Ирена Спасић **Предраг Јаничић**

ТЕОРИЈА АЛГОРИТАМА, ЈЕЗИКА И АУТОМАТА

Збирка задатака

МАТЕМАТИЧКИ ФАКУЛТЕТ

Београд, 2000

Аутори:

мр Ирена Спасић, асистент Економског факултета у Београду
мр Предраг Јаничић, асистент Математичког факултета у Београду

ТЕОРИЈА АЛГОРИТАМА, ЈЕЗИКА И АУТОМАТА
Збирка задатака

Издавач: Математички факултет, Студенцки трг 16, Београд
За издавача: др Неда Бокан

Издавачки одбор:
др Зоран Каделбург, председник
др Трајко Ангелов
др Гојко Калајџић
др Илија Лукачевић
др Гордана Павловић–Лажетић

Рецензенти:
др Гордана Павловић–Лажетић, ванредни професор Математичког факултета у Београду
др Жарко Мијајловић, редовни професор Математичког факултета у Београду

Обрада текста и слика: *аутори*

Штампа и повез: ВЕДЕС, Љешка 57, Београд

CIP - Каталогизација у публикацији Народна библиотека Србије, Београд

510.5(075.8)(076)

СПАСИЋ, Ирена
Теорија алгоритама, језика и аутомата: збирка задатака/
Ирена Спасић, Предраг Јаничић. – Београд : Математички факултет, 2000 (Београд : Ведес). -II 149 стр. : граф. прикази : 24 цм

Тираж 300. - Библиографија: стд. 149.
ISBN: 86-7589-013-3

1. Јаничић, Предраг)
519.713(075.8) (076) 519.76(075.8) (076)
а) Алгоритми - Задаци б) Аутомати - Задаци
ц) Математичка лингвистика - Задаци
ИД = 82247692

Предговор

Збирка која је пред вама настала је на основу белешки за вежбе из предмета *Теорија алгоритама, језика и аутомата* (који се изучава на трећој години студија на смеру Рачунарство и информатика на Математичком факултету Универзитета у Београду), које смо изводили током академских година 1996/97 (мр Ирена Спасић) и 1997/98 и 1998/99 (мр Предраг Јаничић). Надамо се да ће ова збирка олакшати праћење вежби и припрему испита студентима Математичког факултета, али да ће бити занимљива и осталима који се баве теоријом израчунљивости и теоријом формалних језика.

Збирка је подељена на три дела: део који се односи на формалне језике, део који се односи на аутомате и део који се односи на теорију алгоритама. На смеру Рачунарство и информатика на Математичком факултету теорија аутомата се изучава и у оквиру предмета Преводиоци и интерпретатори, па се у оквиру предмета Теорија алгоритама, језика и аутомата (и у овој збирци) излажу само основни резултати из ове области.

Пријатна нам је дужност да се овом приликом захвалимо рецензентима проф. др Гордани Павловић–Лажетић и проф. др Жарку Мијајловићу који су нам низом драгоцених сугестија помогли у припремању ове збирке. Захваљујемо се и свима који су нам указали на пропусте начињене у радној верзији ове збирке.

Београд, фебруар 2000. *Аутори*

Предговор електронском издању

Ово, електронско издање збирке доступно је са интернета, са адресе `www.matf.bg.ac.rs/~janicic`. Ово издање идентично је првом издању, уз исправљене, углавном ситне, грешке на које су нам указали тадашњи студенти Милена Вујошевић, Саша Стевановић и Иван Елчић, на чему смо им веома захвални.

Београд, август 2014. *Аутори*

Садржај

Део 1

Формални језици и граматике

Граматике представљају један од формализама за опис језика, односно њихове структуре. Оне имају нарочит значај у изучавању бесконачних језика. Формалне граматике, као генераторски системи, могу на основу коначних азбука, коришћењем коначно много правила, да генеришу и бесконачне језике, те чине њихову коначну спецификацију. Различитим класама граматика одговарају различити типови језика.

1.1 Формални језици

1.1.1 Слово, азбука, реч, језик

Дефиниција 1.1 Азбука Σ *је неки коначан, непразан скуп симбола. Те симболе називамо* словима.

Дефиниција 1.2 Реч над азбуком Σ *је сваки коначан низ слова из азбуке* Σ. Празна реч, *у ознаци* e, *је реч која не садржи ниједно слово.* Дужина речи x, *у ознаци* $|x|$, *је број слова садржаних у речи* x.

Реч над азбуком Σ се може дефинисати и рекурзивно, на следећи начин:

(i) Празна реч, e, је реч над Σ.

(ii) Ако је a слово и x реч над Σ, онда је и xa реч над Σ.

(iii) Речи над Σ могу бити добијене само коначном применом правила (i) и (ii).

Слично, дужина речи се може дефинисати рекурзивно, на следећи начин:

(i) $|e| = 0$

(ii) Ако је a слово и x реч над Σ, онда је $|xa| = |x| + 1$.

Дефиниција 1.3 *Реч добијена* дописивањем *(*конкатенацијом, производом*) две речи x и y (чије су дужине редом m и n), у ознаци $x \cdot y$ или xy, је реч дужине $m+n$, таква да је i-то слово речи xy једнако i-том слову речи x ако је $i \leq m$, односно $i-m$-том слову речи y ако је $i > m$.*

Теорема 1.1 *Својства конкатенације (дописивања):*

1° *Празна реч, e, је неутрални елемент за конкатенацију:*

$$ex = xe = x$$

2° *Конкатенација је асоцијативна операција:*

$$(xy)z = x(yz)$$

3° *За конкатенацију важе закони скраћивања:*

$$xz = yz \ \Rightarrow \ x = y$$

$$zx = zy \ \Rightarrow \ x = y$$

Дакле, скуп речи неког језика са операцијом конкатенације чини асоцијативни моноид.

Дефиниција 1.4 *Скуп свих речи над азбуком Σ означавамо са Σ^*, а скуп свих непразних речи над азбуком Σ означавамо са Σ^+ ($\Sigma^+ = \Sigma^* \backslash \{e\}$).*

Дефиниција 1.5 *Нека је Σ азбука. Сваки подскуп скупа свих речи Σ^* над Σ називамо* језиком над Σ. *На скупу $\mathcal{P}(\Sigma^*)$ свих језика над Σ дефинишемо следеће операције:*

(i) *скуповне: $\cup$, $\cap$, $\backslash$, $'$ (комплемент у односу на Σ^*);*

(ii) *производ: $L_1 \cdot L_2 = \{x_1 x_2 \mid x_1 \in L_1, x_2 \in L_2\}$;*

(iii) *степен: $L^0 = \{e\}$, $L^{i+1} = L^i \cdot L$;*

(iv) *итерација: $L^* = \bigcup_{i \geq 0} L^i$.*

Задатак 1 *Доказати да не постоји ниједна реч x азбуке $\Sigma = \{a, b\}$ за коју важи једнакост $xa = bx$.*

Решење:

Изведимо доказ математичком индукцијом по дужини речи x.

За празну реч e не важи једнакост $ea = be$ (јер је $a \neq b$), па тврђење важи за реч x дужине 0.

За $|x| = 1$, важи $x = a$ или $x = b$. Међутим, како је $aa \neq ba$ и $ba \neq bb$, следи да тврђење важи за речи x дужине 1.

Претпоставимо да тврђење важи за све речи дужине $n-2$ и докажимо да онда важи и за речи дужине n.

Претпоставимо супротно — да постоји реч x дужине n таква да важи $xa = bx$. Дакле, реч x почиње словом b, а завршава се словом a, па реч x може бити написана у облику $x = bya$, где је y реч дужине $|x| - 2 = n - 2$. Онда важи:

$$byaa = bbya,$$

одакле, на основу закона скраћивања, следи

$$ya = by,$$

тј. реч y је решење задате једначине и $|y| = n - 2$. То, међутим, противречи индуктивној претпоставци, одакле следи да не постоји реч x дужине n таква да важи $xa = bx$.

Тврђење је доказано за речи дужине 0 и 1, па, из доказаног индуктивног корака, следи да тврђење важи за све природне бројеве, чиме је доказано да не постоји ниједна реч x азбуке $\Sigma = \{a, b\}$ за коју важи једнакост $xa = bx$.

Задатак 2 *Решити над азбуком* $\Sigma = \{a, b, c\}$ *једначину по* x*:* $ax = xa$.

Решење:

Доказаћемо да је скуп решења једначине једнак скупу свих речи облика a^n $(n \geq 0)$.

($\supseteq$): За свако $n \geq 0$, реч a^n јесте решење дате једначине, јер $aa^n = a^{n+1} = a^n a$.

($\subseteq$): Доказаћемо математичком индукцијом по дужини речи x да је свако решење дате једначине облика a^n $(n \geq 0)$.

За $|x| = 0$ (тј. $x = e$) важи $x = a^0$.

За $|x| = 1$, из $ax = xa$ следи $x = a$, тј. $x = a^1$.

Претпоставимо да је тврђење тачно за све речи дужине $n-2$ и докажимо да је тачно и за речи дужине n. Нека је $|x| = n$ и нека је $ax = xa$. Дакле, реч x почиње и завршава се словом a, па је $x = aya$, где је y реч над задатом азбуком дужине $n-2$. Скраћивањем се из $aaya = ayaa$ добија $ay = ya$, па је реч y решење задате једначине дужине $n-2$. На основу индуктивне претпоставке, реч y је облика a^n $(n \geq 0)$, па је реч x облика a^{n+2} $(n \geq 0)$.

Задатак 3 *Нека је језик* L *над азбуком* $\Sigma = \{a, b, +, (,)\}$ *дефинисан на следећи начин:*

(i) $a, b \in L$

(ii) *Ако речи* x *и* y *припадају језику* L*, онда језику* L *припада и реч* $(x+y)$.

(*iii*) *Све речи које припадају скупу L добијене су коначном применом правила (i) и (ii).*

Нека је $x \in L$. Означимо са $k(x)$ укупан број појављивања слова (и) у речи x. Изразити у функцији од $k(x)$ број појављивања слова + у речи x.

1.1.2 Левијева лема

Теорема 1.2 (Леви) *Нека су a, b, c и d речи над азбуком Σ. Тада важи једнакост $ab = cd$ ако и само ако је задовољен неки од следећих услова:*

(*i*) $a = c$ *и* $b = d$

(*ii*) *Постоји непразна реч x над азбуком Σ, таква да је $a = cx$ и $d = xb$.*

(*iii*) *Постоји непразна реч y над азбуком Σ, таква да је $c = ay$ и $b = yd$.*

Доказ:

($\Rightarrow$:) Нека је $ab = cd$. Тада ове речи, a и c, почињу истим словима, тј. задовољен је неки од следећих услова:

$a = c$**:** Тада је $ab = ad$, одакле се, након скраћивања, изводи једнакост $b = d$. Дакле, задовољен је услов (i).

$a = cx$**,** $x \neq e$**:** Тада је $cxb = cd$, одакле се, након скраћивања, изводи једнакост $xb = d$. Дакле, задовољен је услов (ii).

$c = ay$**,** $y \neq e$**:** Аналогно претходном случају се закључује да је задовољен услов (iii).

($\Leftarrow$:) Из услова (i) се непосредно изводи једнакост $ab = cd$. Ако је задовољен услов (ii), онда важи следећи низ једнакости:

$$ab = (cx)b = c(xb) = cd,$$

па, дакле, и једнакост $ab = cd$. Слично, исти закључак се може извести и у случају када је задовољен услов (iii). $\square$

Задатак 4 *Решити по x и y једначину $ax = by$, где су a и b дате речи.*

Решење:

На основу Левијеве леме (теорема 1.2), једнакост $ax = by$ важи ако и само ако је задовољен неки од следећих услова:

(*i*) $a = b$, $x = y$

(*ii*) $a = bz_1$, $y = z_1x$ за неку непразну реч z_1

(iii) $b = az_2$, $x = z_2y$ за неку непразну реч z_2

Мотивисани претходним закључком, при решавању дате једначине разликоваћемо следећа четири случаја:

(i) Ако је $a = b$, онда је решење једначине $x = y = c$, где је c произвољна реч.

(ii) Ако је $a = bz_1$, онда је решење једначине $x = c$, $y = z_1c$, где је c произвољна реч.

(iii) Ако је $b = az_2$, онда је решење једначине $x = z_2c$, $y = c$, где је c произвољна реч.

(iv) Ако није задовољен ниједан од услова $(i) - (iii)$, онда једначина нема решења.

Задатак 5 *Азбуку Σ чине симболи константи $(a, b, c, \dots)$, симболи променљивих $(x, y, z, \dots)$, операцијски симбол $*$ дужине 2 и специјални симболи за заграде (и). Над том азбуком дефинишемо* израз *на следећи начин:*

(i) *Константе и променљиве су изрази.*

(ii) *Ако су t_1 и t_2 изрази, онда је и $(t_1 * t_2)$ израз.*

(iii) *Изрази могу бити описани само коначном применом правила (i) и (ii).*

Доказати тврђења:

Ако је t израз, а r било која непразна реч над азбуком Σ, онда tr није израз.

Ако је t израз, а r било која непразна реч над азбуком Σ, онда ни rt није израз.

Решење:

Докажимо тврђење математичком индукцијом по дужини речи t.

Нека је t израз дужине 1. То, због начина на који је израз дефинисан, значи да је t или симбол константе или симбол променљиве. Даље, нека је r произвољна непразна реч над датом азбуком. За дужину речи tr важи $|tr| \geq 2$. Претпоставимо сада супротно – да реч tr јесте израз. То, опет због начина на који је израз дефинисан, значи да је он облика $(t_1 * t_2)$. Одатле следи да $t = ($, што противречи претходно утврђеној чињеници да је t симбол константе, односно променљиве.

Претпоставимо да тврђење важи за све изразе дужине мање од n $(n > 1)$ и докажимо да тврђење важи за изразе дужине n.

Нека је t израз дужине n и r произвољна непразна реч над датом азбуком. Претпоставимо супротно — да реч tr јесте израз. Тада је

$tr = (t_1 * t_2)$, где су t_1 и t_2 изрази. С друге стране, израз t је дужине веће од 1, па је облика $(t' * t'')$, где су t' и t'' изрази. Дакле, важи

$$(t' * t'')r = (t_1 * t_2),$$

одакле се, након скраћивања, изводи

$$t' * t'')r = t_1 * t_2).$$

Одавде се такође може закључити и да је $r = r')$ за неку реч $r' \in \Sigma^*$. Дакле, важи:

$$\underbrace{t'}_{A}\underbrace{*t'')r'}_{B} = \underbrace{t_1}_{C}\underbrace{*t_2}_{D}.$$

Из последње једнакости, на основу Левијеве леме (теорема 1.2), следи да мора бити задовољен један од следећих услова:

$A = C, B = D$**:** Тада је $t' = t_1$ и $*t'')r' = *t_2$. Из последње једнакости се, након скраћивања, добија једнакост $t'')r' = t_2$, која противречи индуктивној претпоставци, јер је $|t''| < |t| = n$.

$A = CX, XB = D$**:** Тада је $t' = t_1X$ и $X * t'')r' = *t_2$ (где је X непразна реч). Прва једнакост противречи индуктивној претпоставци, јер је $|t_1| < |t'| < |t| = n$.

$AY = C, B = YD$**:** Тада је $t'Y = t_1$ и $*t'')r' = Y * t_2$ (где је Y непразна реч). Прва једнакост противречи индуктивној претпоставци, јер је $|t'| < |t| = n$.

Дакле, за израз t било које дужине не постоји непразна реч r над азбуком Σ таква да је tr такође израз.

Аналогно се доказује и да за израз t било које дужине не постоји непразна реч r над азбуком Σ таква да је rt такође израз.

1.2 Формалне граматике

Дефиниција 1.6 *Нека су Σ и N две дисјунктне азбуке и нека је S слово азбуке N ($S \in N$).* Формална граматика (граматика Чомског [1]) *је уређена четворка*

$$G = (N, \Sigma, P, S),$$

где је P (коначан) скуп правила извођења (правила замене *или* продукционих правила) *облика*

$$\alpha \rightarrow_G \beta,$$

при чему је $\alpha \in (N \cup \Sigma)^* N (N \cup \Sigma)^*$, $\beta \in (N \cup \Sigma)^*$.

Скуп Σ називамо скупом завршних (терминалних) слова*, скуп N* скупом незавршних (нетерминалних) слова*, а слово S* почетним *(или* полазним*) словом или* аксиомом граматике.

[1] Avram Noam Chomsky (1928-), амерички лингвиста

(Правила извођења $\alpha \to_G \beta_1$, $\alpha \to_G \beta_2$, ..., $\alpha \to_G \beta_n$, краће записујемо на следећи начин: $\alpha \to_G \beta_1 \mid \beta_2 \mid \ldots \mid \beta_n$).

Пример 1.1 $\Sigma = \{a, b, (,), *\}$
$N = \{S\}$
$P = \{S \to (S * S), S \to a, S \to b\}$

Пример 1.2 $\Sigma = \{p, q, r, (,), \wedge, \vee\}$
$N = \{S\}$
$P = \{S \to (S \vee S), S \to (S \wedge S), S \to p, S \to q, S \to r\}$

Дефиниција 1.7 *Релацију* непосредне последице *(или* непосредне изводивости*) за граматику G, у означи $\Rightarrow_G$ дефинишемо на следећи начин:*

$$\phi\alpha\psi \Rightarrow_G \phi\beta\psi \quad \textit{ако и само ако} \quad \alpha \to_G \beta,$$

при чему су ϕ и ψ ма које речи над азбуком $N \cup \Sigma$. Везу $\gamma \Rightarrow_G \delta$ читамо: реч δ је непосредна последица речи γ *или из* γ се непосредно изводи δ.

Дефиниција 1.8 *Ако важи $\alpha \Rightarrow_G \alpha_1$, $\alpha_1 \Rightarrow_G \alpha_2$, ..., $\alpha_{k-1} \Rightarrow_G \beta$, онда пишемо краће $\alpha \Rightarrow_G^k \beta$, кажемо* реч β се изводи у k корака из речи α, *а за дато извођење кажемо да је* дужине k. *Речи $\alpha, \alpha_1, \alpha_2, \ldots, \beta$ називамо* члановима извођења.

Додатно, уводимо и релацију $\Rightarrow_G^0$ на следећи начин:

$$\alpha \Rightarrow_G^0 \beta \quad \textit{ако и само ако} \quad \alpha = \beta$$

За извођење $\alpha \Rightarrow_G^0 \beta$ кажемо да је дужине 0 и називамо га тривијалним извођењем.

Дефиниција 1.9 *Транзитивно затворење релације $\Rightarrow_G$ означавамо са $\Rightarrow_G^+$, а транзитивно и рефлексивно са $\Rightarrow_G^*$. Везу $\alpha_1 \Rightarrow_G^* \alpha_n$, односно $\alpha_1 \Rightarrow_G^+ \alpha_n$ читамо:* из α_1 се посредно изводи α_n *или* реч α_n је посредна последица речи α_1 *или* из α_1 посредно следи α_n.

Дефиниција 1.10 Језик граматике $G = (N, \Sigma, P, S)$, *у означи $L(G)$, дефинишемо на следећи начин:*

$$L(G) = \{w \mid w \in \Sigma^* \;\wedge\; S \Rightarrow_G^+ w\}$$

Граматика може да се схвати и као посебан тип формалне теорије са коначно много правила извођења од којих су сва дужине два и са једном аксиомом S. Доказ теореме α_n ($\alpha_n \in (N \cup \Sigma)^*$) је коначан низ речи $\alpha_1, \alpha_2, \ldots, \alpha_n$, где су α_i аксиоме (тј. S) или су изведене из претходних чланова низа по неком од правила извођења. Језик генерисан граматиком G или, краће, језик граматике G, у означи $L(G)$, је скуп свих теорема те граматике које не садрже незавршна слова.

1.2.1 Класификација Чомског

Дефиниција 1.11 *Граматика $G = (N, \Sigma, P, S)$ је*

- десно линеарна *ако су сва њена правила облика*

$$A \to w \quad \text{или} \quad A \to wB,$$

где је $A, B \in N$ и $w \in \Sigma^*$;

- лево линеарна *ако су сва њена правила облика*

$$A \to w \quad \text{или} \quad A \to Bw,$$

где је $A, B \in N$ и $w \in \Sigma^*$;

- контекстно слободна *ако су сва њена правила облика*

$$A \to \alpha,$$

где је $A \in N$ и $\alpha \in (N \cup \Sigma)^*$;

- контекстно зависна *ако су сва њена правила облика*

$$\alpha \to \beta,$$

где је $\alpha, \beta \in (N \cup \Sigma)^*$ и $|\alpha| \leq |\beta|$.

Приметимо да су све десно (и лево) линеарне граматике контекстно слободне. Контекстно слободна граматика је контекстно зависна уколико не садржи ниједно e-правило (јер за правило $A \to e$ не важи $1 = |A| \leq |e| = 0$).

За језик L се каже да је десно линеаран, односно контекстно слободан, односно контекстно зависан ако постоји граматика G одговарајућег типа која га генерише, тј. $L = L(G)$. Нагласимо да неки језик L може бити генерисан граматикама различитог типа, што је јасно из малопре наведеног односа међу датим типовима граматика. Тако, на пример, сваки десно (лево) линеаран језик јесте уједно и контекстно слободан, док обратно не мора да важи. То значи да постојање контекстно слободне граматике која генерише неки језик не искључује могућност да тај језик може бити генерисан и неком линеарном граматиком, тј. да такав језик јесте линеаран.

Задатак 6 *Одредити језик генерисан граматиком $G = (N, \Sigma, P, S)$, где је*
$N = \{S\}$,
$\Sigma = \{a, b\}$,
$P = \{S \to aS \ (1^\circ), S \to b \ (2^\circ)\}$.

Решење:

Наведимо најпре, мотивације ради, један пример извођења у граматици G:

$$S \stackrel{1^\circ}{\Rightarrow} aS \stackrel{1^\circ}{\Rightarrow} aaS \stackrel{1^\circ}{\Rightarrow} aaaS \stackrel{2^\circ}{\Rightarrow} aaab$$

Докажимо да важи:[2]

$$L(G) = \{a^n b \mid n \in \mathbf{N}\}$$

$\subseteq$: *Свака завршна реч која се изводи у граматици G је облика $a^n b$ ($n \in \mathbf{N}$).*

Докажимо индукцијом јаче тврђење:

Лема 1.1 *Све речи које могу бити изведене у граматици G су облика $a^n S$ или $a^n b$ ($n \in \mathbf{N}$).*

Доказ индукцијом по дужини извођења, k:

За $k = 0$, у одговарајућем извођењу није примењено ниједно правило извођења, тј. извођење је тривијално. За почетно слово S, дакле, добија се такође реч S. Како је $S = a^0 S$, тврђење важи за $k = 0$.

Претпоставимо да тврђење важи за сва извођења дужине мање од k ($k > 0$) и докажимо да оно важи и за извођења дужине k.

Нека је $S \Rightarrow^k w$, тј. $S \Rightarrow^{k-1} w' \Rightarrow w$. Реч w' се изводи у $k-1$ корака, па је, на основу индуктивне претпоставке, w' облика $a^n S$, односно $a^n b$ ($n \in \mathbf{N}$). Реч w се нетривијално, у овом случају извођењем дужине 1, изводи из речи w', па w' мора да садржи бар једно незавршно слово. Отуда, w' је облика $a^n S$. Ако је у k-том кораку примењено правило 1°, онда је w облика $a^{n+1} S$, а ако је примењено правило 2°, онда је w облика $a^n b$.

Дакле, све речи које могу бити изведене у граматици G су облика $a^n S$ или облика $a^n b$ ($n \in \mathbf{N}$), што је и требало доказати. $\square$

На основу дате леме, сви чланови извођења (све речи које могу бити изведене у граматици G) су облика $a^n S$ или $a^n b$ ($n \in \mathbf{N}$), па, дакле, и завршне речи — речи без незавршних слова. Завршне речи не могу бити облика $a^n S$ (јер је S незавршно слово), па су све завршне речи облика $a^n b$ ($n \in \mathbf{N}$). Значи, $L(G) \subseteq \{a^n b \mid n \in \mathbf{N}\}$.

$\supseteq$: *Свака реч облика $a^n b$, $n \in \mathbf{N}$, може бити изведена у граматици G.*

За произвољно n ($n \in \mathbf{N}$) реч $a^n b$ може бити изведена у граматици G:

[2] Са $\mathbf{N}$ означавамо скуп природних бројева, тј. скуп $\{0, 1, 2, \dots\}$. Са $\mathbf{N}^+$ означавамо скуп позитивних природних бројева, тј. скуп $\{1, 2, \dots\}$.

$$S \underbrace{\stackrel{1^\circ}{\Rightarrow} aS \stackrel{1^\circ}{\Rightarrow} \cdots \stackrel{1^\circ}{\Rightarrow}}_{n} a^n S \stackrel{2^\circ}{\Rightarrow} a^n b$$

Дакле, $L(G) \supseteq \{a^n b \mid n \in \mathbf{N}\}$.

Задатак 7 *Одредити језик генерисан граматиком $G = (N, \Sigma, P, S)$, где је*
$N = \{S\}$,
$\Sigma = \{a, b\}$,
$P = \{S \to aSb\ \ (1^\circ), S \to e\ \ (2^\circ)\}$.

Решење:

Наведимо најпре, мотивације ради, један пример извођења у граматици G:

$$S \stackrel{1^\circ}{\Rightarrow} aSb \stackrel{1^\circ}{\Rightarrow} aaSbb \stackrel{1^\circ}{\Rightarrow} aaaSbbb \stackrel{2^\circ}{\Rightarrow} aaabbb$$

Докажимо да важи:

$$L(G) = \{a^n b^n \mid n \in \mathbf{N}\}$$

$\subseteq$: *Свака завршна реч која се изводи у граматици G је облика $a^n b^n$, $n \in \mathbf{N}$.*

Докажимо индукцијом јаче тврђење:

Лема 1.2 *Све речи које могу бити изведене у граматици G су облика $a^n S b^n$ или облика $a^n b^n$ ($n \in \mathbf{N}$).*

Доказ индукцијом по дужини извођења:

За $k = 0$, у одговарајућем извођењу није примењено ниједно правило извођења, тј. извођење је тривијално. За почетно слово S, дакле, добија се такође реч S. Како је $S = a^0 S b^0$, тврђење важи за $k = 0$.

Претпоставимо да тврђење важи за сва извођења дужине мање од k ($k > 0$) и докажимо да оно важи и за извођења дужине k.

Нека је $S \Rightarrow^k w$, тј. $S \Rightarrow^{k-1} w' \Rightarrow w$. Реч w' се изводи у $k-1$ корака, па је, на основу индуктивне претпоставке, w' облика $a^n S b^n$, односно $a^n b^n$ ($n \in \mathbf{N}$). Реч w се нетривијално, у овом случају извођењем дужине 1, изводи из речи w', па w' мора да садржи бар једно незавршно слово. Отуда, w' је облика $a^n S b^n$. Ако је у k-том кораку примењено правило 1°, онда је w облика $a^{n+1} S b^{n+1}$, а ако је примењено правило 2°, онда је w облика $a^n b^n$.

Дакле, све речи које могу бити изведене у граматици G су облика $a^n S b^n$ или облика $a^n b^n$ ($n \in \mathbf{N}$), што је и требало доказати. $\square$

На основу леме, сви чланови извођења (све речи које могу бити изведене у граматици G) су облика $a^n S b^n$ или $a^n b^n$ ($n \in \mathbf{N}$), па и завршне речи — речи без незавршних слова. Завршне речи не могу бити облика $a^n S b^n$ (јер је S незавршно слово), па су све завршне речи облика $a^n b^n$ ($n \in \mathbf{N}$). Значи, $L(G) \subseteq \{a^n b^n \mid n \in \mathbf{N}\}$.

$\supseteq$: *Свака реч $a^n b^n$, $n \in \mathbf{N}$, може бити изведена у граматици G.*

За произвољно n ($n \in \mathbf{N}$) реч $a^n b^n$ може бити изведена у граматици G:

$$S \underbrace{\overset{1^\circ}{\Rightarrow} aSb \overset{1^\circ}{\Rightarrow} \cdots \overset{1^\circ}{\Rightarrow}}_{n} a^n S b^n \overset{2^\circ}{\Rightarrow} a^n b^n$$

Дакле, $L(G) \supseteq \{a^n b^n \mid n \in \mathbf{N}\}$.

Задатак 8 *Одредити језик генерисан граматиком $G = (N, \Sigma, P, S)$, где је*
$N = \{S, A\}$,
$\Sigma = \{a, b\}$,
$P = \{S \to AA \ \ (1^\circ), A \to AAA \ \ (2^\circ), A \to bA \ \ (3^\circ), A \to Ab \ \ (4^\circ), A \to a \ \ (5^\circ)\}$.

Решење:

Са $\#_x(y)$ означавамо број појављивања слова x (завршног или незавршног) у речи y.

Докажимо да важи:

$$L(G) = \{w \mid w \in \{a,b\}^* \ \wedge \ \#_a(w) \text{ је паран број већи од } 0\}.$$

$\subseteq$: *За сваку завршну реч која се изводи у граматици G важи: $\#_a(w)$ је паран број већи од 0.*

Докажимо индукцијом следеће тврђење:

Лема 1.3 *За све речи w које могу бити изведене у граматици G вредност $\#_a(w) + \#_A(w)$ је паран број.*

Докажимо ово тврђење индукцијом по дужини извођења, k:

За $k = 0$, у извођењу није примењено ниједно правило извођења, тј. извођење је тривијално. За почетно слово S, дакле, добија се такође реч S. Како је $\#_a(S) + \#_A(S) = 0 + 0 = 0$, тврђење важи за $k = 0$.

Претпоставимо да тврђење важи за сва извођења чија је дужина мања од k ($k > 0$) и докажимо да оно важи и за извођења дужине k.

Нека је $S \Rightarrow^k w$, тј. $S \Rightarrow^{k-1} w' \Rightarrow w$. Реч w' се изводи у $k-1$ корака, па је, на основу индуктивне претпоставке вредност $\#_a(w') + \#_A(w')$ паран број већи од 0.

У k-том кораку извођења примењено је једно од правила 1°-5°:

1° Важи $\#_a(w) = \#_a(w')$ и $\#_A(w) = \#_A(w') + 2$, па је $\#_a(w') + \#_A(w') = \#_a(w') + \#_A(w') + 2$. На основу индуктивне претпоставке, број $\#_a(w') + \#_A(w')$ је паран, па је паран и број $\#_a(w) + \#_A(w)$.

2° Из $\#_a(w) = \#_a(w')$ и $\#_A(w) = \#_A(w') + 2$, следи тврђење.

3° Из $\#_a(w) = \#_a(w')$ и $\#_A(w) = \#_A(w')$, следи тврђење.

4° Из $\#_a(w) = \#_a(w')$ и $\#_A(w) = \#_A(w')$, следи тврђење.

5° Из $\#_a(w) = \#_a(w') + 1$ и $\#_A(w) = \#_A(w') - 1$, следи тврђење.

Дакле, за све речи w које могу бити изведене у граматици G вредност $\#_a(w) + \#_A(w)$ је паран.

$\square$

На основу леме, за све чланове извођења w (све речи које могу бити изведене у граматици G) је $\#_a(w)+\#_A(w)$ паран број, па то важи и за све завршне речи. Завршна реч w не може садржавати незавршна слова A, па је $\#_A(w) = 0$, одакле следи да је за сваку завршну реч w број $\#_a(w)$ паран. Лако се доказује да свака завршна реч изведена у граматици G мора да садржи бар једно слово a, па је $L(G) \subseteq \{w \mid w \in \{a, b\}^* \ \wedge \ \#_a(w) \text{ је паран број већи од } 0\}$.

$\supseteq$: *Свака реч $w \in \{a, b\}^*$, таква да је $\#_a(w)$ паран број већи од 0 може бити изведена у граматици G.*

Нека је w облика $b^{m_1}a^{n_1}b^{m_2}\dots b^{m_k}a^{n_k}b^{m_{k+1}}$ (при чему је $n_1 + n_2 + \cdots + n_k = n$ паран број већи од 0.

$$S \overset{1^\circ}{\Rightarrow} AA \overset{2^\circ, \frac{n}{2}-1}{\Rightarrow} A^n \overset{3^\circ, m_1}{\Rightarrow} b^{m_1}A^n \overset{5^\circ, n_1}{\Rightarrow} b^{m_1}a^{n_1}A^{n-n_1} \Rightarrow \dots$$

$$\Rightarrow b^{m_1}a^{n_1}b^{m_2}\dots b^{m_k}A^{n_k} \overset{5^\circ, n_k-1}{\Rightarrow} b^{m_1}a^{n_1}\dots a^{n_k-1}A \Rightarrow$$

$$\overset{4^\circ, m_{k+1}}{\Rightarrow} b^{m_1}a^{n_1}\dots a^{n_k-1}Ab^{m_{k+1}} \overset{5^\circ}{\Rightarrow} b^{m_1}a^{n_1}\dots b^{m_k}a^{n_k}b^{m_{k+1}}$$

Дакле, $L(G) \supseteq \{w \mid w \in \{a, b\}^* \ \wedge \ \#_a(w) \text{ је паран број већи од } 0\}$.

Задатак 9 *Одредити језик генерисан граматиком $G = (N, \Sigma, P, S)$, где је*
$N = \{S, B, C\}$,
$\Sigma = \{a, b, c\}$,
$P = \{S \to aSBC\ (1^\circ), S \to aBC\ (2^\circ), CB \to BC\ (3^\circ), aB \to ab\ (4^\circ), bB \to bb\ (5^\circ), bC \to bc\ (6^\circ), cC \to cc\ (7^\circ)\}$.

Решење:

Наведимо најпре, мотивације ради, два примера извођења у граматици G:

$$S \overset{2^\circ}{\Rightarrow} aBC \overset{4^\circ}{\Rightarrow} abC \overset{6^\circ}{\Rightarrow} abc$$

$$S \overset{1^\circ}{\Rightarrow} aSBC \overset{2^\circ}{\Rightarrow} aaBCBC \overset{3^\circ}{\Rightarrow} aaBBCC$$
$$\overset{4^\circ}{\Rightarrow} aabBCC \overset{5^\circ}{\Rightarrow} aabbCC \overset{6^\circ}{\Rightarrow} aabbcC \overset{7^\circ}{\Rightarrow} aabbcc$$

Докажимо да важи

$$L(G) = \{a^n b^n c^n \mid n \geq 1\}$$

$\subseteq$: *Свака завршна реч која се изводи у граматици G је облика $a^n b^n c^n$ ($n \geq 1$).*

Приметимо најпре да након примене корака 2° више не може бити примењивано ни правило 1° ни правило 2°. Такође, правила 4°, 5°, 6° и 7° не могу да се примењују док се не примени правило 2°.

Дакле, на почетку извођења, правило 1° се примењује k пута ($k \geq 0$), након тога једном се примени правило 2°, а затим се примењују правила 4°, 5°, 6° и 7°. Дакле, почетак сваког извођења има форму:

$$S \overset{1^\circ,k}{\Rightarrow} a^k S(BC)^k \overset{2^\circ}{\Rightarrow} a^{k+1}(BC)^{k+1},$$

где је $k \geq 0$. Индукцијом се може доказати да за сваку реч w која може бити изведена у граматици G важи $\#_a(w) = \#_b(w) + \#_B(w) = \#_c(w) + \#_C(w)$. У завршној речи w нема слова B и C (и S), па важи $\#_a(w) = \#_b(w) = \#_c(w)$.

Индукцијом се може доказати и да у сваком извођењу, у свакој речи сва завршна слова претходе свим незавршним словима.

На реч $a^{k+1}(BC)^{k+1}$ може се применити само правило 4°, па у сваком извођењу, након низа слова a може да се појави само слово b или слово B. У завршним речима, дакле, након низа слова a следи низ слова b.

Једино правило чија лева страна почиње словом c је правило 7°. То је уједно једино правило које елиминише незавршно слово C. Уколико је оно примењено на позицији таквој да десно од ње постоји бар једно слово B (слова a и b се сигурно не појављују, јер у сваком извођењу, у свакој речи сва завршна слова претходе свим незавршним словима) онда се долази до ситуације да на подреч cB не може да се примени ниједно правило. Дакле, у сваком извођењу које води до завршне речи, правило 7° се примењује само на позицијама таквим да десно од њих не постоји ниједно слово B, одакле следи да у свим изведеним завршним речима, сва слова b претходе свим словима c.

Дакле, у свакој завршној речи, број појављивања слова a једнак је броју појављивања слова b и c и сва слова a претходе свим словима b, а сви они претходе свим словима c, па важи $L(G) \subseteq \{a^n b^n c^n \mid n \geq 1\}$.

$\supseteq$: *Свака завршна реч облика $a^n b^n c^n$ $(n \geq 1)$ може се извести у граматици G.*

За произвољно n $(n \geq 1)$ реч $a^n b^n c^n$ може бити изведена у граматици G:

$S \overset{1^\circ,n-1}{\Rightarrow} a^{n-1}S(BC)^{n-1} \overset{2^\circ}{\Rightarrow} a^n(BC)^n \overset{3^\circ,(n-1)(n-2)/2}{\Rightarrow} a^nB^nC^n \overset{4^\circ}{\Rightarrow}$
$a^nbB^{n-1}C^n \overset{5^\circ,n-1}{\Rightarrow} a^nb^nC^n \overset{6^\circ}{\Rightarrow} a^nb^ncC^{n-1} \overset{7^\circ,n-1}{\Rightarrow} a^nb^nc^n$

Дакле, $L(G) \supseteq \{a^n b^n c^n \mid n \geq 1\}$.

Задатак 10 *Одредити језик генерисан граматиком $G = (N, \Sigma, P, S)$, где је*
$N = \{S, A, B, C, D\}$,
$\Sigma = \{a, b\}$,
$P = \{S \to CD\ (1^\circ), C \to aCA\ (2^\circ), C \to bCB\ (3^\circ), AD \to aD\ (4^\circ),$
$BD \to bD\ (5^\circ), Aa \to aA\ (6^\circ), Ab \to bA\ (7^\circ), Ba \to aB\ (8^\circ),$
$Bb \to bB\ (9^\circ), C \to e\ (10^\circ), D \to e\ (11^\circ)\}$.

Решење:

$$L(G) = \{ww \mid w \in \Sigma^*\}$$

Задатак 11 *Одредити граматику која генерише језик $W = \{a^ib^j \mid i \geq j > 0\}$.*

Решење:

Нека је $G = (N, \Sigma, P, S)$, где је
$N = \{S, A, B\}$,
$\Sigma = \{a, b\}$,
$P = \{S \to AB\ (1^\circ), A \to aA\ (2^\circ), A \to a\ (3^\circ), B \to ABb\ (4^\circ), B \to b\ (5^\circ)\}$.
Докажимо да $W = L(G)$.

$\subseteq$: *Ако $w \in W$, тј. $w = a^ib^j$, где је $i \geq j > 0$, онда се w може извести у граматици G.*

$S \overset{1^\circ}{\Rightarrow} AB \overset{4^\circ,j-1}{\Rightarrow} A^jBb^{j-1} \overset{5^\circ}{\Rightarrow} A^jb^j \overset{2^\circ,i-j}{\Rightarrow} a^{i-j}A^jb^j \overset{3^\circ,j}{\Rightarrow} a^ib^j$

Дакле, $W \subseteq L(G)$.

$\supseteq$: *Ако се реч без незавршних слова w може извести у граматици G, онда је $w = a^ib^j$, где је $i \geq j > 0$.*

Индукцијом по дужини извођења може се доказати да су у сваком извођењу у изведеној речи раздвојена слова a и A од слова b и

B. Прецизније, ако је w члан нетривијалног извођења, онда је он или облика $\alpha B\beta$ или облика $\alpha\beta$, где $\alpha \in \{A, a\}^*$ и $\beta \in \{b\}^*$. Отуда, у завршним речима свим словима b претходе сва слова a.

Индукцијом по дужини извођења може се доказати и да за сваку реч w у нетривијалном извођењу важи:

$$\#_a(w) + \#_A(w) \geq \#_b(w) + \#_B(w) > 0.$$

Формулишимо наведена тврђења као лему и докажимо је применом математичке индукције.

Лема 1.4 *Ако је w члан нетривијалног извођења, онда је он или облика $\alpha B\beta$ или облика $\alpha\beta$, где је $\alpha \in \{A, a\}^*$ и $\beta \in \{b\}^*$ и, притом, важи $\#_a(w) + \#_A(w) \geq \#_b(w) + \#_B(w) > 0$.*

За $k = 1$, извођење је $S \Rightarrow AB$, па тврђење очигледно важи.

Претпоставимо да тврђење важе за сва извођења дужине мање од k $(k > 1)$ и докажимо да оно важи и за извођења дужине k. Нека је $S \stackrel{k-1}{\Rightarrow} w' \Rightarrow w$ извођење дужине k. На основу индуктивне претпоставке, тврђење важи за реч w'. У k-том кораку је примењено једно од правила 2°-5°. Ако је примењено правило 2°, онда се у k-том кораку изводи $\alpha' B\beta \Rightarrow \alpha B\beta$, односно $\alpha'\beta \Rightarrow \alpha\beta$, где је $\alpha = \alpha' A$, $\alpha \in \{A, a\}^*$ и $\#_a(w) + \#_A(w) = \#_a(w') + \#_A(w') + 1 \geq \#_b(w') + \#_B(w') + 1 = \#_b(w) + \#_B(w) + 1 > \#_b(w) + \#_B(w)$. тврђење се слично доказује и у преостала три случаја.

Дакле, за све речи које су чланови извођења, па тако и завршне, важи наведено тврђење, па је свака завршна реч w облика $\alpha\beta$, где је $\alpha \in \{a\}^*$ и $\beta \in \{b\}^*$ и притом важи $\#_a(w) \geq \#_b(w) > 0$. Дакле, реч w је облика $a^i b^j$, где је $i = \#_a(w) \geq j = \#_b(w) > 0$, што је и требало доказати.

Дакле, $W \supseteq L(G)$.

Може се показати да дати језик може бити генерисан и формалном граматиком $G = (N, \Sigma, P, S)$, где је
$N = \{S, A\}$,
$\Sigma = \{a, b\}$,
$P = \{S \to aAb \ \ (1°), A \to aAb \ \ (2°), A \to aA \ \ (3°), A \to e \ \ (4°)\}$.

Задатак 12 *Одредити граматику која генерише језик $W = \{a^{2i}b^i \mid i > 0\}$.*

Решење:
Покажимо да граматика $G = (N, \Sigma, P, S)$, где је
$N = \{S\}$,

$\Sigma = \{a, b\}$,
$P = \{S \to aab\ \ (1°), S \to aaSb\ \ (2°)\}$
задовољава тражене услове, тј. $W = L(G)$.

- $\subseteq$: *Ако $w \in W$, тј. $w = a^{2i}b^i$, где је $i > 0$, онда се w може извести у граматици G.*

  $S \overset{2°, i-1}{\Rightarrow} (aa)^{i-1}Sb^{i-1} \overset{1°}{\Rightarrow} (aa)^i b^i$

  Дакле, $W \subseteq L(G)$.

- $\supseteq$: Индукцијом се може доказати да је сваки члан извођења w облика $a^{2i}Sb^i$ $(i \geq 0)$ или облика $a^{2i}b^i$ $(i > 0)$. Завршна реч w не може да садржи слово S, па је облика $a^{2i}b^i$ $(i > 0)$, одакле следи $W \supseteq L(G)$.

Може се показати да дати језик може бити генерисан и формалном граматиком $G = (N, \Sigma, P, S)$, где је
$N = \{S, A\}$,
$\Sigma = \{a, b\}$,
$P = \{S \to aaAb\ \ (1°), A \to aaAb\ \ (2°), A \to e\ \ (3°)\}$.

Задатак 13 *Одредити граматику која генерише све палиндроме над азбуком $\{a, b\}$.*

Решење:

Треба одредити граматику која генерише следећи језик:

$$W = \{w \in \Sigma^* \mid \hat{w} = w\}^3$$

Може се показати да граматика $G = (N, \Sigma, P, S)$, где је
$N = \{S\}$,
$\Sigma = \{a, b\}$,
$P = \{S \to e\ \ (1°), S \to a\ \ (2°), S \to b\ \ (3°), S \to aSa\ \ (4°), S \to bSb\ \ (5°)\}$
задовољава тражени услов.

Задатак 14 *Одредити граматику која генерише језик*
$W = \{a^n b^{[n/2]} \mid n \geq 0\}$.

Решење:

Може се показати да граматика $G = (N, \Sigma, P, S)$, где је
$N = \{S\}$,
$\Sigma = \{a, b\}$,
$P = \{S \to aaSb\ \ (1°), S \to a\ \ (2°), S \to e\ \ (3°)\}$
задовољава тражени услов.

[3] Са $\hat{w}$ је означена реч w записана здесна налево.

1.2.2 Регуларни скупови (регуларни језици)

Дефиниција 1.12 *Нека је* Σ *коначна азбука.* Регуларан скуп (регуларан језик) *над* Σ *дефинише се рекурзивно на следећи начин:*

(*i*) *Празан скуп,* $\emptyset$, *је регуларан.*

(*ii*) *Скуп* $\{e\}$ *је регуларан.*

(*iii*) *Скуп* $\{a\}$ *је регуларан за свако слово* $a \in \Sigma$.

(*iv*) *Ако су скупови* P *и* Q *регуларни, онда су регуларни и следећи скупови:* $P \cup Q$, PQ *и* P^*.

(*v*) *Регуларни скупови над* Σ *су само они који се могу добити коначном применом правила* (*i*)-(*iv*).

Када се говори о регуларним скуповима, често се знак $\cup$ замењује знаком $+$. Нпр: $P^* = \{e\} + P + P^2 + P^3 + \dots$

Теорема 1.3 *Језик над коначном азбуком је регуларан ако и само ако је десно линеаран.*

1.3 Леме о разрастању

1.3.1 Лема о разрастању за регуларне језике

Теорема 1.4 *Нека је* L *регуларан језик. Тада постоји константа* p ($p \in \mathbf{N}^+$) *таква да се свака реч* z ($z \in L$), *за коју је* $|z| \geq p$, *може записати у облику* uvw, *при чему је* $0 < |v| \leq p$ *и све речи* uv^kw ($k = 0, 1, 2, \dots$) *припадају језику* L.[4]

Наведено тврђење даје потребан услов да језик буде регуларан. Оно се најчешће и примењује управо да се би се показало да неки језик *није* регуларан.

Задатак 15 *Доказати да језик* $L = \{a^nb^n \mid n \in \mathbf{N}\}$ *није регуларан.*

Решење:

Нека је z произвољна непразна реч језика L. Покушајмо да изаберемо подреч v ($v \neq e$) из леме о разрастању (теорема 1.4). То можемо да урадимо само на неки од следећих начина:

1°

$$z = \underbrace{a\dots a}_{u}\underbrace{a\dots a}_{v}\underbrace{a\dots ab\dots b}_{w}$$

Тада $uv^0w \notin L$, јер је $\#_a(uv^0w) < \#_b(uv^0w)$, а за све речи z из L важи $\#_a(z) = \#_b(z)$.

[4] У литератури на енглеском језику лема о разрастању назива се *pumping lemma*. Доказ леме се може наћи у [8, 3].

2°

$$z = \underbrace{a\ldots ab\ldots b}_{u}\underbrace{b\ldots b}_{v}\underbrace{b\ldots b}_{w}$$

Тада $uv^0w \notin L$, јер је $\#_a(uv^0w) > \#_b(uv^0w)$, а за све речи z из L важи $\#_a(z) = \#_b(z)$.

3°

$$z = \underbrace{a\ldots a}_{u}\underbrace{a\ldots ab\ldots b}_{v}\underbrace{b\ldots b}_{w}$$

Тада $uv^2w \notin L$, јер распоред слова a и b не одговара оном код речи језика L.

