УНИВЕРЗИТЕТ У БЕОГРАДУ

МАТЕМАТИЧКИ ФАКУЛТЕТ

Јованка Свркота

Непотпуност Пеанове аритметике и Лебова теорема

Мастер рад

Београд, 2017.

Подаци о ментору и члановима комисије

Ментор:

Славко Моцоња, доцент
Универзитет у Београду, Математички факултет

Чланови комисије:

Славко Моцоња, доцент
Универзитет у Београду, Математички факултет

Небојша Икодиновић, доцент
Универзитет у Београду, Математички факултет

Предраг Тановић, ванредни професор
Универзитет у Београду, Математички факултет

Садржај

Предговор

У другој половини XIX века математичари су дошли на идеју да формализују целу математику тиме што ће пронаћи скуп аксиома на којима би она почивала. Пеанова аритметика је списак аксиома о природним бројевима које је крајем XIX века предложио Ђузепе Пеано у свом покушају да формализује аритметику. Циљ овог рада је да се упознамо са Геделовим резултатима о непотпуности Пеанове аритметике, као и са техником кодирања коју је он притом развио. Такође, биће представљена Лебова теорема, те примери тачних, али у Пеановој аритметици недоказивих реченица, које нам ова теорема пружа.

Курт Гедел (1906−1978.) је био аустријско-амерички математичар, логичар и филозоф. Поред Аристотела, Тарског и Фрегеа, сматра се једним од најзначајних логичара у историји човечанства.

Рођен 1906. у данашњем Брну, Чешка, већ како дете је испољавао велику радозналост. Школовање је започео у родном граду 1912. и тамо се школовао све до 1924. године, када одлази на студије у Беч, где се заинтересовао за математику и логику. Сматра се да је предавање Давида Хилберта којем је присуствовао у Болоњи 1928. године одредило Геделов животни правац. 1929. године је докторирао, а 1931. објавио своје две теореме о непотпуности, односно доказао да ниједна теорија која садржи Пеанову аритметику није потпуна, као и да се конзистентност такве теорије не може доказати у самој теорији. Ови Геделови резултати су окончали покушаје да се пронађе скуп аксиома које би биле довољне да се на њима утемељи целокупна математика, односно показали да формализација целе математике није могућа. Да би доказао поменута тврђења, Гедел је морао да пронађе начин како да кодира природне бројеве, тврђења и доказе, те је осмислио оно што данас називамо Геделовим бројевима или кодовима, а што су касније многи математичари, попут Тарског, Черча, Тјуринга, у свом раду користили. Гедел је умро 1978. године у Принстону.

Марин Хуго Леб (1921-2006.) је био немачки математичар. Рођен и одрастао у Берлину, непосредно пред избијање Другог светског рата напушта Немачку и одлази у Уједињено Краљевство. Бива депортован 1940. године у Аустралију, где почиње да се бави математиком. 1943. добија дозволу да се врати у Уједињено Краљевство, а након завршетка рата, започиње студије на Универзитету у Лондону. Након одбране докторске дисертације, постаје асистент на Универзитету у Лидсу, где ће 1967. постати и професор математичке логике. Леб је радио ис-

траживања везана за теорију доказа, модалну логику и теорију израчунљивости. Теорема коју је фомулисао 1955. године је његово најзначајније постигнуће, а данас се њему у част назива Лебова теорема. Она каже да *ако Пеанова аритметика доказује импликацију "ако је реченица F доказива у Пеановој аритметици, онда је F тачна", онда Пеанова аритметика доказује F*. Специјално, Лебова теорема нам даје примере тачних реченица које нису доказиве у Пеановој аритметици. Почетком 1970-их година Леб одлази на Универзитет у Амстердаму, где предаје све до одласка у пензију. Умро је 2006. године у Анену, Холандија.

