Ако би у општем случају исписали реченицу G_T, теорије T, добили бисмо врло дугачку формулу без неког јасног значења.

Пре него што дамо доказ прве теореме о непотпуности у Геделовом духу треба нам још појам *ω-конзистентности.*

Дефиниција 6.3. *Теорија T је ω-инконзистентна ако и само ако је за неку формулу $F(x)$, $\vdash_T \exists x F(x)$ али је и за сваки појединачни природан број n, $\vdash_T \neg F(\boldsymbol{n})$. Теорија је ω-конзистентна ако и само ако није ω-инконзистентна.*

Напоменимо још да ω-конзистентност имплицира конзистентност.

Теорема 6.2. *Ако је T, ω-конзистентна, аксиоматизабилна теорија која садржи $\boldsymbol{Q}$, онда је Геделова реченица G_T неодлучива у T.*

Доказ. Претпоставимо да је G_T доказива у T, тј. $\vdash_T G_T$. Одавде је $\exists$-елементарна реченица $\exists y Prf_T(\ulcorner G_T \urcorner, y)$, тачна а по Теореми 5.3 онда и доказива у T. Али како је G_T Геделова реченица важи $\vdash_T G_T \Leftrightarrow \neg\exists y Prf_T(\ulcorner G_T \urcorner, y)$. Одавде само логиком добијамо $\vdash_T \neg G_T$, али је T онда инконзистентна теорија, што имплицира да је и ω-инконзистентна, контрадикција.

Претпоставимо да је G_T оспорива у T, тј. $\vdash \neg G_T$. Онда је реченица $\exists y Prf_T(\ulcorner G_T \urcorner, y)$ доказива у T. Из конзистентности теорије T добијамо да онда G_T не може бити доказива у T. Због тога за било које n, елементарна реченица $\neg Prf_T(\ulcorner G_T \urcorner, \boldsymbol{n})$ мора бити тачна, а самим тим и доказива у T. Добили смо да је T, ω-инконзистентна теорија, контрадикција.

Овиме смо доказали да T не доказује, нити оспорава G_T из чега следи да је G_T неодлучива реченица. $\square$

Нека је теорија T као у претходној теореми. Можемо отићи и корак даље и показати да је Геделова реченица G_T, тачна у стандардној интерпретацији. Прегледом доказа дијагоналне леме, видимо да је еквиваленција $G_T \Leftrightarrow \neg\exists y Prf_T(\ulcorner G_T \urcorner, y)$ заправо тачна у стандардној интерпретацији. Претпосативмо сада да је Геделова реченица нетачна. Одавде следи да је реченица $\neg\exists y Prf_T(\ulcorner G_T \urcorner, y)$ такође нетачна, то јест да је реченица $\exists y Prf_T(\ulcorner G_T \urcorner, y)$ тачна. Међутим, како је ова реченица $\exists$-елементарна, ако је тачна онда је и доказива (Теорема 5.3). Али онда из:

$$\vdash_T \neg G_T \Leftrightarrow \exists y Prf_T(\ulcorner G_T \urcorner, y)$$

и $\vdash_T \exists y Prf_T(\ulcorner G_T \urcorner, y)$ следи и да је $\vdash_T \neg G_T$ доказива. Ово је у контрадикцији са првом Геделовом теоремом о непотпуности, дакле наша претпоставка је била нетачна. Следи да је G_T тачна реченица у стандардној интерпретацији.

Из Геделове теореме о потпуности добијамо да онда морају да постоје нестандардне интерпретације језика аритметике у којима је реченица G_T нетачна (да ово није случај Геделова реченица би била доказива). У тим интерпретацијама је дакле тачна реченица $\exists y Prf_T(\ulcorner G_T \urcorner, y)$ и самим тим мора постојати неки број y који сведочи доказивости G_T. Међутим, ми знамо да ниједан стандардни број (0,1,2,3...) не задовољава тај услов. Дакле, свака интерпретација у којој је Геделова реченица нетачна мора садржати нестандардне "бесконачне" бројеве који долазе после свих природних бројева.