Очигледно се подреч v, без обзира на дужину речи z, не може изабрати тако да $uv^kw \in L$ за све природне бројеве k. Дакле, није задовољен потребан услов да би језик био регуларан (услов из леме о разрастању (теорема 1.4)), па језик L није регуларан.

Задатак 16 *Доказати да језик* $L = \{a^nba^mba^{n+m} \quad | \quad n, m \in \mathbf{N}\}$ *није регуларан.*

Решење:
Претпоставимо супротно — да језик L јесте регуларан. Нека је p константа из леме о разрастању (теорема 1.4) и нека је $z = a^nba^mba^{n+m}$, при чему је $|z| \geq p$. Важи $z \in L$, па се, на основу леме о разрастању (теорема 1.4), реч z може представити у облику uvw, где $0 < |v| \leq p$, тако да $uv^kw \in L$ за све природне бројеве k. Показаћемо да то не важи. Подреч v можемо да изаберемо само на неки од следећих начина:

1° $\#_b(v) = 0$

$$\overbrace{\underbrace{a\ldots a}_{u}\underbrace{a\ldots a}_{v}a}^{n}b\overbrace{a\ldots a}^{m}b\overbrace{a\ldots a}^{n+m}$$

$$\overbrace{a\ldots a}^{n}b\overbrace{a\ldots a\underbrace{a\ldots a}_{v}a\ldots a}^{m}b\overbrace{a\ldots a}^{n+m}$$

$$\overbrace{a\ldots a}^{n}b\overbrace{a\ldots a}^{m}b\overbrace{a\ldots a\underbrace{a\ldots a}_{v}a\ldots a}^{n+m}$$

У сва три случаја $uv^0w \notin L$, јер број слова a у прве две секвенце речи uw не одговара броју слова a у трећој секвенци.

2° $\#_b(v) \geq 1$

Тада је $\#_b(uv^0w) < 2$, па $uv^0w \notin L$, јер за све речи z из L важи $\#_b(z) = 2$.

Дакле, реч z се не може приказати у облику uvw тако да uv^0w, тј. uw припада језику L, што противречи тврђењу леме о разрастању (теорема 1.4). Дакле, језик L није регуларан.

Задатак 17 *Доказати да језик* $L = \{a^nba^n \mid n \geq 1\}$ *није регуларан.*

Решење:

Слично претходним задацима разликујемо следеће случајеве:

1° $\#_b(v) = 0$

$$\overbrace{\underbrace{a\ldots a}_{u}\underbrace{a\ldots a}_{v}a\ldots a}^{n}b\overbrace{a\ldots a}^{m}$$

$$\overbrace{a\ldots a}^{n}b\overbrace{a\ldots a\underbrace{a\ldots a}_{v}a\ldots a}^{m}$$

У оба случаја $uv^0w \notin L$, због различитог броја слова a у првој и другој секвенци речи uw.

2° $\#_b(v) = 1$

Тада $\#_b(uv^0w) = 0$, па $uv^0w \notin L$, јер за све речи z из L важи $\#_b(z) = 1$.

Задатак 18 *Доказати да језик* $L = \{ww \mid w \in \{a,b\}^*\}$ *није регуларан.*

Решење:

Претпоставимо супротно — да језик L јесте регуларан. Нека је p константа из леме о разрастању (теорема 1.4) и нека је n природан број такав да је $n \geq p$. Нека је $z = a^nb^na^nb^n$. Важи да $z \in L$ и $|z| = 4n > p$. Тада се, на основу леме о разрастању (теорема 1.4), реч z може представити у облику uvw, где $0 < |v| \leq p$, тако да $uv^kw \in L$ за све природне бројеве k. Показаћемо да то не важи. Подреч v можемо да изаберемо само на неки од следећих начина за $i > 0$ и $j > 0$ (јер је $p \leq n$):

1° $v = a^i$

Разликујемо следећа два подслучаја:

(1)

$$a \dots a \overbrace{\underbrace{a \dots a}_{v}}^{i} a \dots a b^n a^n b^n$$

Тада $uv^0w = a^{n-i}b^na^nb^n \notin L$.

(2)

$$a^n b^n a \dots a \overbrace{\underbrace{a \dots a}_{v}}^{i} a \dots a b^n$$

Тада $uv^0w = a^nb^na^{n-i}b^n \notin L$.

2° $v = b^i$

Слично претходном делу, $uv^0w \notin L$ (тј. $a^nb^{n-i}a^nb^n \notin L$, односно $a^nb^na^nb^{n-i} \notin L$).

3° $v = a^ib^j$

Слично претходном делу, $uv^0w \notin L$ (тј. $a^{n-i}b^{n-j}a^nb^n \notin L$, односно $a^nb^na^{n-i}b^{n-j} \notin L$).

4° $v = b^ia^j$

Тада $uv^2w = a^nb^na^jb^ia^nb^n \notin L$.

Дакле, не може се изабрати подреч v тако да $uv^kw \in L$ за било који природан број k, а то противречи тврђењу леме о разрастању (теорема 1.4), па језик L није регуларан.

Задатак 19 *Доказати да језик* $L = \{a^ib^j \mid \text{NZD}(i,j) > 1\}$ *није регуларан.*

Решење:

Претпоставимо супротно — да језик L јесте регуларан. Тада, на основу леме о разрастању за регуларне језике (теорема 1.4), постоји константа p ($p \in \mathbf{N}^+$) таква да се свака реч z из L дужине $\geq p$ може представити у облику uvw и при томе важи $0 < |v| \leq p$ и $uv^kw \in L$ за $k = 0, 1, 2, \dots$. Нека је i прост број и $i > p$. Нека је $z = a^ib^i$. Тада је $\text{NZD}(i,i) = i > 1$ (јер је i прост), па $z \in L$. Важи и $|z| = 2i \geq p$. Подреч v речи z ($0 < |v| \leq p$) можемо изабрати само на неки од следећа три начина:

1° $v = a^mb^n$, $m > 0$, $n > 0$, $m + n \leq p$

Тада $a^{i-m}(a^mb^n)^kb^{i-m} \notin L$ за $k > 1$.

2° $v = a^m$, $0 < m \leq p$

Докажимо да тада реч $a^{i-m}(a^m)^0b^i (= a^{i-m}b^i)$ не припада језику L. Претпоставимо супротно — да $a^{i-m}b^i \in L$. Онда је, на основу дефиниције језика L, $\text{NZD}(i-m, i) > 1$. Како је $0 < i - m < i$, то је $\text{NZD}(i-m,i) < i$. Дакле, имамо да $\text{NZD}(i-m,i)|i$ и $1 < \text{NZD}(i-m,i) < i$, а то противречи чињеници да је i прост број. Стога, $a^{i-m}b^i \notin L$.

3° $v = b^m$, $0 < m \leq p$

Слично као у случају 2° показује се да $a^i b^{i-m} \notin L$.

Дакле, $z \in L$ и $|z| \geq p$, а z се не може записати у облику uvw тако да $uv^kw \in L$ за све природне бројеве k, што противречи тврђењу леме о разрастању (теорема 1.4), па језик L није регуларан.

Задатак 20 *Нека је* $f : \mathbf{N} \longrightarrow \mathbf{N}$ *монотона растућа функција таква да за сваки* n *постоји* m *такав да је* $f(m+1) - f(m) \geq n$. *Доказати да језик*

$$L = \{a^{f(m)} \mid m \geq 1\}$$

није регуларан.

Решење:

Означимо дате претпоставке на следећи начин:

(1) $f \nearrow$

(2) $(\forall n \in \mathbf{N})(\exists m \in \mathbf{N})\ f(m+1) - f(m) \geq n$

Претпоставимо супротно — да скуп L јесте регуларан. Тада, на основу леме о разрастању (теорема 1.4), постоји константа p ($p \in \mathbf{N}^+$) таква да се свака реч z из L дужине $\geq p$, може представити у облику uvw тако да $0 < |v| \leq p$ и $uv^kw \in L$ за сваки $k = 0, 1, 2, \ldots$. То значи да за неко p ($p \in \mathbf{N}^+$) важи следећа импликација:

$$f(m) \geq p \Rightarrow (\exists q \in \mathbf{N})(0 < q \leq p \ \ \wedge \ \ (\forall k \in \mathbf{N})\ a^{f(m)-q}(a^q)^k \in L)$$

Како $a^{f(m)-q}(a^q)^k \in L$ акко $f(m) - q + qk = f(n_k)$ за неко n_k, то важи следећа импликација:

$$\begin{aligned} &f(m) \geq p \\ \Rightarrow &(\exists q \in \mathbf{N})(0 < q \leq p \ \ \wedge \ \ (\forall k \in \mathbf{N})(\exists n_k \in \mathbf{N}) f(m) + (k-1)q = f(n_k)) \end{aligned}$$

Дефинишимо скуп M на следећи начин:

$$M = \{l \mid f(l+1) - f(l) \geq p\}$$

Очигледно важи да $M \subseteq \mathbf{N}$ и $M \neq \emptyset$ (због (2)), па, како је $\mathbf{N}$ добро уређен скуп, постоји $min\, M$. Нека је $m = min\, M$. Како $m \in M$, то важи $f(m+1) \geq f(m) + p$. Одатле следи да $f(m+1) \geq p$ (јер је $f(m) \geq 0$), одакле, на основу претходне импликације), изводимо следеће тврђење:

$$(\exists q \in \mathbf{N})(0 < q \leq p \ \ \wedge \ \ (\forall k \in \mathbf{N})(\exists n_k \in \mathbf{N}) f(m+1) + (k-1)q = f(n_k))$$

Нека је q природан број који задовољава следећи услов:

$$0 < q \leq p \quad \wedge \quad (\forall k \in \mathbf{N})(\exists n_k \in \mathbf{N}) f(m+1) + (k-1)q = f(n_k) \tag{3}$$

Тада за $k = 0$ имамо да $f(m+1) + (0-1)q = f(n_0)$ за неко $n_0 \in \mathbf{N}$, тј.

$$f(m+1) = f(n_0) + q \tag{4}$$

Докажимо да $f(m) \leq f(n_0) < f(m+1)$:

$$\begin{aligned} & f(m+1) = f(n_0) + q \quad \wedge \quad f(m+1) \geq f(m) + p \\ \Rightarrow\ & f(n_0) + q \geq f(m) + p \\ \Rightarrow\ & f(n_0) \geq f(m) + (p - q) \\ \Rightarrow\ & f(n_0) \geq f(m) \qquad (\text{јер је на основу (3) } q \leq p) \end{aligned}$$

$$\begin{aligned} & f(m+1) = f(n_0) + q \\ \Rightarrow\ & f(m+1) > f(n_0) \qquad (\text{јер је на основу (3) } q > 0) \end{aligned}$$

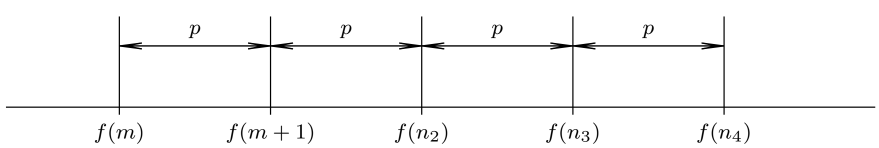
Дакле, $f(m) \leq f(n_0) < f(m+1)$, одакле је, због (1), $f(n_0) = f(m)$. Заменом ове једнакости у (4) добијамо да $f(m+1) = f(m) + q$. Даље,

$$\begin{aligned} & f(m+1) = f(m) + q \quad \wedge \quad f(m+1) \geq f(m) + p \\ \Rightarrow\ & f(m) + q \geq f(m) + p \\ \Rightarrow\ & q \geq p \\ \Rightarrow\ & q = p \qquad (\text{јер је на основу (3) } q \leq p) \end{aligned}$$

Одатле, $f(m+1) = f(m) + p$. Штавише, заменом q са p у (3), добијамо:

$$(\forall k \in \mathbf{N})(\exists n_k \in \mathbf{N}) f(m+1) = f(n_k) + (k-1)p \tag{5}$$

Због (1) важи $n_0 < n_1 < n_2 < n_3 < n_4 < \ldots$, $n_0 = m$ и $n_1 = m+1$. Однос вредности функције f у овим тачкама је приказан на следећој слици:



Сада је јасније зашто, на основу (1) и (5), мора важити и:

$$(\forall l \geq m) f(l+1) - f(l) \leq p \tag{6}$$

С друге стране, због начина избора m важи и:

$$(\forall l < m) f(l+1) - f(l) < p \tag{7}$$

Из (6) и (7) следи:

$$(\forall l \in \mathbf{N}) f(l+1) - f(l) \leq p \tag{8}$$

Нека је $n > p$. Тада, због (8):

$$(\forall l \in \mathbf{N}) f(l+1) - f(l) < n,$$

што је противречи претпоставци (2). Дакле, скуп L није регуларан.

Задатак 21 *Доказати да језик генерисан граматиком*

$$G = (\{S\}, \{a, b, c\}, \{S \longrightarrow aSbS \mid c\}, S)$$

није регуларан.

Задатак 22 *Одредити класу $\mathcal{P}$ полинома са коефицијентима из скупа* $\mathbf{N}$ *такву да важи:*

$$(P \in \mathcal{P}) \Leftrightarrow \text{језик } \{a^n b^{P(n)} \mid n \geq 1\} \text{ је регуларан}$$

Упутство:

Применом леме о разрастању (теорема 1.4) може се доказати да ниједан полином степена већег од нула не припада класи $\mathcal{P}$. С друге стране, може се доказати да десно линеарна граматика $G = (N, \Sigma, P, S)$, где је
$N = \{S\}$,
$\Sigma = \{a, b\}$,
$P = \{S \to aS \ (1^\circ), S \to ab^p \ (2^\circ)\}$
генерише језик $\{a^n b^p \mid n \geq 1\}$, где је p дат природан број.

Из претходна два тврђења следи да је тражена класа полинома класа константних полинома, тј. $\mathcal{P} = \{p \mid p \in \mathbf{N}\}$.

1.3.2 Лема о разрастању за контекстно слободне језике

Теорема 1.5 *Нека је L контекстно слободан језик. Тада постоје константе p и q ($p, q \in \mathbf{N}^+$) такве да се свака реч z језика L, за коју је $|z| > p$, може записати у облику $uvwxy$, при чему је $vx \neq e$ (v или x није празна реч), $|vwx| \leq q$ и све речи uv^kwx^ky ($k = 0, 1, 2\dots$) припадају језику L.*[5]

Наведено тврђење даје потребан услов да језик буде контекстно слободан, те се најчешће користи да се покаже да дати језик *није* контекстно слободан, тј. да не постоји контекстно слободна граматика која га генерише.

[5] У литератури на енглеском језику лема о разрастању назива се *pumping lemma*. Доказ леме се може наћи у [8, 3, 1].

Задатак 23 *Доказати да језик* $L = \{a^n b^n c^n \mid n \geq 1\}$ *није контекстно слободан.*

Решење:

Претпоставимо супротно — да језик L јесте контекстно слободан. Нека су p и q одговарајуће константе из леме о разрастању (теорема 1.5) и нека је $n > p, q$. Нека је $z = a^n b^n c^n$, где је $n \geq 1$. Онда $z \in L$ и $|z| = 3n > 3p > p$. Тада се реч z, на основу леме о разрастању (теорема 1.5), може записати у облику $uvwxy$, где $vx \neq e$, $|vwx| \leq q$ и све речи $uv^k wx^k y$ $(k = 0, 1, 2, \dots)$ припадају језику L. Подреч vwx речи z може се изабрати само на неки од следећих начина (јер је $n > q$):

1°

$$\overbrace{a\dots a\underbrace{a\dots a}_{vwx}a\dots a}^{n}\overbrace{b\dots b}^{n}\overbrace{c\dots c}^{n}$$

Тада је $\#_a(uv^0wx^0y) < \#_b(uv^0wx^0y)$, па $uv^0wx^0y \notin L$.

2°

$$\overbrace{a\dots a}^{n}\overbrace{b\dots b\underbrace{b\dots b}_{vwx}b\dots b}^{n}\overbrace{c\dots c}^{n}$$

Слично као у случају 1° показује се да $uv^0wx^0y \notin L$.

3°

$$\overbrace{a\dots a}^{n}\overbrace{b\dots b}^{n}\overbrace{c\dots c\underbrace{c\dots c}_{vwx}c\dots c}^{n}$$

Слично као у случају 1° показује се да $uv^0wx^0y \notin L$.

4°

$$a\dots a\underbrace{a\dots ab\dots b}_{vwx}b\dots bc\dots c$$

Тада је $\#_a(uv^0wx^0y) < \#_c(uv^0wx^0y)$ (и $\#_b(uv^0wx^0y) < \#_c(uv^0wx^0y)$), па $uv^0wx^0y \notin L$.

5°

$$a\dots ab\dots b\underbrace{b\dots bc\dots c}_{vwx}c\dots c$$

Слично као у случају 4° показује се да $uv^0wx^0y \notin L$.

Напомена: Случај $vwx = a^i b^n c^j$ $(i, j > 0)$ нисмо разматрали, јер би онда важило $|vwx| > n > q$.

Дакле, $z \in L$ и $|z| > p$, а z се не може записати у облику $uvwxy$, где $vx \neq e$, $|vwx| \leq q$, тако да све речи $uv^k wx^k y$ $(k = 0, 1, 2, \dots)$ припадају језику L. Ово противречи тврђењу леме о разрастању (теорема 1.5), па језик L није контекстно слободан.

Задатак 24 *Доказати да језик* $L = \{a^n b^m c^n d^m \mid n \geq 1, \quad m \geq 1\}$ *није контекстно слободан.*

Решење:

Претпоставимо супротно — да језик L јесте контекстно слободан. Нека су p, q одговарајуће константе из леме о разрастању (теорема 1.5) и нека је $n, m > p, q$. Нека је $z = a^n b^m c^n d^m$. Онда $z \in L$ и $|z| = 2(n+m) > 2(p+p) = 4p > p$. Тада се реч z, на основу леме о разрастању (теорема 1.5), може записати у облику $uvwxy$, где $vx \neq e$, $|vwx| \leq q$ и све речи $uv^k wx^k y$ $(k = 0, 1, 2, \ldots)$ припадају језику L. Подреч vwx речи z се може изабрати само на неки од следећих начина:

1° Подреч vwx се састоји само од једне врсте слова.

$$\overbrace{a\underbrace{\ldots}_{(1)}a}^{n}\overbrace{b\underbrace{\ldots}_{(2)}b}^{m}\overbrace{c\underbrace{\ldots}_{(3)}c}^{n}\overbrace{d\underbrace{\ldots}_{(4)}d}^{m}$$

2° Подреч vwx се састоји од тачно две врсте слова.

$$a\ldots\underbrace{ab}_{(1)}\ldots\underbrace{bc}_{(2)}\ldots\underbrace{cd}_{(3)}\ldots d$$

Напомена: Није могуће да реч vwx има више од две врсте слова, јер $|vwx| \leq q$ и $n, m > q$.

Утврдићемо да у сваком од ових случајева $uv^2wx^2y \notin L$. Приметимо да у сваком од седам могућих случајева у речи uv^2wx^2y бар један од блокова a^n, c^n остаје непромењен, а исто важи и за блокове b^m, d^m. То значи да је бар један од бројева $\#_a(uv^2wx^2y)$, $\#_c(uv^2wx^2y)$ једнак броју n, и да је бар један од бројева $\#_b(uv^2wx^2y)$, $\#_d(uv^2wx^2y)$ једнак броју m. На основу леме о разрастању (теорема 1.5) $uv^2wx^2y \in L$, а то значи да

$$\#_a(uv^2wx^2y) = \#_c(uv^2wx^2y) = n \text{ и } \#_b(uv^2wx^2y) = \#_d(uv^2wx^2y) = m.$$

Одатле је $|uv^2wx^2y| = n + m + n + m = |z|$. С друге стране је

$$|uv^2wx^2y| = |uvwxy| + |vx| = |z| + |vx|.$$

Како је $|vx| > 0$, то је $|uv^2wx^2y| > |z|$. Дакле, $z \in L$ и $|z| > p$, а z се не може записати у облику $uvwxy$, где $vx \neq e$, $|vwx| \leq q$, тако да све речи uv^kwx^ky $(k = 0, 1, 2, \ldots)$ припадају језику L. Ово противречи тврђењу леме о разрастању (теорема 1.5), па језик L није контекстно слободан.

Задатак 25 *Доказати да језик* $L = \{a^n \mid n \text{ је прост број } \}$ *није контекстно слободан.*

Решење:

Претпоставимо супротно — да језик L јесте контекстно слободан. Нека су p, q одговарајуће константе из леме о разрастању и нека је n прост број такав да $n > p, q+1$. Нека је $z = a^n$. Онда $z \in L$ и $|z| = n > p$. Тада се реч z, на основу леме о разрастању (теорема 1.5), може записати у облику $uvwxy$, где $vx \neq e$, $|vwx| \leq q$ и све речи uv^kwx^ky $(k = 0, 1, 2, \dots)$ припадају језику L. Дакле, реч z декомпонујемо на следећи начин:

$$z = a^n = \underbrace{a^{n_1}}_{u}\underbrace{a^{n_2}}_{v}\underbrace{a^{n_3}}_{w}\underbrace{a^{n_4}}_{x}\underbrace{a^{n_5}}_{y},$$

где је

$$n_1 + n_2 + n_3 + n_4 + n_5 = n \tag{1.1}$$

$$n_2 + n_4 > 0 \tag{1.2}$$

$$n_2 + n_3 + n_4 \leq q$$

На основу леме о разрастању (теорема 1.5), важи

$$uv^{n+1}wx^{n+1}y \in L,$$

тј.

$$a^{n_1}a^{n_2(n+1)}a^{n_3}a^{n_4(n+1)}a^{n_5} \in L$$

То значи да је дужина ове речи, тј. број $n_1+n_2(n+1)+n_3+n_4(n+1)+n_5$, прост број. Како је

$$\begin{aligned}
& n_1 + n_2(n+1) + n_3 + n_4(n+1) + n_5 \\
= & (n_1 + n_2 + n_3 + n_4 + n_5) + n(n_2 + n_4) \\
= & n + n(n_2 + n_4) \\
& \text{(на основу једнакости 1.1)} \\
= & n(n_2 + n_4 + 1),
\end{aligned}$$

то значи да је $n(n_2 + n_4 + 1)$ прост број. Како је, на основу неједнакости 1.2, $n_2 + n_4 + 1 > 1$, а број n изабран тако да је $n > q + 1$, па сходно томе и $n > 1$, то значи да је $n(n_2 + n_4 + 1)$ сложен број, а то противречи претходном закључку да је посматрани број прост.

Дакле, језик L није контекстно слободан.

Задатак 26 *Доказати да језик* $L = \{a^{n^2} \mid n \geq 1\}$ *није контекстно слободан.*

Решење:

Претпоставимо супротно — да језик L јесте контекстно слободан. Нека су p, q одговарајуће константе из леме о разрастању (теорема 1.5) и нека је $n > p, q$. Нека је $z = a^{n^2}$. Онда $z \in L$ и $|z| = n^2 \geq n > p$. Реч z се, на основу леме о разрастању (теорема 1.5), може записати у облику $uvwxy$, где $vx \neq e$, $|vwx| \leq q$ и све речи uv^kwx^ky $(k = 0, 1, 2, \dots)$ припадају језику L. Како је $|vx| > 0$, имамо да

$$|uv^2wx^2y| = |uvwxy| + |vx| = |z| + |vx| > |z| = n^2$$

С друге стране, како је $vwx \leq q < n$, имамо да

$$\begin{aligned} |uv^2wx^2y| &\leq |uvwxy| + |vwx| = |z| + |vwx| \\ &\leq n^2 + q < n^2 + n < n^2 + 2n + 1 = (n+1)^2 \end{aligned}$$

Дакле, $n^2 < |uv^2wx^2y| < (n+1)^2$, па $uv^2wx^2y \notin L$, а то противречи тврђењу леме о разрастању (теорема 1.5). Према томе, језик L није контекстно слободан.

Задатак 27 *Доказати да језик* $L = \{a^{2^n} \mid n \geq 1\}$ *није контекстно слободан.*

Решење:

Претпоставимо супротно — да језик L јесте контекстно слободан. Нека су p, q одговарајуће константе из леме о разрастању (теорема 1.5) и нека је n такав да $2^n > p, q$. Нека је $z = a^{2^n}$. Онда $z \in L$ и $|z| = 2^n > p$. Реч z се, на основу леме о разрастању (теорема 1.5), може записати у облику $uvwxy$, где $vx \neq e$, $|vwx| \leq q$ и све речи uv^kwx^ky $(k = 0, 1, 2, \dots)$ припадају језику L. Дакле, реч z декомпонујемо на следећи начин:

$$z = a^{2^n} = \underbrace{a^{n_1}}_{u}\underbrace{a^{n_2}}_{v}\underbrace{a^{n_3}}_{w}\underbrace{a^{n_4}}_{x}\underbrace{a^{n_5}}_{y},$$

где је

$$n_1 + n_2 + n_3 + n_4 + n_5 = 2^n \tag{1.3}$$
$$n_2 + n_4 > 0$$
$$n_2 + n_3 + n_4 \leq q \tag{1.4}$$

На основу леме о разрастању (теорема 1.5), важи

$$uv^2wx^2y \in L,$$

тј.

$$a^{n_1}a^{2n_2}a^{n_3}a^{2n_4}a^{n_5} \in L,$$

То значи да је

$$\begin{aligned}
& n_1 + 2n_2 + n_3 + 2n_4 + n_5 \\
= {} & (n_1 + n_2 + n_3 + n_4 + n_5) + (n_2 + n_4) \\
= {} & 2^n + (n_2 + n_4) \\
& \text{(на основу једнакости 1.3)} \\
\leq {} & 2^n + q \\
& \text{(на основу неједнакости 1.4)} \\
\leq {} & 2^n + 2^n \\
= {} & 2^{n+1}
\end{aligned}$$

Дакле, за реч uv^2wx^2y важи $2^n < uv^2wx^2y < 2^{n+1}$, што противречи претпоставци да та реч uv^2wx^2y припада језику L. Према томе, језик L није контекстно слободан.

Задатак 28 *Одредити класу $\mathcal{P}$ полинома са коефицијентима из скупа* $\mathbf{N}$ *такву да важи:*

$$(P \in \mathcal{P}) \;\Leftrightarrow\; \textit{језик } \{a^n b^{P(n)} \mid n \geq 1\} \textit{ је контекстно слободан}$$

Упутство:

Применом леме о разрастању (теорема 1.5) може се доказати да ниједан полином степена већег од један не припада класи $\mathcal{P}$. С друге стране, може се доказати да контекстно слободна граматика $G = (N, \Sigma, P, S)$, где је
$N = \{S\}$,
$\Sigma = \{a, b\}$,
$P = \{S \to aSb^q \;\; (1^\circ), S \to b^p \;\; (2^\circ)\}$
генерише језик $\{a^n b^{p+qn} \mid n \geq 1\}$, где су p и q дати природни бројеви.

Из претходна два тврђења следи да је тражена класа полинома класа линеарних полинома, тј.

$$\mathcal{P} = \{p + qn \mid p, q \in \mathbf{N}\}$$

Део 2

Аутомати

Аутомате су апстрактне машине чији улаз представља нека реч. Ову реч аутомат обрађује у дискретним временским тренуцима, и у сваком од њих аутомат се налази у неком стању. У зависности од стања аутомата, реч са улаза може бити прихваћена или одбачена. Стога аутомате често називамо прихватачким системима, за разлику од формалних граматика, које називамо генераторским системима. Између ова два формализма, ипак, постоји тесна веза. Наиме, за оба је везан појам језика, с тим што аутомат препознаје (прихвата, допушта) речи неког језика, док се формалном граматиком те речи генеришу. Прецизна веза између одређених врста аутомата и формалних граматика биће исказана одговарајућим теоремама.

2.1 Коначни аутомати

Дефиниција 2.1 Коначан аутомат *је уређена петорка*

$$M = (Q, \Sigma, \delta, q_0, F),$$

где је Q непразан (коначан) скуп стања, Σ улазна азбука, $\delta : Q \times \Sigma \to \mathcal{P}(Q)$ функција прелаская, q_0 *($q_0 \in Q$)* почетно стање *и F ($F \subseteq Q$)* скуп завршних стања.

Уређени пар (q, w) ($(q, w) \in Q \times \Sigma^*$) називамо конфигурацијом *коначног аутомата, при чему q представља стање у коме се аутомат налази, а w део речи са улаза који још није прочитан. Конфигурацију (q_0, w) називамо* почетном, *а (q, e), где $q \in F$,* завршном конфигурацијом.

Дефиниција 2.2 Релацију преласка *за коначни аутомат*

$$M = (Q, \Sigma, \delta, q_0, F),$$

у ознаци $\vdash_M$, дефинишемо на следећи начин:

$$(q, aw) \vdash_M (q', w) \quad \textit{ако и само ако} \quad q' \in \delta(q, a),$$

при чему $q, q' \in Q$, $a \in \Sigma$ *и* $w \in \Sigma^*$. *Везу* $(q, aw) \vdash_M (q', w)$ *читамо:* коначни аутомат M може да пређе из конфигурације (q, aw) у конфигурацију (q', w) читајући слово a.

Дефиниција 2.3 *Ако важи* $(q, w) \vdash_M (q_1, w_1)$, $(q_1, w_1) \vdash_M (q_2, w_2)$, $\ldots$, $(q_{k-1}, w_{k-1}) \vdash_M (q_k, w_k)$, *онда пишемо краће* $(q, w) \vdash_M^k (q_k, w_k)$, *и кажемо да* коначан аутомат M прелази из конфигурације (q, w) у конфигурацију (q_k, w_k) у k корака.

Дефиниција 2.4 *Транзитивно затворење релације* $\vdash_M$ *означавамо са* $\vdash_M^+$, *а транзитивно и рефлексивно са* $\vdash_M^*$.

Дефиниција 2.5 Језик допуштен коначним аутоматом

$$M = (Q, \Sigma, \delta, q_0, F),$$

у ознаци $L(M)$, *дефинишемо на следећи начин:*

$$L(M) = \{w \mid w \in \Sigma^* \ \wedge \ (\exists q \in F)\ (q_0, w) \vdash_M^* (q, e)\}$$

Теорема 2.1 *Језик је допуштен неким коначним аутоматом ако и само ако је регуларан.*[1]

Како је језик регуларан ако и само ако је он десно линеаран (видети теорему 1.3), јасна је веза између коначних аутомата и десно линеарних граматика. Аналогно тврђење важи и за лево линеарне граматике.

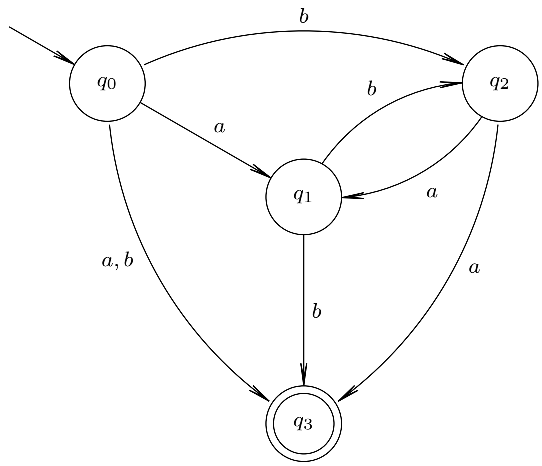
Задатак 29 *Одредити језик допуштен коначним аутоматом*
$M = (Q, \Sigma, \delta, q_0, F)$, *где је*
$Q = \{q_0, q_1, q_2, q_3\}$,
$\Sigma = \{a, b\}$,
$F = \{q_3\}$,
а функција преласка задата следећом таблицом:

	a	b
q_0	$\{q_1, q_3\}$	$\{q_2, q_3\}$
q_1		$\{q_2, q_3\}$
q_2	$\{q_1, q_3\}$	
q_3		

Решење:

Дати коначни аутомат можемо графички представити на следећи начин:

[1] Доказ теореме се може наћи у [8, 1, 3].



Наведимо сада један пример препознавања речи помоћу датог коначног аутомата:

$$(q_0, baba) \vdash_M (q_2, aba) \vdash_M (q_1, ba) \vdash_M (q_2, a) \vdash_M (q_3, e)$$

Докажимо да језик допуштен коначним аутоматом M чине све наизменичне речи (над азбуком Σ), тј. све непразне речи код којих се слова a и b наизменично појављују.

$\supseteq$: *Све наизменичне речи над Σ су допуштене коначним аутоматом M.*

Докажимо ово тврђење индукцијом по дужини наизменичне речи, k:

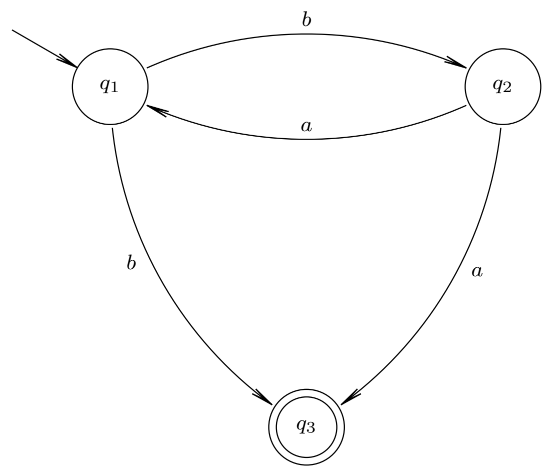
За $k = 1$, одговарајућа наизменична реч је a, односно b. Обе речи су допуштене коначним аутоматом M, јер важи $(q_0, a) \vdash_M (q_3, e)$ и $(q_0, b) \vdash_M (q_3, e)$.

Даље, претпоставимо да су све наизменичне речи дужине k допуштене коначним аутоматом M, и докажимо да исто тврђење важи и за све наизменичне речи дужине $k + 1$. Нека је w наизменична реч дужине $k+1$. Тада је $w = aw'$, где је w' наизменична реч дужине k која почиње словом b, односно $w = bw'$, где је w' наизменична реч дужине k која почиње словом a. Доказаћемо тврђење само за први случај. У другом случају доказ се изводи аналогно.

Дакле, нека је $w = aw'$, где је w' наизменична реч дужине k која почиње словом b. Тада важи $(q_0, aw') \vdash_M (q_1, w')$. Докажимо да важи $(q_1, w') \vdash^*_{M_1} (q_3, e)$, где је $M_1 = (Q_1, \Sigma, \delta_1, q_1, F)$ подаутомат коначног аутомата M за који је $M_1 = (Q_1, \Sigma, \delta_1, q_1, F)$, $Q_1 = \{q_1, q_2, q_3\}$, а функција преласка задата следећом таблицом:

	a	b
q_1		$\{q_2, q_3\}$
q_2	$\{q_1, q_3\}$	
q_3		

Овај коначни аутомат можемо графички представити на следећи начин:



Докажимо следеће тврђење:

Лема 2.1 *Коначни аутомат M_1 допушта све наизменичне речи над Σ које почињу словом b.*

Доказ индукцијом по дужини речи, k:

За $k = 1$, одговарајућа наизменична реч је b, па како важи $(q_1, b) \vdash_{M_1} (q_3, e)$, ова реч је допуштена аутоматом M_1.

Даље, претпоставимо да су све наизменичне речи дужине мање или једнаке k које почињу словом b допуштене коначним аутоматом M_1, и докажимо да исто тврђење важи и за све такве речи дужине $k+1$. Нека је w наизменична реч дужине $k+1$ која почиње словом b. За такву реч важи $w = bw'$, где је w' наизменична реч дужине k која почиње словом a. Ако је $|w'| = 1$, онда је $w' = a$, тј. $w = ba$. Како важи

$$(q_1, ba) \vdash_{M_1} (q_2, a) \vdash_{M_1} (q_3, e),$$

то значи да је реч w допуштена коначним аутоматом M_1. Ако је $|w'| > 1$, онда је $w = baw''$, где је w'' наизменична реч дужине $k-2$ која почиње словом b. Како важи

$$(q_1, baw'') \vdash_{M_1} (q_2, aw'') \vdash_{M_1} (q_1, w'') \vdash^*_{M_1} (q_3, e),$$

то значи да је реч w допуштена коначним аутоматом M_1. $\square$

Дакле, важи $(q_0, aw') \vdash_M (q_1, w) \vdash^*_{M_1} (q_3, e)$, па како је M_1 подаутомат коначног аутомата M, и $(q_0, aw') \vdash^*_M (q_3, e)$, што је и требало доказати.

$\subseteq$: *Свака реч допуштена коначним аутоматом M је наизменична.*

Доказ индукцијом по дужини најкраћег доказа, k:

За $k = 1$, одговарајући доказ је $(q_0, a) \vdash_M (q_3, e)$, односно $(q_0, b) \vdash_M (q_3, e)$. На овај начин допуштена реч је a, односно b, и она јесте наизменична.

Даље, претпоставимо да свака реч са најкраћим доказом дужине мање или једнаке k јесте наизменична, и докажимо да исто тврђење важи и за све речи са најкраћим доказом дужине $k + 1$. Нека је w реч са најкраћим доказом дужине $k + 1$. За такву реч важи $w = aw'$, односно $w = bw'$. Доказаћемо тврђење само за први случај. У другом случају доказ се изводи аналогно.

Дакле, нека је $w = aw'$ и $(q_0, aw') \vdash^{k+1}_M (q_3, e)$ најкраћи доказ за реч aw'. Приметимо да први корак тог доказа мора бити $(q_0, aw') \vdash_M (q_1, w')$, као и да при допуштању било које речи коначни аутомат M не дозвољава повратак у стање q_0. То значи да се у доказу $(q_0, aw') \vdash^{k+1}_M (q_3, e)$ допуштање речи aw' своди на допуштање речи w' од стране раније описаног подаутомата M_1. Прецизније, важи:

$$(q_0, aw') \vdash_M (q_1, w') \vdash^k_{M_1} (q_3, e)$$

Докажимо следеће тврђење:

Лема 2.2 *Све речи допуштене аутоматом M_1 су наизменичне и почињу словом b.*

Доказ индукцијом по дужини најкраћег доказа, k:

За $k = 1$, одговарајући доказ је $(q_1, b) \vdash_{M_1} (q_3, e)$. На овај начин допуштена је b, а она јесте наизменична и почиње словом b.

Даље, претпоставимо да свака реч са најкраћим доказом дужине мање или једнаке k јесте наизменична и да почиње словом b, и докажимо да исто тврђење важи и за све речи са најкраћим доказом дужине $k + 1$. Нека је

$$(q_1, w) \vdash^{k+1}_{M_1} (q_3, e)$$

најкраћи доказ за реч w. Приметимо да одавде, на основу дефиниције аутомата M_1, следи да реч w мора почети словом b, као и да у првом кораку аутомат мора да пређе у стање q_2. Дакле, важи $w = bw'$, а најкраћи доказ за ову реч има следећи облик:

$$(q_1, bw') \vdash_{M_1} (q_2, w') \vdash^k_{M_1} (q_3, e)$$

Одавде следи да реч w' мора почети словом a. Ако је $w' = a$, онда је $w = ba$, и, очигледно, ова реч јесте наизменична. Ако је $w' = aw''$, где је $w'' \neq e$, онда имамо:

$$(q_2, aw'') \vdash_{M_1} (q_1, w'') \vdash^{k-1}_{M_1} (q_3, e)$$

Јасно да је $(q_1, w'') \vdash^{k-1}_{M_1} (q_3, e)$ најкраћи доказ за реч w'', па, на основу индукцијске претпоставке, следи да је w'' наизменична реч која почиње словом b. Како је $w = baw''$, следи да је и w наизменична реч која почиње словом b. $\square$

На основу управо доказане леме, следи да је w' наизменична реч која почиње словом b. Како је $w = aw'$, следи да је w наизменична реч која почиње словом a, што је и требало доказати.

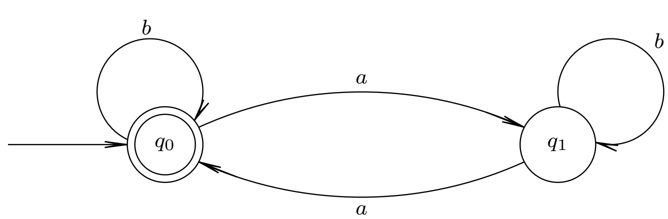
Задатак 30 *Одредити језик допуштен коначним аутоматом*
$M = (Q, \Sigma, \delta, q_0, F)$, *где је*
$Q = \{q_0, q_1, q_2\}$,
$\Sigma = \{a, b\}$,
$F = \{q_0, q_1\}$,
а функција преласка задата следећом таблицом:

	a	b
q_0	$\{q_0\}$	$\{q_1\}$
q_1	$\{q_2\}$	$\{q_1\}$
q_2	$\{q_2\}$	$\{q_2\}$

Упутство:

$$L(M) = \{a^n b^m \mid n, m \in \mathbf{N}_0\}$$

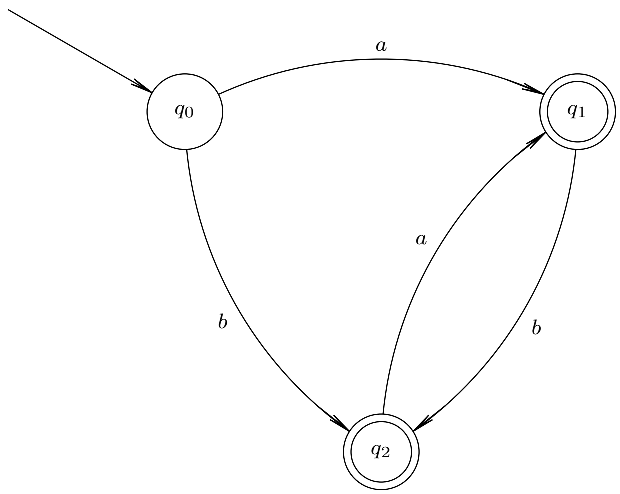
Задатак 31 *Одредити језик допуштен коначним аутоматом који је графички представљен на следећи начин:*



Упутство:

$$L(M) = \{w \mid w \in \{a,b\}^* \ \wedge \ \#_a(w) \text{ је паран број}\}$$

Задатак 32 *Граматика* $G = (N, \Sigma, P, S)$ *је задата на следећи начин:*
$N = \{S, A, B\}$,
$\Sigma = \{a, b\}$,
$P = \{S \to aA \ (1^\circ), S \to bB \ (2^\circ), A \to bB \ (3^\circ), A \to e \ (4^\circ),$
$B \to aA \ (5^\circ), B \to e \ (6^\circ)\}$,
а коначни аутомат M *је графички представљен на следећи начин:*



Доказати да је $L(G) = L(M)$.

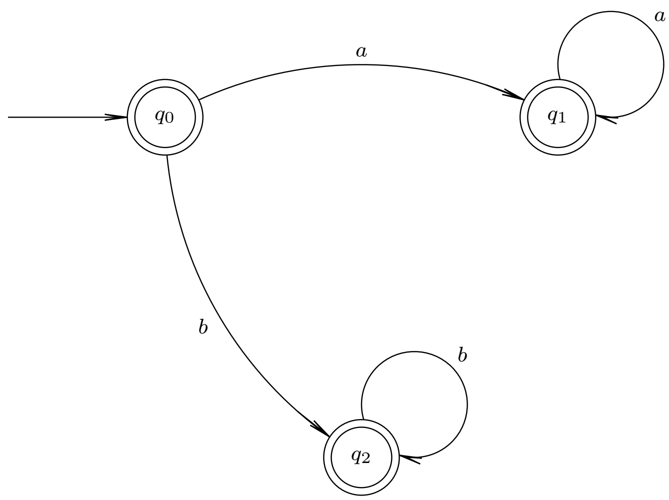
Упутство:

Тражени језик је језик допуштен коначним аутоматом датим у задатку 29. Доказ да је то језик допуштен коначним аутоматом M изводи се слично као у поменутом задатку. С друге стране, доказ да је то језик генерисан граматиком G формално се изводи на начин који је описан у задацима из одељка 1.2.1.

Задатак 33 *Одредити коначни аутомат* M *који прихвата језик генерисан граматиком* $G = (N, \Sigma, P, S)$ *која је задата на следећи начин:*
$N = \{S, A, B\}$,
$\Sigma = \{a, b\}$,
$P = \{S \to e \ (1^\circ), S \to aA \ (2^\circ), S \to bB \ (3^\circ), A \to e \ (4^\circ),$
$A \to aA \ (5^\circ), B \to e \ (6^\circ), B \to bB \ (7^\circ)\}$.

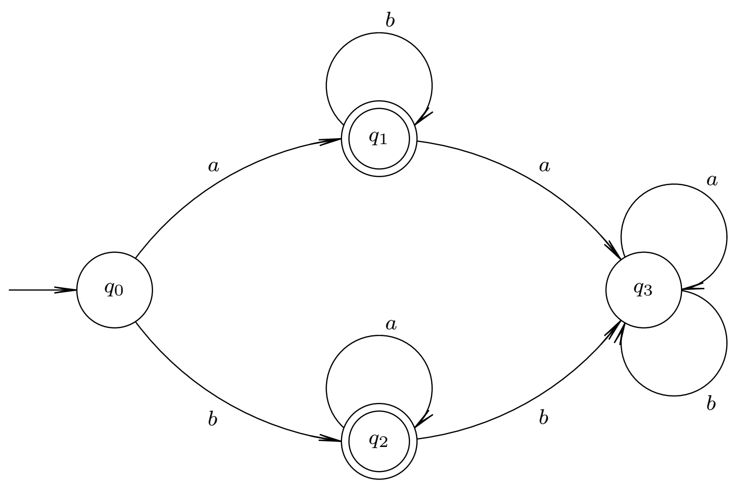
Упутство:

Може се показати да коначни аутомат који је графички приказан на следећи начин:



задовољава дати услов.

Задатак 34 *Одредити десно линеарну граматику која генерише језик допуштен коначним аутоматом који је графички представљен на следећи начин:*



Упутство:

Може се показати да граматика $G = (N, \Sigma, P, S)$ која је задата на следећи начин:
$N = \{S, A, B\}$,
$\Sigma = \{a, b\}$,
$P = \{S \to aB\ \ (1^\circ), S \to bA\ \ (2^\circ), A \to e\ \ (3^\circ), A \to aA\ \ (4^\circ),$
$B \to e\ \ (5^\circ), B \to bB\ \ (6^\circ)\}$
задовољава дати услов.

2.2 Потисни аутомати

Дефиниција 2.6 Потисни аутомат *је уређена седморка*

$$P = (Q, \Sigma, \Gamma, \delta, q_0, Z_0, F),$$

где је Q непразан (коначан) скуп стања, Σ улазна азбука, Γ азбука потисне листе, $\delta : Q \times (\Sigma \cup \{e\}) \times \Gamma \to \mathcal{P}_{\mathrm{k}}(Q \times \Gamma^*)$ функција преласка, q_0 *($q_0 \in Q$)* почетно стање, Z_0 *($Z_0 \in \Gamma$)* почетно слово *потисне листе и F ($F \subseteq Q$)* скуп завршних стања.

Уређену тројку (q, w, α) ($(q, w, \alpha) \in Q \times \Sigma^* \times \Gamma^*$) називамо конфигурацијом *потисног аутомата, при чему q представља стање у коме се аутомат налази, w део речи са улаза који још није прочитан, а α садржај потисне листе. Конфигурацију (q_0, w, Z_0) називамо* почетном, *а (q, e, α), где $q \in F$,* завршном конфигурацијом.

Дефиниција 2.7 Релацију преласка *за потисни аутомат*

$$P = (Q, \Sigma, \Gamma, \delta, q_0, Z_0, F),$$

у ознаци $\vdash_P$, дефинишемо на следећи начин:

$$(q, aw, Z\alpha) \vdash_P (q', w, \gamma\alpha) \quad \textit{ако и само ако} \quad (q', \gamma) \in \delta(q, a, Z),$$

при чему $q, q' \in Q$, $a \in \Sigma \cup \{e\}$, $w \in \Sigma^*$, $Z \in \Gamma$ и $\alpha, \gamma \in \Gamma^*$. Везу $(q, aw, Z\alpha) \vdash_P (q', w, \gamma\alpha)$ читамо: потисни аутомат P може да пређе из конфигурације $(q, aw, Z\alpha)$ у конфигурацију $(q', w, \gamma\alpha)$ читајући a и замењујући прво слово потисне листе са γ.