1 Пеанова аритметика

Пеанова аритметика је теорија првог реда која формализује аритметичка својства природних бројева. Даље у тексту ћемо за овај појам користити ознаку PA. Уместо уобичајеног записа $PA \vdash S$, писаћемо краће $\vdash S$ како бисмо означили да је S теорема Пеанове аритметике. У првом делу рада видећемо да свакој формули S на језику PA можемо доделити терм на језику PA који означавамо $\ulcorner S \urcorner$ и који називамо Геделов код (или број) формуле S. Такође, дефинисаћемо формулу $Bew(x)$ тако да $Bew(\ulcorner S \urcorner)$ каже да се у PA може доказати формула S. $\Sigma-$реченице су реченице изграђене помоћу конјункције, дисјункције, егзистенцијалног квантификатора и ограниченог универзалног кватификатора ("за свако x мање од y"). Циљ првог дела рада је да докажемо следећих пет особина ових појмова.

(i) Ако је $\vdash S$, онда $\vdash Bew(\ulcorner S \urcorner)$,

(ii) $\vdash Bew(\ulcorner (S \to T) \urcorner) \to (Bew(\ulcorner S \urcorner) \to Bew(\ulcorner T \urcorner))$,

(iii) $\vdash Bew(\ulcorner S \urcorner) \to Bew(\ulcorner Bew(\ulcorner S \urcorner) \urcorner)$,

(iv) $Bew(\ulcorner S \urcorner)$ је $\Sigma-$реченица,

(v) Ако је S $\Sigma-$реченица, онда $\vdash S \to Bew(\ulcorner S \urcorner)$.

Услови (i), (ii), (iii) су познати као Хилберт-Бернај-Лебови услови извођења.

1.1 Синтакса и семантика Пеанове аритметике

Азбука Пеанове аритметике се састоји од скупа логичких и скупа нелогичких симбола. Скуп логичких симбола чине бесконачо пребројив скуп променљивих $\{v_0, v_1, v_2 ...\}$, четири логичка симбола $\bot$, $\to$, $\forall$ и знак $=$, те помоћни симболи (и). Скуп нелогичких симбола чине један симбол константе $\mathbf{0}$, један унарни функцијски симбол $\mathbf{s}$ и два бинарна функцијска симбола $+$ и $\cdot$.

У наставку дајемо експлицитне дефиниције појмова који ће нам бити потребни.

Дефиниција 1.1
Уређени пар *за неке објекте a и b је објекат $\langle a, b \rangle$.*

Закон уређених парова: Ако $\langle a, b \rangle = \langle c, d \rangle$, онда $a = b$ и $c = d$.

Дефиниција 1.2
Уређена тројка *$\langle a, b, c \rangle$ за неке објекте a, b и c је објекат $\langle a, \langle b, c \rangle \rangle$.*

Дакле, ако је $\langle a, b, c \rangle = \langle d, e, f \rangle$, онда је $a = d$, $b = e$ и $c = f$.

Дефиниција 1.3

Коначан низ *s је било која уређена $k-$торка (k је природан број), где s_i означава вредност низа на $i-$том месту. Претпостављамо да постоји коначан низ дужине 0, и да за сваки коначан низ s дужине k и сваки објекат a, постоји коначан низ s' дужине $k+1$, такав да за свако $i < k$, $s'_i = s_i$ и $s'_k = a$. Ако је коначан низ s дужине k, онда је s_0 његова прва вредност,а s_{k-1} последња.*

Закон коначних низова: Коначи низови су идентични ако имају исте дужине k и исте вредности за све $i < k$.

Коначан низ s дужине k чији је i-ти члан, $i < k$, једнак s_i, обележавамо $[s_0, s_1, ..., s_{k-1}]$. Стога, [ ] је коначан низ дужине 0.

Напомена

Када су у питању низови коначне дужине, често изостављамо заграде.

Дефиниција 1.4

За t кажемо да је ***терм*** *у PA ако и само ако постоји коначан низ чија је последња вредност t, а свака претходна вредност низа је* ***0****, променљива, уређени пар* ***s****-а и претходне вредности низа, уређена тројка знака $+$ и две претходне вредности низа, или уређена тројка знака $\cdot$ и две претходне вредности низа.*

Напомена

Израз $t = t'$ ћемо сматрати уређеном тројком симбола $=$, t и t'.

Дефиниција 1.5

F је ***атомска формула*** *ако је чини симбол $\perp$, или ако је за неке термове t и t', F једнака изразу $t = t'$.*

Напомена

Израз $F \to F'$ ћемо сматрати уређеном тројком симбола $\to$, F и F', а израз $\forall v F$ уређеном тројком симбола $\forall$, v и F.