Шта ако само додамо ову реченицу G_T као нову аксиому теорије T, зар нећемо тако поправити ову "рупу"? Одговор је не. Нова теорија T^* ће такође бити непотпуна (ако је ω-конзистентна). Геделова реченица теорије T^* уопште не би била иста као реченица G_T. Ово следи из тога што $Prf_T(x,y)$ и $Prf_{T^*}(x,y)$ нису исте формуле, на пример $\exists y Prf_T(\ulcorner G_T \urcorner, y)$ је нетачно, док је $\exists y Prf_{T^*}(\ulcorner G_T \urcorner, y)$ тачно. Дакле, не само да је таква теорија T непотпуна, већ је у одређеном смислу и *неупотпуњива*.

Побољшање претходне теореме дао је *Баркли Росер* 1936. године. Претпоставка ω-конзистентности може се заменити слабијом претпоставком конзистентности ако уместо Геделове, докажемо неодлучивост Росерове реченице. Росерова реченица R_T такође се добија дијагоналном лемом и то на следећи начин:

$$\vdash_T R_T \Leftrightarrow \forall y (Prf(\ulcorner R_T \urcorner, y) \Rightarrow \exists z < y \, Disprf(\ulcorner R_T \urcorner, z)).$$

Ова реченица "каже за саму себе да ако постоји сведок њеној доказивост, постоји и мањи сведок њеној оспоривости".

Теорема 6.3 (**Гедел-Росерова теорема**). *Ако је T конзистентна, аксиоматизабилна теорија која садржи $\boldsymbol{Q}$ онда је Росерова реченица R_T неодлучива у T.*

Доказ ове теореме суштински је сличан доказу неодлучивости Геделове реченице, с тим што је мало компликованији.

До сада смо контруисали два примера неодлучивих реченица, међутим ова тврђења су у неку руку врло "вештачка" и нису нешто с чиме би се математичари типично сусрели. И даље бисмо можда могли наивно да се надамо да су сва "природна"[1] тврђења која би математичаре могла интересовати, доказива у некој теорији као што је **PA**. Ипак, постоје примери врло "природних" тврђења која су неодлучива у **PA**. На пример, *Гудштајнова* теорема, која тврди да одређени низови природних бројева после неког тренутка долазе до броја 0, је неодлучива у **PA**, мада се може доказати у нешто јачим теоријама.[2]

Геделова прва теорема о непотпуности нам дакле говори да не постоји аксиоматизабилна и конзистентна формална теорија у којој би могли да докажемо све истине аритметике. Битна последица овога је да *доказивост* (у неком формалном систему) и *истинитост* (у некој интерпретацији) никако нису иста ствар.

[1] Шта би било "природно", а шта "вештачко" тврђење није јасно дефинисано. Геделова реченица изражава неку законитост међу природним бројевима и у том погледу једнака је било ком другом тврђену о овим бројевима.

[2] За још један пример погледати Парис-Харингтонову теорему.

6.3 Друга теорема о непотпуности

Друга Геделова теорема о непотпуности нам говори да је реченица која изражава конзистентност теорије **PA** (или било које теорије која садржи ову) недоказива унутар **PA**, уз претпоставку да ова теорија јесте конзистентна.

Рекли смо да је теорија T конзистентна ако нису све реченице доказиве у њој. Ово је еквивалентно са многим другим условима, као на пример да ни за једну реченицу S није доказиво S и $\neg S$. Ако теорија T садржи $\boldsymbol{Q}$ (као на пример **PA**) онда као услов да је T конзистентна теорија можемо узети да T не доказује $\mathbf{0} = \mathbf{1}$. Већ знамо из аксиоме $(Q1)$ да $\boldsymbol{Q}$ доказује $\mathbf{0} \neq \mathbf{1}$, из овога следи да ако T доказује и $\mathbf{0} = \mathbf{1}$ да је онда неконзистентна теорија. Такође ако је T неконзистентна теорија онда сигурно доказује и $\mathbf{0} = \mathbf{1}$. Закључујемо да је теорија T која садржи $\boldsymbol{Q}$ конзистентна ако и само ако $\mathbf{0} = \mathbf{1}$ није доказиво у T. Реченицу $\neg Prv_T(\ulcorner \mathbf{0} = \mathbf{1} \urcorner)$ зовемо *реченица конзистентности* теорије T и можемо рећи да у одређеном смислу она изражава конзистентност теорије T.