Аналогно као у случају коначних аутомата дефинишу се релације $\vdash_P^k$, $\vdash_P^+$ и $\vdash_P^*$.

Дефиниција 2.8 Језик допуштен потисним аутоматом

$$P = (Q, \Sigma, \Gamma, \delta, q_0, Z_0, F),$$

у ознаци $L(P)$, дефинишемо на следећи начин:

$$L(P) = \{w \mid w \in \Sigma^* \ \wedge \ (\exists q \in F)(\exists \alpha \in \Gamma)\ (q_0, w, Z_0) \vdash_P^* (q, e, \alpha)\}$$

Теорема 2.2 *Језик је допуштен неким потисним аутоматом ако и само ако је контекстно слободан.*[2]

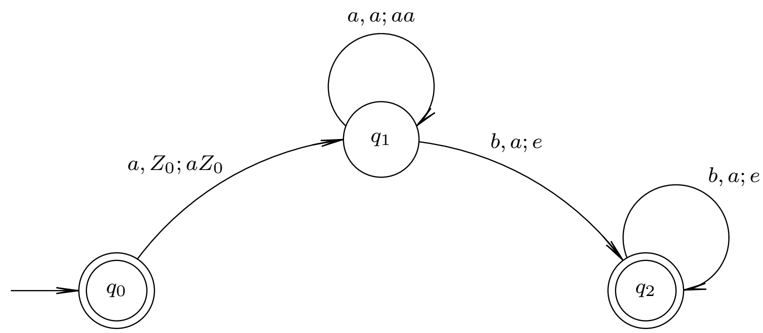
Задатак 35 *Одредити језик допуштен потисним аутоматом $P = (Q, \Sigma, \Gamma, \delta, q_0, Z_0, F)$, где је $Q = \{q_0, q_1, q_2\}$, $\Sigma = \{a, b\}$, $\Gamma = \Sigma \cup \{Z_0\}$, $F = \{q_0, q_2\}$, а функција преласка задата на следећи начин:*

$$\begin{aligned}
\delta(q_0, a, Z_0) &= \{(q_1, aZ_0)\} && (1^\circ)\\
\delta(q_1, a, a) &= \{(q_1, aa)\} && (2^\circ)\\
\delta(q_1, b, a) &= \{(q_2, e)\} && (3^\circ)\\
\delta(q_2, b, a) &= \{(q_2, e)\} && (4^\circ)
\end{aligned}$$

[2] Доказ теореме се може наћи у [8, 3].

Решење:

Дати потисни аутомат можемо графички представити на следећи начин:



Неформално, рад овог потисног аутомата можемо описати на следећи начин. Читајући реч са улаза, слово по слово, сва водеће појаве слова a се смештају у потисну листу. Сваким следећим наиласком на слово b, слово a на врху потисне листе се брише. На крају, то јест након што је прочитана реч са улаза, важи да је број појава слова a у улазној речи једнак броју појава слова b. Приметимо да дати аутомат прихвата и празну реч, јер је почетно стање, q_0, уједно и завршно.

Формално, тврдимо да за језик допуштен датим аутоматом важи:[3]

$$L(P) = \{a^n b^n \mid n \in \mathbf{N}\}$$

Докажимо наведено тврђење.

$\supseteq$: *Свака реч облика $a^n b^n$, $n \in \mathbf{N}$, је допуштена потисним аутоматом P.*

За произвољно n ($n \in \mathbf{N}$) реч $a^n b^n$ може бити допуштена потисним аутоматом P на следећи начин:

$$\begin{aligned}
&(q_0, a^n b^n, Z_0)\\
&\vdash_P (q_1, a^{n-1} b^n, aZ_0) \vdash_P (q_1, a^{n-2} b^n, a^2 Z_0) \vdash_P \ldots \vdash_P (q_1, b^n, a^n Z_0)\\
&\vdash_P (q_2, b^{n-1}, a^{n-1} Z_0) \vdash_P (q_2, b^{n-2}, a^{n-2} Z_0) \vdash_P \ldots \vdash_P (q_2, e, Z_0)
\end{aligned}$$

$\subseteq$: *Свака реч допуштена потисним аутоматом P је облика $a^n b^n$, $n \in \mathbf{N}$.*

Ако приликом доказа за неку реч није примењено ниједно правило прелаза, тада одговарајуће извођење има само један члан и

[3] Упоредити са задатком 7 да би се уочила веза између контекстно слободних граматика (као једног генераторског система) и потисних аутомата (као једног прихватачког система). Генерално, та веза је исказана теоремом 2.2.

то мора бити (q_0, e, Z_0). Празна реч јесте датог облика, јер важи $e = a^0 b^0$.

Претпоставимо да је приликом доказа за неку реч примењено бар једно правило прелаза. Приметимо најпре да је у сваком таквом доказу на почетку извођења примењено правило 1° (и то тачно једном), након чега се евентуално примењује правило 2°, затим се примењује правило 3° (и то тачно једном), и, коначно, евентуално се примењује правило 4° неколико пута. Прецизније, индукцијом се може показати да сваки доказ у коме је примењено бар једно правило прелаза има форму:

$$\begin{aligned}(q_0, w, Z_0) &\overset{1^\circ}{\vdash_P} (q_1, w', aZ_0) \overset{2^\circ,k}{\vdash_P} (q_1, w'', a^{k+1}Z_0)\\ &\overset{3^\circ}{\vdash_P} (q_2, w''', a^k Z_0) \overset{4^\circ,l}{\vdash_P} (q_2, e, \alpha Z_0)\end{aligned}$$

Штавише, може се показати да важе и једнакости $w = aw'$, $w' = a^k w''$, $w'' = bw'''$ и $w''' = b^k$, на основу којих следи једнакост $w = a^{k+1}b^{k+1}$, одакле је очигледно да допуштена реч w јесте датог облика.

Задатак 36 *Одредити потисни аутомат P који прихвата језик $L = \{w \in \Sigma^* \mid \hat{w} = w\}$.*[4]

Упутство:

Може се показати да дати језик јесте језик допуштен потисним аутоматом $P = (Q, \Sigma, \Gamma, \delta, q_0, Z_0, F)$, где је $Q = \{q_0, q_1\}$, $\Sigma = \{a, b\}$, $\Gamma = \Sigma \cup \{Z_0\}$, $F = \{q_1\}$, а функција преласка задата на следећи начин:

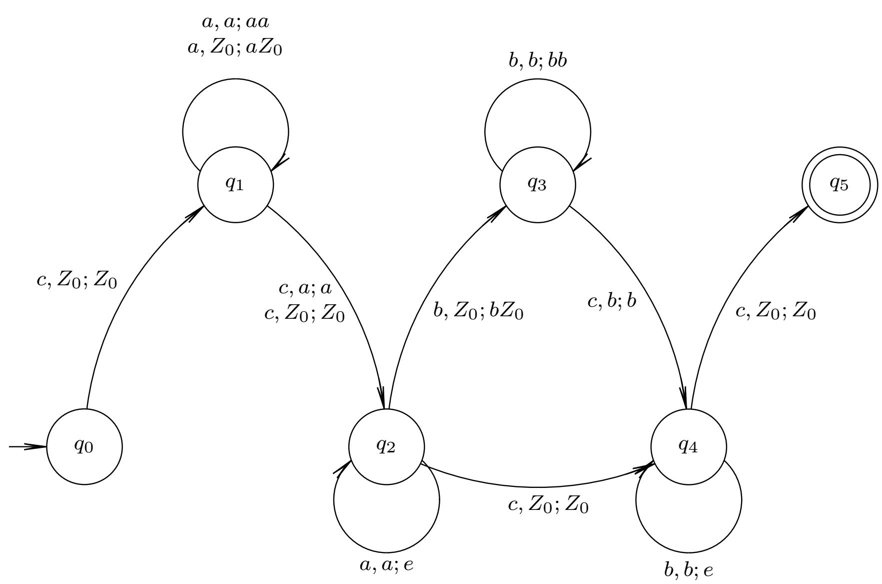
$$\begin{aligned}\delta(q_0, a, Z_0) &= \{(q_0, aZ_0)\}\\ \delta(q_0, b, Z_0) &= \{(q_0, bZ_0)\}\\ \delta(q_0, a, b) &= \{(q_0, ab)\}\\ \delta(q_0, b, a) &= \{(q_0, ba)\}\\ \delta(q_0, a, a) &= \{(q_0, aa), (q_1, e)\}\\ \delta(q_0, b, b) &= \{(q_0, bb), (q_1, e)\}\\ \delta(q_1, a, a) &= \{(q_1, e)\}\\ \delta(q_1, b, b) &= \{(q_1, e)\}\end{aligned}$$

На пример, реч *abba* може бити допуштена на следећи начин:

$$\begin{aligned}(q_0, abba, Z_0) &\vdash_P (q_0, bba, aZ_0)\\ &\vdash_P (q_0, ba, baZ_0)\\ &\vdash_P (q_1, a, aZ_0)\\ &\vdash_P (q_1, e, Z_0)\end{aligned}$$

[4] Са $\hat{w}$ је означена реч w записана здесна налево.

Задатак 37 *Граматика* $G = (N, \Sigma, P, S)$ *је задата на следећи начин:*
$N = \{S, A, B\}$,
$\Sigma = \{a, b, c\}$,
$P = \{S \to cABc\ \ (1^\circ), A \to aAa\ \ (2^\circ), A \to c\ \ (3^\circ), B \to bBb\ \ (4^\circ),$
$B \to c\ \ (5^\circ)\}$,
а потисни аутомат P *је графички представљен на следећи начин:*



Доказати да је $L(G) = L(P)$.

Упутство:

Тражени језик је:

$$L = \{ca^n ca^n b^m cb^m c \mid m, n \in \mathbf{N}\}$$

Доказ да је то језик допуштен потисним аутоматом P изводи се слично као у задатку 35. С друге стране, доказ да је то језик генерисан граматиком G формално се изводи на начин који је описан у задацима из одељка 1.2.1.

Део 3

Теорија алгоритама

Постоји више формализама којима се уводи појам израчунљивости; неки од њих су UR машине, рекурзивне функције, Тјурингове машине, Постове машине, Марковљеви алгоритми. Може се доказати да су класе функција израчунљивих функција идентичне за ове формализме. Черчова теза тврди да је класа интуитивно, неформално израчунљивих функција идентична са тим, строго заснованим класама израчунљивих функција. У даљем тексту, појам израчунљивости биће уведен и изучаван на бази UR машина и рекурзивних функција.

3.1 UR машине

UR машине[1] (URM) су један од формализама за дефинисање појма алгоритма. То су апстрактне машине које представљају математичку идеализацију рачунара. UR машина има неограничен број регистара које означавамо са $R_1, R_2, R_3, \ldots$. Сваки од њих у сваком тренутку садржи неки природан број. Садржај k-тог регистра (регистра R_k) означавамо са r_k.

R_1	R_2	R_3	$\ldots$
r_1	r_2	r_3	$\ldots$

Садржај регистара се мења наредбама (инструкцијама) чији је опис дат у табели 3.1.[2]

Израчунавање на UR машини карактеришу следеће особине:

- URM програм P је низ коначно много наредби ($P : I_1, I_2, \ldots, I_s$).

[1] Од енглеског *unlimited register machine.*

[2] Ознаке URM наредби су усклађене за називима ових наредби на енглеском језику. Наиме, у литератури на овом језику се користе термини *zero instruction, succesor instruction, transfer instruction* и *jump instruction.*

ознака	наредба	дејство
$Z(m)$	нула–наредба	$0 \to R_m$ (тј. $r_m := 0$)
$S(m)$	наредба следбеник	$r_m + 1 \to R_m$ (тј. $r_m := r_m + 1$)
$T(m, n)$	наредба преноса	$r_m \to R_n$ (тј. $r_n := r_m$)
$J(m, n, p)$	наредба скока	ако је $r_m = r_n$, иди на p-ту; иначе иди на следећу наредбу

Табела 3.1: Табела URM наредби

- Почетну конфигурацију чини низ природних бројева $a_1, a_2, \ldots$ у регистрима $R_1, R_2, \ldots$.
- Ако је функција коју треба израчунати $f(x_1, x_2, \ldots, x_n)$, онда се подразумева да су вредности $x_1, x_2, \ldots, x_n$ редом смештене у првих n регистара иза којих следи низ нула, као и да резултат треба сместити у први регистар.
- Наредбе се изршавају секвенцијално (почевши од прве инструкције), осим у случају наредбе скока.
- Израчунавање престаје само онда када не постоји следећа наредба коју треба извршити.

Дефиниција 3.1 *Ако* UR *машина након примене програма P на почетну конфигурацију $a_1, a_2, \ldots, a_n$ стаје са радом, онда пишемо*

$$P(a_1, a_2, \ldots, a_n) \downarrow,$$

иначе пишемо

$$P(a_1, a_2, \ldots, a_n) \uparrow .$$

Дефиниција 3.2 *Ако* UR *машина након примене програма P на почетну конфигурацију $a_1, a_2, \ldots, a_n$ стаје са радом и у њеном првом регистру је, као резултат израчунавања, вредност b, онда пишемо*

$$P(a_1, a_2, \ldots, a_n) \downarrow b.$$

Дефиниција 3.3 *Нека је f парцијална функција*[3] *и P* URM *програм. Кажемо да P* израчунава *f ако и само ако важи*

$$(\forall a_1, a_2, \ldots, a_n, b \in \mathbf{N})(P(a_1, a_2, \ldots, a_n) \downarrow b$$
$$\Leftrightarrow (a_1, a_2, \ldots, a_n) \in \mathrm{Dom}(f) \wedge f(a_1, a_2, \ldots, a_n) = b).$$

Дефиниција 3.4 *Функција је* URM израчунљива *ако постоји* URM *програм који је израчунава.*

[3] За функцију $f : \mathbf{N}^n \to \mathbf{N}$ кажемо да је *парцијална* ако је њен домен подскуп скупа $\mathbf{N}^n$ ($\mathrm{Dom}(f) \subseteq \mathbf{N}^n$), односно кажемо да је *тотална* ако је њен домен $\mathbf{N}^n$ ($\mathrm{Dom}(f) = \mathbf{N}^n$).

Основна хипотеза теорије алгоритама је тзв. теза Черча.[4] Нагласимо да је ово тврђење хипотеза, а не теорема. Наиме, оно говори о интуитивном појму алгоритма, чија својства не могу бити формално испитивана.

Теза Черча 1 *Класа интуитивно израчунљивих функција идентична је са класом* URM *израчунљивих функција.*

Појам формално израчунљивих функција уводи се за:

- UR машине,
- Тјурингове[5] машине,
- Постове[6] машине,
- рекурзивне функције,
- Марковљеве[7] алгоритме,
- формалне граматике.

Може се доказати да су класе израчунљивих функција које одговарају наведеним формализмима идентичне. Одатле проистиче и следећа формулација тезе Черча.

Теза Черча 2 *Класа интуитивно израчунљивих функција идентична је са класом формално израчунљивих функција.*

Из тезе Черча (која је опште прихваћена, иако је недоказива) следи да су појмови интуитивно израчунљивих функција, URM израчунљивих функција, Тјуринг израчунљивих функција итд. еквивалентни. У даљем тексту ће, једноставности ради, најчешће бити коришћен само термин *израчунљиве функције.*

Задатак 38 *Написати* URM *програм који израчунава функцију* $f(x, y) = x + y$.

Решење:

Предложени алгоритам се заснива на следећој особини:

$$x + y = x + \underbrace{1 + 1 + \cdots + 1}_{y}$$

[4]Alonzo Church (1903-1995), амерички логичар
[5]Alan Turing (1912-1954), британски математичар
[6]Emil L. Post (1897-1954), амерички математичар
[7]Андреј Андрејевич Марков (1856-1922), руски математичар

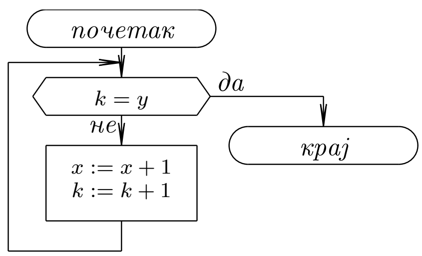
Дакле, вредности x се сукцесивно додаје вредност 1 y пута. Одговарајући URM програм подразумева следећу почетну конфигурацију:

R_1	R_2	R_3	$\ldots$
x	y	0	$\ldots$

и следећу радну конфигурацију:

R_1	R_2	R_3	$\ldots$
$x+k$	y	k	$\ldots$

где $k \in \{0, 1, \ldots, y\}$.



1. $J(3, 2, 100)$
2. $S(1)$
3. $S(3)$
4. $J(1, 1, 1)$

Задатак 39 *Написати* URM *програм који израчунава функцију*

$$f(x, y) = \begin{cases} 0 & , \textit{ако } x \leq y \\ 1 & , \textit{иначе} \end{cases}$$

Решење:

Предложени алгоритам се заснива на следећој особини:

$$x \leq y \Leftrightarrow (\exists k)(k \in \mathbf{N}) \;\; y = x + k$$

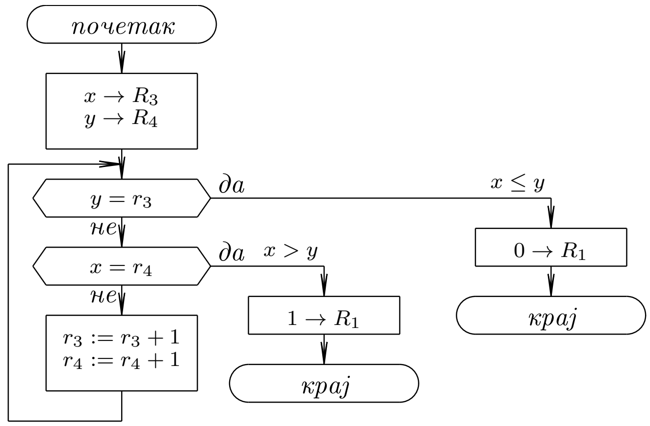
Дакле, вредности x, односно y се сукцесивно додаје вредност 1 све док се не достигне y, односно x. Прва достигнута вредност представља број не мањи од оног другог. У складу са тим закључком и дефиницијом функције f, израчуната вредност је 0 или 1. Одговарајући URM програм подразумева следећу почетну конфигурацију:

R_1	R_2	R_3	$\ldots$
x	y	0	$\ldots$

и следећу радну конфигурацију:

R_1	R_2	R_3	R_4	$\ldots$
x	y	$x+k$	$y+k$	$\ldots$

где k добија редом вредности $0, 1, 2 \ldots$.

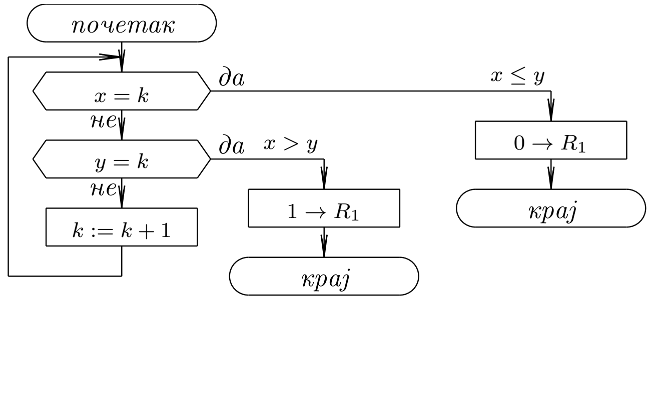


1.	$T(1,3)$	$x \to R_3$
2.	$T(2,4)$	$y \to R_4$
3.	$J(2,3,8)$	$y = r_3$?
4.	$J(1,4,10)$	$x = r_4$?
5.	$S(3)$	$r_3 := r_3 + 1$
6.	$S(4)$	$r_4 := r_4 + 1$
7.	$J(1,1,3)$	
8.	$Z(1)$	$0 \to R_1$
9.	$J(1,1,100)$	крај
10.	$Z(1)$	
11.	$S(1)$	$1 \to R_1$

Исти проблем може бити решен и на други начин. Алтернативни URM програм користи следећу радну конфигурацију:

R_1	R_2	R_3	$\dots$
x	y	k	$\dots$

где k добија редом вредности $0, 1, 2 \dots$ све док не достигне вредност x, односно y. Прва достигнута вредност представља број не мањи од оног другог. У складу са тим закључком и дефиницијом функције f, израчуната вредност је 0 или 1.



1.	$J(1,3,5)$	$x = k?$
2.	$J(2,3,7))$	$y = k?$
3.	$S(3)$	$k := k+1$
4.	$J(1,1,1)$	
5.	$Z(1)$	$0 \to R_1$
6.	$J(1,1,100)$	крај
7.	$Z(1)$	
8.	$S(1)$	$1 \to R_1$

Задатак 40 *Написати* URM *програм који израчунава функцију*

$$f(x,y) = \begin{cases} x - y & , \text{ ако } x > y \\ 0 & , \text{ иначе} \end{cases}$$

Решење:

Предложени алгоритам се заснива на следећој особини:

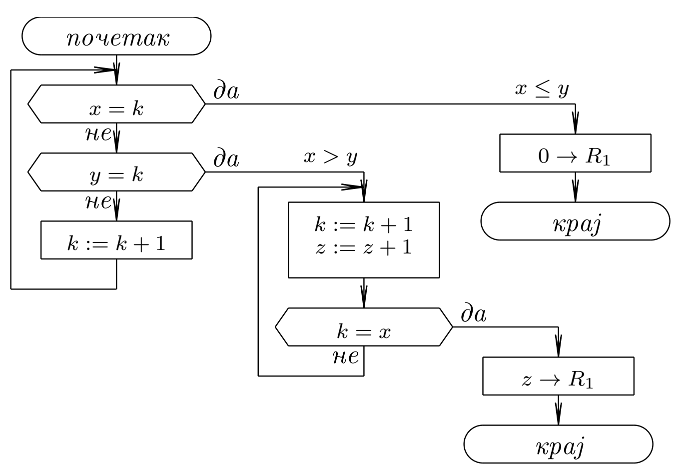
$$z = x - y \Leftrightarrow x = y + z$$

Одговарајући URM програм подразумева следећу почетну конфигурацију:

R_1	R_2	R_3	...
x	y	0	...

и следећу радну конфигурацију:

R_1	R_2	R_3	R_4	...
x	y	k	z	...



1.	$J(1,3,5)$	$x = k?$
2.	$J(2,3,7)$	$y = k?$
3.	$S(3)$	$k := k+1$
4.	$J(1,1,1)$	
5.	$Z(1)$	$0 \to R_1$
6.	$J(1,1,100)$	крај
7.	$S(3)$	$k := k+1$
8.	$S(4)$	$z := z+1$
9.	$J(3,1,11)$	$k = x?$
10.	$J(1,1,7)$	
11.	$T(4,1)$	$z \to R_1$

Задатак 41 *Написати* URM *програм који израчунава функцију*

$$f(x,y) = xy$$

Решење:

Предложени алгоритам се заснива на следећој особини:

$$xy = \underbrace{x + (\overbrace{1+\cdots+1}^{x}) + \cdots + (\overbrace{1+\cdots+1}^{x})}_{y}$$

Одговарајући URM програм подразумева следећу почетну конфигурацију:

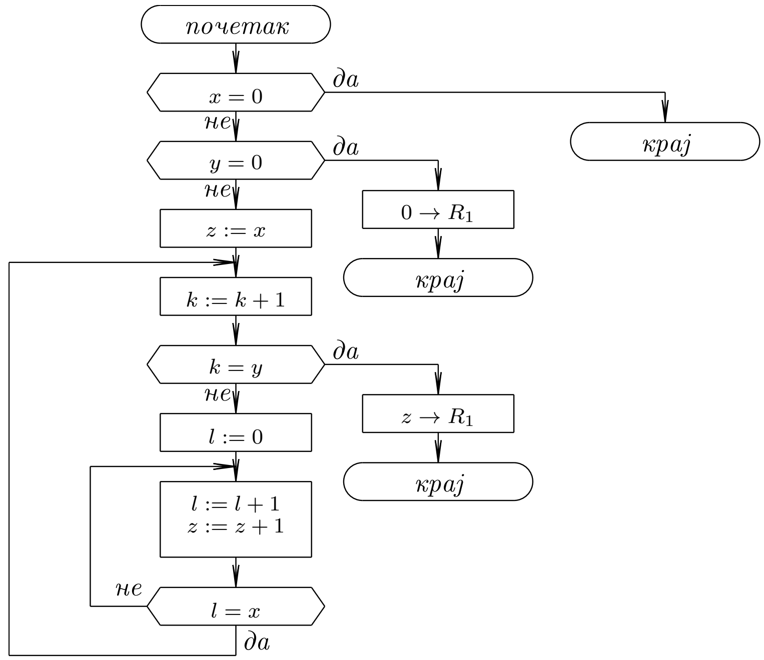
R_1	R_2	R_3	$\ldots$
x	y	0	$\ldots$

и следећу радну конфигурацију:

R_1	R_2	R_3	R_4	R_5	$\ldots$
x	y	z	k	l	$\ldots$

где k добија редом вредности $0, 1, \ldots, y$, а за сваку од ових вредности l добија редом вредности $0, 1, \ldots, x$.

1.	$J(1,10,100)$	ако је $x = 0$, онда крај
2.	$J(2,10,13)$	$y = 0?$
3.	$T(1,3)$	$z := x$
4.	$S(4)$	$k := k+1$
5.	$J(4,2,11)$	$k = y?$
6.	$Z(5)$	$l := 0$
7.	$S(5)$	$l := l+1$
8.	$S(3)$	$z := z+1$
9.	$J(5,1,4)$	
10.	$J(1,1,7))$	
11.	$T(3,1)$	$z \to R_1$
12.	$J(1,1,100)$	
13.	$Z(1)$	$0 \to R_1$



Задатак 42 *Написати* URM *програм који израчунава функцију*

$$f(x) = 2^x$$

Задатак 43 *Написати* URM *програм који израчунава функцију*

$$f(x,y) = \begin{cases} 1 & , \text{ ако } x|y \\ 0 & , \text{ иначе} \end{cases}$$

Задатак 44 *Написати* URM *програм који израчунава функцију*

$$f(x) = [\sqrt{x}]$$

Решење:

Предложени алгоритам се заснива на следећој особини:

$$n = [\sqrt{x}] \Leftrightarrow n^2 \leq x < (n+1)^2$$

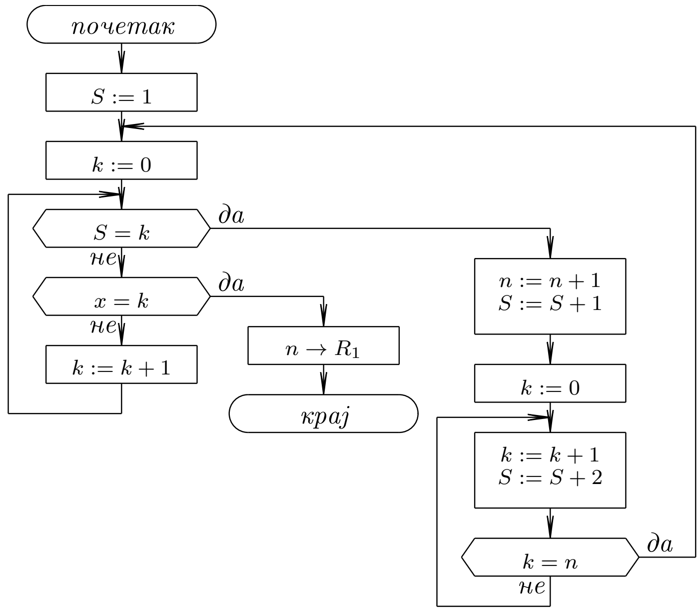
Одговарајући URM програм подразумева следећу почетну конфигурацију:

R_1	R_2	...
x	0	...

и следећу радну конфигурацију:

R_1	R_2	R_3	R_4	...
r_1	r_2	$S = (n{+}1)^2$	k	...

где за вредности n и S важи $S = (n+1)^2$.



1.	$S(3)$	$S := 1$
2.	$Z(4)$	$k := 0$
3.	$J(3,4,7)$	$S = k?$
4.	$J(1,4,15)$	$x = k?$
5.	$S(4)$	$k := k + 1$
6.	$J(1,1,3)$	
7.	$S(2)$	$n := n + 1$
8.	$S(3)$	$S := S + 1$
9.	$Z(4)$	$k := 0$
10.	$S(4)$	$k := k + 1$
11.	$S(3)$	$S := S + 1$
12.	$S(3)$	$S := S + 1$
13.	$J(4,2,2)$	$k = n?$
14.	$J(1,1,10)$	
15.	$T(2,1)$	$n \to R_1$

Задатак 45 *Написати* URM *програм који израчунава функцију*[8]

$$f(x) = \begin{cases} x/3 & , \text{ ако } 3|x \\ \uparrow & , \text{ иначе} \end{cases}$$

Задатак 46 *Написати* URM *програм који израчунава функцију* $f(x) = \left[\frac{2x}{3}\right]$.

[8]Уколико је функција недефинисана за неке вредности аргумента, уместо одговарајуће вредности функције писаћемо $\uparrow$.

Задатак 47 *Написати* URM *програм који израчунава функцију*

$$f(x,y) = \begin{cases} \left[\frac{y}{x}\right] & \text{, ако } x \neq 0 \\ \uparrow & \text{, иначе} \end{cases}$$

Задатак 48 *Написати* URM *програм који израчунава функцију* $f(x) = x!$.

Задатак 49 *Написати* URM *програм који израчунава функцију*

$$f(x,y,z) = \begin{cases} \left[\frac{y}{3}\right] & \text{, ако } 2|z \\ x+1 & \text{, иначе} \end{cases}$$

3.2 Примитивно рекурзивне функције

3.2.1 Примитивна рекурзија

Дефиниција 3.5 *За функцију* $f : \mathbf{N}^{n+1} \rightarrow \mathbf{N}$ *кажемо да је добијена* примитивном рекурзијом *од функција* $g : \mathbf{N}^n \rightarrow \mathbf{N}$ *и* $h : \mathbf{N}^{n+2} \rightarrow \mathbf{N}$*, у ознаци* $f = Rec(g,h)$*, ако и само ако важи:*

$$\begin{array}{l} f(x_1,x_2,\ldots,x_n,0) = g(x_1,x_2,\ldots,x_n) \\ f(x_1,x_2,\ldots,x_n,y+1) = h(x_1,x_2,\ldots,x_n,y,f(x_1,x_2,\ldots,x_n,y)) \end{array}$$

Напомена: Функције g и h из горње дефиниције не морају бити тоталне, па ни функција f не мора бити тотална. У случају када је $n = 0$ функција g, која је тада арности 0, је константа.

Теорема 3.1 *Нека су* $g : \mathbf{N}^n \rightarrow \mathbf{N}$ *и* $h : \mathbf{N}^{n+2} \rightarrow \mathbf{N}$ *тоталне функције. Тада постоји јединствена тотална функција* f *таква да важи:*

$$\begin{array}{l} f(x_1,x_2,\ldots,x_n,0) = g(x_1,x_2,\ldots,x_n) \\ f(x_1,x_2,\ldots,x_n,y+1) = h(x_1,x_2,\ldots,x_n,y,f(x_1,x_2,\ldots,x_n,y)). \end{array}$$

Ако је функција f добијена примитивном рекурзијом, онда сама њена дефиниција имплицира начин за израчунавање вредности функције $f(x_1,x_2,\ldots,x_n,y)$:

$$\begin{array}{ll} f(x_1,x_2,\ldots,x_n,y) & = h(x_1,x_2,\ldots,x_n,y-1,f(x_1,x_2,\ldots,x_n,y-1)) \\ f(x_1,x_2,\ldots,x_n,y-1) & = h(x_1,x_2,\ldots,x_n,y-2,f(x_1,x_2,\ldots,x_n,y-2)) \\ \quad\vdots & \\ f(x_1,x_2,\ldots,x_n,2) & = h(x_1,x_2,\ldots,x_n,1,f(x_1,x_2,\ldots,x_n,1)) \\ f(x_1,x_2,\ldots,x_n,1) & = h(x_1,x_2,\ldots,x_n,0,f(x_1,x_2,\ldots,x_n,0)) \\ f(x_1,x_2,\ldots,x_n,0) & = g(x_1,x_2,\ldots,x_n) \end{array}$$

Одатле је очигледно да ако су функције g и h израчунљиве, онда је таква и функција f. Формално, горе изречено тврђење је исказано следећом теоремом.

Теорема 3.2 *Ако је функција f добијена примитивном рекурзијом од* URM *израчунљивих функција g и h, онда је и та функција* URM *израчунљива.*

3.2.2 Супституција

Дефиниција 3.6 *Нека је $\vec{x} = (x_1, x_2, \ldots, x_n)$, $g_1, g_2, \ldots, g_k : \mathbf{N}^n \to \mathbf{N}$ и $h : \mathbf{N}^k \to \mathbf{N}$. Функција $f : \mathbf{N}^n \to \mathbf{N}$ је добијена* супституцијом *(*слагањем, композицијом*) од функција h и $g_1, g_2, \ldots, g_k$, у ознаци $f = Sub(h; g_1, g_2, \ldots, g_k)$, ако и само ако важи:*

$$f(\vec{x}) = h(g_1(\vec{x}), g_2(\vec{x}), \ldots, g_k(\vec{x}))$$

Теорема 3.3 *Ако је функција добијена супституцијом од* URM *израчунљивих, онда је и она* URM *израчунљива.*

3.2.3 Примитивно рекурзивне функције

Класа примитивно рекурзивних функција је најмања класа функција која садржи основне функције $\mathbf{0}$, s и P_i^n и затворена је за операције примитивне рекурзије и супституције. Класа примитивно рекурзивних функција је веома широка и садржи многе израчунљиве функције. Ипак, постоје и израчунљиве функције (па чак и тоталне израчунљиве функције) које нису примитивно рекурзивне (нпр. видети теорему 3.6).

Основне (базичне) функције су дате у табели 3.2.3.[9]

назив функције	опис
нула–функција	$\mathbf{0}(x) = 0$
функција следбеник	$s(x) = x + 1$
пројективна функција	$P_i^n(x_1, x_2, \ldots, x_n) = x_i,\ 1 \leq i \leq n$

Табела 3.2: Табела основних функција

Напомена: Сви елементи из $\mathbf{N}$ могу се сматрати функцијама арности 0, тј. константама. Константу $\underbrace{s(s(\ldots s}_{n}(0)))$ краће означавамо са n.

Дефиниција 3.7 Скуп примитивно рекурзивних функција*, у ознаци $\mathcal{PR}$, је најмањи скуп функција који садржи основне функције и затворен је за супституцију и примитивну рекурзију.*

[9] Ознаке основних функција су усклађене за називима ових функција на енглеском језику. Наиме, у литератури на овом језику користе се термини *zero function, succesor function* и *projection function*. Очигледна је и аналогија са одговарајућим URM наредбама — нула–наредбом, наредбом следбеник и наредбом преноса.

Скуп n-арних примитивно рекурзивних функција означавамо са $\mathcal{PR}^{(n)}$.

Скуп примитивно рекурзивних функција може се дефинисати и на следећи начин:

Дефиниција 3.8 Скуп примитивно рекурзивних функција *је скуп који задовољава следећа својства:*

(i) Основне функције су примитивно рекурзивне.

(ii) Ако су функције $g_1, g_2, \dots, g_k : \mathbf{N}^n \to \mathbf{N}$ и $h : \mathbf{N}^k \to \mathbf{N}$ примитивно рекурзивне, онда је и $Sub(h; g_1, g_2, \dots, g_k)$ примитивно рекурзивна функција.

(iii) Ако су функције g и h примитивно рекурзивне функције, онда је и $Rec(h, g)$ примитивно рекурзивна функција.

(iv) Примитивно рекурзивне функције су само оне које се могу добити коначном применом правила (i)-(iii).

Битно својство примитивно рекурзивних функција је исказано следећом теоремом.

Теорема 3.4 *Свака примитивно рекурзивна функција је тотална.*[10]

Задатак 50 *Доказати да су следеће функције примитивно рекурзивне:*
(а) $f_1(x, y) = x + y$
(б) $f_2(x, y) = x \cdot y$
(в) $f_3(x, y) = x^y$
(г) $f_4(x) = x!$
(д) $f_5(x) = \underbrace{x^{x^{\cdot^{\cdot^{\cdot^{x}}}}}}_{x+1}$
(ђ)

$$f_6(x) = x \dot{-} 1 = \begin{cases} x - 1 & , \text{ако } x > 0 \\ 0 & , \text{ако } x = 0 \end{cases}$$

(е)

$$f_7(x, y) = x \dot{-} y = \begin{cases} x - y & , \text{ако } x > y \\ 0 & , \text{ако } x \leq y \end{cases}$$

(ж) $f_8(x, y) = |x - y|$

Решење:

[10] Доказ теореме се може наћи у [5].

(а) $f_1(x,0) = x + 0 = x = P_1^1(x)$
$f_1(x, y+1) = x + (y+1) = (x+y) + 1 = f_1(x,y) + 1 = s(f_1(x,y)) = h(x,y,f_1(x,y))$

Дакле, $f_1 = Rec(P_1^1, Sub(s; P_3^3))$, где $P_1^1, P_3^3, s \in \mathcal{PR}$, као основне функције, па $f_1 \in \mathcal{PR}$.

(б) $f_2(x,0) = x \cdot 0 = 0 = \mathbf{0}(x)$
$f_2(x, y+1) = x(y+1) = xy + x = f_2(x,y) + x = f_1(x, f_2(x,y)) = h(x,y,f_2(x,y))$

Дакле, $f_2 = Rec(\mathbf{0}, Sub(f_1; P_1^3, P_3^3))$, где $\mathbf{0}, f_1, P_1^3, P_3^3 \in \mathcal{PR}$, па $f_2 \in \mathcal{PR}$.

(в) $f_3(x,0) = x^0 = 1 = s(\mathbf{0}(x))$
$f_3(x,y+1) = x^{y+1} = x^y \cdot x = f_3(x,y) \cdot x = f_2(x, f_3(x,y)) = h(x,y,f_3(x,y))$

Дакле, $f_3 = Rec(Sub(s; \mathbf{0}), Sub(f_2; P_1^3, P_3^3)) \in \mathcal{PR}$.

(г) $f_4(0) = 1$
$f_4(x+1) = (x+1)! = (x+1) \cdot f_4(x) = s(x) \cdot f_4(x) = f_2(s(x), f_4(x)) = h(x, f_4(x))$

Дакле, $f_4 = Rec(1, Sub(f_2; Sub(s; P_1^2), P_2^2)) \in \mathcal{PR}$.

(д) Нека је функција $g : \mathbf{N}^2 \to \mathbf{N}$ дефинисана на следећи начин:

$$g(x,y) = \underbrace{x^{x^{\cdot^{\cdot^{\cdot^{x}}}}}}_{y+1}$$

Важи

$$g(x,0) = x$$
$$g(x,y+1) = x^{g(x,y)} = f_3(x, g(x,y))$$

Дакле, $g = Rec(P_1^1, Sub(f_3; P_1^3, P_3^3))$, па $g \in \mathcal{PR}$. Даље, важи $f_5(x) = g(x,x) = Sub(g; P_1^1, P_1^1)$, па $f_5 \in \mathcal{PR}$.

(ђ) $f_6(0) = 0$
$f_6(x+1) = (x+1) - 1 = x$

Дакле, $f_6 = Rec(0, P_1^2)$, па $f_6 \in \mathcal{PR}$.

(е) $f_7(x,0) = x \dot{-} 0 = x$
$f_7(x,y+1) = x \dot{-} (y+1) = (x \dot{-} y) \dot{-} 1 = f_6(x \dot{-} y) = f_6(f_7(x,y))$

Дакле, $f_7 = Rec(P_1^1, Sub(f_6; P_3^3))$, па $f_7 \in \mathcal{PR}$.

(ж) $f_8(x,y) = |x - y| = (x \dot{-} y) + (y \dot{-} x) = f_1(f_7(x,y), f_7(y,x))$.

Дакле, $f_8 = Sub(f_1; Sub(f_7; P_1^2, P_2^2), Sub(f_7; P_2^2, P_1^2))$, па $f_8 \in \mathcal{PR}$.

Задатак 51 *Доказати да су следеће функције примитивно рекурзивне:*

(а)

$$sgn(x) = \begin{cases} 1 & , \text{ ако } x > 0 \\ 0 & , \text{ ако } x = 0 \end{cases}$$

(б)

$$\overline{sgn}(x) = \begin{cases} 0 & , \text{ ако } x > 0 \\ 1 & , \text{ ако } x = 0 \end{cases}$$

Решење:

(а) $sgn(0) = 0$
$sgn(x+1) = 1 = s(\mathbf{0}(x))$
Дакле, $sgn = Rec(0, Sub(s; Sub(\mathbf{0}; P_1^2)) \in \mathcal{PR}$.

(б) $\overline{sgn}(0) = 1$
$\overline{sgn}(x+1) = 0 = \mathbf{0}(x)$
Дакле, $\overline{sgn} = Rec(1, Sub(\mathbf{0}; P_1^2)) \in \mathcal{PR}$.

Задатак 52 *Доказати да су следеће функције примитивно рекурзивне:*

(а)

$$gr(x,y) = \begin{cases} 1 & , \text{ ако } x > y \\ 0 & , \text{ ако } x \leq y \end{cases}$$

(б)

$$ls(x,y) = \begin{cases} 1 & , \text{ ако } x < y \\ 0 & , \text{ ако } x \geq y \end{cases}$$

(в)

$$eq(x,y) = \begin{cases} 1 & , \text{ ако } x = y \\ 0 & , \text{ ако } x \neq y \end{cases}$$

(г)

$$ne(x,y) = \begin{cases} 1 & , \text{ ако } x \neq y \\ 0 & , \text{ ако } x = y \end{cases}$$

Решење:

(а) $gr(x,y) = sgn(x \dot{-} y) = sgn(f_7(x,y))$
Дакле, $gr = Sub(sgn; f_7) \in \mathcal{PR}$.

(б) $ls(x,y) = gr(y,x)$
Дакле, $ls = Sub(gr; P_2^2, P_1^2) \in \mathcal{PR}$.

(в) $eq(x,y) = \overline{sgn}(|x-y|) = \overline{sgn}(f_7(x,y))$
Дакле, $eq = Sub(\overline{sgn}; f_7) \in \mathcal{PR}$.

(г) $ne(x,y) = sgn(|x-y|) = sgn(f_7(x,y))$
Дакле, $ne = Sub(sgn; f_7) \in \mathcal{PR}$.

Задатак 53 *Доказати је примитивно рекурзивна функција*

$$g(x,y) = \begin{cases} 3 & ,\ \text{ако } x=1 \text{ и } y=7 \\ 5 & ,\ \text{ако } x=2 \text{ и } y=0 \\ 1 & ,\ \text{ако } x=4 \text{ и } y=4 \\ 0 & ,\ \text{иначе} \end{cases}$$

Решење:
$g(x,y) = 3\cdot eq(x,1)eq(y,7) + 5\cdot eq(x,2)eq(y,0) + eq(x,4)eq(y,4)$

Задатак 54 *Доказати да су следеће функције примитивно рекурзивне:*
(а) $\min(x,y)$
(б) $\max(x,y)$

Решење:
(а) $\min(x,y) = x \dot{-} (x \dot{-} y) = f_7(x, f_7(x,y))$
(б) $\max(x,y) = y + (x \dot{-} y) = f_1(y, f_7(x,y))$

Фукције f_1 и f_7 су примитивно рекурзивне, па како је скуп примитивно рекурзивних функција затворен за супституцију, следи да су и функције min и max примитивно рекурзивне.

Задатак 55 *Доказати да су следеће функције примитивно рекурзивне:*
(а)

$$rm(x,y) = \begin{cases} \text{остатак дељења } y \text{ са } x & ,\ \text{ако } x \neq 0 \\ y & ,\ \text{ако } x = 0 \end{cases}$$

(б)

$$qt(x,y) = \begin{cases} \left[\frac{y}{x}\right] & ,\ \text{ако } x \neq 0 \\ 0 & ,\ \text{ако } x = 0 \end{cases}$$

(в)

$$div(x,y) = \begin{cases} 1 & ,\ \text{ако } x|y \\ 0 & ,\ \text{иначе} \end{cases}$$

Решење:
(а) $rm(x,0) = 0 = \mathbf{0}(x)$

$$\begin{aligned} rm(x,y+1) &= \begin{cases} \text{остатак дељења } y+1 \text{ са } x & ,\ \text{ако } x \neq 0 \\ y+1 & ,\ \text{ако } x = 0 \end{cases} \\ &= \begin{cases} rm(x,y)+1 & ,\ \text{ако } x \neq 0 \ \wedge\ \neg(x|y+1) \\ 0 & ,\ \text{ако } x \neq 0 \ \wedge\ x|y+1 \\ y+1 & ,\ \text{ако } x = 0 \end{cases} \\ &= \begin{cases} rm(x,y)+1 & ,\ \text{ако } x \neq 0 \ \wedge\ rm(x,y) \neq x-1 \\ y+1 & ,\ \text{ако } x = 0 \\ 0 & ,\ \text{иначе} \end{cases} \\ &= (rm(x,y)+1)sgn(x)ne(rm(x,y)+1,x) + (y+1)\overline{sgn}(x) \end{aligned}$$

Функција rm припада класи $\mathcal{PR}$, јер се може добити супституцијом и примитивном рекурзијом из примитивно рекурзивних функција.

(б) $qt(x,0) = 0 = \mathbf{0}(x)$

$$\begin{aligned}
qt(x,y+1) &= \begin{cases} \left[\frac{y+1}{x}\right] & , \text{ако } x \neq 0 \\ 0 & , \text{ако } x = 0 \end{cases} \\
&= \begin{cases} \left[\frac{y}{x}\right] & , \text{ако } x \neq 0 \ \wedge \ \neg(x|y+1) \\ \left[\frac{y}{x}\right] + 1 & , \text{ако } x \neq 0 \ \wedge \ x|y+1 \\ 0 & , \text{ако } x = 0 \end{cases} \\
&= \begin{cases} qt(x,y) & , \text{ако } x \neq 0 \ \wedge \ rm(x,y)+1 \neq x \\ qt(x,y)+1 & , \text{ако } x \neq 0 \ \wedge \ rm(x,y)+1 = x \\ 0 & , \text{ако } x = 0 \end{cases} \\
&= qt(x,y) + sgn(x)eq(rm(x,y)+1, x)
\end{aligned}$$

(в)

$$\begin{aligned}
div(x,y) &= \begin{cases} 1 & , \text{ако } x|y \\ 0 & , \text{иначе} \end{cases} \\
&= \begin{cases} 1 & , \text{ако } x \neq 0 \ \wedge \ rm(x,y) = 0 \\ 0 & , \text{иначе} \end{cases} \\
&= sgn(x)\overline{sgn}(rm(x,y))
\end{aligned}$$

3.2.4 Ограничене суме и производи

Задатак 56 *Нека је $g : \mathbf{N}^{n+1} \to \mathbf{N}$ примитивно рекурзивна функција и нека је функција $f : \mathbf{N}^{n+1} \to \mathbf{N}$ дефинисана на следећи начин:*

$$f(x_1, x_2, \ldots, x_n, y) = \sum_{i=0}^{y} g(x_1, x_2, \ldots, x_n, i).$$

Доказати да је функција f примитивно рекурзивна.