Дефиниција 1.6

F је ***формула*** *у PA ако и само ако постоји коначан низ чија је последња вредност F, а свака претходна вредност низа је атомска формула, уређена тројка симбола $\to$ и две претходне вредности низа, или уређена тројка $\forall$, неке променљиве и неког претходног члана низа.*

Израз $\neg F$, негацију формуле F, дефинишемо као $(F \to \perp)$. $t \neq t'$ је, као и обично, скраћеница за $\neg t = t'$. Такође, претпостављамо да су остали познати логички симболи, попут $\wedge, \vee, \leftrightarrow$ и $\exists$, дефинисани на неки од уобичајених начина.

Кажемо да је формула G последица по *modus ponens*-у формула $(F \to G)$ и F, а $\forall vF$ је последица *генерализације* формуле F. Правила закључивања у PA су modus ponens и правило генерализације. Остаје још да наведемо аксиоме Пеанове аритметике.

Скупу аксиома PA припадају следеће аксиоме за следбеник, збир и производ, тј. наредних шест формула:
(1) $\mathbf{0} \neq \mathbf{s}x$,
(2) $\mathbf{s}x = \mathbf{s}y \to x = y$,
(3) $x + \mathbf{0} = x$,
(4) $x + \mathbf{s}y = \mathbf{s}(x + y)$,
(5) $x \cdot \mathbf{0} = \mathbf{0}$,
(6) $x \cdot \mathbf{s}y = (x \cdot y) + x$,
као и индуктивне аксиоме, под којима се подразумева бесконачно много формула PA облика:

$$F(0) \wedge \forall x(F(x) \to F(sx)) \to \forall xF(x)$$

где је F произвољна формула, а x произвољна променљива.
Према томе, аксиоме PA су логичке аксиоме, аксиоме за следбеник, збир и производ, као и индуктивне аксиоме.

Дефиниција 1.7
Доказ *у PA формуле F је коначан низ формула чија је последња вредност формула F, а свака претходна вредност низа је аксиома PA, последица формула, које чине претходне чланове низа, по modus ponens-у, или последица генерализације формуле која је претходни члан низа.*
Формула F је ***доказива*** *или је* ***теорема*** *у PA, ако постоји доказ формуле F у PA.*

Наводимо још неке дефиниције које ће нам бити значајне у даљем излагању.

Дефиниција 1.8
Затворен терм *је онај у којем се не појављује ниједна променљива.*

Дефиниција 1.9
Променљива v је слободна у формули F *ако постоји коначан низ $h_0, h_1, ..., h_r$ такав да је h_0 атомска формула $t = t'$ у којој се v појављује у t или t', h_r је формула*

F, а за свако $i < r$, за неку формулу F', $h_{i+1} = (h_i \to F')$ или $h_{i+1} = (F' \to h_i)$, или за неку променљиву и различиту од v, $h_{i+1} = \forall u h_i$.

Дефиниција 1.10

Реченица *или* ***затворена формула*** *је формула у којој ниједна променљива није слободна.*

Дефиниција 1.11

Променљива v је замењена термом t у терму t'*, што записујемо $t'_v(t)$, ако постоје два коначна низа исте дужине, од којих један изграђује терм t' и његове подтермове, а други представља низ који се добије као резулатат замене променљиве v термом t у сваком члану првог низа.*

Аналогно дефинишемо замену променљиве v термом t у формули F.
Имајући у виду ове дефиниције, закључујемо да је свака идуктивна аксиома логички еквивалентна следећој формули:

$$F_x(\mathbf{0}) \to (\forall x(F \to F_x(\mathbf{s}x)) \to F).$$

Дефиниција 1.12

Реченица Пеанове аритметике је ***тачна*** *ако је тачна када њене променљиве узимају вредности из скупа природних бројева, односно 0,1,2,..., **0** означава нулу, а **s**, $+$ и $\cdot$ су операције следбеника, сабирања и множења.*

Сваки затворен терм t означава јединствен природан број. **0** означава 0, а ако t и t' означавају i и i', онда $\mathbf{s}t$, $t + t'$ и $t \cdot t'$ означавају бројеве $i + 1$, $i + i'$ и $i \cdot i'$.