Теорема 6.4 (**Геделова друга теорема о непотпуности**)**.** *Ако је T конзистентна, аксиоматизабилна теорија која садржи* **PA***, онда је реченица конзистентности недоказива у T.*

Нажалост, нисмо у позицији да дамо комплетан доказ ове теореме. Не због тежине идеја потребних за њен доказ, већ због гомиле рутинских провера које су у њеном извођењу неопходне. Додатно оправдање за ово је да и Гедел у раду из 1931. године даје само скицу доказа, а да први комплетан доказ објављују *Хилберт* и *Бернајс* тек 1939. године. Ипак, скица доказа коју сада дајемо је и даље корисна за разумевање овог важног резултата.

У доказу Теореме 6.2, видимо да је довољна претпоставка да је T конзистентна теорија да би доказали да је Геделова реченица недоказива у T. То јест ако $\mathbf{0} = \mathbf{1}$ није доказиво у T, онда ни G_T није доказиво. Тако да је следећа реченица тачна:

$$\neg Prv_T(\ulcorner \mathbf{0} = \mathbf{1} \urcorner) \Rightarrow \neg Prv_T(\ulcorner G_T \urcorner).$$

Шта је сада кључно је да се доказ Теореме 6.2 може формализовати у теорији **PA** и самим тим у свакој теорији T која је садржи. Дакле имамо:

$$\vdash_T \neg Prv_T(\ulcorner \mathbf{0} = \mathbf{1} \urcorner) \Rightarrow \neg Prv_T(\ulcorner G_T \urcorner).$$

Како је G_T Геделова реченица имамо и:

$$\vdash_T G_T \Leftrightarrow \neg Prv_T(\ulcorner G_T \urcorner).$$

Одавде следи:

$$\vdash_T \neg Prv_T(\ulcorner \mathbf{0} = \mathbf{1} \urcorner) \Rightarrow G_T.$$

Сада видимо да ако би имали $\vdash_T \neg Prv_T(\ulcorner \mathbf{0} = \mathbf{1} \urcorner)$, имали би и $\vdash_T G_T$, што је у контрадикцији са Теоремом 6.2. Дакле реченица конзистентности је недоказива у T.

Кључан детаљ који нам фали је доказ да се Теорема 6.2 може формализовати у **PA**. Геделови наследници су анализирали која својства *предиката доказивости* Prv_T су нам потребна за доказ друге теореме о непотпуности. Испоставља се да не морамо формализовати целу Теорему 6.2 већ само неке кључне чињенице везане за Prv_T. Илустрације ради, наводимо следећу лему, помоћу које се без превише муке (мада и даље далеко од тривијално) може доказати Теорема 6.4.

Лема 6.3. *Нека је T конзистентна, аксиоматизабилна теорија која садржи* ***PA****. Онда за све реченице A и B важи:*

(P1) Ако $\vdash_T A$ онда $\vdash_T Prv_T(\ulcorner A \urcorner)$

(P2) $\vdash_T Prv_T(\ulcorner A \Rightarrow B \urcorner) \Rightarrow (Prv_T(\ulcorner A \urcorner) \Rightarrow Prv_T(\ulcorner B \urcorner)).$

(P3) $\vdash_T Prv_T(\ulcorner A \urcorner) \Rightarrow Prv_T(\ulcorner Prv_T(\ulcorner A \urcorner) \urcorner).$

Филозофске последице друге теореме о непотпуности су многобројне. Ипак, можда историјски најважнија је тврдња да ова теорема показује да *Хилбертов програм* није остварив.