Решење:

Важи:

$f(x_1, x_2, \ldots, x_n, 0) = g(x_1, x_2, \ldots, x_n, 0)$

$f(x_1, x_2, \ldots, x_n, y+1) = f(x_1, x_2, \ldots, x_n, y) + g(x_1, x_2, \ldots, x_n, y+1)$,

па је функција f примитивно рекурзивна.

Ограничена сума може бити дефинисана и у форми $\sum_{z<y} g(\vec{x}, z)$ на следећи начин:

$$\sum_{z<0} g(\vec{x}, z) = 0$$

$$\sum_{z<y+1} g(\vec{x}, z) = \sum_{z<y} g(\vec{x}, z) + g(\vec{x}, y)$$

На основу саме дефиниције следи да је и овако уведено ограничено сумирање примитивно рекурзивна функција. Важи и:

$$\sum_{z<y+1} g(\vec{x}, z) = \sum_{z=0}^{y} g(\vec{x}, z).$$

Задатак 57 *Нека су* $g : \mathbf{N}^{n+1} \to \mathbf{N}$ *и* $w_1, w_2 : \mathbf{N}^n \to \mathbf{N}$ *примитивно рекурзивне функције. Функција* $f : \mathbf{N}^n \to \mathbf{N}$ *дефинисана је на следећи начин:*

$$f(x_1, x_2, \ldots, x_n) = \sum_{i=w_1(x_1,x_2,\ldots,x_n)}^{w_2(x_1,x_2,\ldots,x_n)} g(x_1, x_2, \ldots, x_n, i)$$

при чему је $f(x_1, x_2, \ldots, x_n) = 0$ *ако је* $w_1(x_1, x_2, \ldots, x_n) > w_2(x_1, x_2, \ldots, x_n)$. *Доказати да је функција* f *примитивно рекурзивна.*

Решење:

Важи

$$f(\vec{x}) = \overline{sgn}(w_1(\vec{x}) \dot{-} w_2(\vec{x})) \sum_{i=0}^{w_2(\vec{x}) \dot{-} w_1(\vec{x})} g'(\vec{x}, i),$$

где је $\vec{x} = (x_1, x_2, \ldots, x_n)$ и $g'(\vec{x}, i) = g(\vec{x}, w_1(\vec{x}) + i)$, па је функција f примитивно рекурзивна на основу претходног задатка.

Задатак 58 *Доказати да су следеће функције примитивно рекурзивне:*

(а)

$$qt_1(x, y) = \begin{cases} \left[\frac{y}{x}\right] & , \text{ако } x \neq 0 \\ y & , \text{ако } x = 0 \end{cases}$$

(б)

$$rm_1(x, y) = \begin{cases} \text{остатак дељења } y \text{ са } x & , \text{ако } x \neq 0 \\ y & , \text{ако } x = 0 \end{cases}$$

(в)

$$\tau(x) = \begin{cases} \text{број делилаца броја } x & , \text{ако } x \neq 0 \\ 0 & , \text{ако } x = 0 \end{cases}$$

(г)

$$\sigma(x) = \begin{cases} \text{сума делилаца броја } x & , \text{ако } x \neq 0 \\ 0 & , \text{ако } x = 0 \end{cases}$$

(д)

$$Pr(x) = \begin{cases} 1 & , \text{ако је } x \text{ прост број} \\ 0 & , \text{ако је } x \text{ сложен број} \end{cases}$$

(ђ)

$$\pi(x) = \text{број простих бројева мањих од } x$$

(е)

$$\tau_1(x) = \begin{cases} \textit{број простих делилаца броја } x & , \textit{ако } x \neq 0 \\ 0 & , \textit{ако } x = 0 \end{cases}$$

Решење:

(а) За $x \neq 0$ важи:

$$\begin{aligned} \left[\frac{y}{x}\right] = k &\Leftrightarrow k \leq \frac{y}{x} < k+1 \\ &\Leftrightarrow kx \leq y < (k+1)x \end{aligned}$$

$$\begin{aligned} kx \leq y &\Leftrightarrow kx \dot{-} y = 0 \\ &\Leftrightarrow \overline{sgn}(kx \dot{-} y) = 1 \end{aligned}$$

$$\left[\frac{y}{x}\right] = \sum_{i=1}^{y} \overline{sgn}(ix \dot{-} y)$$

док за $x = 0$ важи:

$$\sum_{i=1}^{y} \overline{sgn}(i \cdot 0 \dot{-} y) = y \cdot 1 = y = qt_1(x, y)$$

Дакле, у општем случају важи:

$$qt_1(x, y) = \sum_{i=1}^{y} \overline{sgn}(ix \dot{-} y)$$

(б)

$$rm_1(x, y) = y \dot{-} x \cdot qt_1(x, y)$$

(в)

$$\tau(x) = \sum_{i=1}^{x} \overline{sgn}(rm_1(i, x))$$

(г)

$$\sigma(x) = \sum_{i=1}^{x} i \cdot \overline{sgn}(rm_1(i, x))$$

(д)

$$Pr(x) = eq(\tau(x), 2)$$

(ђ)

$$\pi(x) = \sum_{i=1}^{x} Pr(i)$$

(e)

$$\tau_1(x) = \sum_{i=1}^{x} Pr(i)\overline{sgn}(rm_1(i,x))$$

Задатак 59 *Нека је* $g : \mathbf{N}^{n+1} \to \mathbf{N}$ *примитивно рекурзивна функција и нека је функција* $f : \mathbf{N}^{n+1} \to \mathbf{N}$ *дефинисана на следећи начин:*

$$f(x_1, x_2, \ldots, x_n, y) = \prod_{i=0}^{y} g(x_1, x_2, \ldots, x_n, i).$$

Доказати да је функција f *примитивно рекурзивна.*

Решење:

Задатак се решава аналогно задатку 56.

Аналогно ограниченој суми, ограничени производ може бити дефинисан и у форми $\prod_{z<y} g(\vec{x}, z)$ на следећи начин:

$$\prod_{z<0} g(\vec{x}, z) = 1$$
$$\prod_{z<y+1} g(\vec{x}, z) = \prod_{z<y} g(\vec{x}, z) \cdot g(\vec{x}, y)$$

На основу саме дефиниције следи да је и овако уведени ограничени производ примитивно рекурзивна функција. Важи и:

$$\prod_{z<y+1} g(\vec{x}, z) = \prod_{z=0}^{y} g(\vec{x}, z).$$

Задатак 60 *Нека су* $g : \mathbf{N}^{n+1} \to \mathbf{N}$ *и* $w_1, w_2 : \mathbf{N}^n \to \mathbf{N}$ *примитивно рекурзивне функције. Функција* $f : \mathbf{N}^n \to \mathbf{N}$ *дефинисана је на следећи начин:*

$$f(x_1, x_2, \ldots, x_n) = \prod_{i=w_1(x_1,x_2,\ldots,x_n)}^{w_2(x_1,x_2,\ldots,x_n)} g(x_1, x_2, \ldots, x_n, i)$$

при чему је $f(x_1, x_2, \ldots, x_n) = 1$ *ако је* $w_1(x_1, x_2, \ldots, x_n) > w_2(x_1, x_2, \ldots, x_n)$*. Доказати да је функција* f *примитивно рекурзивна.*

Упутство:

Задатак се решава аналогно задатку 57.

3.2.5 Ограничена минимизација

Дефиниција 3.9 *Нека* $g : \mathbf{N}^{n+1} \to \mathbf{N}$ *и* $x_1, x_2, \ldots, x_n \in \mathbf{N}$. Оператор (неограничене) минимизације ((неограничени) μ-оператор) *је функција дефинисана на следећи начин:*

$$\mu y[g(x_1, x_2, \ldots, x_n, y) = 0]$$

$$= \begin{cases} y, & \textit{где је } y \textit{ најмања вредност таква да је } g(x_1, x_2, \ldots, x_n, y) = 0 \\ & \textit{и вредност } g(x_1, x_2, \ldots, x_n, z) \textit{ је дефинисана за све } z < y, \\ & \textit{ако таква вредност постоји} \\ \uparrow, & \textit{иначе} \end{cases}$$

Нека је $f(x_1, x_2, \ldots, x_n) = \mu z[g(x_1, x_2, \ldots, x_n, z) = 0]$. Функција f не мора бити тотална чак и онда када је таква функција g (нпр. у неким случајевима не постоји z такво да је $g(x_1, x_2, \ldots, x_n, z) = 0$). Слично, ако је функција g примитивно рекурзивна, то не мора бити и функција f. Међутим, овако уведени оператор минимизације могуће је модификовати тако да је добијена функција примитивно рекурзивна и тотална ако је таква функција-аргумент, и то на следећи начин.

Дефиниција 3.10 *Нека* $g : \mathbf{N}^{n+1} \to \mathbf{N}$ *и* $x_1, x_2, \ldots, x_n, y \in \mathbf{N}$. Оператор ограничене минимизације (ограничени μ-оператор) *је функција дефинисана на следећи начин:*[11]

$$\mu(z < y)[g(x_1, x_2, \ldots, x_n, z) = 0]$$

$$= \begin{cases} z, & \textit{где је } z \textit{ најмања вредност таква да је } z < y \textit{ и} \\ & g(x_1, x_2, \ldots, x_n, z) = 0, \textit{ ако таква вредност постоји} \\ y, & \textit{иначе} \end{cases}$$

Вредност y *називамо горњим ограничењем минимизације.*

Када је функција g тотална, односно примитивно рекурзивна, таква је и функција која је из ње добијена ограниченом минимизацијом.

Задатак 61 *Нека је функција* $g : \mathbf{N}^{n+1} \to \mathbf{N}$ *примитивно рекурзивна и нека је функција* $f : \mathbf{N}^{n+1} \to \mathbf{N}$ *дефинисана на следећи начин:*

$$f(x_1, \ldots, x_n, y) = \mu(z < y)[g(x_1, \ldots, x_n, z) = 0]$$

Доказати да је функција f *примитивно рекурзивна.*

Решење:
Ако је $y = 0$, тада је $f(x_1, \ldots, x_n, y) = 0$.

[11] Вредност $\mu(z < y)[g(x_1, x_2, \ldots, x_n, z) = 0]$ понекад се означава и на следећи начин: $\overset{y}{\mu}\, z[g(x_1, x_2, \ldots, x_n, z) = 0]$

Претпоставимо да је $y > 0$. Дефинишимо функцију $h : \mathbf{N}^{n+1} \to \mathbf{N}$ на следећи начин:

$$h(x_1, \dots, x_n, k) = \prod_{i=0}^{k} sgn(g(x_1, \dots, x_n, i))$$

Функција g је, по претпоставци задатка, примитивно рекурзивна, а исто важи и за функцију sgn (видети задатак 51). Функција h је добијена из ових функција коришћењем ограниченог производа, па је и она примитивно рекурзивна.

Поред тога, важи:

$$h(x_1, \dots, x_n, k) = \begin{cases} 1 & \text{, ако } g(x_1, \dots, x_n, z) \neq 0 \text{ за све } z \leq k \\ 0 & \text{, иначе} \end{cases}$$

$$\begin{aligned}
& f(x_1, \dots, x_n, y) \\
&= \begin{cases} z, & \text{где је } z \text{ најмања вредност таква да је } z < y \text{ и} \\ & g(x_1, \dots, x_n, z) = 0, \text{ ако таква вредност постоји} \\ y, & \text{иначе} \end{cases} \\
&= \text{број вредности } k \text{ таквих да } 0 \leq k < y \text{ и } g(x_1, \dots, x_n, z) \neq 0 \\
&\quad \text{за све } 0 \leq z \leq k \\
&= \text{број вредности } k \text{ таквих да } 0 \leq k < y \text{ и } h(x_1, \dots, x_n, k) = 1 \\
&= \sum_{k=0}^{y \dot{-} 1} h(x_1, \dots, x_n, k)
\end{aligned}$$

Дакле, за $y > 0$ важи:

$$f(x_1, \dots, x_n, y) = \sum_{k=0}^{y \dot{-} 1} h(x_1, \dots, x_n, k).$$

У општем случају, важи следећа једнакост:

$$f(x_1, \dots, x_n, y) = sgn(y) \cdot \left(\sum_{k=0}^{y \dot{-} 1} \prod_{i=0}^{k} sgn(g(x_1, \dots, x_n, i)) \right).$$

Како је функција f добијена супституцијом и ограниченим сумирањем из примитивно рекурзивних функција, следи да је и она примитивно рекурзивна, што је и требало доказати.

Напомена: Дато тврђење имплицира и следећи закључак: у услову минимизације, уместо знака $=$ $(\mu(\dots)[\dots = \dots])$ може стајати и неки други релацијски знак $(<, >, \leq, \geq, \neq)$, јер се ови могу изразити помоћу примитивно рекурзивних функција (видети задатак 52).

Задатак 62 *Нека су функције* $g : \mathbf{N}^{n+1} \to \mathbf{N}$ *и* $w : \mathbf{N}^n \to \mathbf{N}$ *примитивно рекурзивне и нека је функција* $f : \mathbf{N}^n \to \mathbf{N}$ *дефинисана на следећи начин:*

$$f(x_1, \ldots, x_n) = \mu(z \leq w(x_1, \ldots, x_n))[g(x_1, \ldots, x_n, z) = 0].$$

Доказати да је функција f *примитивно рекурзивна.*

Решење:

$$f(x_1, \ldots, x_n) = \sum_{k=0}^{w(x_1,\ldots,x_n)} \prod_{i=0}^{k} sgn(g(x_1, \ldots, x_n, i)) \Rightarrow f \in \mathcal{PR}$$

Задатак 63 *Доказати да су следеће функције примитивно рекурзивне:*

(а)

$$quo(x, y) = \begin{cases} \left[\frac{y}{x}\right] & , \text{ако } x \neq 0 \\ 0 & , \text{ако } x = 0 \end{cases}$$

(б)

$$rem(x, y) = \begin{cases} \text{остатак при дељењу } y \text{ са } x & , \text{ако } x \neq 0 \\ 0 & , \text{ако } x = 0 \end{cases}$$

(в)

$$div(x, y) = \begin{cases} 1 & , \text{ако } x > 0, y > 0, x|y \\ 0 & , \text{иначе} \end{cases}$$

(г)

$$ndiv(x) = \begin{cases} \text{број делилаца броја } x & , \text{ако } x \neq 0 \\ 0 & , \text{ако } x = 0 \end{cases}$$

(д)

$$pr(x) = \begin{cases} 1 & , \text{ако је } x \text{ прост број} \\ 0 & , \text{иначе} \end{cases}$$

(ђ)

$$pn(x) = \begin{cases} x\text{-ти прост број} & , \text{ако } x \neq 0 \\ 0 & , \text{ако } x = 0 \end{cases}$$

(е)

$$long(x) = \begin{cases} \text{највећи прост делилац броја } x & , \text{ако } x \neq 0 \\ 0 & , \text{ако } x = 0 \end{cases}$$

Решење:

(а) За $x \neq 0$ важи:

$$\begin{aligned} z = quo(x,y) &\Leftrightarrow zx \leq y < (z+1)x \\ &\Rightarrow quo(x,y) = \mu(z < y+1)[gr((z+1)x,y) = 1] \end{aligned}$$

У општем случају важи:

$$quo(x,y) = sgn(x)\mu(z < y+1)[gr((z+1)x,y) = 1],$$

па $quo \in \mathcal{PR}$.

(б) $rem(x,y) = sgn(x)(y \dot{-} x \cdot quo(x,y)) \in \mathcal{PR}$

(в) Важи:

$$\begin{aligned} div(x,y) = 1 &\Leftrightarrow x > 0 \ \wedge \ y > 0 \ \wedge \ x|y \\ &\Leftrightarrow y > 0 \ \wedge \ rem(x,y) = 0 \end{aligned}$$

Дакле, $div(x,y) = sgn(y) \cdot \overline{sgn}(rem(x,y)) \in \mathcal{PR}$.

(г) За $x \neq 0$ важи:

$$ndiv(x) = \sum_{i=1}^{x} div(i,x)$$

За вредност $x = 0$, важи иста једнакост:

$$ndiv(x) = 0 = \sum_{i=1}^{0} div(i,x)$$

Дакле, у општем случају важи:

$$ndiv(x) = \sum_{i=1}^{x} div(i,x),$$

па је дата функција примитивно рекурзивна.

(д) $pr(x) = eq(ndiv(x), 2) \in \mathcal{PR}$

(ђ) Уочимо неколико вредности функције pn:

$$pn(0) = 0,\ pn(1) = 2,\ pn(2) = 3,\ pn(3) = 5,\ \ldots$$

и докажимо да важи:

$$pn(x) < pn(x+1) \leq pn(x)! + 1$$

$$\neg(\ pn(k) | pn(x)! + 1\ )\ ,\ k \le x \Rightarrow pn(x)! + 1 \quad \text{је или прост или је дељив}$$
$$\text{неким простим бројем већим од } pn(x)$$
$$\Rightarrow pn(x+1) \le pn(x)! + 1$$

$$\begin{aligned} pn(0) &= 0 \\ pn(x+1) &= \mu(z \le pn(x)! + 1)[z \text{ је прост број и } z > pn(x)] \\ &= \mu(z < pn(x)! + 2)[pr(z) gr(z, pn(x))] \end{aligned}$$

Исти проблем може бити решен и на следећи начин:

$$pn(x) = \mu(y < 2^{2^x})[\sum_{i=0}^{y} pr(i) = x]$$

Исправност избора горњег ограничења ове минимизације следи из једног од тврђења теорије бројева.

Задатак 64 *Доказати да је следећа функција примитивно рекурзивна:*

$$(x)_y = \begin{cases} \textit{степен броја } pn(y) \textit{ у факторизацији броја } x & , \textit{ ако } x, y > 0 \\ 0 & , \textit{ иначе} \end{cases}$$

Решење:

$$(x)_y = sgn(xy) \cdot \mu(z < x+1)[div(pn(y)^{z+1}, x) = 0]$$

Задатак 65 *Доказати да су следеће функције примитивно рекурзивне:*
(а) $[\sqrt{x}]$
(б) $[\sqrt[y]{x}]$ *(где је* $\sqrt[0]{0} = 0$*)*
(в) $[x\sqrt{2}]$

Решење:

(а) $[\sqrt{x}] = \mu(y < x+1)[ls(x, (y+1)^2) = 1]$

Задатак 66 *Доказати да су следеће функције примитивно рекурзивне:*
(а) $\text{NZS}(x, y)$ *(где је* $\text{NZS}(x, 0) = 0$*)*
(б) $\text{NZD}(x, y)$ *(где је* $\text{NZD}(x, 0) = 0$*)*
(в) $\phi(x)$ = *број ненегативних целих бројева који су мањи или једнаки* x *и узајамно су прости са* x[12].

[12] Овако дефинисану функцију називамо *Ојлеровом функцијом*.

Решење:

(а)

$$\begin{aligned}\text{NZS}(x,y) &= \mu(z < x\cdot y)[x|z \wedge y|z]\\ &= \mu(z < x\cdot y)[div(x,z) = 1 \wedge div(y,z) = 1]\\ &= \mu(z < x\cdot y)[div(x,z)\cdot div(y,z) = 1]\\ &= \mu(z < x\cdot y)[\overline{sgn}(div(x,z)\cdot div(y,z)) = 0]\end{aligned}$$

(б)

$$\text{NZD}(x,y) = quo(x\cdot y, \text{NZS}(x,y))$$

Задатак 67 *Доказати да су следеће функције примитивно рекурзивне:*
(а) $f(n) = [e \cdot n]$
(б) $f(n) = [n \cdot \sqrt[3]{e}]$

Решење:

(а) Запишимо број e у облику реда:

$$e = \sum_{k=0}^{\infty} \frac{1}{k!} = \sum_{k=0}^{n} \frac{1}{k!} + r_n,$$

где је

$$r_n = \sum_{k=n+1}^{\infty} \frac{1}{k!},$$

и дефинишимо функцију $S : \mathbf{N} \to \mathbf{N}$ на следећи начин:

$$S_n = \sum_{k=0}^{n} \frac{n!}{k!}$$

За $n > 0$ важи:

$$e\cdot n = n(\sum_{k=0}^{n} \frac{1}{k!} + r_n) = \frac{S_n}{(n-1)!} + R_n,$$

где је $R_n = n \cdot r_n$. Даље, може се показати да важи:

$$\left[\frac{S_n}{(n-1)!} + R_n\right] = \left[\frac{S_n}{(n-1)!}\right],$$

одакле, на основу горње једнакости и дефиниције функције f, следи:

$$f(n) = \left[\frac{S_n}{(n-1)!}\right].$$

Очигледно, дата функција се може представити као композиција примитивно рекурзивних функција, па је и сама таква.

3.2.6 Примери рекурзија које се своде на примитивну рекурзију

Задатак 68 *Функција $f : \mathbf{N} \to \mathbf{N}$ дефинисана је на следећи начин:*
$f(0) = 0$
$f(1) = 1$
$f(n+2) = f(n) + f(n+1)$, $n \geq 0$ [13]
Доказати да је функција f примитивно рекурзивна.

Решење:

Дефинишимо функцију $\Phi : \mathbf{N} \to \mathbf{N}$ на следећи начин:

$$\Phi(n) = 2^{f(n)} \cdot 3^{f(n+1)}$$

Приметимо да важи $f(n) = (\Phi(n))_1$, тј. $f(n)$ је степен броја $pn(1)(= 2)$ у факторизацији броја $\Phi(n)$. Довољно је, дакле, доказати да је функција Φ примитивно рекурзивна, јер ће, на основу задатака 64 и затворености скупа примитивно рекурзивних функција за супституцију, таква бити и функција f. Докажимо онда да је функција Φ примитивно рекурзивна.

$$\begin{aligned}
\Phi(0) &= 2^{f(0)} \cdot 3^{f(1)} = 2^1 \cdot 3^1 = 6 \\
\Phi(n+1) &= 2^{f(n+1)} \cdot 3^{f(n+2)} \\
&= 2^{f(n+1)} \cdot 3^{f(n)+f(n+1)} \\
&= 2^{f(n+1)} \cdot 3^{f(n)} \cdot 3^{f(n+1)} \\
&= 2^{(\Phi(n))_2} \cdot 3^{(\Phi(n))_1} \cdot 3^{(\Phi(n))_2} \\
&= g(\Phi(n))
\end{aligned}$$

где је функција $g : \mathbf{N} \to \mathbf{N}$ дефинисана на следећи начин:

$$g(n) = 2^{(n)_2} \cdot 3^{(n)_1} \cdot 3^{(n)_2}$$

Функција g је примитивно рекурзивна, одакле следи да је таква и функција Φ, што је и требало доказати.

Задатак 69 *Функција $f : \mathbf{N} \to \mathbf{N}$ дефинисана је на следећи начин:*
$f(0) = 1$
$f(1) = 4$
$f(2) = 6$
$f(n+3) = f(n) + (f(n+1))^2 + (f(n+2))^3$, $n \geq 0$.
Доказати да је функција f примитивно рекурзивна.

Решење:

Искористити функцију $\Phi(n) = 2^{f(n)} \cdot 3^{f(n+1)} 5^{f(n+2)}$.

[13] Овако дефинисану функцију називамо *Фибоначијевим низом.*

Задатак 70 *Нека су a и b дати природни бројеви, а функције $f, g : \mathbf{N} \to \mathbf{N}$ дефинисане су на следећи начин:*

$f(0) = a$
$g(0) = b$
$f(n+1) = h_1(n, f(n), g(n))$
$g(n+1) = h_2(n, f(n), g(n))$

где су функције $h_1, h_2 : \mathbf{N}^3 \to \mathbf{N}$ примитивно рекурзивне. Доказати да су функције f и g примитивно рекурзивне.

Решење:

Искористити функцију $\Phi(n) = 2^{f(n)} \cdot 3^{g(n)}$.

Задатак 71 *Функција $f : \mathbf{N}^2 \to \mathbf{N}$ дефинисана је на следећи начин:*

$$f(x, y) = \binom{x+y}{x}$$

Доказати да је функција f примитивно рекурзивна.

Решење:

Дату функцију можемо изразити као композицију примитивно рекурзивних функција на следећи начин:

$$f(x, y) = \left[\frac{(x+y)!}{x!y!}\right]$$

Напомена: Иако је вредност $\frac{(x+y)!}{x!y!}$ природан број користимо целобројно дељење, јер дељење *није* операција скупа $\mathbf{N}$.

Исти задатак можемо решити и другачије, коришћењем тзв. двоструке рекурзије. Наиме, важи:

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

Може се показати да је функција f дефинисана на следећи начин:

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

примитивно рекурзивна. Дефинишимо најпре функцију $\Phi : \mathbf{N} \to \mathbf{N}$ на следећи начин:

$$\Phi(n) = \prod_{k=0}^{n} pn(k+1)^{f(k,n-k)}$$

Важи:

$$f(x,y) = (\Phi(x+y))_{x+1}$$

Може се доказати да је функција Φ примитивно рекурзивна, одакле следи да је и функција f примитивно рекурзивна.

3.3 Рекурзивне функције

Као што је већ напоменуто у одељку 3.2.3, примитивно рекурзивне функције покривају широку класу израчунљивих функција, али не све. Нпр. за Акерманову[14] функцију се може доказати да је израчунљива, али не и примитивно рекурзивна. Помоћу оператора за неограничену минимизацију (неограничени μ оператор) могу бити описане још неке израчунљиве функције.

3.3.1 Акерманова функција

Дефинишимо низ функција α_1, α_2, $\ldots : \mathbf{N} \to \mathbf{N}$ на следећи начин:

$\alpha_0(x) = s(x)$

$\alpha_{n+1}(0) = \alpha_n(1)$

$\alpha_{n+1}(x+1) = \alpha_n(\alpha_{n+1}(x))$

Неколико првих вредности ових функција дато је у следећој табели:

$\backslash x$	0	1	2	3	4	5	6	...
α_0	1	2	3	4	5	6	7	...
α_1	2	3	4	5	6	7	8	...
α_2	3	5	7	9	11	13	15	...
α_3	5	13	29	61	125	253	509	...
α_4	13	65533						...
α_5	65533							...
$\vdots$								...

Може се доказати да важе следеће једнакости:

$\alpha_0(x) = x+1$

$\alpha_1(x) = x+2$

$\alpha_2(x) = 2x+3$

$\alpha_3(x) = 2^{x+3} - 3$

...

[14] Wilhelm Ackermann (1896-1962), немачки логичар

Акерманова функција $A : \mathbf{N}^2 \to \mathbf{N}$ може бити дефинисана на следећи начин:

$$A(x, y) = \alpha_x(y)$$

Важе и следеће једнакости:
$A(0, y) = \alpha_0(y) = s(y) = y + 1$
$A(x + 1, 0) = \alpha_{x+1}(0) = \alpha_x(1) = A(x, 1)$
$A(x + 1, y + 1) = \alpha_{x+1}(y + 1) = \alpha_x(\alpha_{x+1}(y)) = A(x, A(x + 1, y))$
Штавише, може се доказати да постоји јединствена функција $A : \mathbf{N}^2 \to \mathbf{N}$ која задовољава дате услове и тотална је, то јест Акерманова функција може бити добро дефинисана датим једнакостима (видети задатак 148).

Дефиниција 3.11 Акерманова функција *је функција* $A : \mathbf{N}^2 \to \mathbf{N}$ *која задовољава следеће једнакости:*

(i) $A(0, y) = y + 1$

(ii) $A(x + 1, 0) = A(x, 1)$

(iii) $A(x + 1, y + 1) = A(x, A(x + 1, y))$

Лема 3.1 *Акерманова функција задовољава следеће услове:*

(i) $A(x, y) > y$

(ii) $A(x, y + 1) > A(x, y)$

(iii) $y_1 < y_2 \Rightarrow A(x, y_1) < A(x, y_2)$

(iv) $A(x + 1, y) \geq A(x, y + 1)$

(v) $A(x, y) > x$

(vi) $x_1 < x_2 \Rightarrow A(x_1, y) < A(x_2, y)$

(vii) $A(x + 2, y) > A(x, 2y)$

Доказ:

(i) тврђење ћемо доказати индукцијом по x.

За $x = 0$ важи $A(0, y) = y + 1 > y$.

Претпоставимо да важи $A(x, y) > y$ и докажимо да тада важи и $A(x + 1, y) > y$. Последњу неједнакост ћемо доказати индукцијом по y.

За $y = 0$ важи $A(x+1, 0) = A(x, 1) > 1 > 0$. Претпоставимо да важи $A(x+1, y) > y$ и докажимо да тада важи и $A(x+1, y+1) > y+1$.

$$\begin{aligned} A(x+1, y+1) =& A(x, A(x+1, y)) \\ & \text{(на основу дефиниције Акерманове функције)} \\ >& A(x+1, y) \\ & \text{(на основу индуктивне претпоставке (за } x\text{))} \\ \geq& y+1 \\ & \text{(на основу индуктивне претпоставке (за } y\text{))} \end{aligned}$$

(*ii*) тврђење ћемо доказати индукцијом по x.

За $x = 0$ важи $A(0, y+1) = y+1+1 > y+1 = A(0, y)$.

Претпоставимо да важи $A(x, y+1) > A(x, y)$ и докажимо да тада важи $A(x+1, y+1) > A(x+1, y)$.

$$\begin{aligned} A(x+1, y+1) =& A(x, A(x+1, y)) \\ & \text{(на основу дефиниције Акерманове функције)} \\ >& A(x+1, y) \\ & \text{(на основу услова } (i)\text{)} \end{aligned}$$

(*iii*) Докажимо да важи $A(x, y_1) < A(x, y_2)$, где је $y_1 < y_2$, индукцијом по y_2 за фиксирано y_1.

За $y_2 = y_1 + 1$ важи $A(x, y_1) < A(x, y_2)$ на основу услова (*ii*).

За $y_2 > y_1$ претпоставимо да важи $A(x, y_1) < A(x, y_2)$ и докажимо да тада важи $A(x, y_1) < A(x, y_2 + 1)$.

$$\begin{aligned} A(x, y_1) <& A(x, y_2) \\ & \text{(на основу индуктивне претпоставке)} \\ <& A(x, y_2 + 1) \\ & \text{(на основу услова } (ii)\text{)} \end{aligned}$$

(*iv*) тврђење ћемо доказати индукцијом по y.

За $y = 0$ важи $A(x+1, 0) = A(x, 1) = A(x, 0+1)$.

Претпоставимо да важи $A(x+1, y) \geq A(x, y+1)$ и докажимо да тада важи $A(x+1, y+1) \geq A(x, y+2)$.

Како важи

$$\begin{aligned} A(x+1, y) \geq& A(x, y+1) \\ & \text{(на основу индуктивне претпоставке)} \\ \geq& y+2 \\ & \text{(на основу услова } (i)\text{)} \end{aligned}$$

то, на основу услова (iii), следи:

$$A(x, A(x, y+1)) \geq A(x, y+2)$$

одакле се, користећи дефиницију Акерманове функције, непосредно изводи:

$$A(x+1, y+1) \geq A(x, y+2)$$

што је и требало доказати.

(v) Да би доказали да је $A(x, y) > x$ искористићемо следећу идеју:

$$A(x, y) \geq A(x-1, y+1) \geq \cdots \geq A(0, x+y) = x+y+1 > x$$

Индукцијом по x доказаћемо следеће тврђење:

$$A(x, y) \geq A(0, x+y)$$

За $x = 0$ важи $A(0, y) = A(0, 0+y)$, па онда и $A(0, y) \geq A(0, 0+y)$.

Претпоставимо да важи $A(x, y) \geq A(0, x+y)$ и докажимо да тада важи и $A(x+1, y) \geq A(0, x+y+1)$.

$$\begin{aligned} A(x+1, y) \geq & A(x, y+1) \\ & \text{(на основу услова } (iv)) \\ \geq & A(0, x+y+1) \\ & \text{(на основу индуктивне претпоставке)} \end{aligned}$$

Сада лако доказујемо дато тврђење:

$$\begin{aligned} A(x, y) \geq & A(0, x+y) \\ & \text{(на основу претходно доказаног тврђења)} \\ \geq & x+y+1 \\ & \text{(на основу дефиниције Акерманове функције)} \\ > & x \end{aligned}$$

(vi) Из услова (iii) и (iv) следи да важи следећа неједнакост:

$$A(x, y) < A(x+1, y) \qquad (*)$$

Докажимо да важи $A(x_1, y) < A(x_2, y)$, где је $x_1 < x_2$, индукцијом по x_2 за фиксирано x_1.

За $x_2 = x_1 + 1$ важи $A(x_1, y) < A(x_2, y)$ на основу неједнакости (*).

За $x_2 > x_1$ претпоставимо да важи $A(x_1, y) < A(x_2, y)$ и докажимо да тада важи $A(x_1, y) < A(x_2+1, y)$.

$$\begin{aligned} A(x_1, y) < & A(x_2, y) \\ & \text{(на основу индуктивне претпоставке)} \\ < & A(x_2+1, y) \\ & \text{(на основу неједнакости (*))} \end{aligned}$$

(vii) тврђење ћемо доказати индукцијом по y.

За $y = 0$ важи:

$$\begin{aligned} A(x+2,0) >&A(x,0) \\ &\text{(на основу услова } (vi)) \\ =&A(x, 2\cdot 0) \end{aligned}$$

Претпоставимо да важи $A(x+2,y) > A(x, 2\cdot y)$ и докажимо да тада важи и $A(x+2, y+1) > A(x, 2(y+1))$.

$$\begin{aligned} &A(x+2,y+1) \\ =&A(x+1, A(x+2,y)) \\ &\text{(на основу дефиниције Акерманове функције)} \\ >&A(x+1, A(x, 2\cdot y)) \\ &\text{(на основу индуктивне претпоставке и услова } (iii)) \\ \geq&A(x, A(x, 2\cdot y)+1) \\ &\text{(на основу услова } (iv)) \\ \geq&A(x, 2\cdot y+1+1) \\ &\text{(на основу услова } (i) \text{ и } (iii)) \\ =&A(x, 2(y+1)) \end{aligned}$$

□

Може се показати да Акерманова функција није примитивно рекурзивна иако оне јесте израчуњива. То говори да класа примитивно рекурзивних функција није ,,довољно јака” да покрије класу свих израчуњивих функција.

Доказ да Акерманова функција није примитивно рекурзивна може се извести тако што се показује да она ,,расте брже” од било које примитивно рекурзивне функције. Прецизније, за сваку примитивно рекурзивну функцију f може се показати да важи:

$$(\exists k \in \mathbf{N})(\forall x_1, \ldots, x_n \in \mathbf{N})\ A(k, \max(x_1, \ldots, x_n)) > f(x_1, \ldots, x_n)$$

Наведена неједнакост може бити доказана индукцијом по сложености функције f.

Лема 3.2 *За функције $h : \mathbf{N}^m \rightarrow \mathbf{N}$ и $g_1, \ldots, g_m : \mathbf{N}^n \rightarrow \mathbf{N}$, функција $f : \mathbf{N}^n \rightarrow \mathbf{N}$ дефинисана је са $f = Sub(h; g_1, \ldots, g_m)$.*

Ако су задовољени услови:

(i) *Број k_i ($k_i \in \mathbf{N}$) је такав да за све природне бројеве $x_1, \ldots, x_n$ важи:*

$$A(k_i, \max(x_1, \ldots, x_n)) > g_i(x_1, \ldots, x_n) \ \ (i = 1, \ldots, m)$$

(*ii*) *Број* k_0 ($k_0 \in \mathbf{N}$) *је такав да за све природне бројеве* $x_1, \dots, x_m$ *важи:*

$$A(k_0, \max(x_1, \dots, x_m)) > h(x_1, \dots, x_m)$$

(*iii*) $k = \max(k_0, k_1, \dots, k_m) + 2$

онда за све природне бројеве $x_1, \dots, x_n$ *важи:*

$$A(k, \max(x_1, \dots, x_n)) > f(x_1, \dots, x_n)$$

Доказ:
Нека $x_1, \dots, x_n \in \mathbf{N}$ и означимо $\hat{x} = \max(x_1, \dots, x_n)$.

$$\begin{aligned} A(k, \hat{x}) &= A(k - 1 + 1, \hat{x}) \\ &\geq A(k - 1, \hat{x} + 1) \\ &\quad \text{(на основу леме 3.1 под } (iv)) \\ &= A(k - 2 + 1, \hat{x} + 1) \\ &= A(k - 2, A(k - 1, \hat{x})) \\ &\quad \text{(на основу дефиниције Акермановe функције)} \end{aligned}$$

С друге стране, за $i = 1, \dots, m$ важи:

$$\begin{aligned} A(k - 1, \hat{x})) &> A(k_i, \hat{x}) \\ &\quad \text{(на основу леме 3.1 под } (vi), \\ &\quad \text{јер је } k - 1 > k_i \text{ због услова } (iii)) \\ &> g_i(x_1, \dots, x_n) \\ &\quad \text{(због услова } (i)) \end{aligned}$$

из чега, на основу леме 3.1 под (*iii*), следи:

$$A(k - 2, A(k - 1, \hat{x})) > A(k - 2, g_i(x_1, \dots, x_n))$$

за све $i = 1, \dots, m$, па отуда и:

$$\begin{aligned} A(k - 2, A(k - 1, \hat{x})) &> A(k - 2, \max(g_1(x_1, \dots, x_n), \dots, g_m(x_1, \dots, x_n))) \\ &\geq A(k_0, \max(g_1(x_1, \dots, x_n), \dots, g_m(x_1, \dots, x_n))) \\ &\quad \text{(на основу леме 3.1 под } (vi), \\ &\quad \text{јер је } k - 2 > k_0 \text{ због услова } (iii)) \\ &> h(g_1(x_1, \dots, x_n), \dots, g_m(x_1, \dots, x_n)) \\ &\quad \text{(због услова } (ii)) \\ &= f(x_1, \dots, x_n) \\ &\quad \text{(на основу дефиниције функције } f) \end{aligned}$$

Дакле важи,

$$A(k, \hat{x}) \geq A(k - 2, A(k - 1, \hat{x})) > f(x_1, \dots, x_n),$$

одакле непосредно следи дато тврђење. □

Лема 3.3 *За функције* $g : \mathbf{N}^n \to \mathbf{N}$ *и* $h : \mathbf{N}^{n+2} \to \mathbf{N}$, *функција* $f : \mathbf{N}^{n+1} \to \mathbf{N}$ *дефинисана са* $f = Rec(g, h)$. *Ако су задовољени услови:*

(i) *Број* k_g ($k_g \in \mathbf{N}$) *је такав да за све природне бројеве* $x_1, \ldots, x_n$ *важи:*

$$A(k_g, \max(x_1, \ldots, x_n)) > g(x_1, \ldots, x_n)$$

(ii) *Број* k_h ($k_h \in \mathbf{N}$) *је такав да за све природне бројеве* $x_1, \ldots, x_n, y, z$ *важи:*

$$A(k_h, \max(x_1, \ldots, x_n, y, z)) > h(x_1, \ldots, x_n, y, z)$$

(iii) $k = \max(k_g, k_h) + 3$

онда за све природне бројеве $x_1, \ldots, x_n, y$ *важи:*

$$A(k, \max(x_1, \ldots, x_n, y)) > f(x_1, \ldots, x_n, y)$$

Доказ:

Нека $x_1, \ldots, x_n, \in \mathbf{N}$ и означимо $\hat{x} = \max(x_1, \ldots, x_n)$. Докажимо најпре да $A(k-2, \hat{x}+y) > f(x_1, \ldots, x_n, y)$ важи за све вредности y ($y \in \mathbf{N}$). Доказ изводимо индукцијом по y.

За $y = 0$ имамо:

$$\begin{aligned} A(k-2, \hat{x}+0) =& A(k-2, \hat{x}) \\ >& A(k_g, \hat{x}) \\ & \text{(на основу леме 3.1 под } (vi), \\ & \text{јер је } k-2 > k_g \text{ због услова } (iii)) \\ >& g(x_1, \ldots, x_n) \\ & \text{(због услова } (i)) \\ =& f(x_1, \ldots, x_n, 0) \\ & \text{(на основу дефиниције функције } f) \end{aligned}$$

Претпоставимо да $A(k-2, \hat{x}+y) > f(x_1, \ldots, x_n, y)$ и докажимо да тада важи $A(k-2, \hat{x}+y+1) > f(x_1, \ldots, x_n, y+1)$. Како је, на основу индуктивне претпоставке,

$$A(k-2, \hat{x}+y) > f(x_1, \ldots, x_n, y)$$

и

$$\begin{aligned} A(k-2, \hat{x}+y) >& \hat{x}+y \\ & \text{(на основу леме 3.1 под } (i)) \\ \geq& x_1, \ldots, x_n, y \end{aligned}$$

тачна је следећа неједнакост:

$$A(k-2, \hat{x}+y) > \max(x_1, \ldots, x_n, y, f(x_1, \ldots, x_n, y))$$

Одавде, на основу дефиниције Акермановe функције, непосредно изводимо

$$A(k-3, \hat{x}+y+1) > \max(x_1, \ldots, x_n, y, f(x_1, \ldots, x_n, y))$$

Даље,

$$\begin{aligned}
A(k-3, A(k-2, \hat{x}+y)) >& A(k-3, \max(x_1, \ldots, x_n, y, f(x_1, \ldots, x_n, y)) \\
& \text{(на основу леме 3.1 под } (iii) \\
& \text{ због последњег услова)} \\
\geq& A(k_h, \max(x_1, \ldots, x_n, y, f(x_1, \ldots, x_n, y)) \\
& \text{(на основу леме 3.1 под } (vi), \\
& \text{ јер је } k-3 > k_h \text{ због услова } (iii)) \\
>& h(x_1, \ldots, x_n, y, f(x_1, \ldots, x_n, y)) \\
& \text{(због услова } (ii)) \\
=& f(x_1, \ldots, x_n, y+1) \\
& \text{(на основу дефиниције функције } f)
\end{aligned}$$

Дакле, важи:

$$A(k-2, \hat{x}+y+1) > f(x_1, \ldots, x_n, y+1)$$

што је и требало доказати. Коначно,

$$\begin{aligned}
A(k, \max(x_1, \ldots, x_n, y)) =& A(k, \max(\hat{x}, y)) \\
=& A(k-2+2, \max(\hat{x}, y)) \\
>& A(k-2, 2 \cdot \max(\hat{x}, y)) \\
& \text{(на основу леме 3.1 под } (vii)) \\
\geq& A(k-2, \hat{x}+y) \\
& \text{(на основу леме 3.1 под } (vi)) \\
>& f(x_1, \ldots, x_n, y)
\end{aligned}$$

□

Теорема 3.5 *Нека је функција* $f : \mathbf{N}^n \to \mathbf{N}$ *примитивно рекурзивна. Тада постоји вредност* k *(*$k \in \mathbf{N}$*) таква да за све природне бројеве* $x_1, \ldots, x_n$ *важи:*

$$A(k, \max(x_1, \ldots, x_n)) > f(x_1, \ldots, x_n)$$

Доказ:

Нека $x_1, \ldots, x_n \in \mathbf{N}$ и означимо $\hat{x} = \max(x_1, \ldots, x_n)$. Доказ изводимо индукцијом по сложености функције f.

Ако је сложеност функције f једнака 0, тј. у њеној дефиницији не користе се ни супституција ни примитивна рекурзија, тј. ако је f основна функција, онда су могућа следећа три случаја:

$f = \mathbf{0}$**:** Тада је $f(x) = 0$ за све x ($x \in \mathbf{N}$). Ако је $k = 0$, онда важи:

$$\begin{aligned} A(k, \hat{x}) =& A(0, x) \\ >& 0 \\ & \text{(на основу леме 3.1 под } (v)) \\ =& f(x) \end{aligned}$$

$f = P_i^n$**:** Тада је $f(x_1, \dots, x_n) = x_i$ ($1 \le i \le n$). Ако је $k = 0$, онда важи:

$$A(k, \hat{x}) = A(0, \hat{x}) = \hat{x} + 1 > x_i = f(x_1, \dots, x_n)$$

$f = s$**:** Тада је $f(x) = x + 1$ за све x ($x \in \mathbf{N}$). Ако је $k = 1$, онда важи:

$$\begin{aligned} A(k, \hat{x}) =& A(1, x) \\ >& A(0, x) \\ & \text{(на основу леме 3.1 под } (vi)) \\ =& x + 1 \\ =& f(x) \end{aligned}$$

Претпоставимо да је тврђење теореме тачно за све функције сложености мање или једнаке w. Нека је функција f сложености $w + 1$. Докажимо да је тврђење тачно и за такву функцију. Могућа су следећа два случаја:

$f = Sub(h; g_1, \dots, g_m)$**:** Тада је свака од функција $h, g_1, \dots, g_n$ сложености мање или једнаке w, па, на основу индуктивне претпоставке, постоје константе $k_0, k_1, \dots, k_m$ које задовољавају услове леме 3.2. На основу леме 3.2, постоји вредност k таква да је $A(k, \hat{x}) > f(x_1, \dots, x_n)$.

$f = Rec(g, h)$**:** Тада је свака од функција h, g сложености мање или једнаке w, па на основу индуктивне претпоставке, постоје константе k_g и k_h које задовољавају услове леме 3.3. На основу леме 3.3, постоји вредност k таква да је $A(k, \hat{x}) > f(x_1, \dots, x_n)$. □

Теорема 3.6 *Акерманова функција није примитивно рекурзивна.*

Доказ:

Претпоставимо супротно — да Акерманова функција јесте примитивно рекурзивна. Тада, на основу теореме 3.5, постоји вредност k ($k \in \mathbf{N}$) таква да за све вредности x и y важи $A(k, \max(x, y)) > A(x, y)$. За $x = y = k$ онда важи $A(k, \max(k, k)) > A(k, k)$, одакле се непосредно изводи нетачна неједнакост $A(k, k) > A(k, k)$. Дакле, Акерманова функција није примитивно рекурзивна. □

Задатак 72 *Нека је* $A : \mathbf{N}^2 \to \mathbf{N}$ *Акерманова функција, а функција* $f : \mathbf{N}^2 \to \mathbf{N}$ *дефинисана на следећи начин:*

$$f(x,y) = \begin{cases} A(\left[\frac{x}{3}\right],y) & \text{, ако је } x \text{ дељиво са 3} \\ x^x & \text{, иначе} \end{cases}$$

Испитати да ли је функција f *примитивно рекурзивна.*

Решење:

Претпоставимо да функција f јесте примитивно рекурзивна. Важи $A(x,y) = f(3x,y)$, одакле следи да је Акерманова функција примитивно рекурзивна као композиција таквих функција. То, међутим, противречи теореми 3.6. Дакле, функција f није примитивно рекурзивна.

Задатак 73 *Нека је* $A : \mathbf{N}^2 \to \mathbf{N}$ *Акерманова функција, а функција* $f : \mathbf{N}^2 \to \mathbf{N}$ *дефинисана на следећи начин:*

$$f(x,y) = \begin{cases} A(x,y) & \text{, ако је } x = 2 \\ x^x & \text{, иначе} \end{cases}$$

Испитати да ли је функција f *примитивно рекурзивна.*

Решење:

Може се доказати да важи $A(2,y) = 2y+3$. Штавише, важи

$$f(x) = eq(x,2)\cdot(2y+3) + ne(x,2)\cdot f_3(x,x),$$

где је f_3 функција из задатка 50, а eq и ne функције из задатка 52. На основу ова два задатка, следи да је функција f примитивно рекурзивна као композиција таквих функција.