Дефиниција 1.13

Нумерал $\mathbf{i}$ *за број i је затворен терм који се добије везивањем i појављивања знака следбеника **s** за **0**.*

Дакле, **3** је **sss0**, **1** је **s0**, итд.

Пре разматрања (i)-(v) и њихових доказа, мораћемо да се осврнемо на способност PA да докаже разне чињенице о природним бројевима. Наиме, једини нелогички симболи које PA садржи су **0**, **s**, $+$ и $\cdot$, те није очигледно да она може да искаже, а камоли докаже разне значајне формуле. Показаћемо да су у PA доказиве неке познате законитости које важе за природне бројеве.

Теорема 1.1

$\vdash x = \boldsymbol{0} \vee \exists y\, x = \boldsymbol{s}y$.

Доказ

Нека је F формула $(x = \mathbf{0} \vee \exists y\ x = \mathbf{s}y)$. Тада су $\forall x(x = \mathbf{0} \to F)$ и $\forall x(x = \mathbf{s}y \to F)$ истините, односно важи $\vdash \forall x(x = \mathbf{0} \to F)$ и $\vdash \forall y(\forall x(x = y \to F) \to \forall x(x = \mathbf{s}y \to F))$. Према индуктивној аксиоми, следи $\vdash F$, односно $\vdash x = \mathbf{0} \vee \exists y\ x = \mathbf{s}y$. $\square$

Теорема 1.2

$\vdash x + y = y + x$.

Доказ

Због аксиоме (3), важи $\vdash \mathbf{0}{+}\mathbf{0} = \mathbf{0}$. Претпоставимо да важи $\vdash \mathbf{0}{+}x = x$ и докажимо $\vdash \mathbf{0}{+}\mathbf{s}x = \mathbf{s}x$. Из аксиоме (4) и индукцијске хипотезе следи $\vdash \mathbf{0}{+}\mathbf{s}x = \mathbf{s}(\mathbf{0}{+}x) = \mathbf{s}x$, одакле према индуктивној аксиоми $\vdash \mathbf{0}{+}x = x$. Из аксиоме (3) имамо $\vdash x = x{+}\mathbf{0}$, те $\vdash \mathbf{0}{+}x = x{+}\mathbf{0}$. Претпоставимо да важи $\vdash x{+}y = y{+}x$ и докажимо $\vdash x{+}\mathbf{s}y = \mathbf{s}y{+}x$.

Најпре, из аксиома (3) и (4) имамо $\vdash y + \mathbf{s}\mathbf{0} = \mathbf{s}(y + \mathbf{0}) = \mathbf{s}y = \mathbf{s}y + \mathbf{0}$, а ако претпоставимо $\vdash y{+}\mathbf{s}x = \mathbf{s}y{+}x$, из аксиоме (4) и ове претпоставке следи $\vdash y{+}\mathbf{s}\mathbf{s}x = \mathbf{s}(y + \mathbf{s}x) = \mathbf{s}(\mathbf{s}y + x) = \mathbf{s}y + \mathbf{s}x$, те према индуктивној аксиоми $\vdash y + \mathbf{s}x = \mathbf{s}y + x$.

Сада, из управо доказаног тврђења, индукцијске хипотезе и аксиоме (4) имамо $\vdash x{+}\mathbf{s}y = \mathbf{s}(x{+}y) = \mathbf{s}(y{+}x) = y{+}\mathbf{s}x = \mathbf{s}y{+}x$. Дакле, према индуктивној аксиоми, $\vdash x + y = y + x$. $\square$

Тврђења следећих теорема су добро позната, а докази се изводе слично као што смо показали у теореми 1.1.

Теорема 1.3

$\vdash x + (y + z) = (x + y) + z$.

Теорема 1.4

$\vdash x \cdot (y + z) = (x \cdot y) + (x \cdot z)$.

Теорема 1.5

$\vdash x \cdot (y \cdot z) = (x \cdot y) \cdot z$.

Теорема 1.6

$\vdash x \cdot y = y \cdot x$.

Теорема 1.7

Ако $i + j = k$, *онда* $\vdash \boldsymbol{i} + \boldsymbol{j} = \boldsymbol{k}$.