Када се испоставило да су рани покушаји да се направи опширна и свеобухватна формализација основа математике били пуни парадокса и неконзистентности, један од најзначајнијих математичара прошлог века, Давид Хилберт, предложио је план (програм) који је за циљ имао да реши проблеме у основама математике. Хилберт је предлагао да се за основу математике узме један формалан (аксиоматски) систем, за који би користећи се само *финитарном* математиком могли да докажемо да је конзистентна и такође да конзистентност јачих система буде последица доказане конзистентности слабијег система. Не постоји опште прихваћена дефиниција финитарне математике, међутим генерално се сматра да она подразумева мање од целокупне Пеанове аритметике, **PA**. Хилберт није хтео да одбаци сву математику која се позива на бесконачности, већ је хтео да кроз неоспориву, финитарну математику оправда њено коришћење. Дакле, угрубо говорећи Хилберт је хтео да конзистентност формалних систем јачих од **PA** докаже помоћу формалних система слабијих од **PA**.

Геделова друга теорема о непотпуности, међутим доказује да ни цела теорија **PA** не може доказати конзистентност ње саме, а камоли теорија јачих од ње (попут **ZFC**). Дакле, Хилбертов програм, барем облику у ком га је сам Хилберт замислио, не може се остварити.

6.4 Погрешна тумачења

Геделове теореме о непотпуности једне су од најпознатијих тврђења логике и славу уживају не само међу математичарима и филозофима, већ и у широј јавности. Делом вероватно и зато што се ова тврђења на један не сасвим прецизан начин могу формулисати и наизглед разумети без неког значајног предзнања. Из ових разлога, постоје бројна погрешна или барем делом погрешна тумачења Геделових теорема.

У овом одељку додатно ћемо појаснити шта Геделове теореме заправо доказују и анализирати нека погрешна тумачења.

Фокусирајмо се за почетак на прву теорему о непотпуности. Наша формулација исте је гласила:

Ако је T конзистентна, аксиоматизабилна теорија која садржи теорију минималне аритметике $\boldsymbol{Q}$, онда је T непотпуна.

Нагласимо да су све претпоставке о теорији T неизоставне, у смислу да без иједне од њих теорема не би важила.

1.(*Конзистентност*) Ако теорија T није конзистентнна онда су све реченице доказиве у њој, па је онда T тривијално потпуна теорија.

2.(*Аксиоматизабилност*) Посматрајмо теорију T_A која као аксиоме садржи све истините реченице (у стандардној интерпретацији), ова теорија је опет тривијално потпуна. Међутим, она није аксиоматизабилна. Теорија T_A је конзистентна и садржи $\boldsymbol{Q}$, па по Леми 6.2, скуп Геделових бројева теорема од T_A није дефинабилан у T_A. Али како су сви рекурзивни скупови дефинабилни у T_A и како су теореме од T_A заправо и њене аксиоме то следи да овај скуп аксиома није рекурзиван, то јест T_A није аксиоматизабилна.

3.(*Садржи* $\boldsymbol{Q}$) Као примере нетривијалних теорија које не садрже $\boldsymbol{Q}$ и потпуне су, погледати Пресбургерову аритметику или теорију реалних затворених поља (**RCF**). Напоменимо да језик аритметике L_A, није званичан језик ових теорија.

Једно од најчешћих погрешних тумачења Геделове прве теореме је следеће:

"Геделова прва теорема о непотпуности показује да постоје истине аритметике које нису доказиве."

Проблем с овим тумачењем је да се позива на доказивост у апсолутном смислу. Не постоји ниједна истина аритметике, која апсолутно није доказива. За било коју тачну реченицу S можемо додати S као додатну аксиому теорије **PA**, и тиме добити теорију у којој је S тривијално доказиво. Наравно, овакав "доказ" не задовољава нашу математичку интуицију, али илуструје чињеницу да не постоје недоказиве истине у апсолутном смислу. Иако је Геделова реченица за конзистентну, аксиоматизабилну теорију T која садржи $\boldsymbol{Q}$ недоказива у тој теорији, то не значи да се она не може доказати у јачим теоријама. На пример, Геделова реченица теорије **PA** је доказива у **ZFC**.