Задатак 74 *Нека је* $A : \mathbf{N}^2 \to \mathbf{N}$ *Акерманова функција, а функција* $f : \mathbf{N}^2 \to \mathbf{N}$ *дефинисана на следећи начин:* $f(x,y) = A(rm(3,x),y)$*, где је* $rm(3,x)$ *остатак при дељењу* x *са* 3*. Испитати да ли је функција* f *примитивно рекурзивна.*

Решење:

Дефинишимо функције $a_0, a_1, a_2 : \mathbf{N} \to \mathbf{N}$ на следећи начин:
$a_0(y) = A(0,y)$
$a_1(y) = A(1,y)$
$a_2(y) = A(2,y)$

Важи $a_0(0) = A(0,0) = 0+1 = 1$ и $a_0(y+1) = A(0,y+1) = y+2$, па је $a_0 \in \mathcal{PR}$. Важи $a_1(0) = A(1,0) = A(0,1) = 1+1 = 2$ и $a_1(y+1) = A(1,y+1) = A(0,A(1,y)) = a_0(a_1(y))$, па је $a_1 \in \mathcal{PR}$. Важи $a_2(0) = A(2,0) = A(1,1) = A(0,A(1,0)) = A(0,A(0,1)) = A(0,2) = 3$ и $a_2(y+1) = A(2,y+1) = A(1,A(2,y)) = a_1(a_2(y))$, па је $a_2 \in \mathcal{PR}$. (Може се показати и да важи: $a_0(y) = y+1$, $a_1(y) = y+2$ и $a_2(y) = 2y+3$.)

Функције a_0, a_1, a_2, rm и eq су примитивно рекурзивне, па из

$$f(x,y) = eq(rm(3,x),0)\cdot a_0(y) + eq(rm(3,x),1)\cdot a_1(y) + eq(rm(3,x),2)\cdot a_2(y)$$

следи да је и функција f примитивно рекурзивна.

Приметимо да се може доказати и општије тврђење — функција f дефинисана на следећи начин: $f(x,y) = A(rm(k,x),y)$, где је k фиксиран позитиван цео број је примитивно рекурзивна функција.

3.3.2 Минимизација

Примитивно рекурзивне функције покривају широку класу израчунљивих функција, али не све (нпр. Акерманова функција је израчунљива, али није примитивно рекурзивна). Помоћу оператора за неограничену минимизацију (неограничени μ оператор) могу бити описане још неке израчунљиве функције.

Дефиниција 3.12 *Нека* $g : \mathbf{N}^{n+1} \to \mathbf{N}$ *и* $x_1, x_2, \ldots, x_n \in \mathbf{N}$. Оператор (неограничене) минимизације ((неограничени) μ-оператор) *је функција дефинисана на следећи начин:*

$$\mu y[g(x_1, x_2, \ldots, x_n, y) = 0]$$

$$= \begin{cases} y, & \textit{где је } y \textit{ најмања вредност таква да је } g(x_1,x_2,\ldots,x_n,y)=0 \\ & \textit{и вредност } g(x_1,x_2,\ldots,x_n,z) \textit{ је дефинисана за све } z<y, \\ & \textit{ако таква вредност постоји} \\ \uparrow, & \textit{иначе} \end{cases}$$

Вредност y у дефиницији очигледно зависи од вредности $x_1, x_2, \ldots, x_n$, па се μ-оператором добија функција $f : \mathbf{N}^n \to \mathbf{N}$ на следећи начин:

$$f(x_1, x_2, \ldots, x_n) = \mu y[g(x_1, x_2, \ldots, x_n, y) = 0]$$

Тако добијена функција f не мора бити тотална, чак и када функција g јесте таква.

Пример 3.1 *Нека је функција* $g : \mathbf{N}^2 \to \mathbf{N}$ *дефинисана са* $g(x,y) = |x-3y|$, *а функција* $f : \mathbf{N} \to \mathbf{N}$ *са:*

$$f(x) = \mu y[g(x,y)=0] = \begin{cases} x/3 & , \textit{ако } 3|x \\ \uparrow & , \textit{иначе} \end{cases}$$

Овако дефинисана функција f није тотална, иако функција g јесте.

Уз супституцију и примитивну рекурзију, коришћењем минимизације из основних функција могуће је генерисати још неке функције, поред оних које се могу добити коришћењем супституције и примитивне рекурзије.

Напомена: За разлику од ограничене минимизације, (неограничена) минимизација *не* може бити изражена помоћу супституције и примитивне рекурзије.

3.3.3 μ-рекурзивне функције

Дефиниција 3.13 Скуп μ-рекурзивних функција,[15] *у ознаци $\mathcal{R}$, је скуп који задовољава следеће услове:*

(*i*) *Основне функције су μ-рекурзивне.*

(*ii*) *Ако су функције $g_1, g_2, \ldots, g_k : \mathbf{N}^n \to \mathbf{N}$ и $h : \mathbf{N}^k \to \mathbf{N}$ μ-рекурзивне, онда је и $Sub(h; g_1, g_2, \ldots, g_k)$ μ-рекурзивна функција.*

(*iii*) *Ако су функције g и h μ-рекурзивне функције, онда је и $Rec(h, g)$ μ-рекурзивна функција.*

(*iv*) *Ако је $g : \mathbf{N}^{n+1} \to \mathbf{N}$ μ-рекурзивна функција, онда је и функција добијена из g минимизацијом такође μ-рекурзивна.*

(*v*) *μ-рекурзивне функције су само оне које се могу добити коначном применом правила $(i) - (iv)$.*

Скуп свих n-арних μ-рекурзивних функција означавамо са $\mathcal{R}^{(n)}$. μ-рекурзивне функције краће називамо рекурзивним функцијама.

Теорема 3.7 *Свака примитивно рекурзивна функција је рекурзивна, а обратно не важи (тј. $\mathcal{PR} \subset \mathcal{R}$).*

Доказ:
На основу дефиниција 3.8 и 3.13 непосредно следи да свака примитивно рекурзивна функција јесте рекурзивна (тј. $\mathcal{PR} \subseteq \mathcal{R}$). Постоји функција која је рекурзивна, али не и примитивно рекурзивна. На пример, Акерманова функција задовољава тај услов (видети теореме 3.9 и 3.6). Дакле, $\mathcal{PR} \neq \mathcal{R}$, па важи $\mathcal{PR} \subset \mathcal{R}$. □

Дефиниција 3.14 *Класа $\mathcal{R}_0$ μ-рекурзивних функција је најмањи скуп тоталних функција који садржи основне функције и затворен је за операције супституције, рекурзије и минимизације примењене на тоталне функције (тј. μ-оператор је дозвољен само ако као резултат даје тоталну функцију).*[16]

Теорема 3.8 *Класа $\mathcal{C}$ свих* URM *израчунљивих функција једнака је класи $\mathcal{R}$ свих рекурзивних функција.*[17]

Теорема 3.9 *Доказати да је Акерманова функција рекурзивна.*

---

[15] Неки аутори посебно дефинишу μ-рекурзивне функције и тзв. *опште рекурзивне функције*, а затим показују да су те две класе функција једнаке и користе термин *рекурзивне функције* и за једну и за другу класу.

[16] Неки аутори разликују појмове интуитивно израчунљивих и ефективно израчунљивих функција. На основу те поделе интуитивно израчунљивим функцијама одговарају рекурзивне функције, а ефективно израчунљивим функцијама тоталне рекурзивне функције, односно класа $\mathcal{R}_0$.

[17] Доказ теореме се може наћи у [4].

Доказ:

За Акерманову функцију важи:

(1) $A(0,y)=y+1$

(2) $A(x+1,0)=A(x,1)$

(3) $A(x+1,y+1)=A(x,A(x+1,y))$

Уређеној n-торки $(x_1,\dots,x_n)$ придружимо број[18]

$$2^{x_1+1}3^{x_2+1}\dots pn(n)^{x_n+1}$$

(Геделов[19] број n-торке $(x_1,\dots,x_n)$).

Наводимо најпре један пример израчунавања вредности Акерманове функције ($A(1,2)=4$):

корак	израчунавање	низ арг.	правило	Геделов бр. низа арг.
0	$A(1,2)$	1,2	(3)	$2^2 3^3=108$
1	$A(0,A(1,1))$	0,1,1	(3)	$2^1 3^2 5^2=450$
2	$A(0,A(0,A(1,0)))$	0,0,1,0	(2)	$2^1 3^1 5^2 7^1=1050$
3	$A(0,A(0,A(0,1)))$	0,0,0,1	(1)	$2^1 3^1 5^1 7^2=1470$
4	$A(0,A(0,2))$	0,0,2	(1)	$2^1 3^1 5^3=750$
5	$A(0,3)$	0,3	(1)	$2^1 3^4=162$
6	4	4		$2^5=32$

Дата табела илуструје схему израчунавања вредности Акерманове функције помоћу кодираног низа природних бројева. Кораци тог израчунавања означени су са $0,1,2,\dots$.

Правило (1) примењује се ако је у низу аргумената претпоследњи члан једнак 0. Правило (2) примењује се ако је у низу аргумената претпоследњи члан већи од 0, а последњи једнак 0. Правило (3) примењује се ако су у низу аргумената последња два члана већа од 0.

Дефинишимо функцију $f:\mathbf{N}^3\to\mathbf{N}$ на следећи начин:

$$f(x,y,n)=\text{„Геделов број низа аргумената у } n\text{-том кораку израчунавања вредности } A(x,y)\text{"}$$

Ако се израчунавање вредности $A(x,y)$ заврши у n_0-том кораку и ако је $f(x,y,n_0)=z$, онда је по договору $f(x,y,n)=z$ за све $n>n_0$. Нпр: $f(1,2,4)=750,\ f(1,2,6)=f(1,2,7)=f(1,2,8)=\dots=32$.

Докажимо да је функција f примитивно рекурзивна. Дефинишимо предикате $P_k(z),\ k=1,2,3$ на следећи начин:

$$P_k(z)\Leftrightarrow\text{„}z\text{ је Геделов број низа аргумената на које се примењује } k\text{-то правило"}$$

[18] У доказу теореме користи се функција $pn(x)$ дефинисана у задатку 63 и функција $(x)_y$ дефинисана у задатку 64.

[19] Kurt Gödel (1906-1978), амерички логичар аустријског порекла

Дефинишимо функције $h_k : \mathbf{N} \to \mathbf{N}$, $k = 1, 2, 3$ на следећи начин:[20]

$$h_k(z) = \begin{cases} \text{,,Геделов број низа аргумената који се добија} \\ \text{када се } k\text{−то правило примени на низ аргумената} \\ \text{чији је Геделов број } z\text{", ако } P_k(z) \\ 0, \quad \text{иначе} \end{cases}$$

Тада важи:

$$f(x, y, n+1) = \begin{cases} h_1(f(x, y, n)) & \text{, ако } P_1(f(x, y, n)) \\ h_2(f(x, y, n)) & \text{, ако } P_2(f(x, y, n)) \\ h_3(f(x, y, n)) & \text{, ако } P_3(f(x, y, n)) \\ f(x, y, n) & \text{, иначе} \end{cases}$$

Да би се доказало да је функција f примитивно рекурзивна, довољно је доказати да су предикати P_k $(k = 1, 2, 3)$ примитивно рекурзивни[21] и да су функције h_k $(k = 1, 2, 3)$ примитивно рекурзивне.

Дефинишимо функцију $i : \mathbf{N} \to \mathbf{N}$ на следећи начин:

$$i(z) = \begin{cases} \text{,,највећа вредност } j \text{ за коју важи } pn(j)|z\text{"} & \text{, ако је } z > 1 \\ 0 & \text{, ако је } z \leq 0 \end{cases}$$

Ако је z Геделов број, онда је $i(z)$ дужина низа којем он одговара.

Правило (1) примењује се ако z представља низ чији је претпоследњи члан једнак 0. Дакле,

$$P_1(z) \Leftrightarrow i(z) > 1 \wedge (z)_{i(z) \dot{-} 1} = 1$$

Правило (2) примењује се ако z представља низ чији је претпоследњи члан већи од 0, а последњи једнак 0. Дакле,

$$P_2(z) \Leftrightarrow i(z) > 1 \wedge (z)_{i(z)} = 1 \wedge (z)_{i(z) \dot{-} 1} > 1$$

Правило (3) примењује се ако z представља низ чија су последња два члана већа од 0. Дакле,

$$P_3(z) \Leftrightarrow i(z) > 1 \wedge (z)_{i(z)} > 1 \wedge (z)_{i(z) \dot{-} 1} > 1$$

Разликујемо, дакле, три случаја:

1° Ако важи $P_1(z)$, онда

$$z = 2^{x_1+1} \cdot 3^{x_2+1} \ldots pn(i(z) \dot{-} 1)^1 \cdot pn(i(z))^{(z)_{i(z)}}$$

$$\overset{f}{\mapsto} 2^{x_1+1} \cdot 3^{x_2+1} \ldots pn(i(z) \dot{-} 1)^{(z)_{i(z)}+1}$$

[20] Функција h_k у случају $\neg P_k(z)$ може имати било коју другу вредност, а не само 0, јер та вредност не утиче на вредности функције f.

[21] Предикат P је *примитивно рекурзиван* ако је његова карактеристична функција C_P:

$$C_P(x_1, \ldots, x_n) = \begin{cases} 1 & \text{, ако } P(x_1, \ldots, x_n) \\ 0 & \text{, ако } \neg P(x_1, \ldots, x_n) \end{cases}$$

примитивно рекурзивна.

$$z \overset{f}{\mapsto} \left[\frac{z \cdot pn(i(z)\dot{-}1)^{(z)_{i(z)}}}{pn(i(z))^{(z)_{i(z)}}}\right] = h_1(z)$$

2° Ако важи $P_2(z)$, онда

$$z = 2^{x_1+1} \cdot 3^{x_2+1} \dots pn(i(z)\dot{-}1)^{(z)_{i(z)\dot{-}1}} \cdot pn(i(z))^1 \overset{f}{\mapsto}$$

$$\overset{f}{\mapsto} 2^{x_1+1} \cdot 3^{x_2+1} \dots pn(i(z)\dot{-}1)^{(z)_{i(z)\dot{-}1}\dot{-}1} \cdot pn(i(z))^2$$

$$z \overset{f}{\mapsto} \left[\frac{z \cdot pn(i(z))}{pn(i(z)\dot{-}1)}\right] = h_2(z)$$

3° Ако важи $P_3(z)$, онда

$$z = 2^{x_1+1} \cdot 3^{x_2+1} \dots pn(i(z)\dot{-}1)^{(z)_{i(z)\dot{-}1}} \cdot pn(i(z))^{(z)_{i(z)}} \overset{f}{\mapsto}$$

$$\overset{f}{\mapsto} 2^{x_1+1} \cdot 3^{x_2+1} \dots pn(i(z)\dot{-}1)^{(z)_{i(z)\dot{-}1}\dot{-}1} \cdot pn(i(z))^{(z)_{i(z)\dot{-}1}} \cdot pn(i(z)+1)^{(z)_{i(z)}\dot{-}1}$$

$$z \overset{f}{\mapsto} \left[\frac{z \cdot pn(i(z))^{(z)_{i(z)\dot{-}1}} \cdot pn(i(z)+1)^{(z)_{i(z)}\dot{-}1}}{pn(i(z)\dot{-}1) \cdot pn(i(z))^{(z)_{i(z)}}}\right] = h_3(z)$$

Означимо вредност $f(x, y, n)$ са z.

$$f(x, y, n+1) = \begin{cases} \left[\frac{z \cdot pn(i(z)\dot{-}1)^{(z)_{i(z)}}}{pn(i(z))^{(z)_{i(z)}}}\right] & \text{, ако } P_1(z) \\ \left[\frac{z \cdot pn(i(z))}{pn(i(z)\dot{-}1)}\right] & \text{, ако } P_2(z) \\ \left[\frac{z \cdot pn(i(z))^{(z)_{i(z)\dot{-}1}} \cdot pn(i(z)+1)^{(z)_{i(z)}\dot{-}1}}{pn(i(z)\dot{-}1) \cdot pn(i(z))^{(z)_{i(z)}}}\right] & \text{, ако } P_3(z) \\ z & \text{, иначе} \end{cases}$$

Важи:

$$f(x, y, 0) = 2^{x+1}3^{y+1}$$

$$\begin{aligned} f(x, y, n+1) = {} & \left[\frac{z \cdot pn(i(z)\dot{-}1)^{(z)_{i(z)}}}{pn(i(z))^{(z)_{i(z)}}}\right] \cdot C_{P_1}(z) + \left[\frac{z \cdot pn(i(z))}{pn(i(z)\dot{-}1)}\right] \cdot CP_2(z) \\ & + \left[\frac{z \cdot pn(i(z))^{(z)_{i(z)\dot{-}1}} \cdot pn(i(z)+1)^{(z)_{i(z)}\dot{-}1}}{pn(i(z)\dot{-}1) \cdot pn(i(z))^{(z)_{i(z)}}}\right] \cdot CP_3(z) \\ & + z \cdot \overline{sgn}(C_{P_1}(z) + C_{P_2}(z) + C_{P_3}(z)) \end{aligned}$$

Дакле, функција f јесте примитивно рекурзивна.

$$A(x, y) = (f(x, y, \mu n[f(x, y, n) = f(x, y, n+1)])_1 \dot{-} 1$$

Одатле следи да је функција A рекурзивна као функција добијена композицијом и минимизацијом из рекурзивних функција. □

Задатак 75 *Нека је* $f : \mathbf{N} \to \mathbf{N}$ *тотална рекурзивна функција која је „1-1”. Доказати да је функција* f^{-1} *такође рекурзивна.*

Решење:

Како функција f^{-1} задовољава услов

$$x = f^{-1}(y) \Leftrightarrow y = f(x)$$

можемо је представити као

$$f^{-1}(y) = \mu x[f(x) = y]$$

одакле следи тврђење.

Задатак 76 *Нека је* $p(x)$ *полином са ненегативним целобројним коефицијентима. Функција* $f : \mathbf{N} \to \mathbf{N}$ *дефинисана је на следећи начин:*

$$f(a) = \begin{cases} y, & \text{где је } y \text{ најмањи ненегативни целобројни корен} \\ & \text{полинома } p(x) - a, \\ & \text{ако полином } p(x) - a \text{ има ненегативан целобројан корен} \\ \uparrow, & \text{ако полином } p(x) - a \text{ нема ненегативан целобројан корен} \end{cases}$$

Доказати да је функција f *рекурзивна, као и да постоји примитивно рекурзивна функција* g *која је проширење*[22] *функције* f.

Решење:

Функцију f можемо представити на следећи начин:

$$f(a) = \mu x[p(x) = a]$$

што је довољно да закључимо да она јесте рекурзивна. Покушајмо сада да одредимо једно примитивно рекурзивно проширење ове функције.

Запишимо најпре полином $p(x)$ у облику:

$$p(x) = a_n \cdot x^n + \cdots + a_1 x + a_0$$

Даље, претпоставимо да је $p(y) - a = 0$, где је $y \in \mathbf{N}$. Да бисмо одредили горње ограничење за y, разликоваћмо следећа два случаја:

1° Ако је $a_0 - a \neq 0$, онда због

$$0 = p(y) - a = \underbrace{a_n \cdot y^n + \cdots + a_1 \cdot y}_{\text{дељиво са } y} + a_0 - a$$

важи $y \mid a_0 - a$, одакле следи да $y |\ |a_0 - a|$, односно $y \leq |a_0 - a|$. Користећи неједнакост троугла коначно добијамо горње ограничење за y у облику:

$$y \leq |a_0| + |a| = a_0 + a = p(0) + a$$

[22] Кажемо да је функција g *проширење* функције f, у ознаци $f \subseteq g$, ако и само ако је $\mathrm{Dom}(f) \subseteq \mathrm{Dom}(g)$ и $f(x) = g(x)$ за све x ($x \in \mathrm{Dom}(f)$).

2° Ако је $a_0 - a = 0$, онда је $p(0) - a = a_0 - a = 0$, па је 0 најмањи ненегативни корен полинома $p(x) - a$. Важи $0 = p(0) + a$, па и у овом случају имамо исто ограничење $0 \leq p(0) + a$.

Дакле, ако полином $p(x) - a$ има ненегативне целобројне корене, онда за најмањи такав корен y важи ограничење $y \leq p(0) + a$. Онда тражена функција g ($f \subseteq g$) може бити дефинисана на следећи начин:

$$g(a) = (\mu x < p(0) + a + 1)[|p(x) - a| = 0]$$

која очигледно јесте примитивно рекурзивна.

3.3.4 Одлучиви предикати

Нека је $P \subseteq \mathbf{N}^n$ n-арни предикат. У даљем тексту, када се говори о одлучивости, често ће уместо термина предикат бити коришћен термин проблем.

Дефиниција 3.15 Карактеристичну функцију $C_P : \mathbf{N}^n \to \{0, 1\}$ *предиката* P *дефинишемо на следећи начин:*

$$C_P(x_1, \ldots, x_n) = \begin{cases} 1 & , \text{ ако } P(x_1, \ldots, x_n) \\ 0 & , \text{ ако } \neg P(x_1, \ldots, x_n) \end{cases}$$

Дефиниција 3.16 *Предикат* P *је* одлучив (рекурзиван) *ако је његова карактеристична функција* C_P *рекурзивна.*

Дефиниција 3.17 *Скуп* M *је* одлучив (рекурзиван) *ако је одлучив предикат „*$x \in M$*”. Карактеристичну функцију предиката „*$x \in M$*” називамо* карактеристичном функцијом скупа M*:*

$$C_M(x_1, \ldots, x_n) = \begin{cases} 1 & , \text{ ако } x \in M \\ 0 & , \text{ ако } x \notin M \end{cases}$$

Задатак 77 *Нека су* $P, Q \subseteq \mathbf{N}^n$ *одлучиви предикати. Доказати да су следећи предикати одлучиви:*

(а) $\neg P$
(б) $P \wedge Q$
(в) $P \vee Q$

Решење:

(а) $C_{\neg P}(\vec{x}) = 1 \dot{-} C_P(\vec{x})$
(б) $C_{P \wedge Q}(\vec{x}) = C_P(\vec{x}) \cdot C_Q(\vec{x})$
(в) $C_{P \vee Q}(\vec{x}) = \max(C_P(\vec{x}), C_Q(\vec{x}))$

Задатак 78 *Нека је $P \subseteq \mathbf{N}^{n+1}$ одлучив предикат. Доказати да су следећи предикати одлучиви:*
(а) $Q(\vec{x}, y) \equiv (\exists z < y) P(\vec{x}, z) \ \ (\equiv (\exists z)(z < y \ \wedge \ P(\vec{x}, z)))$
(б) $R(\vec{x}, y) \equiv (\forall z < y) P(\vec{x}, z) \ \ (\equiv (\forall z)(z < y \ \Rightarrow \ P(\vec{x}, z)))$

Решење:
(а) $C_Q(\vec{x}, y) = sgn(\sum_{z<y} C_P(\vec{x}, z))$
(б) $C_R(\vec{x}, y) = \prod_{z<y} C_P(\vec{x}, z)$

Задатак 79 *Доказати да су следећи предикати одлучиви:*
(а) $N(x) \equiv x$ *је непаран*
(б) $K(x) \equiv x$ *је потпун куб*
(в) $SP(x) \equiv x$ *је степен простог броја*

Решење:

(а)

$$C_N(x) = \begin{cases} 1 & , \text{ако } \neg\, 2|x \\ 0 & , \text{ако } 2|x \end{cases} = rm(2, x)$$

(б) За природне бројеве важи:

$$x = y^3 \Rightarrow x \geq y$$

Због тога дати предикат можемо записати на следећи начин:

$$K(x) \Leftrightarrow (\exists y \leq x)\ x = y^3$$

па се његова карактеристична функција може изразити као композиција примитивно рекурзивних функција:

$$C_K(x) = sgn\left(\sum_{y<x+1} eq(x, y^3)\right)$$

Дакле, ова функција је примитивно рекурзивна, па онда и рекурзивна, одакле следи тврђење о одлучивости датог предиката.

(в) Нека је p прост број, $k \in \mathbf{N}\backslash\{0\}$ и $x = p^k$. Тада важи $p \leq x$ и $k \leq x$. То значи да за произвољан y ($y \in \mathbf{N}$) и $pn(y)^k = x$ важи $pn(y) \leq x$, односно $y \leq x$, јер је $pn(y) > y$. Дакле, за дати предикат важи:

$$\begin{aligned} SP(x) &\Leftrightarrow (\exists p \leq x)(\exists k \leq x)(x = p^k \wedge Pr(p)) \\ &\Leftrightarrow (\exists y \leq x)(\exists k \leq x)\ x = pn(y)^k \end{aligned}$$

па његову карактеристичну функцију можемо записати на следећи начин:

$$C_{SP}(x) = sgn\left(\sum_{y<x+1} \sum_{k<x+1} eq(x, pn(y)^k)\right)$$

одакле је очигледно да је она примитивно рекурзивна, па онда и рекурзивна, одакле следи тврђење о одлучивости датог предиката.

Задатак 80 *Нека су функције* $f_1, \ldots, f_m : \mathbf{N}^n \to \mathbf{N}$ *рекурзивне и нека су* $P_1, \ldots, P_m \subseteq \mathbf{N}^n$ *одлучиви предикати такви да за сваку* n*-торку* $\vec{x} = (x_1, \ldots, x_n)$ $\vec{x} \in \mathbf{N}^n$ *важи тачно један од њих. Доказати да је функција* f *дефинисана на следећи начин:*

$$f(x) = \begin{cases} f_1(\vec{x}) & \text{, ако } P_1(\vec{x}) \\ \vdots & \\ f_m(\vec{x}) & \text{, ако } P_m(\vec{x}) \end{cases}$$

рекурзивна.

Решење:

$$f(\vec{x}) = \sum_{i=1}^{m} f_i(x) \cdot C_{P_i}(x) \in \mathcal{R}$$

Напомена: Нагласимо да домен неке од функција f_i може бити и празан скуп, тј. да она није дефинисана ни за један природан број. Такву функцију често означавамо са $f_\emptyset$, а у оквиру дефиниције функције f, као у овом задатку, уместо $f_\emptyset$ краће пишемо $\uparrow$. Приметимо да функција $f_\emptyset$ јесте рекурзивна. На пример, она се може изразити помоћу рекурзивних функција на следећи начин:

$$f_\emptyset(\vec{x}) = \mu y[0 = 1]$$

Задатак 81 *Нека је* $P \subseteq \mathbf{N}^{n+1}$ *одлучив предикат. Доказати да је функција* $g : \mathbf{N}^n \to \mathbf{N}$ *дефинисана на следећи начин:*

$$\begin{aligned} g(\vec{x}) &= \mu y[P(\vec{x}, y)] \\ &= \begin{cases} \text{најмања вредност } y \text{ таква да је } P(\vec{x}, y) \\ \uparrow, \ \text{ако не постоји вредност } y \text{ таква да је } P(\vec{x}, y) \end{cases} \end{aligned}$$

рекурзивна.

Решење:

$$g(\vec{x}) = \mu y[C_P(\vec{x}, y) = 1] = \mu y[\overline{sgn}(C_P(\vec{x}, y)) = 0]$$

3.4 Енумерација

3.4.1 Ефективно набројиви скупови

Дефиниција 3.18 *Скуп* X *је* набројив *ако и само ако постоји бијекција* $f : X \to \mathbf{N}$.

Дефиниција 3.19 *Скуп X је* ефективно набројив *ако и само ако постоји бијекција $f : X \to \mathbf{N}$ таква да су функције f и f^{-1} интуитивно израчунљиве.*

Напомена: Приметимо да се у овој дефиницији користи појам интуитивно израчунљивих функција чији домен није $\mathbf{N}$. Формална дефиниција захтева уопштење строго заснованог појма израчунљивости проширивањем овог појма и на функције чији домен може бити произвољан пребројив скуп.

Дефиниција 3.20 Енумерација *скупа X је пресликавање $g : \mathbf{N} \overset{,,на"}{\to} X$. Тада пишемо $X = \{x_0, x_1, \dots\}$ (где је $x_n = g(n)$).*

Ако је функција g ,,1-1", онда кажемо да је g енумерација без понављања.

Теорема 3.10 *Следећи скупови су ефективно набројиви:*

(i) $\mathbf{N} \times \mathbf{N}$

(ii) $\mathbf{N}^+ \times \mathbf{N}^+ \times \mathbf{N}^+$

(iii) $\bigcup_{k=1}^{\infty} \mathbf{N}^k$ *(скуп свих коначних низова)*

Доказ:

(i) Нека је функција $\pi : \mathbf{N}^2 \to \mathbf{N}$ дефинисана на следећи начин:

$$\pi(m,n) = 2^m(2n+1) - 1$$

Докажимо да је овако дефинисана функција бијекција. Најпре ћемо доказати да је π ,,1-1" функција.

$$\begin{aligned}
\pi(m,n) = \pi(x,y) &\Rightarrow 2^m(2n+1) - 1 = 2^x(2y+1) - 1 \\
&\Rightarrow 2^m = 2^x \wedge 2n+1 = 2y+1 \\
&\Rightarrow m = x \wedge n = y \\
&\Rightarrow (m,n) = (x,y)
\end{aligned}$$

Докажимо сада да је π ,,на" функција.

$$\begin{aligned}
\pi(m,n) = x &\Rightarrow 2^m(2n+1) - 1 = x \\
&\Rightarrow 2^m(2n+1) = x+1 = 2^{(x+1)_1} \frac{x+1}{2^{(x+1)_1}} \\
&\Rightarrow m = (x+1)_1,\ n = \frac{1}{2}\left(\frac{x+1}{2^{(x+1)_1}} - 1\right)
\end{aligned}$$

Приметимо да $\frac{1}{2}\left(\frac{x+1}{2^{(x+1)_1}}-1\right) \in \mathbf{N}$. Важи:

$$\pi((x+1)_1, \frac{1}{2}\left(\frac{x+1}{2^{(x+1)_1}}-1\right)) = 2^{(x+1)_1}\left(2\frac{1}{2}\left(\frac{x+1}{2^{(x+1)_1}}-1\right)+1\right)-1 = x$$

па функција π јесте бијекција.

Даље, функција π је примитивно рекурзивна, као композиција примитивно рекурзивних функција. Она је онда и рекурзивна, одакле, на основу Черчове тезе, следи да је она израчунљива.

Докажимо сада да постоје функције $\pi_1, \pi_2 : \mathbf{N} \to \mathbf{N}$ такве да је $\pi^{-1}(x) = (\pi_1(x), \pi_2(x))$ и да су оне израчунљиве (довољно је доказати да су примитивно рекурзивне). Лако се проверава да функције:

$$\begin{aligned}
\pi_1(x) &= (x+1)_1 \\
\pi_2(x) &= \left[\frac{\left[\frac{x+1}{2^{(x+1)_1}}\right] \dot{-} 1}{2}\right]
\end{aligned}$$

задовољавају тражене услове.

Алтернативно, функције π_1 и π_2 се могу дефинисати и на следећи начин, користећи особину да је π бијекција и да $m, n \leq \pi(m,n)$ за све m, n $(m, n \in \mathbf{N})$:

$$\begin{aligned}
\pi_1(x) &= \mu(m \leq x)\left[(\exists_1 n)(0 \leq n \leq x \wedge \pi(m,n) = x)\right] \\
&= \mu(m < x+1)\left[\sum_{n=0}^{x} eq(\pi(m,n), x) = 1\right] \in \mathcal{PR} \\
\pi_2(x) &= \mu(n < x+1)\left[\sum_{m=0}^{x} eq(\pi(m,n), x) = 1\right] \in \mathcal{PR}
\end{aligned}$$

(ii) Нека је функција $\xi : \mathbf{N^+}^3 \to \mathbf{N}$ дефинисана на следећи начин:

$$\xi(m,n,p) = \pi(\pi(m-1, n-1), p-1)$$

Како је функција π примитивно рекурзивна и бијективна, следи да је и функција ξ примитивно рекурзивна и бијективна:

$$\begin{aligned}
\xi(m,n,p) = x &\Leftrightarrow \pi(\pi(m-1,n-1), p-1) = x \\
&\Leftrightarrow \pi(m-1, n-1) = \pi_1(x) \wedge p-1 = \pi_2(x) \\
&\Leftrightarrow m-1 = \pi_1(\pi_1(x)) \wedge n-1 = \pi_2(\pi_1(x)) \wedge p-1 = \pi_2(x) \\
&\Leftrightarrow \xi^{-1}(x) = (\pi_1(\pi_1(x))+1, \pi_2(\pi_1(x))+1, \pi_2(x)+1)
\end{aligned}$$

(*iii*) Сваки природан број x се јединствено може изразити у облику $x = \sum_{i=0}^{\infty} \alpha_i 2^i$, где је $\alpha_i \in \{0,1\}$ за све i ($i \in \mathbf{N}$). Одатле, сваки позитиван цео број x може се јединствено изразити у облику $x = 2^{b_1} + 2^{b_2} + \cdots + 2^{b_l}$, где $0 \leq b_1 < b_2 < \cdots < b_l$. Даље, следи да се сваки позитиван цео број x може јединствено изразити у облику $x = 2^{a_1} + 2^{a_1+a_2+1} + \cdots + 2^{a_1+a_2+\cdots+a_l+(l-1)}$, где $0 \leq a_i$, $1 \leq l$.

Користећи претходну идеју можемо дефинисати функцију $\tau : \bigcup_{k=1}^{\infty} \mathbf{N}^k \to \mathbf{N}$ на следећи начин:

$$\tau(a_1, a_2, \ldots, a_k) = 2^{a_1} + 2^{a_1+a_2+1} + \cdots + 2^{a_1+a_2+\cdots+a_k+k-1} - 1$$

Функције τ и τ^{-1} су бијективне и примитивно рекурзивне, одакле следи да је скуп $\bigcup_{k=1}^{\infty} \mathbf{N}^k$ ефективно набројив.

Напомена: За енумерацију (кодирање) коначних низова може се користити и неки други начин кодирања, на пример:

$$\tau(x_1, \ldots, x_n) = 2^{x_1} 3^{x_2} \cdots pn(n)^{x_n}$$

$\square$

3.4.2 Енумерација програма

Теорема 3.11 *Скуп $\mathcal{P}$ свих* URM *програма је ефективно набројив.*

Доказ:

Сваки URM програм састоји се од коначног низа инструкција из скупа $\mathcal{I}$.[23] Сваку инструкцију из тог низа могуће је погодно кодирати неким природним бројем, па онда тврђење следи на основу теореме 3.10 (део (*iii*)).

Дефинишимо функцију $\beta : \mathcal{I} \to \mathbf{N}$ на следећи начин:

$\beta(Z(n)) = 4(n \dot{-} 1)$

$\beta(S(n)) = 4(n \dot{-} 1) + 1$

$\beta(T(m,n)) = 4\pi(m \dot{-} 1, n \dot{-} 1) + 2$

$\beta(J(m,n,p)) = 4\xi(m,n,p) + 3$

Функција β је израчунљива, бијективна и за функцију β^{-1} важи (нека је $x = 4u + r$, $0 \leq r \leq 3$):

$\beta^{-1}(x) = Z(u+1)$, ако $r = 0$

$\beta^{-1}(x) = S(u+1)$, ако $r = 1$

$\beta^{-1}(x) = T(\pi_1(u)+1, \pi_2(u)+1)$, ако $r = 2$

$\beta^{-1}(x) = J(\pi_1(\pi_1(u))+1, \pi_2(\pi_1(u))+1, \pi_2(u)+1)$, ако $r = 3$

Дакле, и функција β^{-1} је израчунљива, па је скуп $\mathcal{I}$ ефективно набројив. На основу теореме 3.10 (део (*iii*)), следи да је и скуп $\bigcup_{k=1}^{\infty} \mathcal{I}^k$ ефективно набројив, тј. скуп $\mathcal{P}$ свих URM програма је ефективно набројив. Постоји више различитих одговарајућих бијекција (различитих

[23] $\mathcal{I}$ је скуп свих URM инструкција.

кодирања), али ми ћемо у даљем тексту користити следећу бијекцију $\gamma : \bigcup_{k=1}^{\infty} \mathcal{I}^k \to \mathbf{N}$:

$$\gamma(I_1, I_2, \ldots, I_k) = \tau(\beta(I_1), \beta(I_2), \ldots, \beta(I_k))$$

□

Дефиниција 3.21 *За* URM *програм* P *вредност* $\gamma(P)$ *називамо* индексом (кодним бројем) *програма* P *или* Геделовим бројем *програма* P*.*

Дефиниција 3.22 URM *програм* P *за који важи* $P = \gamma^{-1}(n)$ *називамо* n-тим URM програмом *и означавамо га са* P_n*.*

Напомена: За различите вредности m и n, програми P_m и P_n се разликују, али то не мора да значи да они израчунавају различите функције.

3.4.3 Енумерација израчунљивих функција

За $a \in \mathbf{N}$ и $n \geq 1$ уводимо следеће ознаке:

$$\begin{aligned} \Phi_a^{(n)} &= f_{P_a}^{(n)} = n\text{-арна функција коју израчунава програм } P_a \\ W_a^{(n)} &= \mathrm{Dom}(\Phi_a^{(n)}) = \{(x_1, x_2, \ldots, x_n) \mid P_a(x_1, \ldots, x_n) \downarrow\} \\ E_a^{(n)} &= \mathrm{Range}(\Phi_a^{(n)}) = \{\Phi_a^{(n)}(x_1, x_2, \ldots, x_n) \mid (x_1, x_2, \ldots, x_n) \in \mathrm{Dom}(\Phi_a^{(n)})\} \end{aligned}$$

Уколико експлицитно не нагласимо другачије сматрамо да је реч о *унарним* израчунљивим функцијама и уместо $\Phi_a^{(1)}$, $W_a^{(1)}$, $E_a^{(1)}$ пишемо краће Φ_a, W_a, E_a.

Свака унарна израчунљива функција појављује се у енумерацији $\Phi_0, \Phi_1, \Phi_2, \ldots$, при чему је то енумерација са понављањем (јер постоје различити програми који израчунавају исту функцију).

Све израчунљиве функције могу бити енумерисане и на другачији начин. Може се кренути од рекурзивних функција (уместо од URM програма). Оне могу бити енумерисане и та енумерација индукује и енумерацију израчунљивих функција (то је енумерација са понављањем као и у првом приступу).

Теорема 3.12 *Скуп свих n-арних израчунљивих функција $\mathcal{C}^{(n)}$ је набројив.*

Теорема 3.13 *Скуп свих израчунљивих функција $\mathcal{C}$ је набројив.*

Доказ:

$$\mathcal{C} = \bigcup_{n \geq 1} \mathcal{C}^{(n)}$$

Како је набројива унија набројивих скупова такође набројив скуп, следи да је скуп свих израчунљивих функција $\mathcal{C}$ набројив. □

Задатак 82 *Доказати да свака израчунљива функција има пребројиво много појављивања (пребројиво много индекса) у енумерацији свих израчунљивих функција.*

Решење:

Нека је функција f израчунљива. Тада, на основу тезе Черча, постоји (бар један) програм P који је израчунава. Функција f се, дакле, у енумерацији свих израчунљивих функција појављује на $\gamma(P)$-том месту (тј. $f = \Phi_a$, где је $a = \gamma(P)$).

Програму P можемо додати неку наредбу без дејства (нпр. $T(1,1)$). Тако измењени програм има различит кôд (тј. одговара му други индекс), али и даље израчунава исту функцију f. Понављајући овај поступак можемо да закључимо да функција f има бесконачно много индекса у низу свих израчунљивих функција (јер има бесконачно много програма који је израчунавају).

Индекси функције f чине, дакле, бесконачан подскуп скупа $\mathbf{N}$, па је и тај подскуп пребројив. Дакле, свака израчунљива функција f има пребројиво много индекса у низу свих израчунљивих функција.

Задатак 83 *Доказати да тоталних неизрачунљивих функција* $f : \mathbf{N} \to \mathbf{N}$ *има непребројиво много.*

Решење:

У општем случају за број пресликавања из скупа A у скуп B важи следећа једнакост:

$$|\{f \mid f : A \to B\}| = |B|^{|A|}$$

У случају тоталних функција $f : \mathbf{N} \to \mathbf{N}$, она се своди на:

$$|\{f \mid f : \mathbf{N} \to \mathbf{N}\}| = \aleph_0^{\aleph_0} = \mathcal{C}$$

Дакле, тоталних функција $f : \mathbf{N} \to \mathbf{N}$ има непребројиво много, па како тоталних *израчунљивих* функција $f : \mathbf{N} \to \mathbf{N}$ има пребројиво много, следи да тоталних *неизрачунљивих* функција $f : \mathbf{N} \to \mathbf{N}$ има непребројиво много.

3.4.4 Метод дијагонализације

Метод дијагонализације заснива се на идеји коју је Кантор[24] искористио у свом доказу да је скуп реалних бројева непребројив.

Метод дијагонализације користи се у проблемима следећег типа: *„Нека је $\phi_0, \phi_1, \ldots$ енумерација објеката неког типа. Потребно је конструисати објекат ϕ истог типа који се разликује од свих објеката $\phi_0, \phi_1, \ldots$".*

[24]Georg Cantor (1845-1918), немачки математичар руског порекла

Метод дијагонализације заснива се, генерално, на следећем приступу: *,,Нека се конструисани објекат ϕ разликује од ϕ_n на n-тој позицији (у неком смислу)".* Наведена општа схема има различите интерпретације у зависности од конкретног домена.

Задатак 84 *Доказати да постоји тотална унарна функција која није израчунљива.*

Решење:

Нека је функција $f : \mathbf{N} \to \mathbf{N}$ дефинисана на следећи начин:

$$f(n) = \begin{cases} \Phi_n(n) + 1 & \text{, ако је } \Phi_n(n) \text{ дефинисано (тј. ако } \Phi_n(n)\downarrow) \\ 0 & \text{, ако } \Phi_n(n) \text{ није дефинисано (тј. ако } \Phi_n(n)\uparrow) \end{cases}$$

Покажимо да се функција f разликује за свако n од функције Φ_n у тачки n. Ако је вредност $\Phi_n(n)$ дефинисана, онда је $f(n) = \Phi_n(n) + 1 \neq \Phi_n(n)$. Ако вредност $\Phi_n(n)$ није дефинисана, онда је функција f дефинисана у тачки n ($f(n) = 0$), па је $f \neq \Phi_n$.

Како се функција f разликује од свих унарних израчунљивих функција, онда се она не појављује у енумерацији $\mathcal{C}^{(1)}$, па она није израчунљива. С друге стране, на основу дефиниције функције f је очигледно да је она тотална.

Задатак 85 *Нека је $f : \mathbf{N}^2 \to \mathbf{N}$ тотална израчунљива функција. Нека је фамилија функција $g_n : \mathbf{N} \to \mathbf{N}$ ($n \in \mathbf{N}$) дефинисана на следећи начин:*

$$g_n(y) = f(n, y).$$

Конструисати тоталну израчунљиву функцију $h : \mathbf{N} \to \mathbf{N}$ такву да је $h \neq g_n$ за све n ($n \in \mathbf{N}$).

Решење:

Дефинишимо функцију $h : \mathbf{N} \to \mathbf{N}$ на следећи начин:

$$h(x) = f(x, x) + 1$$

Функција f је тотална и израчунљива, па је таква и функција h.

Докажимо да је $h \neq g_n$ за све n ($n \in \mathbf{N}$). Претпоставимо супротно — да важи $h = g_n$ за неко n ($n \in \mathbf{N}$). Тада:

$$\begin{aligned} h = g_n &\Rightarrow (\forall x) h(x) = g_n(x) \\ &\Rightarrow h(n) = g_n(n) \\ &\Rightarrow f(n, n) + 1 = f(n, n) \end{aligned}$$

што је противречност. Дакле, $h \neq g_n$ за све n ($n \in \mathbf{N}$).

Задатак 86 *Нека је $f_0, f_1, f_2, \ldots$ низ унарних парцијалних функција. Конструисати унарну парцијалну функцију g такву да је $\mathrm{Dom}(g) \neq \mathrm{Dom}(f_n)$ за све n $(n \in N)$.*

Решење:

Дефинишимо функцију $g : \mathbf{N} \to \mathbf{N}$ на следећи начин:[25]

$$g(x) \simeq \begin{cases} 0 & \text{, ако } x \notin \mathrm{Dom}(f_x) \text{ (тј. } f_x(x)\uparrow) \\ \uparrow & \text{, ако } x \in \mathrm{Dom}(f_x) \text{ (тј. } f_x(x)\downarrow) \end{cases}$$

Докажимо да $\mathrm{Dom}(g) \neq \mathrm{Dom}(f_n)$ важи за све n $(n \in \mathbf{N})$. Претпоставимо супротно — да за неко n $(n \in N)$ важи $\mathrm{Dom}(g) = \mathrm{Dom}(f_n)$.

Ако је $n \in \mathrm{Dom}(f_n)$, онда $g(n)\uparrow$, па је $n \notin \mathrm{Dom}(g)$, одакле следи $\mathrm{Dom}(g) \neq \mathrm{Dom}(f_n)$. Ако је $n \notin \mathrm{Dom}(f_n)$, онда је $g(n)\downarrow 0$, па $n \in \mathrm{Dom}(g)$, одакле следи $\mathrm{Dom}(g) \neq \mathrm{Dom}(f_n)$.

У оба случаја се добија да је $\mathrm{Dom}(g) \neq \mathrm{Dom}(f_n)$, што противречи претпоставци $\mathrm{Dom}(g) = \mathrm{Dom}(f_n)$. Дакле, важи $\mathrm{Dom}(g) \neq \mathrm{Dom}(f_n)$ за све n $(n \in N)$, што је и требало доказати.

Задатак 87 *Тотална унарна функција је монотоно растућа ако и само ако $f(n+1) > f(n)$ важи за све природне бројеве n. Доказати да монотоно растућих функција има непребројиво много.*

Решење:

Претпоставимо супротно — да монотоно растућих функција има највише пребројиво много. Нека је $f_0, f_1, f_2, \ldots$ енумерација свих монотоно растућих функција. Дефинишимо функцију $g : \mathbf{N} \to \mathbf{N}$ на следећи начин:

$$\begin{aligned} g(0) &= f_0(0) + 1 \\ g(n+1) &= f_{n+1}(n+1) + g(n) \end{aligned}$$

Докажимо да је овако дефинисана функција g монотоно растућа. За произвољан природан број n важи:

$$\begin{aligned} g(n+1) = & f_{n+1}(n+1) + g(n) \\ & \text{(на основу дефиниције функције } g) \\ > & g(n) \\ & \text{(јер је } f_{n+1} \geq 0 \text{ и } f_{n+1} \text{ је монотоно растућа функција)} \end{aligned}$$

Дакле, функција g јесте монотоно растућа. С друге стране, докажимо да се функција g не појављује у енумерацији свих монотоно растућих функција, тј. да $g(n) \neq f_n(n)$ за све природне бројеве n.

За $n = 0$ важи

$$g(0) = f_0(0) + 1 > f_0(0),$$

[25] Пишемо $f(x_1, \ldots, x_n) \simeq g(x_1, \ldots, x_n)$ ако су за n-торку $(x_1, \ldots, x_n)$ вредности функција f и g или обе недефинисане или обе дефинисане и имају исту вредност.

одакле следи да је $g \neq f_0$. Даље, за произвољан природан број n важи:

$$g(n+1) = f_{n+1}(n+1) + g(n) > f_{n+1}(n+1),$$

јер је $g(0) > 0$ и функција g је монотоно растућа, па је и $g(n) > 0$.

Дакле, $g(n) \neq f_n(n)$ за све природне бројеве n, што, због претпоставке да је $f_0, f_1, f_2, \ldots$ енумерација *свих* монотоно растућих функција, значи да функција g није монотоно растућа. То, међутим, противречи претходном закључку да она то јесте. Дакле, монотоно растућих функција има непребројиво много.