Доказ

Индукцијом по j. Ако је $i+j=k$ и $j=0$, онда је $i=k$, нумерал $\mathbf{j}$ је $\mathbf{0}$, према томе $\vdash \mathbf{i}+\mathbf{j}=\mathbf{i}+\mathbf{0}=\mathbf{i}=\mathbf{k}$. Претпоставимо да за свако k важи $\vdash \mathbf{i}+\mathbf{j}=\mathbf{k}$, кад год је $i+j=k$. Показујемо да тада исто важи и за $j+1$. Ако је $i+(j+1)=k$, онда за неко m важи $i+j=m$, односно $k=m+1$ и нумерал $\mathbf{k}$ је $\mathbf{sm}$. Следи $\vdash \mathbf{i}+\mathbf{j}=\mathbf{m}$, односно $\vdash \mathbf{i}+\mathbf{sj}=\mathbf{s}(\mathbf{i}+\mathbf{j})=\mathbf{sm}=\mathbf{k}$. □

Теорема 1.8

Ако је $i\cdot j=k$, онда је $\vdash \boldsymbol{i}\cdot\boldsymbol{j}=\boldsymbol{k}$.

Доказ

Слично као доказ претходне теореме. □

Теорема 1.9

Ако је t затворен терм, а i његова вредност у природним бројевима, онда $\vdash t=\boldsymbol{i}$.

Доказ

Индукцијом по конструкцији терма t. Ако је терм t $\mathbf{0}$, онда је 0 његова вредност у природним бројевима. Ако је вредност терма t у природним бројевима i, а вредност терма t' је j, онда је $i+j$ вредност терма $t+t'$ у природним бројевима. Нека је $k=i+j$. Према индукцијској хипотези, $\vdash t=\mathbf{i}$ и $\vdash t'=\mathbf{j}$. Према теореми 1.7, $\vdash \mathbf{i}+\mathbf{j}=\mathbf{k}$. Стога, $\vdash t+t'=\mathbf{i}+\mathbf{j}=\mathbf{k}$. Слично за следбеника и множење. □

Теорема 1.10

Ако су t и t' затворени и $t=t'$ тачно, онда $\vdash t=t'$.

Доказ

Ако термови t и t' означавају бројеве i и i', према теореми 1.9, $\vdash t=\mathbf{i}$ и $\vdash t'=\mathbf{i}'$. Ако је $t=t'$ тачно, онда је $i=i'$ и $\mathbf{i}$ је једнак нумералу $\mathbf{i}'$. Дакле, $\vdash t=t'$. □

Дефиниција 1.14

$x<y$ је формула $\exists z\, x+\boldsymbol{s}z=y$.

Дефиниција 1.15

$x>y$ је формула $y<x$.

$x\leq y$ је формула $(x<y\vee x=y)$.

$x\geq y$ је формула $y\leq x$.

Теорема 1.11

$\vdash \neg x<\boldsymbol{0}$.

Доказ

Ако претпоставимо да је $x < \mathbf{0}$, онда $\exists z\ x + \mathbf{s}z = 0$. Међутим, због аксиома (4) и (1), важи следеће: $\vdash x + \mathbf{s}z = \mathbf{s}(x + z) \neq \mathbf{0}$. Контрадикција. $\square$

Теорема 1.12

$\vdash x < \boldsymbol{s}y \leftrightarrow x < y \vee x = y.$

Доказ

$\vdash x < \mathbf{s}y \leftrightarrow \exists z\ x + \mathbf{s}z = \mathbf{s}y$

$\leftrightarrow \exists \mathbf{s}(x + z) = \mathbf{s}y$

$\leftrightarrow \exists z\ x + z = y$. На основу теорме 1.1, имамо

$\leftrightarrow (x + \mathbf{0} = y\ \vee\ \exists w\ x + \mathbf{s}w = y)$

$\leftrightarrow x = y\ \vee\ x < y\ .\square$

Дефиниција 1.16

$\vee\{x = \boldsymbol{j} : j < i\}$ *је дисјункција свих реченица* $x = \boldsymbol{j}$ *за* $j < i$ *и* $\perp$ *је ако је* $i = 0$.

Теорема 1.13

$\vdash x < \boldsymbol{i} \leftrightarrow \vee\{x = \boldsymbol{j} : j < i\}$.