Честа је и тврдња да Геделове теореме оповргавају филозофију *механицизма*, то јест да показују да људски ум бесконачно превазилази сваку машину или формални систем. Сличну тврдњу износи и Роџер Пенроуз, математички физичар, уједно и добитник Нобелове награде. Он у Геделовим теоремама види доказ да људска самосвест није само компјутација. Овакви ставови се генерално правдају на следећи начин:

"За било коју машину, која је конзистентна и може да изврши основне операције аритметике, постојаће Геделова реченица за коју ми људи видимо да је тачна, међутим машина неће моћи да је докаже."

Кључна тврдња овде је да људи могу, ослањајући се на нашу математичку интуицију, видети да је Геделова реченица тачна. Међутим, наше резоновање да је Геделова реченица тачна (а и доказ прве теореме о непотпуности), ослањају се на претпоставку да је теорија о којој причамо конзистентна. Дакле, да би горе наведена тврдња била тачна, људи морају бити у могућности да распознају да ли је нека теорија конзистентна. Испоставља се да је ово врло проблематично.

Да би видели зашто, требаће нам једна чињеница о *Римановој хипотези*. Доказано је да је Риманова хипотеза еквивалентна једној $\forall$-елементарној реченици језика аритметике, назовимо ову реченицу RH. Додајмо сада у аксиоме теорије **PA** још и реченицу RH. Ова нова теорија је заправо конзистентна ако и само ако је Риманова хипотеза тачна[3]. У једном смеру импликација је тривијална, а ако би Риманова

[3]Наравно овде би требало да додамо и услов да је **PA** конзистентна теорија, међутим као што ћемо видети, то је задовољено.

хипотеза била нетачна онда би $\neg RH$ била тачна $\exists$-елементарна реченица па би по Теореми 5.3 била и доказива, одакле су обе реченице RH и $\neg RH$ доказиве па је посматрана теорија неконзистентна.

Дакле, да би ми били у могућности да распознамо да ли је ова нова теорија конзистентна, морамо и бити у могућности да одредимо да ли је Риманова хипотеза тачна. Ово међутим не умемо урадити.

За крај, погледајмо једно неисправно тумачење Геделове друге теореме о непотпуности.

"Геделова друга теорема о непотпуности нам казује да никада не можемо знати да ли је неки формални систем конзистентан."

Геделова друга теорема нам међутим не казује то, већ да **унутар** тог формалног система његову конзистентност не можемо доказати. То не значи да не постоји неки "обичан" математички доказ те чињенице, где под обичним доказом мислимо на стандардне математичке доказе с којима смо се сретали целог живота.

Геделова друга теорема о непотпуности доказује да се унутар теорије **PA** не може доказати њена конзистентност. Ипак, *Герхард Генцен* је 1936. године објавио доказ конзистентности **PA**, уз коришћење трансфинитне индукције до ординала ε_0. Оваква индукција не може се извршити унутар саме **PA**, па се овај резултат не коси са другом теоремом о непотпуности. Такође, конзистентност теорије **PA** може се доказати унутар **ZFC**.

7 Закључак

У овом раду смо представили Геделове теореме о непотпуности и сву теорију потребну за њихово разумевање. Циљ нам је био да на један разумљив, али и математички формалан начин, прикажемо ове важне резултате. Читалац који би хтео да сазна нешто више о Геделовим теоремама може погледати [2], док они које занима теорија израчунљивости и њена примена у логици могу погледати [1].

Овом приликом бих хтео и да се захвалим свом ментору, др Зорану Петрићу, на издвојеном времену и бројним корисним коментарима и сугестијама.

Литература

[1] G.S. Boolos, J.P. Burgess, R.C. Jeffrey, *Computability and Logic*, Fifth edition, 2007.

[2] Peter Smith, *An Introduction to Gödel's Theorems*, Second edition, 2013.

[3] Коста Дошен, *Основна логика*, 2013.

[4] Ж. Мијајловић, З. Марковић, К. Дошен, *Хилбертови проблеми и логика*, (1986), 51-89.

[5] `https://plato.stanford.edu/entries/goedel`

[6] `https://plato.stanford.edu/entries/hilbert-program/`