Задатак 88 *Нека је f унарна парцијална функција (не нужно израчунљива) и m дат природан број. Конструисати неизрачунљиву функцију $g : \mathbf{N} \to \mathbf{N}$ такву да важи:*

$$(\forall x \leq m) g(x) \simeq f(x).$$

Решење:

Дефинишимо функцију $g : \mathbf{N} \to \mathbf{N}$ на следећи начин:

$$g(x) \simeq \begin{cases} f(x) & \text{, ако } x \leq m \\ \Phi_{x-m-1}(x) + 1 & \text{, ако } x > m \text{ и } \Phi_{x-m-1}(x) \downarrow \\ 0 & \text{, ако } x > m \text{ и } \Phi_{x-m-1}(x) \uparrow \end{cases}$$

Из дефиниције функције g следи $(\forall x \leq m) g(x) \simeq f(x)$. Докажимо да функција g није израчунљива. Претпоставимо супротно — да функција g јесте израчунљива. Тада је $g = \Phi_n$ за неко n ($n \in \mathbf{N}$). Из $g = \Phi_n$ следи $g(m+n+1) \simeq \Phi_n(m+n+1)$. Приметимо да је $m+n+1 > m$. Користећи дефиницију функције g, ако $\Phi_n(m+n+1) \downarrow$, онда:

$$\begin{aligned} g(m+n+1) &= \Phi_{m+n+1-m-1}(m+n+1) + 1 \\ &= \Phi_n(m+n+1) + 1 \\ &\neq \Phi_n(m+n+1) \end{aligned}$$

а ако је $\Phi_n(m+n+1) \uparrow$, онда је $g(m+n+1) = 0$, па је $g(m+n+1) \neq \Phi_n(m+n+1)$. Дакле, у оба случаја следи да $g(m+n+1) \neq \Phi_n(m+n+1)$, што противречи претпоставци да $g = \Phi_n$. Према томе, не постоји вредност n ($n \in \mathbf{N}$) таква да је $g = \Phi_n$, тј. функција g се не појављује у енумерацији *свих* израчунљивих функција, што значи да она није израчунљива.

3.4.5 $s - m - n$ теорема

Нека је $f(x, y)$ израчунљива функција (не нужно тотална). Тада, за сваку фиксирану вредност a променљиве x, функција f представља неку унарну израчунљиву функцију g_a, тј.

$$g_a(y) \simeq f(a, y).$$

Функција g_a је израчунљива, па постоји индекс e такав да је $g_a = \Phi_e$ и, дакле, $\Phi_e(y) \simeq f(a, y)$.

Простији облик $s - m - n$ теореме тврди да тај индекс e може бити ефективно израчунат на основу a. Општи облик $s - m - n$ теореме представља одговарајуће уопштење тог тврђења.

Ова теорема се често назива и теоремом параметризације.

Теорема 3.14 ($s - m - n$) [26] *Ако је $f(x, y)$ израчунљива функција, онда постоји тотална израчунљива функција $k(x)$ таква да важи:*[27]

$$f(x, y) \simeq \Phi_{k(x)}(y).$$

Постојање функције k која је тотална и израчунљива и задовољава услов $f(x, y) \simeq \Phi_{k(x)}(y)$ доказује се помоћу UR машине која израчунава функцију f. Зато функција k зависи и од избора конкретног таквог програма P_e, па је $k(x) = s(e, x) = s_1^1(e, x)$.

Теорема 3.15 ($s - m - n$) [28] *За било које вредности m, n ($m, n \in \mathbf{N}$) такве да је $m, n \geq 1$, постоји тотална израчунљива функција*

$$s_n^m(e, x_1, x_2, \ldots, x_m)$$

(арности $m + 1$) таква да важи:[29]

$$\Phi_e^{(m+n)}(x_1, x_2, \ldots x_m, y_1, y_2, \ldots, y_n) \simeq \Phi^{(n)}_{s_n^m(e, x_1, x_2, \ldots, x_m)}(y_1, y_2, \ldots, y_n).$$

Наведену теорему називамо $s - m - n$ теоремом због нотације s_n^m. Исто називамо и њен простији облик.

Задатак 89 *Доказати да постоји тотална израчунљива функција k : $\mathbf{N} \to \mathbf{N}$ таква да је за сваку вредност x ($x \in \mathbf{N}$), вредност функције $k(x)$ једнака индексу функције $f(x, y) = \left[\sqrt[x]{y}\right]$.*

Решење:

Сходно задатку 65 и теореми 3.7, важи:

$$f(x, y) \in \mathcal{PR}^{(2)} \subset \mathcal{R}^{(2)}$$

па се она јавља у енумерацији свих бинарних израчунљивих функција, тј. важи:

$$(\exists e \in \mathbf{N}) f(x, y) \simeq \Phi_e^{(2)}(x, y).$$

[26] Простији облик $s - m - n$ теореме.
[27] Доказ теореме се може наћи у [4].
[28] Општи облик $s - m - n$ теореме.
[29] Доказ теореме се може наћи у [4, 5].

Фиксирајмо једну такву вредност за e. На основу $s-m-n$ теореме, постоји тотална, израчунљива функција $s : \mathbf{N}^2 \to \mathbf{N}$ таква да важи:

$$\Phi_e^{(2)}(x,y) \simeq \Phi_{s(e,x)}(y).$$

За изабрано, фиксирано e, дефинишимо тражену функцију k као $k(x) \simeq s(e,x)$. Тада:

$$[\sqrt[x]{y}] \simeq \Phi_{k(x)}(y).$$

Задатак 90 *Доказати да постоји тотална израчунљива функција* $k : \mathbf{N} \to \mathbf{N}$ *таква да за сваку вредност* x *(*$x \in \mathbf{N}$*) важи*

$$W_{k(x)} = \{y^x \mid y \in \mathbf{N}\}.$$

Решење:

Дефинишимо функцију $f : \mathbf{N}^2 \to \mathbf{N}$ на следећи начин:

$$f(x,y) = \mu z[z^x = y].$$

Важи $f \in \mathcal{R}^2$, па постоји индекс e такав да је $f(x,y) \simeq \Phi_e^{(2)}(x,y)$. Фиксирајмо један такав индекс e. На основу $s-m-n$ теореме је

$$\Phi_e^{(2)}(x,y) \simeq \Phi_{k(x)}(y),$$

где је $k(x)$ тотална израчунљива функција. Дакле, важи

$$f(x,y) \simeq \Phi_{k(x)}(y),$$

па је

$$\begin{aligned} y \in W_{k(x)} &\Leftrightarrow \Phi_{k(x)}(y) \downarrow \\ &\Leftrightarrow f(x,y) \downarrow \\ &\Leftrightarrow (\exists z \in \mathbf{N})\ y = z^x \\ &\Rightarrow W_{k(x)} = \{z^x \mid z \in \mathbf{N}\} \end{aligned}$$

Задатак 91 *Нека је* $n \geq 1$. *Доказати да постоји тотална израчунљива функција* $k : \mathbf{N} \to \mathbf{N}$ *таква да важи*

$$W_{k(x)}^{(n)} = \{(y_1, \ldots, y_n) \mid \sum_{i=1}^{n} y_i = x\}.$$

Решење:

Дефинишимо функцију $f : \mathbf{N}^{n+1} \to \mathbf{N}$ на следећи начин:

$$f(x, y_1, \ldots, y_n) = \begin{cases} 0 & , \text{ако } \sum_{i=1}^{n} y_i = x \\ \uparrow & , \text{иначе} \end{cases}$$

Предикат $P(x, y_1, \ldots, y_n)$ дефинисан са:

$$P(x, y_1, \ldots, y_n) \Leftrightarrow \sum_{i=1}^{n} y_i = x$$

је одлучив, јер је израчунљива његова карактеристична функција:

$$C_P(x, y_1, \ldots, y_n) = \overline{sgn}(|\sum_{i=1}^{n} y_i \dot{-} x|) \in \mathcal{PR},$$

па је функција f израчунљива. Дакле, постоји (бар један) индекс e такав да је

$$f(x, y_1, \ldots, y_n) \simeq \Phi_e^{(n+1)}(x, y_1, \ldots, y_n).$$

Фиксирајмо један такав индекс e. На основу $s - m - n$ теореме важи

$$\Phi_e^{(n+1)}(x, y_1, \ldots, y_n) \simeq \Phi_{s(e,x)}^{(n)}(y_1, \ldots, y_n).$$

За фиксирану вредност e је $k(x) = s(e, x)$, па је

$$f(x, y_1, \ldots, y_n) \simeq \Phi_{k(x)}^{(n)}(y_1, \ldots, y_n).$$

Како важи низ еквиваленција:

$$\begin{aligned} (y_1, \ldots, y_n) \in W_{k(x)}^{(n)} &\Leftrightarrow \Phi_{k(x)}^{(n)}(y_1, \ldots, y_n) \downarrow \\ &\Leftrightarrow f(x, y_1, \ldots, y_n) \downarrow \\ &\Leftrightarrow \sum_{i=1}^{n} y_i = x \end{aligned}$$

на основу дефиниције једнакости скупова, важи:

$$W_{k(x)}^{(n)} = \{(y_1, \ldots, y_n) \mid \sum_{i=1}^{n} y_i = x\}$$

што је и требало показати.

3.5 Универзалне функције

Дефиниција 3.23 *Парцијална функција* $g : \mathbf{N}^{n+1} \to \mathbf{N}$ *је* универзална функција *за фамилију* $\mathcal{F}$ *n-арних парцијалних функција ако и само ако:*

(*i*) $(\forall i \in \mathbf{N})\ g(i, x_1, \ldots, x_n) \in \mathcal{F}$

(*ii*) $(\forall f \in \mathcal{F})(\exists i \in \mathbf{N})(\forall x_1, \ldots, x_n \in \mathbf{N})\ f(x_1, \ldots, x_n) \simeq g(i, x_1, \ldots, x_n)$

(тј. све функције из фамилије $\mathcal{F}$ могу да буду поређане у низ $g(0, x_1, \ldots, x_n)$, $g(1, x_1, \ldots, x_n)$, $g(2, x_1, \ldots, x_n)$, ...).

Напомена: Дефиниција универзалне функције за дату фамилију зависи од начина индексирања фамилије. Промена начина индексирања, у општем случају, имплицира промену дефиниције универзалне функције.

Ако је $i : \mathcal{F} \to \mathbf{N}$ нека енумерација фамилије $\mathcal{F}$, онда је функција $g : \mathbf{N}^{n+1} \to \mathbf{N}$ дефинисана на следећи начин:

$$g(i, x_1, \ldots, x_n) \simeq f_i(x_1, \ldots, x_n)$$

универзална за фамилију $\mathcal{F}$.

Дакле, функција $\Psi_U^{(n)} : \mathbf{N}^{n+1} \to \mathbf{N}$ дефинисана са

$$\Psi_U^{(n)}(e, x_1, \ldots, x_n) \simeq \Phi_e^{(n)}(x_1, \ldots, x_n)$$

је *универзална функција за класу n-арних израчунљивих функција.*

Уместо $\Psi_U^{(1)}$ писаћемо краће Ψ_U мислећи на *унарне* израчунљиве функције, уколико не нагласимо другачије.

Теорема 3.16 *За сваки природан број n, функција $\Psi_U^{(n)}$ је израчунљива.*[30]

Универзалне функције имају следеће важне примене:

- конструкција неизрачунљивих функција и неодлучивих предиката;
- конструкција тоталне израчунљиве функције која није примитивно рекурзивна;
- са $s - m - n$ теоремом у доказима да су одређене операције над индексима израчунљивих функција израчунљиве.

Задатак 92 *Доказати да универзална функција за класу $\mathcal{T}$ тоталних унарних израчунљивих функција није тотална израчунљива функција.*

Решење:

Нека је $g : \mathbf{N}^2 \to \mathbf{N}$ универзална функција за фамилију функција $\mathcal{T}$. Претпоставимо супротно — да функција g јесте тотална и израчунљива. Дефинишимо функцију $h : \mathbf{N} \to \mathbf{N}$ на следећи начин:

$$h(n) = g(n, n) + 1$$

[30] Доказ теореме се може наћи у [4].

Како је функција g тотална израчунљива функција, то је и унарна функција h тотална и израчунљива (тј. $h \in \mathcal{T}$). Одатле следи да постоји индекс m такав да важи

$$(\forall n) h(n) = g(m, n).$$

За ту, фиксирану, вредност m важи:

$$g(m, m) = h(m),$$

што противречи дефиницији функције h, на основу које је

$$h(m) = g(m, m) + 1.$$

Дакле, функција g није тотална израчунљива функција.

Задатак 93 *Доказати да универзална функција за класу $\mathcal{PR}^{(1)}$ није примитивно рекурзивна функција.*

Задатак 94 *Доказати да скуп $M = \{x \mid \Psi_U(x, x) = 0\}$ није одлучив.*

Решење:

Претпоставимо супротно — да скуп M јесте одлучив. Тада је карактеристична функција C_M скупа M израчунљива:

$$C_M(x) = \begin{cases} 1 & \text{, ако } x \in M \\ 0 & \text{, ако } x \notin M \end{cases}$$

Функција C_M је израчунљива, па постоји индекс m такав да је

$$(\forall x \in \mathbf{N})\ C_M(x) = \Psi_U(m, x)$$

За ту, фиксирану, вредност m важи

$$\begin{aligned} \Psi_U(m, m) = 1 &\Leftrightarrow C_M(m) = 1 \\ &\Leftrightarrow m \in M \\ &\Leftrightarrow \Psi_U(m, m) = 0 \end{aligned}$$

што је противречно. Дакле, скуп M није одлучив.

Задатак 95 *Проблем „Φ_x је тотална” није одлучив.*

Решење:

Претпоставимо супротно — да предикат „Φ_x је тотална” јесте одлучив. Нека је $g : \mathbf{N} \to \mathbf{N}$ карактеристична функција тог предиката:

$$g(x) = \begin{cases} 1 & \text{, ако је } \Phi_x \text{ тотална} \\ 0 & \text{, ако } \Phi_x \text{ није тотална} \end{cases}$$

Како је предикат одлучив, функција g је израчунљива.

Дефинишимо функцију $f : \mathbf{N} \to \mathbf{N}$ тако да се разликује од свих тоталних израчунљивих функција:

$$f(x) = \begin{cases} \Phi_x(x) + 1 & \text{, ако је } \Phi_x \text{ тотална} \\ 0 & \text{, ако } \Phi_x \text{ није тотална} \end{cases}$$

Функција f је тотална и разликује се (на x-тој позицији) од сваке тоталне израчунљиве функције, па следи да она није израчунљива.

Функције f може се, еквивалентно, дефинисати и на следећи начин:

$$f(x) = \begin{cases} \Psi_U(x,x) + 1 & \text{, ако } g(x) = 1 \\ 0 & \text{, ако } g(x) = 0 \end{cases}$$

Како су функције Ψ_U и g израчунљиве, следи да је таква и функција f, што противречи претходном закључку. Дакле, проблем ,,Φ_x је тотална" није одлучив.

Задатак 96 *Нека је фамилија функција $\mathcal{F}^{(n)}$ задата на следећи начин:*

$$f_i^{(n)}(x_1, x_2, \ldots, x_n) = x_1 + x_2 + \cdots + x_n + i.$$

Наћи у $\mathcal{F}^{(n+1)}$ универзалну функцију за $\mathcal{F}^{(n)}$.

Решење:

Фамилија $\mathcal{F}^{(n+1)}$ је задата на следећи начин:

$$f_i^{(n+1)}(x_1, \ldots, x_{n+1}) = x_1 + \cdots + x_{n+1} + i$$

Приметимо да за функцију

$$f_0^{(n+1)}(x_1, \ldots, x_{n+1}) = x_1 + \cdots + x_{n+1}$$

из те фамилије важи:

$$f_0^{(n+1)}(i, x_1, \ldots, x_n) = i + x_1 + \cdots + x_n = f_i^{(n)}(x_1, \ldots, x_n)$$

па је управо она тражена универзална функција.

3.5.1 Примене $s - m - n$ теореме

Задатак 97 *Доказати да постоји тотална израчунљива функција $s : \mathbf{N}^2 \to \mathbf{N}$ таква да за све x, y ($x, y \in \mathbf{N}$) важи:*

$$\Phi_{s(x,y)} = \Phi_x \cdot \Phi_y$$

Решење:

Дефинишимо функцију $f : \mathbf{N}^3 \to \mathbf{N}$ на следећи начин:

$$f(x, y, z) \simeq \Phi_x(z) \cdot \Phi_y(z)$$

Тада важи

$$\begin{aligned} f(x, y, z) &\simeq \Phi_x(z) \cdot \Phi_y(z) \\ &\simeq \psi_U(x, z) \cdot \psi_U(y, z) \\ &\simeq Sub(\cdot; Sub(\psi_U; P_1^3, P_3^3), Sub(\psi_U; P_2^3, P_3^3)), \end{aligned}$$

па је функција f израчунљива (као композиција израчунљивих функција). Дакле, постоји вредност e ($e \in \mathbf{N}$) таква да за све природне бројеве x, y, z важи:

$$f(x, y, z) \simeq \Phi_e^{(3)}(x, y, z)$$

За ту, фиксирану, вредност e, на основу $s - m - n$ теореме, постоји тотална израчунљива функција $s : \mathbf{N}^2 \to \mathbf{N}$ таква да важи $\Phi_e(x, y, z) \simeq \Phi_{s(x,y)}(z)$ (функција s зависи и од вредности e, али за фиксирано e, можемо је сматрати функцијом од само две променљиве — x и y). Тада важи:

$$f(x, y, z) \simeq \Phi_{s(x,y)}(z)$$

Дакле,

$$\Phi_{s(x,y)}(z) \simeq \Phi_x(z) \cdot \Phi_y(z),$$

где је $s : \mathbf{N}^2 \to \mathbf{N}$ тотална израчунљива функција.

Задатак 98 *Доказати да постоји тотална израчунљива функција g : $\mathbf{N} \to \mathbf{N}$ таква да за све вредности x ($x \in \mathbf{N}$) важи:*

$$(\Phi_x)^2 = \Phi_{g(x)}$$

Решење:

Нека је $s : \mathbf{N}^2 \to \mathbf{N}$ функција која за све природне бројеве x, y, z задовољава услов:

$$\Phi_{s(x,y)}(z) \simeq \Phi_x(z) \cdot \Phi_y(z) \ \text{(видети задатак 97)}$$

Дефинишимо функцију g на следећи начин:

$$g(x) = s(x, x)$$

Тада важи:

$$\Phi_{g(x)} = \Phi_{s(x,x)} = \Phi_x \cdot \Phi_x = (\Phi_x)^2$$

Задатак 99 *Доказати да постоји тотална израчунљива функција* $s : \mathbf{N}^2 \to \mathbf{N}$ *таква да за све вредности* x, y $(x, y \in \mathbf{N})$ *важи:*

$$\Phi_{s(x,y)} = Sub(\Phi_x; \Phi_y) = \Phi_x \circ \Phi_y$$

Решење:

Дефинишимо функцију $f : \mathbf{N}^3 \to \mathbf{N}$ на следећи начин:

$$f(x, y, z) \simeq \Phi_x(\Phi_y(z)) \simeq \psi_U(x, \psi_U(y, z)) \simeq Sub(\psi_U; P_1^3, Sub(\Psi_U; P_2^3, P_3^3))$$

Функција f је израчунљива (као композиција израчунљивих функција), па на основу $s-m-n$ теореме, постоји тотална израчунљива функција $s : \mathbf{N}^2 \to \mathbf{N}$ таква да за све природне бројеве x, y, z важи:

$$f(x, y, z) \simeq \Phi_{s(x,y)}(z)$$

Дакле, важи

$$\Phi_{s(x,y)} = \Phi_x \circ \Phi_y,$$

где је $s(x, y)$ тотална израчунљива функција.

Задатак 100 *Доказати да постоји израчунљива функција* $g : \mathbf{N}^2 \to \mathbf{N}$ *која задовољава следеће услове:*

(i) *Вредност* $g(x, y)$ *је дефинисана ако и само ако је* $y \in E_x$.

(ii) *Ако важи* $y \in E_x$, *онда је* $g(x, y) \in W_x$ *и* $\Phi_x(g(x, y)) = y$ *(тј.* $g(x, y) \in \Phi^{-1}(\{y\})$*).*

Ако је функција Φ_x *инјективна, доказати да постоји тотална израчунљива функција* $k : \mathbf{N} \to \mathbf{N}$ *таква да је* $\Phi_{k(x)} = \Phi_x^{-1}$ *и* $E_{k(x)} = W_x$.

Теорема 3.17 *За сваки природан број* n, *следећи предикати су одлучиви:*

(i) $S_n(e, x_1, \ldots, x_n, y, t) \equiv$ *„*$P_e(x_1, \ldots, x_n) \downarrow y$ *за* $\leq t$ *корака"*

(ii) $H_n(e, x_1, \ldots, x_n, t) \equiv$ *„*$P_e(x_1, \ldots, x_n) \downarrow$ *за* $\leq t$ *корака"* [31]

Напомена: Важи и јаче тврђење — да су наведени предикати *примитивно* рекурзивни.

Напоменимо да у даљем тексту нећемо писати индекс n предиката S_n и H_n када је он јасан из контекста.

Задатак 101 *Доказати да постоји тотална израчунљива функција* $s : \mathbf{N}^2 \to \mathbf{N}$ *таква да за све вредности* x, y $(x, y \in \mathbf{N})$ *важи*

$$W_{s(x,y)} = W_x \cup W_y.$$

[31] Доказ теореме се може наћи у [4].

Решење:

Дефинишимо функцију $f : \mathbf{N}^3 \to \mathbf{N}$ на следећи начин:

$$f(x,y,z) \simeq \begin{cases} 1 & \text{, ако } z \in W_x \text{ или } z \in W_y \\ \uparrow & \text{, иначе} \end{cases}$$

Тада важи:

$$\begin{aligned} f(x,y,z) &\simeq s(\mathbf{0}(\mu t[H(x,z,t) \vee H(y,z,t)])) \\ &\simeq \mathbf{1}(\mu t[H(x,z,t) \vee H(y,z,t)]). \end{aligned}$$

Предикати $H(x,z,t)$ и $H(y,z,t)$ су одлучиви, па је функција f израчунљива. На основу $s-m-n$ теореме, постоји тотална израчунљива функција $s : \mathbf{N}^2 \to \mathbf{N}$ таква да је

$$f(x,y,z) \simeq \Phi_{s(x,y)}(z).$$

Одатле, на основу дефиниције функције f, следи

$$W_{s(x,y)} = W_x \cup W_y.$$

Израчунљивост функције f може да се покаже и коришћењем Черчове тезе. Наиме, функција Ψ_U је израчунљива, па постоји алгоритам, тј. URM програм који је израчунава. Нека се на двема UR машинама симултано извршава дати програм за низ улазних вредности x,z, односно y,z. Ако се на некој од ове две машине стане са извршавањем програма, онда нека је $f(x,y,z) = 1$, а иначе нека је $f(x,y,z)$ недефинисано. На основу Черчове тезе следи да је функција f израчунљива.

Задатак 102 *Доказати да постоји тотална израчунљива функција* $s : \mathbf{N}^2 \to \mathbf{N}$ *таква да за све вредности* x, y $(x, y \in \mathbf{N})$ *важи*

$$E_{s(x,y)} = E_x \cup E_y.$$

Решење:

Дефинишимо функцију $f : \mathbf{N}^3 \to \mathbf{N}$ на следећи начин:

$$f(x,y,z) \simeq \begin{cases} z & \text{, ако } (\exists n)(\Phi_x(n) = z \vee \Phi_y(n) = z) \\ \uparrow & \text{, иначе} \end{cases}$$

Важи

$$\begin{aligned} & (\exists n)(\Phi_x(n) = z \vee \Phi_y(n) = z) \\ \Leftrightarrow & (\exists n,t)(\Phi_x(n) \downarrow z \text{ за } \leq t \text{ корака} \vee \Phi_x(n) \downarrow z \text{ за } \leq t \text{ корака} \\ \Leftrightarrow & (\exists n,t)(S(x,n,z,t) \vee S(y,n,z,t)) \\ \Leftrightarrow & (\exists n,t)\ Q(x,y,z,n,t) \\ & \text{(овако уводимо предикат } Q\text{, који је одлучив као} \\ & \text{дисјункција одлучивих предиката)} \\ \Leftrightarrow & (\exists m)\ Q(x,y,z,(m)_1,(m)_2) \end{aligned}$$

За функцију f важи

$$f(x,y,z) \simeq z \cdot \mathbf{1}(\mu m[Q(x,y,z,(m)_1,(m)_2)=1]),$$

па је она израчунљива. Одатле, на основу $s-m-n$ теореме, постоји тотална израчунљива функција $s : \mathbf{N}^2 \to \mathbf{N}$ таква да важи:

$$f(x,y,z) \simeq \Phi_{s(x,y)}(z),$$

одакле следи

$$\begin{aligned} E_{s(x,y)} &= \{f(x,y,z) | (x,y,z) \in \mathrm{Dom}(f)\} \\ &= \{z | (\exists n)(z = \Phi_x(n) \vee z = \Phi_y(n))\} \\ &= \{z | z \in E_x \vee z \in E_y\} \\ &= E_x \cup E_y \end{aligned}$$

Задатак 103 *Доказати да постоје тоталне израчунљиве функције* $f, g : \mathbf{N} \to \mathbf{N}$ *такве да важи:*

(а) $E_{f(x)} = W_x$

(б) $W_{g(x)} = E_x$

Решење:

(а) Дефинишимо функцију $\phi : \mathbf{N}^2 \to \mathbf{N}$ на следећи начин:

$$\phi(x,y) \simeq \begin{cases} y & \text{, ако } y \in W_x \\ \uparrow & \text{, иначе} \end{cases}$$

За функцију ϕ важи

$$\phi(x,y) \simeq y \cdot \mathbf{1}(\Psi_U(x,y)),$$

па је она израчунљива. На основу $s-m-n$ теореме, постоји тотална израчунљива функција $f : \mathbf{N} \to \mathbf{N}$ таква да важи:

$$\phi(x,y) \simeq \Phi_{f(x)}(y).$$

Тада је

$$\begin{aligned} E_{f(x)} &= \{\Phi_{f(x)}(y) \mid y \in W_{f(x)}\} \\ &= \{\phi(x,y) \mid (x,y) \in \mathrm{Dom}(\phi)\} \\ &= \{y \mid y \in W_x\} \\ &= W_x \end{aligned}$$

(б) Дефинишимо функцију $\phi : \mathbf{N}^2 \to \mathbf{N}$ на следећи начин:

$$\phi(x,y) \simeq \begin{cases} 1 & \text{, ако } y \in E_x \\ \uparrow & \text{, иначе} \end{cases}$$

Важи

$$\begin{aligned} y \in E_x \Leftrightarrow & (\exists n,t)(P_x(n) \downarrow y \text{ за } \leq t \text{ корака}) \\ \Leftrightarrow & (\exists n,t) S(x,n,y,t) \\ \Leftrightarrow & (\exists m) S(x,(m)_1,y,(m)_2) \\ \Leftrightarrow & (\exists m) Q(x,y,m) \\ & \text{(овако уводимо предикат } Q\text{, који је одлучив)} \end{aligned}$$

За функцију ϕ важи

$$\phi(x,y) \simeq \mathbf{1}(\mu z[Q(x,y,z)]),$$

па је она израчунљива. На основу $s-m-n$ теореме, постоји тотална израчунљива функција $g : \mathbf{N} \to \mathbf{N}$ таква да важи:

$$\phi(x,y) \simeq \Phi_{g(x)}(y).$$

Тада је

$$W_{g(x)} = \{y \mid \phi(x,y)\downarrow\} = \{y \mid y \in E_x\} = E_x$$

Задатак 104 *Нека је $f : \mathbf{N} \to \mathbf{N}$ израчунљива функција. Доказати да постоји израчунљива функција $k : \mathbf{N} \to \mathbf{N}$ таква да важи*

$$W_{k(x)} = f^{-1}(W_x)$$

Задатак 105 *Доказати да постоје тоталне израчунљиве функције $f, g : \mathbf{N} \to \mathbf{N}$ такве да важи:*

(а) $\Phi_i(W_j) = W_{f(i,j)}$

(б) $\Phi_i^{-1}(W_j) = W_{g(i,j)}$

3.6 Одлучивост, неодлучивост, парцијална одлучивост

3.6.1 Одлучивост и неодлучивост

Појам одлучивости за скупове и теорије заснива се на појму одлучивих предиката (проблема). Стога, поново наводимо следећу дефиницију:

Дефиниција 3.24 *Предикат $P(x_1, \ldots, x_n)$ је* одлучив *(*рекурзиван, израчунљив*) ако и само ако је израчунљива његова карактеристична функција C_P дата са:*

$$C_P(x_1, \ldots, x_n) = \begin{cases} 1 & , \textit{ако } P(x_1, \ldots, x_n) \\ 0 & , \textit{ако } \neg P(x_1, \ldots, x_n) \end{cases}$$

Дефиниција 3.25 *Предикат P је* неодлучив *ако и само ако није одлучив.*

Теорема 3.18 *Проблем „$x \in W_x$" (тј. „$\Phi_x(x)$ је дефинисано", „$\Psi_U(x,x)$ је дефинисано", „$P_x(x)\downarrow$") је неодлучив.*

Доказ:

Нека је $f : \mathbf{N} \to \mathbf{N}$ карактеристична функција овог проблема, тј. нека је

$$f(x) = \begin{cases} 1 & , \text{ако } x \in W_x \\ 0 & , \text{ако } x \notin W_x \end{cases}$$

Претпоставимо супротно — да проблем „$x \in W_x$" јесте одлучив. Одатле следи да је функција f израчунљива. Дефинишимо функцију $g : \mathbf{N} \to \mathbf{N}$ на следећи начин:

$$g(x) \simeq \begin{cases} 0 & , \text{ако } x \notin W_x \text{ (тј. } f(x) = 0) \\ \uparrow & , \text{ако } x \in W_x \text{ (тј. } f(x) = 1) \end{cases}$$

Важи $g(x) = \mathbf{0}(\mu y[f(x) = 0])$, па како је функција f израчунљива, израчунљива је и функција g. Дакле, постоји вредност m ($m \in \mathbf{N}$) таква да је $g = \Phi_m$, па, према томе, и $\mathrm{Dom}(g) = W_m$. Отуда, $m \in W_m \Leftrightarrow m \in \mathrm{Dom}(g)$. С друге стране, на основу дефиниције функције g, следи $m \in \mathrm{Dom}(g) \Leftrightarrow m \notin W_m$, што противречи претходном закључку. Дакле, проблем „$x \in W_x$" је неодлучив. □

Напомена: Наведена теорема не тврди да ни за коју конкретну вредност a не можемо да утврдимо да ли јесте или није дефинисана вредност $\Phi_a(a)$. За неке вредности то је веома једноставно (нпр. ако је Φ_e нека тотална функција, онда $e \in W_e$ свакако важи). Наведена теорема тврди да не постоји *општи метод* за утврђивање да ли је вредност $\Phi_x(x)$ дефинисана и који се може применити за *све* вредности x ($x \in \mathbf{N}$).

Наведена теорема важна је због тога што се неодлучивост за многе проблеме може доказати њиховим свођењем на проблем „$x \in W_x$". Генерално, неодлучивост проблема најчешће се доказује или свођењем на проблем „$x \in W_x$" или директном дијагоналном конструкцијом.

Задатак 106 *Доказати да постоји израчунљива функција $h : \mathbf{N} \to \mathbf{N}$ таква да су проблеми „$x \in \mathrm{Dom}(h)$" и „$x \in \mathrm{Range}(h)$" неодлучиви.*

Решење:

Дефинишимо функцију h на следећи начин:

$$h(x) \simeq \begin{cases} x & , \text{ако } x \in W_x \\ \uparrow & , \text{ако } x \notin W_x \end{cases}$$

За функцију h важи

$$h(x) \simeq x + \mathbf{0}(\Psi_U(x,x)),$$

па је она израчунљива (као композиција израчунљивих функција). Такође важи следећи низ еквиваленција:

$$\begin{aligned} x \in \mathrm{Dom}(h) \Leftrightarrow & x \in W_x \\ \Leftrightarrow & x \in \mathrm{Range}(h) \end{aligned}$$

па како предикат „$x \in W_x$" није одлучив, следи да ни њему еквивалентни предикати „$x \in \mathrm{Dom}(h)$" и „$x \in \mathrm{Range}(h)$" нису одлучиви. Значи, функција h задовољава услове задатка.

Задатак 107 *Доказати да је неодлучив проблем „$y \in W_x$".*[32]

Решење:

Нека је $g : \mathbf{N}^2 \to \mathbf{N}$ карактеристична функција датог проблема, тј. нека је:

$$g(x,y) = \begin{cases} 1 & , \text{ако } y \in W_x \\ 0 & , \text{ако } y \notin W_x \end{cases}$$

Претпоставимо супротно — да проблем „$y \in W_x$" јесте одлучив. То значи да је функција g израчунљива. Дефинишимо функцију $f : \mathbf{N} \to \mathbf{N}$ на следећи начин:

$$f(x) = g(x,x)$$

Како је функција g израчунљива, следи да је и функција f израчунљива. За функцију f важи:

$$f(x) = \begin{cases} 1 & , \text{ако } g(x,x) = 1 \text{ (тј. } x \in W_x) \\ 0 & , \text{ако } g(x,x) = 0 \text{ (тј. } x \notin W_x) \end{cases}$$

одакле следи да је предикат „$x \in W_x$" одлучив, што је нетачно. Дакле, проблем „$y \in W_x$" је неодлучив.

Задатак 108 *Доказати да су следећи проблеми неодлучиви:*

(а) „$\Phi_x = \mathbf{0}$"

(б) „$\Phi_x = \Phi_y$"

[32] Овај проблем називамо *проблемом заустављања* (енгл. *halting problem*).

Решење:

(а) Дефинишимо функцију $f : \mathbf{N}^2 \to \mathbf{N}$ на следећи начин:

$$f(x,y) \simeq \begin{cases} 0 & \text{, ако } x \in W_x \\ \uparrow & \text{, ако } x \notin W_x \end{cases}$$

За функцију f важи

$$f(x,y) \simeq \mathbf{0}(\Psi_U(x,x))$$

па је она израчунљива (као композиција израчунљивих функција). На основу $s-m-n$ теореме, постоји тотална израчунљива функција $k : \mathbf{N} \to \mathbf{N}$ таква да важи:

$$f(x,y) \simeq \Phi_{k(x)}(y)$$

Приметимо да важи $\Phi_{k(x)} = \mathbf{0}$ ако и само ако је $x \in W_x$. Даље, нека је $g : \mathbf{N} \to \mathbf{N}$ карактеристична функција проблема „$\Phi_x = \mathbf{0}$", тј. нека је:

$$g(x) = \begin{cases} 1 & \text{, ако } \Phi_x = \mathbf{0} \\ 0 & \text{, ако } \Phi_x \neq \mathbf{0} \end{cases}$$

Претпоставимо супротно — претпоставимо да предикат „$\Phi_x = \mathbf{0}$" јесте одлучив. Онда је функција g израчунљива. Дефинишимо функцију $h : \mathbf{N} \to \mathbf{N}$ на следећи начин:

$$h(x) = g(k(x)) = Sub(g;k)$$

Функција h је израчунљива (као композиција израчунљивих функција) и притом важи:

$$h(x) = \begin{cases} 1 & \text{, ако } g(k(x)) = 1 \text{ (тј. } \Phi_{k(x)} = \mathbf{0}\text{, односно } x \in W_x) \\ 0 & \text{, ако } g(k(x)) = 0 \text{ (тј. } \Phi_{k(x)} \neq \mathbf{0}\text{, односно } x \notin W_x) \end{cases}$$

Дакле, израчунљива функција h је карактеристична функција предиката „$x \in W_x$", што противречи чињеници да проблем „$x \in W_x$" није одлучив. Дакле, проблем „$\Phi_x = \mathbf{0}$" је неодлучив.

(б) Нека је $f : \mathbf{N}^2 \to \mathbf{N}$ карактеристична функција датог проблема:

$$f(x,y) = \begin{cases} 1 & \text{, ако } \Phi_x = \Phi_y \\ 0 & \text{, ако } \Phi_x \neq \Phi_y \end{cases}$$

Претпоставимо супротно — предикат „$\Phi_x = \Phi_y$" јесте одлучив. Одатле следи да је функција f израчунљива.

Нека је вредност e таква да је $\Phi_e = \mathbf{0}$. Дефинишимо функцију $g : \mathbf{N} \to \mathbf{N}$ на следећи начин:

$$g(x) = f(x,e)$$

Функција f је израчунљива, па је израчунљива и функција g. С друге стране, за функцију g важи:

$$g(x) = \begin{cases} 1 & \text{, ако } f(x,e) = 1 \text{ (тј. } \Phi_x = \Phi_e = \mathbf{0}) \\ 0 & \text{, ако } f(x,e) = 0 \text{ (тј. } \Phi_x \neq \Phi_e = \mathbf{0}) \end{cases}$$

Како је функција g израчунљива, следи да је предикат „$\Phi_x = \mathbf{0}$" одлучив, што противречи тврђењу доказаном у делу задатка под (а). Дакле, проблем „$\Phi_x = \Phi_y$" је неодлучив.

Задатак 109 *Нека је a дат природан број. Доказати да су следећи проблеми неодлучиви:*
(а) „$a \in W_x$"[33]
(б) „$a \in E_x$"[34]

Решење:
Дефинишимо функцију $f : \mathbf{N}^2 \to \mathbf{N}$ на следећи начин:

$$f(x,y) \simeq \begin{cases} y & \text{, ако } x \in W_x \\ \uparrow & \text{, ако } x \notin W_x \end{cases}$$

За функцију f важи $f(x,y) \simeq y \cdot \mathbf{1}(\Psi_U(x,x))$, па је она израчунљива (као композиција израчунљивих функција). На основу $s-m-n$ теореме, постоји тотална израчунљива функција $k : \mathbf{N} \to \mathbf{N}$ таква да важи:

$$f(x,y) \simeq \Phi_{k(x)}(y).$$

На основу дефиниције функције f следи:

$$x \in W_x \Rightarrow W_{k(x)} = \mathbf{N}(= E_{k(x)}) \Rightarrow a \in W_{k(x)} \text{ (и } a \in E_{k(x)})$$

$$x \notin W_x \Rightarrow W_{k(x)} = \emptyset(= E_{k(x)}) \Rightarrow a \notin W_{k(x)} \text{ (и } a \notin E_{k(x)})$$

Дакле, за функцију k важи:

$$x \in W_x \Leftrightarrow a \in W_{k(x)} \text{ (и } a \in E_{k(x)})$$

(а) Нека је $g : \mathbf{N} \to \mathbf{N}$ карактеристична функција проблема „$a \in W_x$", тј. нека је

$$g(x) = \begin{cases} 1 & \text{, ако } a \in W_x \\ 0 & \text{, ако } a \notin W_x \end{cases}$$

Претпоставимо супротно — да проблем „$a \in W_x$" јесте одлучив. Одатле следи да је функција g израчунљива. Дефинишимо функцију $h : \mathbf{N} \to \mathbf{N}$ на следећи начин:

$$h(x) = g(k(x)) = Sub(g; k)$$

[33] Овај проблем називамо *проблемом улаза* (енгл. *input problem*).
[34] Овај проблем називамо *проблемом излаза* (енгл. *output problem*).

Како су функције g и k израчунљиве, следи да је и функција h израчунљива. С друге стране, за функцију h важи

$$h(x) = \begin{cases} 1 & \text{, ако } g(k(x)) = 1 \text{ (тј. } a \in W_{k(x)}\text{, односно } x \in W_x\text{)} \\ 0 & \text{, ако } g(k(x)) = 0 \text{ (тј. } a \notin W_{k(x)}\text{, односно } x \notin W_x\text{)} \end{cases}$$

Дакле, функција h је карактеристична функција проблема ,,$x \in W_x$" који је неодлучив, па функција h није израчунљива, што противречи претходном закључку. Дакле, проблем ,,$a \in W_x$" није одлучив, што је и требало доказати.

Задатак 110 *Доказати да су следећи предикати неодлучиви:*
(а) ,,$x \in E_x$"
(б) ,,$x \in E_y$"

Решење:

(а) Нека је $f : \mathbf{N} \to \mathbf{N}$ карактеристична функција проблема ,,$x \in E_x$":

$$f(x) = \begin{cases} 1 & \text{, ако } x \in E_x \\ 0 & \text{, ако } x \notin E_x \end{cases}$$

Претпоставимо супротно — да проблем ,,$x \in E_x$" јесте одлучив. Одатле следи да је функција f израчунљива. Дефинишимо функцију $g : \mathbf{N} \to \mathbf{N}$ на следећи начин:

$$g(x) \simeq \begin{cases} x & \text{, ако } x \notin E_x \text{ (тј. } f(x) = 0) \\ \uparrow & \text{, ако } x \in E_x \text{ (тј. } f(x) = 1) \end{cases}$$

Функција f је израчунљива, па је и функција g израчунљива. Одатле следи да постоји вредност m ($m \in \mathbf{N}$) таква да важи $g = \Phi_m$, па, према томе, и $\text{Range}(g) = E_m$. За ту, фиксирану вредност m важи:

$$\begin{aligned} m \in E_m \Leftrightarrow & m \in \text{Range}(g) \\ & \text{(јер је } \text{Range}(g) = E_m) \\ \Leftrightarrow & m \notin E_m \\ & \text{(на основу дефиниције функције } g) \end{aligned}$$

што је немогуће. Дакле, проблем ,,$x \in E_x$" је неодлучив.

(б) Нека је функција $g : \mathbf{N}^2 \to \mathbf{N}$ карактеристична функција проблема ,,$x \in E_y$":

$$g(x, y) = \begin{cases} 1 & \text{, ако } x \in E_y \\ 0 & \text{, ако } x \notin E_y \end{cases}$$

Претпоставимо супротно — да проблем ,,$x \in E_y$" јесте одлучив. Одатле следи да је функција g израчунљива. Дефинишимо функцију $f : \mathbf{N} \to \mathbf{N}$ на следећи начин:

$$f(x) = g(x, x) = Sub(g; P_1^1, P_1^1)$$

Функција f је израчунљива (као композиција израчунљивих функција). С друге стране, за функцију f важи:

$$f(x) = \begin{cases} 1 & , \text{ако } g(x,x) = 1 \text{ (тј. } x \in E_x) \\ 0 & , \text{ако } g(x,x) = 0 \text{ (тј. } x \notin E_x) \end{cases}$$

Дакле, функција f је карактеристична функција проблема ,,$x \in E_x$", који је, на основу дела задатка под (а), неодлучив, па она није израчунљива, што противречи претходном закључку. Дакле, проблем ,,$x \in E_y$" је неодлучив, што је и требало доказати.

Задатак 111 *Доказати да су следећи проблеми неодлучиви:*
(а) ,,$\Phi_x(x) = 0$"
(б) ,,$\Phi_x(y) = 0$"

Решење:

(а) Нека је $f : \mathbf{N} \to \mathbf{N}$ карактеристична функција проблема ,,$\Phi_x(x) = 0$", тј. нека је:

$$f(x) = \begin{cases} 1 & , \text{ако } \Phi_x(x) = 0 \\ 0 & , \text{ако } \Phi_x(x) \neq 0 \end{cases}$$

Претпоставимо супротно — да проблем ,,$\Phi_x(x) = 0$" јесте одлучив. Одатле следи да је функција f израчунљива, па постоји вредност m ($m \in \mathbf{N}$) таква да важи $f = \Phi_m$. За ту, фиксирану вредност m важи:

$$\begin{aligned} f(m) = 1 \Leftrightarrow & \Phi_m(m) = 0 \\ & \text{(на основу дефиниције функције } f) \\ \Leftrightarrow & f(m) = 0 \\ & \text{(јер је } f = \Phi_m) \end{aligned}$$

што је немогуће. Дакле, проблем ,,$\Phi_x(x) = 0$" је неодлучив, што је и требало доказати.

(б) Нека је $g : \mathbf{N}^2 \to \mathbf{N}$ карактеристична функција проблема ,,$\Phi_x(y) = 0$":

$$g(x, y) = \begin{cases} 1 & , \text{ако } \Phi_x(y) = 0 \\ 0 & , \text{ако } \Phi_x(y) \neq 0 \end{cases}$$

Претпоставимо супротно — да проблем ,,$\Phi_x(y) = 0$" јесте одлучив. Одатле следи да је функција g израчунљива. Дефинишимо функцију $f : \mathbf{N} \to \mathbf{N}$ на следећи начин:

$$f(x) = g(x, x) = Sub(g; P_1^1, P_1^1)$$

Функција g је израчунљива, па је израчунљива и функција f (као композиција израчунљивих функција). За функцију f важи

$$f(x) = \begin{cases} 1 & , \text{ако } g(x,x) = 1 \text{ (тј. } \Phi_x(x) = 0) \\ 0 & , \text{ако } g(x,x) = 0 \text{ (тј. } \Phi_x(x) = 1) \end{cases}$$

Дакле, функција f је карактеристична функција проблема ,,$\Phi_x(x) = 0$", који је, на основу дела задатка под (а), неодлучив. Одатле, функција f није израчунљива, што противречи претходном закључку. Дакле, предикат ,,$\Phi_x(y) = 0$" неодлучив, што је и требало доказати.

Задатак 112 *Доказати да је проблем ,,$W_x = W_y$" неодлучив.*

Решење:

Претпоставимо супротно — да проблем ,,$W_x = W_y$" јесте одлучив. Одатле следи да је његова карактеристична функција израчунљива:

$$f(x, y) = \begin{cases} 1 & , \text{ако } W_x = W_y \\ 0 & , \text{ако } W_x \neq W_y \end{cases}$$

Нека је Φ_e произвољна тотална израчунљива функција. Како је функција Φ_e тотална, то за њен домен важи $W_e = \mathbf{N}$. Дефинишимо функцију $g : \mathbf{N} \to \mathbf{N}$ на следећи начин:

$$g(x) = f(x, e)$$

Функција f је израчунљива, па је израчунљива и функција g. За функцију g важи:

$$g(x) = \begin{cases} 1 & , \text{ако је } \Phi_x \text{ тотална} \\ 0 & , \text{ако } \Phi_x \text{ није тотална} \end{cases}$$

Дакле, израчунљива функција g је карактеристична функција предиката ,,Φ_x је тотална", што противречи чињеници да је овај предикат неодлучив (видети задатак 95). Дакле, предикат ,,$W_x = W_y$" је неодлучив, што је и требало доказати.

Теорема 3.19 (Рајс) *Ако је $\mathcal{A}$ непразан прави подскуп скупа $\mathcal{C}^{(1)}$, онда проблем ,,$\Phi_x \in \mathcal{A}$" није одлучив.*

Доказ:

Предикат ,,$\Phi_x \in \mathcal{A}$" је одлучив ако и само ако је одлучив предикат ,,$\Phi_x \in \mathcal{C}^{(1)} \setminus \mathcal{A}$" (јер важи $\Phi_x \in \mathcal{A} \Leftrightarrow \neg(\Phi_x \in \mathcal{C}^{(1)} \setminus \mathcal{A})$), па, без нарушавања општости, можемо претпоставити да функција $f_\emptyset$ која није дефинисана ни за једну вредност не припада скупу $\mathcal{A}$ (у супротном, можемо да докажемо тврђење за скуп $\mathcal{C}^{(1)} \setminus \mathcal{A}$).

Нека је g функција која припада скупу $\mathcal{A}$ и нека је функција $f : \mathbf{N}^2 \to \mathbf{N}$ дефинисана на следећи начин:

$$f(x,y) \simeq \begin{cases} g(y) & \text{, ако } x \in W_x \\ \uparrow & \text{, ако } x \notin W_x \end{cases}$$

Важи $f(x,y) \simeq g(y) + \mathbf{0}(\Psi_U(x,x))$, па је функција f израчунљива (као композиција израчунљивих функција). На основу $s-m-n$ теореме постоји тотална израчунљива функција $k : \mathbf{N} \to \mathbf{N}$ таква да је $f(x,y) \simeq \Phi_{k(x)}(y)$. Тада важи:

$$\begin{gathered} x \in W_x \Rightarrow \Phi_{k(x)} = g \Rightarrow \Phi_{k(x)} \in \mathcal{A} \\ x \notin W_x \Rightarrow \Phi_{k(x)} = f_\emptyset \Rightarrow \Phi_{k(x)} \notin \mathcal{A} \end{gathered}$$

Дакле, важи $x \in W_x \Leftrightarrow \Phi_{k(x)} \in \mathcal{A}$.