Доказ

Индукцијом по i. Ако је $i = 0$, како је $\vdash \neg x < \mathbf{0}$, следи $\vdash x < \mathbf{0} \leftrightarrow \perp$. Претпоставимо да $\vdash x < \mathbf{i} \leftrightarrow \vee\{x = \mathbf{j} : j < i\}$. Према теореми 1.12 $\vdash x < \mathbf{si} \leftrightarrow (x < \mathbf{i}\ \vee\ x = \mathbf{i})$, па према индукцијској хипотези имамо $\vdash x < \mathbf{si} \leftrightarrow (\vee\{x = \mathbf{j} : j < i\} \vee x = \mathbf{i})$, одакле коначно добијамо $\vdash x < \mathbf{si} \leftrightarrow \vee\{x = \mathbf{j} : j < i + 1\}$. $\square$

Теорема 1.14 (Потпуна индукција)

За произвољну формулу $F(x)$,

$$\vdash \forall x(\forall y(y < x \to F(y)) \to F(x)) \to F(x).$$

Доказ

Претпоставимо

$$(*)\ \forall x(\forall y(y < x \to F(y)) \to F(x)).$$

Дефинишимо $G(x)$ као $\forall y(y < x \to F(y)) \wedge F(x))$, те ћемо показати $G(x)$, одакле следи $F(x)$. Индукцијом, довољно је показати $G(\mathbf{0})$ и $\forall x(G(x) \to G(\mathbf{s}x))$. Да бисмо доказали $G(\mathbf{0})$, према теореми 1.11 имамо $\forall y\ \neg y < \mathbf{0}$, одакле следи $\forall y(y < \mathbf{0} \to F(y))$, а из $(*)$ имамо $F(\mathbf{0})$, па према томе и $G(\mathbf{0})$. Даље желимо да покажемо $\forall x(G(x) \to G(\mathbf{s}x))$. Претпоставимо $G(x)$, тј. $\forall y(y < x \to F(y))$ и $F(x)$. Према теореми 1.12 , $\forall y(y < \mathbf{s}x \to F(y))$, одакле према $(*)$ имамо $F(\mathbf{s}x)$, па је и $G(\mathbf{s}x)$. $\square$

Принцип најмањег броја:
$\vdash F(x) \rightarrow \exists x(F(x) \wedge \forall y(y < x \rightarrow \neg F(y)))$, коришћењем контрапозиције, следи директно из потпуне индукције заменом $\neg F(x)$ уместо $F(x)$.

Теорема 1.15

$\neg x < x$;

$x < y < z \rightarrow x < z$;

$x < y \vee x = y \vee y < x$;

$x < y \rightarrow x + z < y + z$;

$x < y \wedge \boldsymbol{0} < z \rightarrow x \cdot z < y \cdot z$.

Теорема 1.16

Ако $i < j$, *онда* $\vdash \boldsymbol{i} < \boldsymbol{j}$.

Ако $i \neq j$, *онда* $\vdash \boldsymbol{i} \neq \boldsymbol{j}$.

Ако $i \geq j$, *онда* $\vdash \neg \boldsymbol{i} < \boldsymbol{j}$.

Доказ

Ако је $i < j$, онда је за неко k, $i + (k+1) = j$ и $\vdash \mathbf{i} + \mathbf{sk} = \mathbf{j}$ према теореми 1.7, те је $\vdash \mathbf{i} < \mathbf{j}$. Ако је $i \neq j$, онда $i < j$ или $j < i$ и $\vdash \mathbf{i} < \mathbf{j}$ или $\vdash \mathbf{j} < \mathbf{i}$, одакле $\vdash \mathbf{i} \neq \mathbf{j}$ према првом конјункту из теореме 1.15. Ако $i \geq j$, онда $j < i$ или $j = i$, одакле $\vdash \mathbf{j} < \mathbf{i}$ или $\vdash \mathbf{j} = \mathbf{i}$ и онда је према другом конјункту из теореме 1.15, $\vdash \neg \mathbf{i} < \mathbf{j}$. $\square$

1.2 Псеудотермови и $\Sigma-$формуле

С обзиром на то да су једини нелогички симболи Пеанове аритметике константа $\mathbf{0}$, унарни функцијски симбол следбеника $\mathbf{s}$, и два бинарна функцијска симбола $+$ и $\cdot$, делује да PA није у могућности да се бави великим бројем функција. У наставку показујемо на који начин се PA бави функцијама које нису означене ниједним њеним термом.