Нека је ϕ карактеристична функција проблема ,,$\Phi_x \in \mathcal{A}$", тј. нека је

$$\phi(x) \simeq \begin{cases} 1 & \text{, ако } \Phi_x \in \mathcal{A} \\ 0 & \text{, ако } \Phi_x \notin \mathcal{A} \end{cases}$$

Претпоставимо супротно — да проблем ,,$\Phi_x \in \mathcal{A}$" јесте одлучив. Одатле следи да је функција ϕ израчунљива. Дефинишимо функцију $h : \mathbf{N} \to \mathbf{N}$ на следећи начин:

$$h(x) = \phi(k(x)) = Sub(\phi; k).$$

Функција h је израчунљива (као композиција израчунљивих функција) и за њу важи:

$$h(x) = \begin{cases} 1 & \text{, ако } \phi(k(x)) = 1 \text{ (тј. } \Phi_{k(x)} \in \mathcal{A}\text{, односно } x \in W_x) \\ 0 & \text{, ако } \phi(k(x)) = 0 \text{ (тј. } \Phi_{k(x)} \notin \mathcal{A}\text{, односно } x \notin W_x) \end{cases}$$

Дакле, функција h је карактеристична функција проблема ,,$x \in W_x$", који је неодлучив (видети теорему 3.18). Отуда, функција h није израчунљива, што противречи претходном закључку. Дакле, предикат ,,$\Phi_x \in \mathcal{A}$" је неодлучив, што је и требало доказати. □

Задатак 113 *Доказати да су следећи проблеми неодлучиви:*

(а) ,,Φ_x је тотална и константна"

(б) ,,$W_x = \emptyset$"

(в) ,,E_x је бесконачан"

(г) ,,$\Phi_x = g$" (где је g дата израчунљива функција)

Решење:

(а) Нека је $\mathcal{A} = \{\Phi_x \mid \Phi_x$ је тотална и константа$\}$. Како $\mathbf{0} \in \mathcal{A}$ и $\mathbf{s} \notin \mathcal{A}$, следи да је $\mathcal{A}$ непразан прави подскуп скупа $\mathcal{C}^{(1)}$ ($\emptyset \neq \mathcal{A} \subset \mathcal{C}^{(1)}$, $\mathcal{A} \neq \mathcal{C}^{(1)}$), па је, на основу Рајсове теореме (теорема 3.19), предикат $\Phi_x \in \mathcal{A}$, тј. предикат „Φ_x је тотална и константна" неодлучив.

(б) Нека је $\mathcal{A} = \{\Phi_x \mid W_x = \emptyset\}$. Како $f_\emptyset \in \mathcal{A}$ и $\mathbf{0} \notin \mathcal{A}$, следи да је $\mathcal{A}$ непразан прави подскуп скупа $\mathcal{C}^{(1)}$, па је, на основу Рајсове теореме (теорема 3.19), предикат $\Phi_x \in \mathcal{A}$, тј. предикат „$W_x = \emptyset$" неодлучив.

(в) Нека је $\mathcal{A} = \{\Phi_x \mid E_x$ је бесконачан$\}$. Како $\mathbf{s} \in \mathcal{A}$ и $\mathbf{0} \notin \mathcal{A}$, следи да је $\mathcal{A}$ непразан прави подскуп скупа $\mathcal{C}^{(1)}$, па је, на основу Рајсове теореме (теорема 3.19), предикат $\Phi_x \in \mathcal{A}$, тј. предикат „E_x је бесконачан" неодлучив.

(г) Нека је $\mathcal{A} = \{g\}$. Важи $g \in \mathcal{A}$ и $\mathcal{A} \subset \mathcal{C}^{(1)}$. Поред тога, важи $\mathbf{s} \neq g$ или $\mathbf{0} \neq g$, па је $\mathbf{s} \notin \mathcal{A}$ или $\mathbf{0} \notin \mathcal{A}$, одакле следи $\mathcal{A} \neq \mathcal{C}^{(1)}$. Дакле, $\mathcal{A}$ је непразан прави подскуп скупа $\mathcal{C}^{(1)}$, па је, на основу Рајсове теореме (теорема 3.19), предикат $\Phi_x \in \mathcal{A}$, тј. предикат „$\Phi_x = g$" неодлучив.

Задатак 114 *Доказати да не постоји тотална израчунљива функција $f : \mathbf{N} \to \mathbf{N}$ таква да важи:*

$$P_x(y)\downarrow \;\Leftrightarrow\; P_x(y)\downarrow \text{ за } \leq f(x,y) \text{ корака.}$$

Решење:

Претпоставимо супротно — да постоји таква функција f. Важи $H(x,y,f(x,y)) \Leftrightarrow y \in W_x$, па како је предикат $H(x,y,f(x,y))$ одлучив, следи да је и проблем „$y \in W_x$" (проблем заустављања) одлучив, што противречи чињеници да је овај проблем неодлучив (видети задатак 107). Дакле, не постоји функција f са задатим својствима, што је и требало доказати.

3.6.2 Парцијална одлучивост

Дефиниција 3.26 *Предикат $P \subseteq \mathbf{N}^n$ је* парцијално одлучив *(тј.* парцијално решив, полуизрачунљив, рекурзивно набројив, полуодлучив*) ако и само ако је израчунљива његова* парцијална карактеристична функција*:*

$$f(x_1, x_2, \ldots, x_n) \simeq \begin{cases} 1 & , \text{ ако } P(x_1, x_2, \ldots, x_n) \\ \uparrow & , \text{ ако } \neg P(x_1, x_2, \ldots, x_n) \end{cases}$$

Ако је предикат P парцијално одлучив, алгоритам који израчунава његову парцијалну карактеристичну функцију зовемо парцијална процедура одлучивања.

Теорема 3.20 *Предикат* $P \subseteq \mathbf{N}^n$ *је парцијално одлучив ако и само ако постоји израчунљива функција* $g(x_1, x_2, \ldots, x_n)$ *таква да важи:*

$$P(x_1, x_2, \ldots, x_n) \Leftrightarrow (x_1, x_2, \ldots, x_n) \in \mathrm{Dom}(g).$$

Доказ:

($\Rightarrow$:) Претпоставимо да је предикат P парцијално одлучив. Тада је израчунљива његова парцијална карактеристична функција f:

$$f(x_1, x_2, \ldots, x_n) \simeq \begin{cases} 1 & \text{, ако } P(x_1, x_2, \ldots, x_n) \\ \uparrow & \text{, ако } \neg P(x_1, x_2, \ldots, x_n) \end{cases}$$

За функцију f важи:

$$P(x_1, x_2, \ldots, x_n) \Leftrightarrow (x_1, x_2, \ldots, x_n) \in \mathrm{Dom}(f),$$

па она задовољава услове тврђења.

($\Leftarrow$:) Претпоставимо да постоји функција g која задовољава услове тврђења. Нека је f парцијална карактеристична функција предиката P:

$$f(x_1, x_2, \ldots, x_n) \simeq \begin{cases} 1, & \text{ако } P(x_1, x_2, \ldots, x_n) \\ & \text{(тј. } (x_1, x_2, \ldots, x_n) \in \mathrm{Dom}(g)) \\ \uparrow, & \text{ако } \neg P(x_1, x_2, \ldots, x_n) \\ & \text{(тј. } (x_1, x_2, \ldots, x_n) \notin \mathrm{Dom}(g)) \end{cases}$$

Важи

$$f(x_1, x_2, \ldots, x_n) \simeq \mathbf{1}(g(x_1, x_2, \ldots, x_n)),$$

па је функција f израчунљива (као композиција израчунљивих функција), одакле следи да је предикат P парцијално одлучив.□

Теорема 3.21 *Предикат* $P \subseteq \mathbf{N}^n$ *је парцијално одлучив ако и само ако постоји одлучив предикат* $Q \subseteq \mathbf{N}^{n+1}$ *такав да је*

$$P(x_1, x_2, \ldots, x_n) \Leftrightarrow (\exists y) Q(x_1, x_2, \ldots, x_n, y).$$

Доказ:

($\Rightarrow$:) Претпоставимо да је предикат P парцијално одлучив. Онда је његова парцијална карактеристична функција f израчунљива, тј. постоји вредност e ($e \in \mathbf{N}$) таква да је $f = \Phi_e$. Нека је за ту, фиксирану вредност e предикат $Q \subseteq \mathbf{N}^{n+1}$ дефинисан на следећи начин:

$$Q(x_1, x_2, \ldots, x_n, y) = H(e, x_1, x_2, \ldots, x_n, y).$$

Предикат H је одлучив, па је одлучив и предикат Q и важи

$$P(x_1, x_2, \ldots, x_n) \Leftrightarrow (\exists y) Q(x_1, x_2, \ldots, x_n, y).$$

($\Leftarrow$:) Претпоставимо да за неки предикат $Q \subseteq \mathbf{N}^{n+1}$ важи

$$P(x_1, x_2, \ldots, x_n) \Leftrightarrow (\exists y) Q(x_1, x_2, \ldots, x_n, y).$$

Дефинишимо функцију $g : \mathbf{N}^n \to \mathbf{N}$ на следећи начин:

$$g(x_1, x_2, \ldots, x_n) = \mu y[Q(x_1, x_2, \ldots, x_n, y)].$$

Предикат Q је одлучив, па је функција g израчунљива и важи:

$$P(x_1, x_2, \ldots, x_n) \Leftrightarrow (x_1, x_2, \ldots, x_n) \in \mathrm{Dom}(g).$$

На основу теореме 3.20 следи да је предикат P парцијално одлучив. $\square$

Теорема 3.22 *Ако је предикат $P(x_1, x_2, \ldots, x_n, y)$ парцијално одлучив, онда је и предикат $(\exists y) P(x_1, x_2, \ldots, x_n, y)$ парцијално одлучив.*

Доказ:

Ако је предикат P парцијално одлучив, онда, на основу теореме 3.21, постоји одлучив предикат Q такав да важи:

$$P(x_1, x_2, \ldots, x_n, y) \Leftrightarrow (\exists z) Q(x_1, x_2, \ldots, x_n, y, z),$$

па је

$$(\exists y) P(x_1, x_2, \ldots, x_n, y) \Leftrightarrow (\exists y)(\exists z) Q(x_1, x_2, \ldots, x_n, y, z),$$

тј.

$$(\exists y) P(x_1, x_2, \ldots, x_n, y) \Leftrightarrow (\exists u) Q(x_1, x_2, \ldots, x_n, (u)_1, (u)_2).$$

Предикат $R(x_1, x_2, \ldots, x_n, u) \equiv Q(x_1, x_2, \ldots, x_n, (u)_1, (u)_2)$ је одлучив, па је, на основу теореме 3.21, предикат $(\exists y) P(x_1, x_2, \ldots, x_n, y)$ парцијално одлучив, што је и требало доказати. $\square$

Непосредну последицу ове теореме представља следећа теорема.

Теорема 3.23 *Ако је предикат $P(x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_m)$ парцијално одлучив, онда је и предикат*

$$(\exists y_1)(\exists y_2) \ldots (\exists y_m)\ P(x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_m)$$

парцијално одлучив.

Теорема 3.24 *Парцијална функција $f : \mathbf{N}^n \to \mathbf{N}$ је израчунљива ако и само ако је предикат „$f(x_1, x_2, \ldots, x_n) \simeq y$" парцијално одлучив.*[35]

[35] Доказ теореме се може наћи у [4].

Задатак 115 *Доказати да су следећи предикати парцијално одлучиви:*
(а) ,,$x \in E_y^{(n)}$"
(б) ,,$W_x \neq \emptyset$"
(в) ,,$E_x^{(n)} \neq \emptyset$"
(г) ,,$\Phi_x(y)$ *је потпун квадрат*"
(д) ,,n *је Фермаов број*[36]"

Решење:

(а)

$$\begin{aligned}
& x \in E_y^{(n)} \\
\Leftrightarrow & (\exists z_1)(\exists z_2)\ldots(\exists z_n)(\exists t)(P_y(z_1, z_2, \ldots, z_n) \downarrow x \ \text{ за } \ \leq t \text{ корака}) \\
\Leftrightarrow & (\exists u)(P_y((u)_1, (u)_2, \ldots, (u)_n) \downarrow x \ \text{ за } \ \leq (u)_{n+1} \text{ корака}) \\
\Leftrightarrow & (\exists u) \underbrace{S(y, (u)_1, (u)_2, \ldots, (u)_n, x, (u)_{n+1})}_{\equiv P(x,y,u) \text{ – одлучив предикат}}
\end{aligned}$$

Дакле, из
$$x \in E_y^{(n)} \Leftrightarrow (\exists u) P(x, y, u),$$
на основу теореме 3.21, следи да је предикат ,,$x \in E_y^{(n)}$" парцијално одлучив.

Тврђење може бити доказано и на следећи начин. Важи
$$x \in E_y^{(n)} \Leftrightarrow (\exists z_1)(\exists z_2)\ldots(\exists z_n)(\exists t) S(y, z_1, z_2, \ldots, z_n, x, t),$$
па, како је предикат S (парцијално) одлучив, на основу теореме 3.23, следи да је предикат ,,$x \in E_y^{(n)}$" парцијално одлучив.

(б) Из $W_x \neq \emptyset \Leftrightarrow (\exists y)(\exists t) H(x, y, t)$, како је предикат H (парцијално) одлучив, на основу теореме 3.23, следи да је предикат ,,$W_x \neq \emptyset$" парцијално одлучив.

Задатак 116 *Нека су $P, Q \subseteq \mathbf{N}^n$ парцијално одлучиви предикати. Доказати да су парцијално одлучиви и предикати $P \wedge Q$ и $P \vee Q$.*

Решење:

Како су предикати P и Q парцијално одлучиви, на основу теореме 3.21 постоје одлучиви предикати $M, N \subseteq \mathbf{N}^{n+1}$ такви да важи:

$$\begin{aligned}
P(x_1, x_2, \ldots, x_n) &\Leftrightarrow (\exists y) M(x_1, x_2, \ldots, x_n, y) \\
Q(x_1, x_2, \ldots, x_n) &\Leftrightarrow (\exists y) N(x_1, x_2, \ldots, x_n, y)
\end{aligned}$$

[36]Број n је Фермаов ако и само ако $(\exists x, y, z > 0)\; x^n + y^n = z^n$.

Тада важи:

$$\begin{aligned}&P(x_1,\dots,x_n)\wedge Q(x_1,\dots,x_n)\\ \Leftrightarrow&(\exists y)M(x_1,x_2,\dots,x_n,y)\wedge(\exists z)N(x_1,x_2,\dots,x_n,z)\\ \Leftrightarrow&(\exists y)(\exists z)(M(x_1,x_2,\dots,x_n,y)\wedge N(x_1,x_2,\dots,x_n,z))\end{aligned}$$

Предикат $M(x_1,x_2,\dots,x_n,y)\wedge N(x_1,x_2,\dots,x_n,z)$ је (парцијално) одлучив, па је, на основу теореме 3.23, предикат $P\wedge Q$ парцијално одлучив.

Задатак 117 *Доказати да проблем „$x\in W_x$" јесте, а проблем „$x\notin W_x$" није парцијално одлучив.*

Решење:

Нека је $f:\mathbf{N}\to\mathbf{N}$ парцијална карактеристична функција проблема „$x\in W_x$":

$$f(x)\simeq\begin{cases}1 & \text{, ако } x\in W_x\\ \uparrow & \text{, ако } x\notin W_x\end{cases}$$

За функцију f важи

$$f(x)\simeq\mathbf{1}(\Psi_U(x,x)),$$

па је она израчунљива, одакле следи да је проблем „$x\in W_x$" парцијално одлучив.

Нека је $g:\mathbf{N}\to\mathbf{N}$ парцијална карактеристична функција проблема „$x\notin W_x$":

$$g(x)\simeq\begin{cases}1 & \text{, ако } x\notin W_x\\ \uparrow & \text{, ако } x\in W_x\end{cases}$$

Важи

$$x\in\mathrm{Dom}(g)\Leftrightarrow x\notin W_x,$$

па за све вредности x ($x\in\mathbf{N}$) важи $\mathrm{Dom}(g)\neq W_x$. Одатле следи да за све вредности x ($x\in\mathbf{N}$) важи $g\neq\Phi_x$, па функција g није израчунљива и проблем „$x\notin W_x$" није парцијално одлучив.

Теорема 3.25 (Пост) *Предикат $P\subseteq\mathbf{N}^n$ је одлучив ако и само ако су предикати P и $\neg P$ парцијално одлучиви.*

Доказ:

($\Rightarrow$:) Претпоставимо да је предикат P одлучив. Тада је и предикат $\neg P$ одлучив, па су предикати P и $\neg P$ и парцијално одлучиви.

($\Leftarrow$:) Претпоставимо да су предикати P и $\neg P$ парцијално одлучиви. Тада, на основу теореме 3.21, постоје одлучиви предикати $Q, R \subseteq \mathbf{N}^{n+1}$ такви да важи:

$$P(x_1, \ldots, x_n) \Leftrightarrow (\exists y) Q(x_1, \ldots, x_n, y)$$
$$\neg P(x_1, \ldots, x_n) \Leftrightarrow (\exists y) R(x_1, \ldots, x_n, y).$$

Дефинишимо функцију $f : \mathbf{N}^n \to \mathbf{N}$ на следећи начин:

$$f(x_1, \ldots, x_n) = \mu y [Q(x_1, \ldots, x_n, y) \vee R(x_1, \ldots, x_n, y)].$$

Предикат $Q(x_1, \ldots, x_n, y) \vee R(x_1, \ldots, x_n, y)$ је одлучив и задовољен за све вредности $x_1, \ldots, x_n$ (јер за све вредности $x_1, \ldots, x_n$ важи или P или $\neg P$). Одатле следи да је функција f израчунљива и тотална. Поред тога, важи

$$P(x_1, \ldots, x_n) \Leftrightarrow Q(x_1, \ldots, x_n, f(x_1, \ldots, x_n)),$$

па како је предикат Q одлучив, следи да је и предикат P одлучив, што је и требало доказати. $\square$

Задатак 118 *Доказати да проблем „$P_x(y) \uparrow$”*[37] *није парцијално одлучив.*

Решење:

Нека је $f : \mathbf{N}^2 \to \mathbf{N}$ парцијална карактеристична функција за проблем заустављања, тј:

$$f(x, y) \simeq \begin{cases} 1 & , \text{ако } P_x(y) \downarrow \\ \uparrow & , \text{ако } P_x(y) \uparrow \end{cases}$$

Важи

$$f(x, y) \simeq \mathbf{1}(\psi_U(x, y)),$$

па је функција f израчунљива, одакле следи да је проблем „$P_x(y) \downarrow$” парцијално одлучив.

Проблем заустављања је неодлучив (видети задатак 107), па, на основу Постове теореме (теорема 3.25), предикати „$P_x(y) \downarrow$” и „$\neg(P_x(y) \downarrow)$” (тј. „$P_x(y) \uparrow$”) не могу бити истовремено парцијално одлучиви. Како је предикат „$P_x(y) \downarrow$” парцијално одлучив, следи да предикат „$P_x(y) \uparrow$” није парцијално одлучив, што је и требало доказати.

Задатак 119 *Нека је $P \subseteq \mathbf{N}^{n+1}$ парцијално одлучив предикат. Доказати да су следећи предикати парцијално одлучиви:*

(а) $Q(\vec{x}, z) \equiv (\exists y \leq z) P(\vec{x}, y) \quad (\equiv (\exists y)(y \leq z \ \wedge \ P(\vec{x}, y)))$

(б) $R(\vec{x}, z) \equiv (\forall y \leq z) P(\vec{x}, y) \quad (\equiv (\forall y)(y \leq z \ \Rightarrow \ P(\vec{x}, y)))$

(где је $\vec{x} = (x_1, x_2, \ldots, x_n)$).

[37] Овај проблем називамо *проблемом дивергенције* (енгл. *divergence problem*).

Решење:

(а) Предикат P је парцијално одлучив, па, на основу теореме 3.21, постоји одлучив предикат $M \subseteq \mathbf{N}^{n+2}$ такав да важи $P(\vec{x}, y) \Leftrightarrow (\exists z)M(\vec{x}, y, z)$. Онда важи:

$$\begin{aligned} Q(\vec{x}, z) &\Leftrightarrow P(\vec{x}, 0) \vee P(\vec{x}, 1) \vee \cdots \vee P(\vec{x}, z) \\ &\Leftrightarrow (\exists y)M(\vec{x}, 0, y) \vee (\exists y)M(\vec{x}, 1, y) \vee \cdots \vee (\exists y)M(\vec{x}, z, y) \\ &\Leftrightarrow (\exists y)(M(\vec{x}, 0, y) \vee M(\vec{x}, 1, y) \vee \cdots \vee M(\vec{x}, z, y)) \end{aligned}$$

Предикат $M(\vec{x}, 0, y) \vee M(\vec{x}, 1, y) \vee \cdots \vee M(\vec{x}, z, y)$ је одлучив, па је, на основу теореме 3.21, предикат $Q(\vec{x}, z)$ парцијално одлучив.

(б) Предикат P је парцијално одлучив, па, на основу теореме 3.21, постоји одлучив предикат $M \subseteq \mathbf{N}^{n+2}$ такав да важи $P(\vec{x}, y) \Leftrightarrow (\exists z)M(\vec{x}, y, z)$. Онда важи:

$$\begin{aligned} &R(\vec{x}, z) \\ &\quad \Leftrightarrow P(\vec{x}, 0) \wedge P(\vec{x}, 1) \wedge \cdots \wedge P(\vec{x}, z) \\ &\quad \Leftrightarrow (\exists y_1)M(\vec{x}, 0, y_1) \wedge (\exists y_2)M(\vec{x}, 1, y_2) \wedge \cdots \wedge (\exists y_z)M(\vec{x}, z, y_z) \\ &\quad \Leftrightarrow (\exists y_1)(\exists y_2) \ldots (\exists y_z)(M(\vec{x}, 0, y_1) \wedge M(\vec{x}, 1, y_2) \wedge \cdots \wedge M(\vec{x}, z, y_z)) \end{aligned}$$

Предикат $M(\vec{x}, 0, y_1) \wedge M(\vec{x}, 1, y_2) \vee \cdots \vee M(\vec{x}, z, y_z)$ је одлучив, па је, на основу теореме 3.21, предикат $R(\vec{x}, z)$ парцијално одлучив.

Задатак 120 *Доказати да је предикат $P \subseteq \mathbf{N}^n$ одлучив ако и само ако постоје одлучиви предикати $Q, R \subseteq \mathbf{N}^{n+1}$ такви да важи*

$$\begin{aligned} P(\vec{x}) &\Leftrightarrow (\exists y)Q(\vec{x}, y) \\ P(\vec{x}) &\Leftrightarrow (\forall y)R(\vec{x}, y) \end{aligned}$$

(где је $\vec{x} = (x_1, x_2, \ldots, x_n)$).

Решење:

($\Rightarrow$:) Претпоставимо да је предикат P одлучив. На основу Постове теореме (теорема 3.25), предикати P и $\neg P$ су парцијално одлучиви, па, на основу теореме 3.21, постоје одлучиви предикати $Q, R_1 \subseteq \mathbf{N}^{n+1}$ такви да важи:

$$\begin{aligned} P(\vec{x}) &\Leftrightarrow (\exists y)Q(\vec{x}, y) \\ \neg P(\vec{x}) &\Leftrightarrow (\exists y)R_1(\vec{x}, y) \end{aligned}$$

Последњу еквиваленцију даље трансформишемо:

$$\begin{aligned} P(\vec{x}) &\Leftrightarrow \neg(\exists y)R_1(\vec{x}, y) \\ &\Leftrightarrow (\forall y)\neg R_1(\vec{x}, y) \\ &\Leftrightarrow (\forall y)R(\vec{x}, y) \end{aligned}$$

где је $R(\vec{x}, y) \equiv \neg R_1(\vec{x}, y)$. Предикати Q и R задовољавају тврђење задатка.

($\Leftarrow$:) Претпоставимо да постоје одлучиви предикати $Q, R \subseteq \mathbf{N}^{n+1}$ такви да важи

$$P(\vec{x}) \Leftrightarrow (\exists y)Q(\vec{x}, y)$$
$$P(\vec{x}) \Leftrightarrow (\forall y)R(\vec{x}, y)$$

На основу теореме 3.21, из $P(\vec{x}) \Leftrightarrow (\exists y)Q(\vec{x}, y)$ следи да је предикат P парцијално одлучив. Предикат $\neg R(\vec{x}, y)$ је одлучив, па из

$$\begin{aligned}\neg P(\vec{x}) &\Leftrightarrow \neg(\forall y)R(\vec{x}, y)\\ &\Leftrightarrow (\exists y)\neg R(\vec{x}, y)\end{aligned}$$

на основу теореме 3.21, следи да је предикат $\neg P$ парцијално одлучив.

Дакле, предикати P и $\neg P$ су парцијално одлучиви, па, на основу Постове теореме (теорема 3.25), следи да је предикат P одлучив.

3.6.3 Одлучиве и неодлучиве теорије

Нека је $\mathcal{L}$ језик теорије $\mathcal{T}$ и нека је скуп симбола тог језика рекурзиван. Нека је g_s „1-1" функција која пресликава скуп симбола језика $\mathcal{L}$ у скуп природних бројева. Геделова функција g_e је функција која низ симбола $s_1, s_2, \ldots, s_n$ језика $\mathcal{L}$ пресликава у број (тј. кôд):

$$\prod_{i=1}^{n} pn(i)^{1+g_s(s_i)},$$

где је $pn(i)$ i-ти прост број. Може се показати да је овако дефинисана функција g_e и инјективна, тј. различитим низовима симбола одговарају различити кодови. Скуп кодова свих реченица језика $\mathcal{L}$ је одлучив (рекурзиван) подскуп скупа $\mathbf{N}$.

Језик $\mathcal{L}$ којем је на описани начин придружена функција g_e називамо *ефективизованим језиком* и означавамо са $\hat{\mathcal{L}}$. Кôд $g_e(\phi)$ означава се најчешће са $\ulcorner\phi\urcorner$.

Дефиниција 3.27 *Нека је $\mathcal{T}$ теорија првог реда ефективизованог језика $\hat{\mathcal{L}}$ и g_e његова Геделова функција. За теорију $\mathcal{T}$ кажемо да је* одлучива[38]

[38]Термин *одлучив* има сасвим другачији смисао када је у питању појединачна формула: кажемо да је формула ϕ непротивречне теорије $\mathcal{T}$ *одлучива* ако је или ϕ или $\neg\phi$ теорема теорије $\mathcal{T}$. Ако је теорија потпуна, све реченице на њеном језику су одлучиве. Теорија може да буде непотпуна и одлучива.

(или разрешива*) ако је скуп* $\{\lceil\phi\rceil \mid \phi \in \mathcal{T}\}$ *одлучив (рекурзиван), тј. ако је карактеристична функција теорије* $\mathcal{T}$ $f_{\mathcal{T}} : \mathbf{N} \to \mathbf{N}$*:*

$$f_{\mathcal{T}}(\lceil\phi\rceil) = \begin{cases} 1 & \text{, ако } \phi \in \mathcal{T} \\ 0 & \text{, ако } \phi \notin \mathcal{T} \end{cases}$$

рекурзивна. Функцију $f_{\mathcal{T}}$ *тада називамо и* процедуром одлучивања *за теорију* $\mathcal{T}$*.*

Дефиниција 3.28 *Нека је* $\mathcal{T}$ *теорија првог реда ефективизованог језика* $\hat{\mathcal{L}}$ *и* g_e *његова Геделова функција. За теорију* $\mathcal{T}$ *кажемо да је* полуодлучива *ако је скуп* $\{\lceil\phi\rceil \mid \phi \in \mathcal{T}\}$ *парцијално одлучив (полуодлучив), тј. ако је функција* $h_{\mathcal{T}} : \mathbf{N} \to \mathbf{N}$*:*

$$h_{\mathcal{T}}(\lceil\phi\rceil) = \begin{cases} 1 & \text{, ако } \phi \in \mathcal{T} \\ 0 \text{ или недефинисано} & \text{, ако } \phi \notin \mathcal{T} \end{cases}$$

рекурзивна. Функцију $h_{\mathcal{T}}$ *тада називамо и* процедуром полуодлучивања *за теорију* $\mathcal{T}$*.*

Претходним дефиницијама строго је уведен појам одлучиве теорије. Тај појам могуће је увести и нешто неформалније, интуитивно, на следећи начин: уколико постоји ефективан алгоритам (поступак, процедура) такав да за сваку реченицу α даје одговор *да* ако и само ако је α теорема теорије $\mathcal{T}$ (и *не* иначе), онда кажемо да је теорија $\mathcal{T}$ одлучива. Веза између формално и неформално уведеног појма одлучиве теорије базира се (између осталог) и на Черчовој тези која тврди да су класе рекурзивних и ефективно израчунљивих функција идентичне.

Дефиниција 3.29 *За теорију* $\mathcal{T}$ *кажемо да је* неодлучива *ако није одлучива. За теорију* $\mathcal{T}$ *кажемо да је* есенцијално неодлучива *ако је неодлучива теорија* $\mathcal{T}$*, као и било које њено непротивречно проширење.*

За теорију $\mathcal{T}$ над рекурзивним (одлучивим) језиком $\mathcal{L}$ кажемо да је *аксиоматибилна* ако постоји рекурзиван непротивречан скуп A реченица језика $\mathcal{L}$ такав да је реченица α теорема теорије $\mathcal{T}$ ако и само ако она може бити изведена из скупа A (тј. ако и само ако важи $A \vdash \alpha$).

Наредна теорема даје потребне и довољне услове да потпуна теорија буде одлучива [10]:

Теорема 3.26 *За потпуну теорију* $\mathcal{T}$ *следећи услови су еквивалентни:*

- $\mathcal{T}$ *је неодлучива.*
- $\mathcal{T}$ *је есенцијално неодлучива.*
- $\mathcal{T}$ *није аксиоматибилна.*

Постоји значајна методолошка разлика у проучавању одлучивости и неодлучивости, упркос чињеници да су та два појма у непосредној вези. Да би се показало да је нека теорија неодлучива обично се посеже за строгим формализмима израчунљивих функција. С друге стране, за доказ одлучивости неке теорије довољно је постојање ефективног поступка који за сваку реченицу утврђује да ли јесте или није теорема дате теорије. Због тога су први резултати у вези са одлучивошћу претходили увођењу појма рекурзивних функција средином тридесетих година, док су се први резултати у вези са неодлучивошћу појавили тек након тога.

Неке од одлучивих теорија су: исказни рачун, теорија еквиваленције, теорија Булових алгебри, Презбургерова аритметика, теорија множења природних бројева, теорија Абелових група, теорија алгебарски затворених поља, теорија реално затворених поља, елементарна еуклидска геометрија, елементарна хиперболичка геометрија. Неке од неодлучивих теорија су: предикатски рачун првог реда, Пеанова аритметика, ZF теорија скупова, теорија група, теорија прстена, теорија поља, пројективна геометрија. Више о одлучивим теоријама видети у [9]; више о неолучивим теоријама видети у [10].

Може се разматрати и (не)одлучивост неке класе тврђења у једној теорији. Уколико у некој теорији постоји класа неодлучивих тврђења, онда је и та теорија неодлучива. Наредни примери илуструју два важна резултата тог типа.

Пример 3.2 *Претпоставимо да је G група са јединичним елементом e и да је G генерисана елементима из скупа $S = \{g_1, g_2, \ldots, g_n\} \subseteq G$.* Реч *над S је терм попут $g_2^{-1}g_3^6g_1g_2^5g_8$ који укључује елементе скупа S и операције групе. Свака реч одговара неком елементу групе G. Каже се да је група G генерисана скупом S, ако сваком елементу групе G одговара нека реч над S.* Проблем речи *за G (у односу на S) је проблем утврђивања да ли за реч w над S важи $w = e$. Проблем речи за групе је неодлучив.*

Пример 3.3 *Проблем „целобројни полином $p(x_1, x_2, \ldots, x_n)$ има целобројне нуле" је неодлучив.*

3.7 Рекурзивни и рекурзивно набројиви скупови

3.7.1 Рекурзивни скупови

Постоји блиска веза између унарних предиката над природним бројевима и подскупова скупа природних бројева. Наиме, предикату $M(x)$ одговара скуп $\{x \mid M(x)\}$, а скупу $A \subseteq \mathbf{N}$ одговара предикат „$x \in A$".

Дефиниција 3.30 *Скуп $A \subseteq \mathbf{N}$ је* рекурзиван (одлучив) *ако је* карактеристична функција скупа *A:*

$$C_A(x) = \begin{cases} 1 & , \text{ ако } x \in A \\ 0 & , \text{ ако } x \notin A \end{cases}$$

израчунљива (тј. ако је предикат „$x \in A$" одлучив).

Рекурзивне скупове називамо и *израчунљивим скуповима.* Ако је функција C_A примитивно рекурзивна, онда кажемо да је скуп A *примитивно рекурзиван.* Појам рекурзивних скупова може бити природно проширен на подскупове скупа $\mathbf{N}^n$. Довољно је, међутим, разматрати подскупове скупа $\mathbf{N}$, јер се уређене n-торке природних бројева могу ефективно кодирати природним бројевима.

Задатак 121 *Доказати да су следећи скупови рекурзивни:*
(а) $\mathbf{N}$
(б) било који коначан скуп
(в) P_2 *– скуп свих парних бројева*
(г) P *– скуп свих простих бројева.*

Решење:

(а) $C_{\mathbf{N}}(x) = \mathbf{1}(x) = s(\mathbf{0}(x))$
$C_{\mathbf{N}} = Sub(s; \mathbf{0})$

(б) Ако је $A = \emptyset$, онда је $C_A(x) = \mathbf{0}(x)$. У супротном, важи $A = \{a_1, a_2, \ldots, a_n\}$, па је $C_A(x) = sgn(\sum_{i=1}^{n} eq(x, a_i))$.

(в) $C_{P_2}(x) = div(2, x)$

(г) $C_P(x) = pr(x)$ (видети задатак 63 (д))

Задатак 122 *Ако су A и B рекурзивни скупови, онда су рекурзивни и следећи скупови:*
(а) $\overline{A}$
(б) $A \cap B$
(в) $A \cup B$

Решење:
(а) $C_{\overline{A}}(x) = 1 \dot{-} C_A(x)$
(б) $C_{A \cap B} = C_A(x) \cdot C_B(x)$
(в) $C_{A \cup B} = \max(C_A(x), C_B(x))$ [39]

[39]Приметимо аналогију између предиката и скупова и одговарајућих операција на њима (видети задатак 77).

Задатак 123 *Нека су A и B подскупови скупа $\mathbf{N}$. Скупови $A \bigoplus B$ и $A \bigotimes B$ дефинисани су на следећи начин:*

$$A \bigoplus B = \{2x \mid x \in A\} \cup \{2x+1 \mid x \in B\}$$
$$A \bigotimes B = \{\pi(x,y) \mid x \in A \ \text{ и } \ y \in B\}$$

где је функција π дефинисана на следећи начин: $\pi(x,y) = 2^x(2y+1) - 1$.
Доказати да важи:

(а) Скуп $A \bigoplus B$ је рекурзиван ако и само ако су и A и B рекурзивни.

(б) Ако је $A, B \neq \emptyset$, онда је $A \bigotimes B$ рекурзиван ако и само ако су и A и B рекурзивни.

Задатак 124 *Доказати да следећи скупови нису рекурзивни:*
(а) $\{x \mid \Phi_x$ *је тотална*$\}$
(б) $\{x \mid x \in W_x\}$
(в) $\{x \mid \Phi_x = \mathbf{0}\}$

3.7.2 Рекурзивно набројиви скупови

Дефиниција 3.31 *Скуп $A \subseteq \mathbf{N}$ је* рекурзивно набројив скуп *ако је његова* парцијална карактеристична функција*:*

$$f(x) = \begin{cases} 1 & , \text{ако } x \in A \\ \uparrow & , \text{ако } x \notin A \end{cases}$$

израчунљива (тј. ако је предикат „$x \in A$" парцијално одлучив).

За рекурзивно набројив скуп A краће пишемо A је *р.н. скуп*. За р.н. скупове користе се и термини *полурекурзивни скупови* и *полуизрачунљиви скупови*.

Пример 3.4 *Скуп $K = \{x \mid x \in W_x\}$ јесте р.н. скуп, али није рекурзиван скуп. Скуп $\overline{K} = \{x \mid x \notin W_x\}$ није р.н. скуп.*

Теорема 3.27 (Пост) *Скуп A је рекурзиван ако и само ако су скупови A и $\overline{A}$ р.н. скупови.*[40]

Приметимо аналогију између ове теореме и теореме 3.25, чије се тврђење односи на предикате.

[40] Доказ теореме се може наћи у [4].

Теорема 3.28 *Нека је $A \subseteq \mathbf{N}$. Тада су следећи услови еквивалентни:*[41]

(*i*) *A је р.н. скуп.*

(*ii*) $(\exists e)A = W_e$

(*iii*) *$x \in A \Leftrightarrow (\exists y)P(x,y)$ за неки одлучив предикат $P \subseteq \mathbf{N}^2$.*

(*iv*) *$x \in A \Leftrightarrow (\exists y_1)(\exists y_2)\ldots(\exists y_n)M(x,y_1,y_2,\ldots,y_n)$ за неки одлучив предикат $M \subseteq \mathbf{N}^{n+1}$.*

(*v*) *Ако је $A \neq \emptyset$, онда је $A = \mathrm{Range}(f)$ за неку унарну тоталну израчунљиву функцију.*

(*vi*) *$A = \mathrm{Range}(f)$ за неку (парцијалну) израчунљиву функцију.*

Наведена теорема, између осталог, говори да је енумерација

$$W_0, W_1, W_2, \ldots$$

домена унарних израчунљивих функција енумерација (са понављањем) *свих* р.н. скупова. Ако је $A = W_c$, онда c називамо *индекс скупа* A. Теорема, такође, тврди да је и енумерација

$$E_0, E_1, E_2, \ldots$$

рангова унарних израчунљивих функција енумерација (са понављањем) *свих* р.н. скупова.

Задатак 125 *Доказати да је скуп $A = \{x \mid \Phi_x$ није ,,1-1''$\}$ р.н.*

Решење:

$$\begin{aligned}
&x \in A\\
\Leftrightarrow&\Phi_x \text{ није ,,1-1''}\\
\Leftrightarrow&(\exists y,z)(y \neq z \wedge \Phi_x(y) = \Phi_x(z))\\
\Leftrightarrow&(\exists y,z,s,t)(y \neq z \wedge P_x(y)\downarrow s \text{ за } \leq t \text{ корака } \wedge P_x(z)\downarrow s \text{ за } \leq t \text{ корака})\\
\Leftrightarrow&(\exists y,z,s,t)(y \neq z \wedge S(x,y,s,t) \wedge S(x,z,s,t))\\
\Leftrightarrow&(\exists y)(\underbrace{(y)_1 \neq (y)_2 \wedge S(x,(y)_1,(y)_3,(y)_4) \wedge S(x,(y)_2,(y)_3,(y)_4))}_{\equiv Q(x,y) - \text{ одлучив предикат}}
\end{aligned}$$

Дакле, важи $x \in A \Leftrightarrow (\exists y)Q(x,y)$, где је Q одлучив предикат, па, на основу теореме 3.21, следи да је предикат ,,$x \in A$'' парцијално одлучив, тј. скуп A је р.н.

[41] Доказ теореме се може наћи у [4].

Задатак 126 *Доказати да скуп $A = \{x \mid \Phi_x$ је тотална$\}$ није р.н.*

Решење:

Функција $\mathbf{0}$ је тотална и израчунљива, па постоји индекс e такав да важи $\Phi_e = \mathbf{0}$. Тада важи $e \in A$, па скуп A није празан.

Претпоставимо супротно — да скуп A јесте р.н. На основу теореме 3.28[(v)], следи да постоји унарна тотална израчунљива функција f таква да важи $A = \mathrm{Range}(f)$, тј. $A = \{f(x) \mid x \in \mathbf{N}\}$. Тада је низ

$$\Phi_{f(0)}, \Phi_{f(1)}, \Phi_{f(2)}, \ldots$$

низ свих унарних тоталних израчунљивих функција. Дефинишимо функцију $g : \mathbf{N} \to \mathbf{N}$ на следећи начин:

$$g(x) = \Phi_{f(x)}(x) + 1.$$

Функција g је тотална и израчунљива, па постоји индекс m такав да важи $g = \Phi_{f(m)}$. За ту, фиксирану вредност m важи

$$\begin{aligned} \Phi_{f(m)}(m) =& g(m) \\ & (\text{јер је } g = \Phi_{f(m)}) \\ =& \Phi_{f(m)}(m) + 1 \\ & (\text{на основу дефиниције функције } g) \end{aligned}$$

што је немогуће. Дакле, скуп A није р.н.

Задатак 127 *Нека су $A, B \subseteq \mathbf{N}$ р.н. скупови. Доказати да су онда р.н. и скупови $A \cap B$ и $A \cup B$.*

Решење:

Ако су скупови A и B р.н, онда, на основу теореме 3.28[(ii)], постоје израчунљиве функције f и g такве да је $A = \mathrm{Dom}(f)$ и $B = \mathrm{Dom}(g)$. Важи $A \cap B = \mathrm{Dom}(f \cdot g)$ и $f \cdot g$ је израчунљива функција, па, на основу исте теореме, следи да је скуп $A \cap B$ р.н.

Ако је $A = \emptyset$ или $B = \emptyset$, онда је скуп $A \cup B$ очигледно р.н. Претпоставимо да је $A \neq \emptyset$ и $B \neq \emptyset$. На основу теореме 3.28[(v)], постоје тоталне израчунљиве функције f и g такве да је $A = \mathrm{Range}(f)$ и $B = \mathrm{Range}(g)$. Дефинишимо функцију $h : \mathbf{N} \to \mathbf{N}$ на следећи начин:

$$\begin{aligned} h(2x) &= f(x) \\ h(2x+1) &= g(x) \end{aligned}$$

Функција h је израчунљива и важи $A \cup B = \mathrm{Range}(h)$, па, на основу исте теореме, следи да је скуп $A \cup B$ р.н.

Задатак 128 *Нека су* $A, B \subseteq \mathbf{N}$ *р.н. скупови. Доказати да постоје р.н. скупови* A' *и* B' *такви да важи*

$$A' \cap B' = \emptyset \ \wedge \ A \cup B = A' \cup B'.$$

Задатак 129 *Доказати да је функција* $f : \mathbf{N}^n \to \mathbf{N}$ *рекурзивна ако и само је њен график*[42]*, скуп* Γ_f*, рекурзивно набројив.*

Решење:

($\Rightarrow$:) Претпоставимо да је функција f рекурзивна. Онда $f = \Phi_e$ за неку вредност e ($e \in \mathbf{N}$). Важи:

$$\begin{aligned}(\vec{x}, y) \in \Gamma_f &\Leftrightarrow y = f(\vec{x}) \\ &\Leftrightarrow (\exists t)(P_e(\vec{x}) \downarrow y \text{ за } \leq t \text{ корака}) \\ &\Leftrightarrow (\exists t) \qquad \underbrace{S(e, \vec{x}, y, t)}_{\text{одлучив предикат}}\end{aligned}$$

На основу теореме 3.28[(iii)], следи да је скуп Γ_f р.н.

($\Leftarrow$:) Претпоставимо да је скуп Γ_f р.н. На основу теореме 3.28[(iii)], постоји одлучив предикат P такав да важи:

$$(\vec{x}, y) \in \Gamma_f \ \Leftrightarrow \ (\exists z) P(\vec{x}, y, z)$$

Важи:

$$\begin{aligned}&\text{вредност } f(\vec{x}) \text{ је дефинисана} \\ \Leftrightarrow &(\exists y)((\vec{x}, y) \in \Gamma_f) \\ \Leftrightarrow &(\exists y)(\exists z) P(\vec{x}, y, z) \\ \Leftrightarrow &(\exists t) \qquad \underbrace{P(\vec{x}, (t)_1, (t)_2)}_{Q(\vec{x},t) - \text{ одлучив предикат}}\end{aligned}$$

па је

$$f(\vec{x}) \simeq (\mu t[Q(\vec{x}, t)])_1 \,,$$

одакле следи да је функција f рекурзивна.

Задатак 130 *Нека је* $A \subseteq \mathbf{N}$ *бесконачан р.н. скуп. Доказати да постоји тотална израчунљива функција* f *која је „1-1” и за коју важи* $A = \mathrm{Range}(f)$.

[42] График функције $f : \mathbf{N}^n \to \mathbf{N}$ је скуп

$$\Gamma_f = \{(x_1, x_2, \ldots, x_n, f(x_1, x_2, \ldots, x_n)) \mid (x_1, x_2, \ldots, x_n) \in \mathrm{Dom}(f)\}.$$

Решење:

Скуп A је непразан (јер је бесконачан) и р.н, па, на основу теореме 3.28[(v)], следи да постоји тотална израчунљива функција $g : \mathbf{N} \to \mathbf{N}$ таква да важи $A = \mathrm{Range}(g)$.

Дефинишимо функцију $f : \mathbf{N} \to \mathbf{N}$ на следећи начин:

$$\begin{aligned} f(0) &= g(0) \\ f(x+1) &= g(\mu\, y[g(y) \notin \{f(0), f(1), \ldots, f(x)\}]) \end{aligned}$$

Скуп A је бесконачан, па за сваку вредност $x + 1$ постоји вредност y таква да је $g(y) \notin \{f(0), f(1), \ldots, f(x)\}$. Скуп $\{f(0), f(1), \ldots, f(x)\}$ је коначан, па је рекурзиван, одакле следи да је предикат $g(y) \notin \{f(0), f(1), \ldots, f(x)\}$ одлучив и да је функција f израчунљива. Може се и ефективно показати да је функција f израчунљива. Нпр:

$$f(x+1) = g(\mu y\, [\sum_{z=0}^{x} eq(g(y), f(z)) = 0]).$$

За функцију f важи да је ,,1-1" и $\{f(x) \mid x \in \mathbf{N}\} = \{g(x) \mid x \in \mathbf{N}\} = A$.

Задатак 131 *Бесконачан скуп $A \subseteq \mathbf{N}$ је рекурзиван ако и само ако постоји строго растућа тотална израчунљива функција $f : \mathbf{N} \to \mathbf{N}$ таква да важи $A = \mathrm{Range}(f)$.*

Решење:

($\Rightarrow$:) Претпоставимо да је скуп A рекурзиван. Дефинишимо функцију $f : \mathbf{N} \to \mathbf{N}$ на следећи начин:

$$\begin{aligned} f(0) &= \mu y[y \in A] = \mu y[C_A(y) = 1] \\ f(x+1) &= \mu y[y \in A \wedge y > f(x)] \end{aligned}$$

Скуп A је рекурзиван, па је предикат $y \in A$ одлучив. Одлучив је и предикат $y \in A \ \wedge \ y > f(x)$, па је функција f израчунљива. Поред тога, скуп A је бесконачан, па је функција f дефинисана у свакој тачки.

Дакле, функција f је тотална, израчунљива, строго растућа и важи $A = \mathrm{Range}(f)$.

($\Leftarrow$:) Претпоставимо да постоји функција f која је тотална, израчунљива, строго растућа и важи $A = \mathrm{Range}(f)$.

Важи $f(0) < f(1) < f(2) < \ldots$, па се једноставно доказује да из $y = f(x)$ следи $x \leq y$.

Важи:

$$y \in A \Leftrightarrow y \in \mathrm{Range}(f) \Leftrightarrow (\exists x) y = f(x) \Leftrightarrow (\exists x \leq y) y = f(x)$$

Предикат $(\exists x \leq y)\; y = f(x)$ је одлучив, па је скуп A рекурзиван.

Задатак 132 *Нека је $A \subseteq \mathbf{N}$ бесконачан р.н. скуп. Доказати да A има бесконачан рекурзиван подскуп.*

Решење:

Скуп A је непразан (јер је бесконачан) и р.н, па, на основу теореме 3.28[(v)], следи да постоји тотална израчунљива функција f таква да је $A = \mathrm{Range}(f)$.

Дефинишимо функцију $g : \mathbf{N} \to \mathbf{N}$ на следећи начин:

$$g(0) = f(0)$$
$$g(x+1) = f(\mu y[f(y) > g(x)]$$

Предикат $f(y) > g(x)$ је одлучив, па је функција g израчунљива. Скуп $Range(f) = A$ је бесконачан, па је функција g дефинисана у свакој тачки.

Нека је $B = \mathrm{Range}(g)$. Функција g је тотална израчунљива и строго растућа функција, па је, на основу задатка 131, скуп B рекурзиван. Функција g је строго растућа, па је скуп $B = \mathrm{Range}(g)$ бесконачан. Важи и $B = \mathrm{Range}(g) \subseteq \mathrm{Range}(f) = A$, па следи да је скуп B бесконачан рекурзиван подскуп скупа A.

Теорема 3.29 (Рајс-Шапиро) *Нека је $\mathcal{A}$ скуп унарних израчунљивих функција такав да је скуп $\{x \mid \Phi_x \in \mathcal{A}\}$ р.н. Тада за сваку унарну израчунљиву функцију f важи:*

$$f \in \mathcal{A} \ \Leftrightarrow \ \text{постоји коначна функција } \theta \text{ таква да је } \theta \in \mathcal{A} \text{ и } \theta \subseteq f$$

У теореми се под *коначном функцијом* подразумева функција чији је домен коначан скуп. Као и раније, $\theta \subseteq f$ значи да је функција f проширење функције θ.

Главна примена наведене теореме је у доказима да неки скуп није р.н.

Задатак 133 *Доказати да следећи скупови нису р.н.*

(а) $\{x \mid \Phi_x$ *је тотална*$\}$

(б) $\{x \mid \Phi_x$ *није тотална*$\}$

Решење:

(а) Скупу индекса $A = \{x \mid \Phi_x$ је тотална$\}$ одговара скуп функција $\mathcal{A} = \{f \mid f \in \mathcal{C}^{(1)}$ и f је тотална$\}$, на који примењујемо Рајс-Шапироову теорему (теорема 3.29). Како ни за једну функцију f $(f \in \mathcal{A})$ не постоји коначна функција θ $(\theta \subseteq f)$ таква да је $\theta \in \mathcal{A}$, то скуп A није р.н.

(б) Слично, скупу индекса $B = \{x \mid \Phi_x$ није тотална$\}$ одговара скуп функција $\mathcal{B} = \{f \mid f \in \mathcal{C}^{(1)}$ и f није тотална$\}$, на који примењујемо Рајс-Шапироову теорему (теорема 3.29). Ако је функција f тотална израчунљива функција, онда $f \notin \mathcal{B}$, а свака коначна функција $\theta \subseteq f$ припада скупу $\mathcal{B}$. Дакле, скуп $\mathcal{B}$ није р.н.

Задатак 134 *Доказати да следећи предикати нису парцијално одлучиви:*

(а) ,,$W_x = \emptyset$"
(б) ,,Φ_x је 1-1"
(в) ,,W_x је коначан"
(г) ,,W_x је бесконачан"
(д) ,,$\Phi_x = \mathbf{0}$"
(ђ) ,,$\Phi_x \neq \mathbf{0}$"
(е) ,,Φ_x је тотална"
(ж) ,,Φ_x није тотална"

Решење:

(а) Нека је $\mathcal{A} = \{f \mid f \in \mathcal{C}^{(1)}$ и $\mathrm{Dom}(f) = \emptyset\}$ и нека је $f_\emptyset$ израчунљива функција која није нигде дефинисана (тј. $\mathrm{Dom}(f_\emptyset) = \emptyset$). Претпоставимо да је скуп $A = \{x \mid \Phi_x \in \mathcal{A}\} = \{x \mid W_x = \emptyset\}$ рекурзивно набројив.

Функција $f_\emptyset$ је коначна, припада скупу $\mathcal{A}$ и важи $f_\emptyset \subseteq \mathbf{0}$, па, на основу теореме 3.29, следи $\mathbf{0} \in \mathcal{A}$, што је нетачно. Дакле, претпоставка је била погрешна, па следи да скуп $A = \{x \mid W_x = 0\}$ није р.н, тј. предикат ,,$W_x = 0$" није парцијално одлучив.

(г) Нека је $\mathcal{A} = \{f \mid f \in \mathcal{C}^{(1)}$ и $\mathrm{Dom}(f)$ је бесконачан$\}$. Претпоставимо да је скуп $A = \{x \mid W_x$ је бесконачан$\}$ рекурзивно набројив. Скуп $\mathcal{A}$ је непразан, па постоји функција f која му припада. На основу теореме 3.29, следи да постоји коначна функција θ таква да је $\theta \subseteq f$ и $\theta \in \mathcal{A}$. Та функција θ је и коначна и има бесконачан домен, што је контрадикција, па следи да је претпоставка била погрешна и да скуп $A = \{x \mid W_x$ је бесконачан$\}$ није р.н, тј. предикат ,,W_x је бесконачан" није парцијално одлучив.

(е) Нека је $\mathcal{A} = \{f \mid f \in \mathcal{C}^{(1)}$ и f је тотална$\}$. Претпоставимо да је скуп $A = \{x \mid \Phi_x$ је тотална$\}$ рекурзивно набројив. Функција $\mathbf{0}$ је тотална и израчунљива, па, на основу теореме 3.29, следи да постоји коначна функција θ таква да је $\theta \subseteq \mathbf{0}$ и $\theta \in \mathcal{A}$. Та функција θ је коначна, а њен домен је скуп $\mathbf{N}$, што је контрадикција, па следи да је претпоставка била погрешна и да скуп $A = \{x \mid \Phi_x$ је тотална$\}$ није р.н, тј. предикат ,,Φ_x је тотална" није парцијално одлучив.

Задатак 135 *Нека је $\mathcal{A}$ подскуп скупа унарних рекурзивних функција, тј. $\mathcal{A} \subseteq \mathcal{C}^{(1)}$. Доказати да ако је скуп $A = \{x \mid \Phi_x \in \mathcal{A}\}$ рекурзиван, онда је $\mathcal{A} = \emptyset$ или $\mathcal{A} = \mathcal{C}^{(1)}$.*[43]

Решење:

Претпоставимо да је скуп A рекурзиван и нека је $f_\emptyset$ израчунљива функција која није нигде дефинисана (тј. $\mathrm{Dom}(f_\emptyset) = \emptyset$). Постоје две могућности:

$f_\emptyset \in \mathcal{A}$: Нека је f произвољна унарна израчунљива функција. Функција $f_\emptyset$ је коначна и важи $f_\emptyset \subseteq f$, $f_\emptyset \in \mathcal{A}$, па, на основу теореме 3.29, следи да функција f припада скупу $\mathcal{A}$. Дакле, за произвољну израчунљиву функцију f важи $f \subseteq \mathcal{A}$, па, како важи и $\mathcal{A} \subseteq \mathcal{C}^{(1)}$, следи $\mathcal{A} = \mathcal{C}^{(1)}$.

$f_\emptyset \notin \mathcal{A}$: Ако важи $f_\emptyset \notin \mathcal{A}$, онда важи $f_\emptyset \in \mathcal{C}^{(1)} \setminus \mathcal{A}$, па се аналогно првом делу, доказује да важи $\mathcal{C}^{(1)} \setminus \mathcal{A} = \mathcal{C}^{(1)}$, тј. $\mathcal{A} = \emptyset$.

Задатак 136 *Испитати да ли је р.н. следећи скуп:*

$$A = \{x \mid W_x \neq \emptyset \ \wedge \Phi_x \circ \Phi_x \text{ је ,,1-1''}\}$$

Решење:

Скупу индекса A одговара следећи скуп функција:

$$\mathcal{A} = \{f \mid f \in \mathcal{C}^{(1)} \ \wedge \ \mathrm{Dom}(f) \neq \emptyset \ \wedge \ f \circ f \text{ је ,,1-1''}\}.$$

Претпоставимо да је скуп A р.н. Дефинишимо функцију $\theta : \mathbf{N} \to \mathbf{N}$ на следећи начин:

$$\theta(x) = \begin{cases} 0 & \text{, ако } x = 0 \\ \uparrow & \text{, ако } x \neq 0 \end{cases}$$

Функција θ је израчунљива и важи $\mathrm{Dom}(\theta) = \{0\} \neq \emptyset$ и $\theta \circ \theta$ јесте ,,1-1'', па важи $\theta \in \mathcal{A}$. Функција θ је коначна и важи $\theta \subseteq \mathbf{0}$ и $\theta \in \mathcal{A}$, па, на основу теореме 3.29, следи $\mathbf{0} \in \mathcal{A}$. Отуда, $\mathbf{0} \circ \mathbf{0} (= \mathbf{0})$ је ,,1-1'' функција, што је нетачно. Дакле, скуп A није рекурзивно набројив.

3.7.3 Продуктивни и креативни скупови

Креативни скупови су р.н. скупови чији комплементи нису р.н, али са додатним, појачаним условима.

Дефиниција 3.32 *Скуп A је* продуктиван *ако постоји тотална израчунљива функција g таква да важи:*

$$W_x \subseteq A \Rightarrow g(x) \in A \setminus W_x$$

Функцију g називамо продуктивном функцијом *за скуп A.*

[43] Приметимо да је тврђење које треба доказати еквивалентно тврђењу Рајсове теореме (теорема 3.19).

Ако је A продуктиван скуп, онда за сваки скуп $W_x \subseteq A$ важи $W_x \neq A$, па скуп A није р.н. Штавише, постоји ефективан начин за одређивање елемента који припада скупу $A \setminus W_x$.

Пример 3.5 *Следећи скупови су продуктивни:*

(*i*) $\{x \mid \Phi_x \neq \mathbf{0}\}$

(*ii*) $\{x \mid c \notin W_x\}$ *(где је c дат природан број)*

(*iii*) $\{x \mid c \notin E_x\}$ *(где је c дат природан број)*

Дефиниција 3.33 *Скуп је* креативан *ако и само ако је рекурзивно набројив и његов комплемент је продуктиван.*

Пример 3.6 *Следећи скупови су креативни:*
(а) $\{x \mid \Phi_x(x) = 0\}$
(б) $\{x \mid c \in W_x\}$ *(где је c дат природан број)*
(в) $\{x \mid c \in E_x\}$ *(где је c дат природан број)*

Теорема 3.30 *Продуктиван скуп садржи бесконачан р.н. скуп.*[44]

Последица 3.1 *Ако је скуп A креативан, онда скуп $\overline{A}$ садржи бесконачан р.н. скуп.*

3.7.4 Прости скупови

Дефиниција 3.34 *Скуп A је* прост *ако важи*

(*i*) *A је р.н;*

(*ii*) $\overline{A}$ *је бесконачан;*

(*iii*) $\overline{A}$ *не садржи бесконачан р.н. скуп.*

Задатак 137 *Доказати да прост скуп није ни рекурзиван ни креативан.*

[44] Доказ теореме се може наћи у [4].

Решење:

Нека је A прост скуп. Тада је, на основу дефиниције простог скупа, скуп $\overline{A}$ бесконачан и не садржи бесконачан р.н. скуп. Одатле следи да он није р.н. (видети задатак 132).

Претпоставимо супротно — да скуп A јесте рекурзиван. Онда, на основу Постове теореме (теорема 3.27), следи да је скуп $\overline{A}$ р.н. што противречи претходном закључку да $\overline{A}$ не садржи бесконачан р.н. подскуп. Дакле, скуп A није рекурзиван.

Слично, ако би скуп A био креативан, онда би његов комплемент садржао бесконачан р.н. скуп, а то би, на основу последице 3.1, противречило чињеници да је скуп A прост. Дакле, скуп A није креативан.

Задатак 138 *Нека је $f : \mathbf{N} \to \mathbf{N}$ тотална израчунљива „1-1” функција и нека скуп* $\mathrm{Range}(f)$ *није рекурзиван. Доказати да је прост скуп*

$$A = \{x \mid (\exists y > x)\ f(y) < f(x)\}.$$

3.8 Сводљивост и степени

Често се у решавању проблема теорије израчунљивости користи принцип редукције, то јест свођења једног проблема на други. На пример, тај приступ смо користили у доказу Рајсове теореме (теорема 3.19), где смо доказали да постоји тотална израчунљива функција k таква да је $x \in W_x \Leftrightarrow \Phi_{k(x)} \in \mathcal{A}$, чиме смо проблем „$\Phi_x \in \mathcal{A}$” свели на проблем „$x \in W_x$”.

Могуће је прецизније увести појам сводљивости[45] чиме је индукован и појам степена (или тежине). Уместо сводљивости између проблема чешће се разматра појам сводљивости између скупова који се неформално може описати на следећи начин: „*Ако је дата процедура одлучивања за проблем ‘$x \in B$’, онда је могуће конструисати процедуру одлучивања за проблем ‘$x \in A$’.*”

3.8.1 m-сводљивост

Дефиниција 3.35 *Скуп A је* m-сводљив[46] *на скуп B, у ознаци $A \leq_m B$, ако постоји тотална израчунљива функција f таква да за сваку вредност x ($x \in \mathbf{N}$) важи:*

$$x \in A \;\Leftrightarrow\; f(x) \in B$$

Са $f : A \leq_m B$ означавамо да је f тотална израчунљива функција која доказује сводљивост скупа A на скуп B.

[45] Уобичајена су два приступа: m-сводљивост и Тјуринг сводљивост.

[46] Термин m-сводљивост је скраћени облик од *many-one* сводљивост.

Теорема 3.31 *Релација $\leq_m$ задовољава следеће услове:*[47]

(*i*) *Релација $\leq_m$ је рефлексивна и транзитивна.*

(*ii*) $A \leq_m B \ \Leftrightarrow\ \overline{A} \leq_m \overline{B}$

(*iii*) *Ако је скуп A рекурзиван и $B \leq_m A$, онда је и скуп B рекурзиван.*

(*iv*) *Ако је скуп A рекурзиван, $B \neq \emptyset$ и $B \neq \mathbf{N}$, онда је $A \leq_m B$.*

(*v*) *Ако је A р.н. скуп и $B \leq_m A$, онда је и B р.н. скуп.*

(*vi*) $A \leq_m \mathbf{N} \ \Leftrightarrow\ A = \mathbf{N}$

(*vii*) $A \leq_m \emptyset \ \Leftrightarrow\ A = \emptyset$

(*viii*) $\mathbf{N} \leq_m A \ \Leftrightarrow\ A \neq \emptyset$

(*ix*) $\emptyset \leq_m A \ \Leftrightarrow\ A \neq \mathbf{N}$

Теорема 3.32 *Скуп A је р.н. ако и само ако важи $A \leq_m K$, где је $K = \{x \mid x \in W_x\}$.*[48]

Задатак 139 *Нека је $A = \{2x+1 \mid x \in \mathbf{N}\}$ и $B = \{x^2 \mid x \in \mathbf{N}\}$. Доказати да важи $A \leq_m B$.*

Решење:

Дефинишимо функцију $f : \mathbf{N} \to \mathbf{N}$ на следећи начин:

$$f(x) = \begin{cases} x^2 & \text{, ако је } x \text{ непаран} \\ 2 & \text{, ако је } x \text{ паран} \end{cases}$$

Функција f је тотална и израчунљива и важи:

$$\begin{aligned} x \in A \ &\Leftrightarrow\ x \text{ је непаран} \\ &\Leftrightarrow\ f(x) \in B, \end{aligned}$$

па важи $A \leq_m B$, што је и требало доказати.

Задатак 140 *Нека је $A = \{x \mid \Phi_x = \mathbf{0}\}$. Доказати да важи $K \leq_m A$, где је $K = \{x \mid x \in W_x\}$.*

[47] Доказ теореме се може наћи у [4].
[48] Доказ теореме се може наћи у [4].

Решење:

Дефинишимо функцију $f : \mathbf{N}^2 \to \mathbf{N}$ на следећи начин:

$$f(x,y) \simeq \begin{cases} 0 & , \text{ако } x \in W_x \\ \uparrow & , \text{ако } x \notin W_x \end{cases}$$

Функција f је израчунљива, па на основу $s-m-n$ теореме важи:

$$f(x,y) \simeq \Phi_{k(x)}(y)$$

за неку тоталну израчунљиву функцију $k : \mathbf{N} \to \mathbf{N}$. Важи:

$$\begin{aligned} x \in K & \Leftrightarrow x \in W_x \\ & \Leftrightarrow (\forall y) f(x,y) = 0 \\ & \Leftrightarrow (\forall y) \Phi_{k(x)}(y) = 0 \\ & \Leftrightarrow \Phi_{k(x)} = \mathbf{0} \\ & \Leftrightarrow k(x) \in A \end{aligned}$$

одакле следи $k :\ K \leq_m A$, што је и требало доказати.

Задатак 141 *Нека је $A = \{x \mid x \in E_x\}$. Доказати да важи $K \leq_m A$, где је $K = \{x \mid x \in W_x\}$.*

Решење:

Дефинишимо функцију $f : \mathbf{N}^2 \to \mathbf{N}$ на следећи начин:

$$f(x,y) = \begin{cases} y & , \text{ако } x \in W_x \\ \uparrow & , \text{ако } x \notin W_x \end{cases}$$

Функција f је израчунљива, па на основу $s-m-n$ теореме важи:

$$f(x,y) \simeq \Phi_{k(x)}(y)$$

за неку тоталну израчунљиву функцију $k : \mathbf{N} \to \mathbf{N}$. Важи:

$$\begin{aligned} x \in K & \Leftrightarrow x \in W_x \\ & \Leftrightarrow f(x, k(x)) = k(x) \\ & \Leftrightarrow \Phi_{k(x)}(k(x)) = k(x) \\ & \Leftrightarrow k(x) \in E_{k(x)} \\ & \Leftrightarrow k(x) \in A, \end{aligned}$$

одакле следи да важи $k :\ K \leq_m A$, што је и требало доказати.

Задатак 142 *Доказати да је скуп A р.н. ако и само ако је $A \leq_m K$, где је $K = \{x \mid x \in W_x\}$.*

Решење:

(⇒:) Претпоставимо да је скуп A р.н. Нека је функција $f : \mathbf{N}^2 \to \mathbf{N}$ дефинисана на следећи начин:

$$f(x,y) = \begin{cases} 1 & \text{, ако } x \in A \\ \uparrow & \text{, ако } x \notin A \end{cases}$$

Скуп A је р.н, па је функција f израчунљива. На основу $s-m-n$ теореме важи:

$$f(x,y) \simeq \Phi_{k(x)}(y)$$

за неку тоталну израчунљиву функцију $k : \mathbf{N} \to \mathbf{N}$. Важи:

$$\begin{aligned} x \in A &\Leftrightarrow f(x,k(x)) = 1 \\ &\Leftrightarrow \Phi_{k(x)}(k(x)) \downarrow \\ &\Leftrightarrow k(x) \in W_{k(x)} \\ &\Leftrightarrow k(x) \in K \end{aligned}$$

одакле следи да $k :\ A \leq_m K$, што је и требало доказати.

(⇐:) Претпоставимо да важи $f :\ A \leq_m K$, тј. претпоставимо да је $f : \mathbf{N} \to \mathbf{N}$ тотална, израчунљива функција таква да је

$$x \in A \Leftrightarrow f(x) \in K.$$

Скуп K је р.н, па, на основу теореме 3.28, следи да постоји израчунљива функција g таква да је $K = \mathrm{Dom}(g)$. Важи:

$$\begin{aligned} x \in A &\Leftrightarrow f(x) \in K \\ &\Leftrightarrow f(x) \in \mathrm{Dom}(g) \\ &\Leftrightarrow g(f(x)) \downarrow \\ &\Leftrightarrow x \in \mathrm{Dom}(g \circ f). \end{aligned}$$

Дакле, $A = \mathrm{Dom}(g \circ f)$, па, како је функција $g \circ f$ израчунљива, на основу теореме 3.28, следи да је скуп A р.н.

3.8.2 m-еквивалентност и степени

Дефиниција 3.36 *Скупови A и B су* m-еквивалентни, *у ознаци $A \equiv_m B$ ако и само ако важи $A \leq_m B$ и $B \leq_m A$.*

Теорема 3.33 *Релација $\equiv_m$ је релација еквиваленције.*

Дефиниција 3.37 *Класу еквиваленције скупа A за релацију $\equiv_m$ називамо* m-степеном *скупа A, у ознаци $d_m(A)$. Дакле,*

$$d_m(A) = \{B \mid A \equiv_m B\}.$$

Дефиниција 3.38 *Нека су* $\mathbf{a}$ *и* $\mathbf{b}$ *m-степени.*

(*i*) *Ако постоје скупови* A *и* B *такви да важи* $A \in \mathbf{a}$, $B \in \mathbf{b}$ *и* $A \leq_m B$, *онда то записујемо* $\mathbf{a} \leq_m \mathbf{b}$.

(*ii*) *Ако важи* $\mathbf{a} \leq \mathbf{b}$ *и* $\mathbf{a} \neq \mathbf{b}$, *онда то записујемо* $\mathbf{a} <_m \mathbf{b}$.

Дефиниција 3.39 *Релација* $<_m$ *је парцијално уређење m-степена.*

Задатак 143 *Нека је* A *рекурзиван скуп такав да је* $A \neq \emptyset$ *и* $A \neq \mathbf{N}$. *Доказати да је* $A \equiv_m \overline{A}$.

Решење:

Како је $A \neq \emptyset$ и $A \neq \mathbf{N}$, то је $\overline{A} \neq \emptyset$ и $\overline{A} \neq \mathbf{N}$. Даље, скуп A је рекурзиван, па је, на основу теореме 3.31 (*iv*), $A \leq_m \overline{A}$. Одавде, на основу исте теореме (*ii*), важи и обратно, тј. $\overline{A} \leq_m A$. Дакле, важи $A \leq_m \overline{A}$ и $\overline{A} \leq_m A$, па значи и $A \equiv_m \overline{A}$, што је и требало доказати.

Задатак 144 *Нека је* A *рекурзивно набројив али не и рекурзиван скуп. Доказати да не важи* $A \equiv_m \overline{A}$.

Решење:

Претпоставимо супротно — да важи $A \equiv_m \overline{A}$. Одатле следи да $\overline{A} \leq_m A$. Одатле, како је A рекурзивно набројив скуп, на основу теореме 3.31 под (*v*), следи да је и скуп $\overline{A}$ такав. Како су A и $\overline{A}$ рекурзивно набројиви скупови, то, на основу Постове теореме (теорема 3.27), значи да је скуп A рекурзиван. То, међутим, противречи претпоставци да овај скуп није рекурзиван. Дакле, не важи $A \equiv_m \overline{A}$.

Задатак 145 *Доказати да важи* $\{x \mid \Phi_x \text{ је тотална}\} \equiv_m \{x \mid \Phi_x = \mathbf{0}\}$.

Решење:

Означимо са T скуп $\{x \mid \Phi_x \text{ је тотална}\}$, а са A скуп $\{x \mid \Phi_x = \mathbf{0}\}$.

($T \leq_m A$:) Нека је функција $f : \mathbf{N}^2 \rightarrow \mathbf{N}$ дефинисана на следећи начин:

$$f(x,y) = \begin{cases} 0 & \text{, ако } y \in W_x \\ \uparrow & \text{, ако } y \notin W_x \end{cases}$$

Важи $f(x,y) \simeq \mathbf{0}(\Psi_u(x,y))$, па је функција f израчунљива. На основу $s-m-n$ теореме важи:

$$f(x,y) \simeq \Phi_{k(x)}(y)$$

за неку тоталну израчунљиву функцију $k : \mathbf{N} \to \mathbf{N}$. Важи:

$$\begin{aligned} x \in T &\Leftrightarrow \Phi_x \text{ је тотална} \\ &\Leftrightarrow W_x = \mathbf{N} \\ &\Leftrightarrow (\forall y) y \in W_x \\ &\Leftrightarrow (\forall y) f(x,y) = 0 \\ &\Leftrightarrow (\forall y) \Phi_{k(x)}(y) = 0 \\ &\Leftrightarrow \Phi_{k(x)} = \mathbf{0} \\ &\Leftrightarrow k(x) \in A. \end{aligned}$$

Дакле, $k : T \leq_m A$.

($A \leq_m T$:) Нека је функција $f : \mathbf{N}^2 \to \mathbf{N}$ дефинисана на следећи начин:

$$f(x,y) = \begin{cases} 0 & \text{, ако } \Phi_x(y) = 0 \\ \uparrow & \text{, ако } \Phi_x(y) \neq 0 \end{cases}$$

Предикат $\Phi_x(y) = 0$ је парцијално одлучив, па је функција f израчунљива. На основу $s - m - n$ теореме важи:

$$f(x,y) \simeq \Phi_{k(x)}(y)$$

за неку тоталну израчунљиву функцију $k : \mathbf{N} \to \mathbf{N}$. Важи:

$$\begin{aligned} x \in A &\Leftrightarrow \Phi_x = \mathbf{0} \\ &\Leftrightarrow (\forall y) \Phi_x(y) = 0 \\ &\Leftrightarrow (\forall y) f(x,y) \downarrow \\ &\Leftrightarrow (\forall y) \Phi_{k(x)}(y) \downarrow \\ &\Leftrightarrow \Phi_{k(x)} \text{ је тотална} \\ &\Leftrightarrow k(x) \in T. \end{aligned}$$

Дакле, важи $k :\ A \leq_m T$.

Задатак 146 *Доказати да важи* $\{x \mid \text{скуп } W_x \text{ је бесконачан}\} \equiv_m \{x \mid \Phi_x = \mathbf{0}\}$.

Задатак 147 *Ако за* $A \in \mathbf{a}$ *са* $\mathbf{a}^*$ *означимо* m*-степен* $d_m(\overline{A})$ *доказати:*

(а) $\mathbf{a}^*$ *не зависи од* A

(б) $(\mathbf{a} \cup \mathbf{a}^*)^* = \mathbf{a} \cup \mathbf{a}^*$

Решење:

(а) Треба доказати да за произвољне елементе m-степена $\mathbf{a}$, A и B, важи $d_m(\overline{A}) = d_m(\overline{B})$. То, на основу дефиниције m-степена, значи да $\overline{A} \equiv_m \overline{B}$ треба да важи кад год је $A \equiv_m B$:

$$\begin{aligned} A \equiv_m B \Leftrightarrow & A \leq_m B \wedge B \leq_m A \\ & \text{(на основу дефиниције релације } \equiv_m) \\ \Leftrightarrow & \overline{A} \leq_m \overline{B} \wedge \overline{B} \leq_m \overline{A} \\ & \text{(на основу теореме 3.31 } (ii)) \\ \Leftrightarrow & \overline{A} \equiv_m \overline{B} \\ & \text{(на основу дефиниције релације } \equiv_m) \end{aligned}$$

(б) На основу дефиниције m-степена и делу задатка под (а) непосредно се изводи следеће тврђење:

$$A \in \mathbf{a} \Leftrightarrow \overline{A} \in \mathbf{a}^* \tag{3.1}$$

Сада се једноставно изводи тражено тврђење на следећи начин:

$$\begin{aligned} A \in \mathbf{a} \cup \mathbf{a}^* \Leftrightarrow & A \in \mathbf{a} \vee A \in \mathbf{a}^* \\ \Leftrightarrow & \overline{A} \in \mathbf{a}^* \vee \overline{A} \in \mathbf{a} \\ & \text{(на основу (3.1))} \\ \Leftrightarrow & \overline{A} \in \mathbf{a} \cup \mathbf{a}^* \\ \Leftrightarrow & A \in (\mathbf{a} \cup \mathbf{a}^*)^* \\ & \text{(на основу 3.1)} \end{aligned}$$

3.9 Теореме рекурзије

3.9.1 Прва теорема рекурзије

Дефиниција 3.40 Оператором *називамо пресликавање* $\Phi : \mathcal{F}_m \to \mathcal{F}_n$ *(где је* $\mathcal{F}_n$ *класа свих парцијалних функција из* $\mathbf{N}^n$ *у* $\mathbf{N}$*). Оператор* Φ *је* рекурзиван *ако и само ако постоји израчунљива функција* $\phi : \mathbf{N}^{n+1} \to \mathbf{N}$ *таква да за сваку функцију* f $(f \in \mathcal{F}_m)$ *и* $\vec{x}$ $(\vec{x} \in \mathbf{N}^n)$, y $(y \in \mathbf{N})$ *важи:*

$$\Phi(f)(\vec{x}) \simeq y \;\Leftrightarrow\; \textit{постоји коначна функција } \theta \subseteq f \textit{ таква да је } \phi(\tilde{\theta}, \vec{x}) \simeq y$$

(где је $\tilde{\theta}$ *кôд коначне функције* θ*).*[49]

Пример 3.7 *Оператор* $\Phi(f) = 2f$ *је рекурзиван. То се може доказати коришћењем функције* $\phi : \mathbf{N}^2 \to \mathbf{N}$ *дефинисане на следећи начин:*

$$\phi(z, x) \simeq \begin{cases} 2\theta(x) & , \textit{ако } z = \tilde{\theta} \textit{ и } x \in \mathrm{Dom}(\theta) \\ \uparrow & , \textit{иначе} \end{cases}$$

[49] Приметимо да функција ϕ не мора да буде тотална.

Функција ϕ је израчунљива и важи

$$\Phi(f)(x) \simeq y \;\Leftrightarrow\; \text{постоји коначна функција } \theta \subseteq f \text{ таква да је } \phi(\tilde{\theta}, x) \simeq y,$$

па је оператор Φ рекурзиван.

Теорема 3.34 (Прва теорема рекурзије) *Нека је $\Phi : \mathcal{F}_n \to \mathcal{F}_n$ рекурзиван оператор. Тада постоји израчунљива функција $f_\Phi : \mathbf{N}^n \to \mathbf{N}$ која је најмања непокретна тачка пресликавања Φ, тј:*

(*i*) $\Phi(f_\Phi) = f_\Phi$

(*ii*) *Ако је $\Phi(g) = g$, онда је $f_\Phi \subseteq g$.*

Дакле, ако је функција f_Φ тотална, онда је она једина непокретна тачка пресликавања Φ.[50]

Пример 3.8 *Нека је рекурзивни оператор $\Phi : \mathcal{F}_1 \to \mathcal{F}_1$ дефинисан са:*

$$\begin{gathered}\Phi(f)(0) = 1 \\ \Phi(f)(x+1) \simeq f(x+2)\end{gathered}$$

Најмања непокретна тачка овако дефинисаног рекурзивног оператора је функција f_Φ за коју је $f_\Phi(0) = 1$ и вредност $f_\Phi(x+1)$ није дефинисана за све x ($x \in \mathbf{N}$).

Прва теорема рекурзије, између осталог, користи се за давање значења рекурзивним програмима (који се могу описати везом $f(\vec{x}) = \tau(f, \vec{x})$).

Задатак 148 *Доказати да постоји тачно једна функција $A : \mathbf{N}^2 \to \mathbf{N}$ која задовољава услове:*

(*i*) $A(0, y) = y + 1$

(*ii*) $A(x+1, 0) = A(x, 1)$

(*iii*) $A(x+1, y+1) = A(x, A(x+1, y))$

и да је она тотална и израчунљива.[51]

---

[50] Ова теорема се често назива првом теоремом о непокретној тачки, односно првом теоремом о фиксној тачки. Доказ теореме се може наћи у [4].

[51] У одељку 3.3.1 смо на овај начин дефинисали Акерманову функцију.

Решење:

Дефинишимо оператор $\Phi : \mathcal{F}_2 \to \mathcal{F}_2$ на следећи начин:

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

Докажимо да је овако дефинисан оператор рекурзиван.

Дефинишимо функцију $\phi : \mathbf{N}^3 \to \mathbf{N}$ на следећи начин:

$$\begin{aligned}\phi(\tilde{\theta},0,y) &= y+1\\ \phi(\tilde{\theta},x+1,0) &= \theta(x,1)\\ \phi(\tilde{\theta},x+1,y+1) &= \theta(x,f(x+1,y))\end{aligned}$$

Користећи метод аналоган оном коришћеном у задатку 71 и тврђење о ефективној набројивости свих URM програма (теорема 3.11), па, на основу Черчове тезе, и свих израчунљивих функција, може се доказати да је функција ϕ израчунљива. То значи да дати оператор, Φ, јесте рекурзиван. Отуда, на основу прве теореме рекурзије (теорема 3.34), постоји *израчунљива* функција $f_\Phi : \mathbf{N}^2 \to \mathbf{N}$ која је непокретна тачка пресликавања Φ, тј. $\Phi(f_\Phi) = f_\Phi$, или прецизније:

$$\begin{aligned}f_\Phi(0,y) &= y+1\\ f_\Phi(x+1,0) &= f_\Phi(x,1)\\ f_\Phi(x+1,y+1) &= f_\Phi(x,f(x+1,y))\end{aligned}$$

Приметимо да функција A дефинисана једнакостима (i)-(iii) задовољава ове услове, тј. да она јесте непокретна тачка пресликавања Φ. Ако је ова функција још и *тотална*, онда ће она, на основу прве теореме рекурзије (теорема 3.34), бити и *једина* непокретна тачка пресликавања Φ, то јест једнакости (i)-(iii) ће задовољавати тачно једна функција A. Докажимо, дакле, да функција дефинисана једнакостима (i)-(iii) јесте тотална. Доказ изводимо индукцијом по x.

За $x = 0$ важи $A(0,y) = y+1$ (на основу једнакости (i)), па је вредност $A(0,y)$ дефинисана за све природне бројеве y.

Претпоставимо да је вредност $A(x,y)$ дефинисана за све природне бројеве y и докажимо да исто важи и за вредност $A(x+1,y)$. То ћемо учинити користећи индукцију по y.

За $x = 0$ важи $A(x+1,0) = A(x,1)$ (на основу једнакости (ii)), па како је, на основу индукцијске претпоставке, вредност $A(x,1)$ дефинисана, исто важи и за вредност $A(x+1,0)$.

Даље, претпоставимо да је вредност $A(x+1,y)$ дефинисана и докажимо да то важи и за вредност $A(x+1,y+1)$. На основу једнакости (iii)

важи $A(x+1, y+1) = A(x, A(x+1, y))$. Вредност $A(x+1, y)$ је дефинисана (на основу индукцијске претпоставке (за y)), па је онда дефинисана и вредност $A(x, A(x+1, y))$ (на основу индукцијске претпоставке (за x)). Отуда, дефинисана је и вредност $A(x+1, y+1)$.

Дакле, вредност $A(x, y)$ је дефинисана за све природне бројеве x и y, тј. функција A је тотална, што је и требало доказати.

3.9.2 Друга теорема рекурзије

Теорема 3.35 (Друга теорема рекурзије) *Нека је f тотална унарна израчунљива функција. Тада постоји вредност n ($n \in \mathbf{N}$) таква да је*[52]

$$\Phi_{f(n)} = \Phi_n.$$

Доказ:
На основу $s{-}m{-}n$ теореме, постоји тотална израчунљива функција $s : \mathbf{N} \to \mathbf{N}$ таква да за све вредности x ($x \in \mathbf{N}$) важи:

$$\Phi_{f(\Phi_x(x))}(y) \simeq \Phi_{s(x)}(y),$$

где израз на левој страни не мора увек да буде дефинисан. Нека је m вредност таква да је $s = \Phi_m$. Тада важи:

$$\Phi_{f(\Phi_x(x))}(y) \simeq \Phi_{\Phi_m(x)}(y).$$

За $x = m$ и $n = \Phi_m(m)$ добијамо:

$$\Phi_{f(n)}(y) \simeq \Phi_n(y),$$

што доказује тврђење теореме. $\Box$

Последица 3.2 *Ако је f тотална унарна израчунљива функција, онда постоји вредност n ($n \in \mathbf{N}$) таква да важи:*

$$W_{f(n)} = W_n \ \wedge \ E_{f(n)} = E_n.$$

Последица 3.3 *Ако је $f : \mathbf{N} \to \mathbf{N}$ израчунљива функција, онда постоји вредност $e \in \mathbf{N}$ таква да за све вредности y важи:*

$$f(e, y) \simeq \Phi_e(y).$$

[52] Ова теорема се често назива другом теоремом о непокретној тачки, односно другом теоремом о фиксној тачки.

Доказ:
Како је f израчунљива функција, на основу $s-m-n$ теореме следи да постоји тотална израчунљива функција $k : \mathbf{N} \to \mathbf{N}$ таква да важи:

$$f(x, y) \simeq \Phi_{k(x)}(y).$$

С друге стране, на основу друге теореме о непокретној тачки (теорема 3.35), постоји вредност e ($e \in \mathbf{N}$) таква да важи:

$$\Phi_{k(e)} = \Phi_e.$$

За ту, фиксирану вредност e важи:

$$f(e, y) \simeq \Phi_{k(e)} \simeq \Phi_e(y).$$

$\square$

Задатак 149 *Доказати да важи:*

$$(\exists n)(\forall x)\ \Phi_n(x) = x^n.$$

Решење:
Дефинишимо функцију $f : \mathbf{N}^2 \to \mathbf{N}$ на следећи начин:

$$f(m, x) = x^m.$$

Функција f је израчунљива, па, на основу последице 3.3 друге теореме о непокретној тачки, за све вредности x ($x \in \mathbf{N}$) важи:

$$(\exists n)\ f(n, x) \simeq \Phi_n(x),$$

односно

$$(\exists n)\ \Phi_n(x) = x^n.$$

Задатак 150 *Доказати да постоји природан број n такав да важи* $W_n = E_n = \{n\}$.

Решење:
Дефинишимо функцију $f : \mathbf{N}^2 \to \mathbf{N}$ на следећи начин:

$$f(x, y) \simeq \begin{cases} 0 & \text{, ако } x = y \\ \uparrow & \text{, иначе} \end{cases}$$

Функција f је израчунљива, па, на основу $s - m - n$ теореме, постоји тотална израчунљива функција $k : \mathbf{N} \to \mathbf{N}$ таква да важи:

$$f(x, y) \simeq \Phi_{k(x)}(y)$$

На основу друге теореме о непокретној тачки (теорема 3.35), постоји вредност n ($n \in \mathbf{N}$) за коју је

$$\Phi_{k(n)} = \Phi_n$$

Нека је n једна таква вредност. За њу онда важи и:

$$f(n,y) \simeq \Phi_n(y) \tag{3.2}$$

за све вредности y ($y \in \mathbf{N}$). Докажимо да ова вредност задовољава задати услов.

$$\begin{aligned} W_n =& \{y \mid \Phi_n(y)\downarrow\} \\ =& \{y \mid f(n,y)\downarrow\} \\ & \text{(на основу (3.2))} \\ =& \{y \mid y = n\} \\ & \text{(на основу дефиниције функције } f) \\ =& \{n\} \end{aligned}$$

$$\begin{aligned} E_n =& \Phi_n(W_n) \\ =& \Phi_n(\{n\}) \\ & \text{(на основу горње једнакости)} \\ =& \{n\} \\ & \text{(на основу (3.2) и дефиниције функције } f) \end{aligned}$$

Задатак 151 *Испитати да ли постоји природан број x такав да $\Phi_x(y) \simeq \Phi_y(x)$ важи за све природне бројеве y.*

Решење:

Дефинишимо функцију $f : \mathbf{N}^2 \to \mathbf{N}$ на следећи начин:

$$f(x,y) \simeq \Phi_y(x)$$

Функција f је израчунљива, па, на основу $s-m-n$ теореме, постоји тотална израчунљива функција $k : \mathbf{N} \to \mathbf{N}$ таква да важи:

$$f(x,y) \simeq \Phi_{k(x)}(y)$$

На основу друге теореме о непокретној тачки (теорема 3.35), постоји вредност x ($x \in \mathbf{N}$) за коју је

$$\Phi_{k(x)} = \Phi_x$$

Нека је x једна таква вредност. Из последње две једнакости следи да

$$f(x,y) \simeq \Phi_x(y)$$

за све вредности y ($y \in \mathbf{N}$). На основу последње једнакости и начина на који је дефинисана функција f следи да је

$$\Phi_x(y) \simeq \Phi_y(x)$$

за све y ($y \in \mathbf{N}$).

Задатак 152 *Нека је скуп $\mathcal{A}$ непразан, прави подскуп скупа $\mathcal{C}^{(1)}$. Доказати да скуп $A = \{x \mid \Phi_x \in \mathcal{A}\}$ није рекурзиван.*[53]

Решење:

Претпоставимо супротно — да скуп A јесте рекурзиван. Скуп $\mathcal{A}$ је непразан, прави подскуп скупа $\mathcal{C}^{(1)}$, па постоје вредности a и b такве да је $a \in \mathcal{A}$ и $b \notin \mathcal{A}$. За те, фиксиране вредности a и b, дефинишимо функцију $f : \mathbf{N} \to \mathbf{N}$ на следећи начин:

$$f(x) = \begin{cases} b & \text{, ако } x \in A \\ a & \text{, ако } x \notin A \end{cases}$$

Скуп A је, на основу претпоставке, рекурзиван, па је функција f израчунљива. На основу друге теореме о непокретној тачки (теорема 3.35) следи да постоји вредност n ($n \in \mathbf{N}$) таква да важи:

$$\Phi_{f(n)} = \Phi_n.$$

За ту, фиксирану вредност n важи:

$$\begin{aligned} f(n) \in A \; & \Leftrightarrow \Phi_{f(n)} \in \mathcal{A} \\ & \quad \text{(на основу дефиниције скупа } A\text{)} \\ & \Leftrightarrow \Phi_n \in \mathcal{A} \\ & \quad \text{(јер је } \Phi_{f(n)} = \Phi_n\text{)} \\ & \Leftrightarrow n \in A \\ & \quad \text{(на основу дефиниције скупа } A\text{)} \end{aligned}$$

што противречи дефиницији функције f, на основу које је

$$f(x) \in A \;\Leftrightarrow\; x \notin A.$$

Дакле, скуп A није рекурзиван.

Задатак 153 *Нека је f тотална унарна израчунљива функција. Доказати да постоји бесконачно много вредности n ($n \in \mathbf{N}$) таквих да важи:*

$$\Phi_{f(n)} = \Phi_n.$$

[53]Приметимо да је тврђење које треба доказати еквивалентно тврђењу Рајсове теореме (теорема 3.19).

Решење:

Нека је k произвољан природан број. Нека је вредност c таква да важи

$$\Phi_c \neq \Phi_0, \Phi_1, \ldots, \Phi_k.$$

Напомињемо да оваква вредност постоји, јер израчунљивих функција има бесконачно много.

Дефинишимо функцију $g : \mathbf{N} \to \mathbf{N}$ на следећи начин:

$$g(x) = \begin{cases} c & \text{, ако } x \leq k \\ f(x) & \text{, ако } x > k \end{cases}$$

Предикати $x \leq k$ и $x > k$ су одлучиви, па је функција g израчунљива. На основу друге теореме о непокретној тачки (теорема 3.35) постоји вредност n таква да важи:

$$\Phi_{g(n)} = \Phi_n.$$

Не важи $n \leq k$ (јер из $n \leq k$ следи $\Phi_{g(n)} = \Phi_c \neq \Phi_n$). Дакле, важи $n > k$ и $g(n) = f(n)$, па је $\Phi_{f(n)} = \Phi_{g(n)} = \Phi_n$, тј. n је непокретна тачка за функцију f. Како је $n > k$, а k је произвољна вредност, следи да постоји бесконачно много вредности n ($n \in \mathbf{N}$) таквих да важи:

$$\Phi_{f(n)} = \Phi_n,$$

што је и требало доказати.

Задатак 154 *Нека је $f : \mathbf{N} \to \mathbf{N}$ тотална растућа функција таква да важи:*

(*i*) *Ако $m \neq n$, онда $\Phi_{f(m)} \neq \Phi_{f(n)}$.*

(*ii*) *Вредност $f(n)$ је најмањи индекс функције $\Phi_{f(n)}$.*

Доказати да функција f није израчунљива.

Решење:

Претпоставимо супротно — да функција f јесте израчунљива. На основу услова (*i*), функција f није идентичка функција, па, како она јесте растућа, постоји вредност k таква да је

$$f(n) > n \ \text{ за } n \geq k,$$

одакле, на основу услова (*ii*), следи

$$\Phi_{f(n)} \neq \Phi_n \ \text{ за } n \geq k.$$

С друге стране, функција f је тотална израчунљива функција, па, на основу задатка 153, постоји вредност $n \geq k$ таква да је $\Phi_{f(n)} = \Phi_n$, што противречи услову (*i*). Дакле, функција f није израчунљива, што је и требало доказати.

Задатак 155 *Функција $f : \mathbf{N} \to \mathbf{N}$ је тотална и израчунљива.*

(а) *Доказати да постоји природан број n такав да важи $\Phi_{f(n+1999)} = \Phi_n$.*

(б) *Доказати да постоји природан број n такав да важи $\Phi_{f(n)} = \Phi_{n+1999}$.*

Решење:

(а) Дефинишимо функцију $g : \mathbf{N} \to \mathbf{N}$ на следећи начин:

$$g(n) = f(n + 1999)$$

Функција f је тотална и израчунљива, па је таква и функција g. На основу друге теореме рекурзије (3.35), постоји вредност n ($n \in \mathbf{N}$) таква да важи:

$$\Phi_{g(n)} = \Phi_n$$

За такву вредност n, на основу последње две једнакости, важи:

$$\Phi_{f(n+1999)} = \Phi_n,$$

што је и требало показати.

(б) Дефинишимо функцију $g : \mathbf{N} \to \mathbf{N}$ на следећи начин:

$$g(n) = f(n \dot{-} 1999)$$

Функција f је тотална и израчунљива, па је таква и функција g. На основу задатка 153 следи да постоји бесконачно много вредности m ($m \in \mathbf{N}$) таквих да важи $\Phi_{g(m)} = \Phi_m$. Дакле, постоји вредност n' ($n' > 1999$) за коју важи

$$\Phi_{g(n')} = \Phi_{n'}$$

Тада важи:

$$\Phi_{g(n')} = \Phi_{f(n' \dot{-} 1999)} = \Phi_{n'} \tag{3.3}$$

Нека је n' једна таква вредност и $n = n' \dot{-} 1999$. Како је $n' > 1999$ следи да је $n' = n + 1999$. Користећи ову једнакост, на основу (3.3), добијамо:

$$\Phi_{f(n)} = \Phi_{n+1999},$$

чиме смо доказали тражено тврђење.

Литература

[1] Brainerd, B. – *Introduction to the Mathematics of Language Studies.* American Elsevier Publishing Company, Inc., New York, 1977.

[2] Brookshear, J. G. – *Theory of Computation - Formal Languages, Automata, and Complexity.* The Banjamin/Cummings Publishing Company, Inc., 1989.

[3] Мадарас, Р. и С. Црвенковић. – *Увод у теорију аутомата и формалних језика.* Stylos и Природно-математички факултет Универзитета у Новом Саду, Нови Сад, 1995.

[4] Cutland, N. J. – *Computability - An Introduction to Recursive Function Theory.* Cambridge University Press, Cambridge, 1980.

[5] Hennie, F. – *Introduction to Computability.* Addison-Wesley Publishing Company, Roading, 1977.

[6] Лавров, И. А, Л. Л. Максимова. – *Задачи по теории множеств, математической логике и теории алгоритмов.* Наука, Москва, 1984.

[7] Mendelson, E. – *Introduction to Mathematical Logic.* D. Van Nostrand Company, Inc., Princeton, 1964.

[8] Прешић, М. – *Теорија формалних језика.* Скрипта, Математички факултет, Београд.

[9] Rabin, O. M. – *Decidable theories.* In Jon, Barwise, (ed.), *Handbook of Mathematical Logic*, pp. 595–629. North–Holland Publishing Company. 1977.

[10] Tarski, A., A. Mostowski, and M. R. Robinson. – *Undecidable Theories.* North Holland. 1953.