Дефиниција 1.17

Формулу $F(\boldsymbol{x}, y)$ *у* PA *називамо* ***псеудотерм*** *ако је формула* $\exists! y\ (F(\boldsymbol{x}, y))$, *односно формула* $\exists y(F(\boldsymbol{x}, y) \wedge \forall z(F(\boldsymbol{x}, z) \rightarrow y = z))$, *доказива у* PA.

Сваки псеудотерм $F(\mathbf{x}, y)$ дефинише једну n-арну функцију и стога многе функције које нису означене термовима у PA, ипак могу бити разматране у њој, у смислу псеудотермова који их дефинишу.

Често ћемо записивати $f(\mathbf{x})$, уместо $F(\mathbf{x}, y)$, односно изостављаћемо променљиву y и писати мало уместо велико слово f.

Ако је $A(y)$ формула у PA и $F(\mathbf{x}, y)$ псеудотерм, пишемо $A(f(\mathbf{x}))$ да бисмо означили формулу $\exists y(F(\mathbf{x}, y) \wedge A(y))$ у PA. Приметимо да када је $\exists! y\, F(\mathbf{x}, y)$ доказиво, формула $A(f(\mathbf{x}))$, тј. $\exists y\, (F(\mathbf{x}, y) \wedge A(y))$ је еквивалентна формули $\forall y\, (F(\mathbf{x}, y) \to A(y))$.

Користимо изразе $\forall y < xF$ и $\exists y < xF$ да бисмо краће записали изразе $\forall y(y < x \to F)$ и $\exists y(y < x \wedge F)$.

Дефиниција 1.18

Формулу називамо ***стриктна*** $\Sigma-$***формула*** *ако припада најмањој класи која садржи све формуле* $u = v, \mathbf{0} = u, \mathbf{s}u = v, u + v = w$ *и* $v \cdot u = w$, *и садржи све* $(F \wedge G), (F \vee G), \exists xF$ *и* $\forall x < yF$, *кадгод садржи формуле* F *и* G.
$\Sigma-$***формула*** *је формула која је у* PA *логички еквивалентна стриктној* $\Sigma-$*формули.*

Све атомске формуле су $\Sigma-$формуле, с обзиром да је свака атомска формула еквивалентна формули која настаје применом конјункције и егзистенцијалног квантификатора на формуле $u = v, \mathbf{0} = u, \mathbf{s}u = v, u+v = w$ и $u \cdot v = w$. Нпр. $x + \mathbf{s}y = \mathbf{s}0$ је еквивалентна формули $\exists u \exists v \exists w(\mathbf{s}y = u \ \wedge \ x + u = v \ \wedge \ \mathbf{0} = w \ \wedge \ \mathbf{s}w = v)$.

Дакле, можемо да закључимо да је и $x < y$, односно $\exists z(x + \mathbf{s}z = y)$ једна $\Sigma-$формула. Наиме, ако је F једна $\Sigma-$формула, онда је и $\exists x < yF$, што значи да су $\Sigma-$формуле затворене и за ограничени универзални, као и за ограничени егзистенцијални квантификатор.

Имајући у виду да је, према теореми 1.15 негација било које атомске формуле $\neg x = y$ еквивалентна формули $x < y \vee y < x$, можемо да тврдимо да је негација сваке атомске формуле такође $\Sigma-$формула.

$\Sigma-$формуле које су уједно и псеудотермови, кратко називамо $\Sigma-$псеудотерм.

Дефиниција 1.19

$\Sigma-$***реченица*** *је* $\Sigma-$*формула која је реченица.*

Ако је F $\Sigma-$формула, а S реченица добијена од F заменом затворених термова за слободне променљиве у F, онда је S исто тако $\Sigma-$реченица.

Теорема 1.17

Ако је S *тачна* $\Sigma-$*реченица, онда* $\vdash S$.

Доказ

Ако је S тачна атомска формула, онда је, према теореми 1.10 $\vdash S$. Ако је $(S \wedge S')$ тачна, онда су S и S' тачне, одакле следи $\vdash S$ и $\vdash S'$, па је и $\vdash (S \wedge S')$. Ако је

$(S \vee S')$ тачно, онда је S или S' тачно, одакле $\vdash S$ или $\vdash S'$, па је и $\vdash (S \vee S')$. Ако је $\exists x F$ тачна, онда је за неко i, формула $F(\mathbf{i})$ која се добије заменом промењиве x термом $\mathbf{i}$ тачна, па је $\vdash F(\mathbf{i})$, те следи и $\vdash \exists x F$. Ако је $\forall x < \mathbf{i} F$ тачно, онда је за свако $j < i$, $F(\mathbf{j})$ тачно, па је и за свако $j < i$, $\vdash F(\mathbf{j})$ и $\vdash x = \mathbf{j} \to F$. Међутим, према теореми 1.13 $\vdash x < \mathbf{i} \leftrightarrow \vee\{x = \mathbf{j} : j < i\}$, па је $\vdash x < \mathbf{i} \to F$ и $\vdash \forall x < \mathbf{i}\, F$. Коначно, ако је S еквивалентно доказивој реченици, и S је доказива. $\square$

Дефиниција 1.20

Формула A је $\Delta-$***формула*** *ако су A и $\neg A$ $\Sigma-$формуле.*

Наводимо неке особине $\Delta-$формула.

• Свака атомска формула $t = t'$ је $\Delta-$формула, јер смо претходно показали да су свака атомска формула, као и свака негација атомске формуле $\Sigma-$формула.

• $t < t'$ је $\Delta-$формула јер је еквивалентна формули $\exists x \exists y (t = x \wedge t' = y \wedge x < y)$, која је $\Sigma-$формула, а $\neg t < t'$ је еквивалентно формули $t = t' \vee t' < t$, која је такође $\Sigma-$формула.

• Негација $\Delta-$формуле је очигледно $\Delta-$формула. Ако су A и B $\Delta-$формуле, онда је то и њихова конјункција. Наиме, тада важи да су $A, B, \neg A$ и $\neg B$ $\Sigma-$формуле, па су формула $A \wedge B$ и њена негација $\neg A \vee \neg B$ такође $\Sigma-$формуле, односно следи тврђење. Аналогно се показује да је и дисјункција формула A и B $\Delta-$формула. Дакле, $\Delta-$формуле су затворене за све Булове операције.

• С обзиром да су $\Sigma-$формуле затворене за оба ограничена квантификатора, онда су то и $\Delta-$формуле. Наиме, ако су A и $\neg A$ $\Sigma-$формуле, и $\forall x < y A$ је $\Sigma-$формула, а $\neg \forall x < y A$ је еквивалентна $\Sigma-$формули $\exists x < y \neg A$. Слично се показује да тврђење важи и за ограничени егзистенцијални квантификатор.

• Ако је $F(\mathbf{x}, y)$ $\Sigma-$формула и псеудотерм, онда је она и $\Delta-$формула. Наиме, како је $\exists! y\ F(\mathbf{x}, y)$ доказива, онда је $\neg F(\mathbf{x}, y)$ еквивалнетна $\Sigma-$формули $\exists z (F(\mathbf{x}, z) \wedge \neg z = y)$.

• Ако је $A(y)$ $\Delta-$формула и $F(\mathbf{x}, y)$ $\Sigma-$псеудотерм, онда је $A(f(\mathbf{x}))$ $\Delta-$формула јер $A(f(\mathbf{x}))$ је $\Sigma-$формула $\exists y (F(\mathbf{x}, y) \wedge A(y))$, а с обзиром да је она еквивалентна формули $\forall y (F(\mathbf{x}, y) \to A(y))$, $\neg A(f(\mathbf{x}))$ је еквивалентна $\Sigma-$формули $\exists y (F(\mathbf{x}, y) \wedge \neg A(y))$.

Најкраће речено, $\Delta-$формуле садрже све атомске формуле и све формуле $t < t'$, и затворене су за Булове операције, ограничене квантификаторе и замену $\Sigma-$псеудотермова.

Писаћемо $\exists x \leq yF$ уместо $\exists x < \mathbf{s}yF$ и $\forall x \leq yF$ уместо $\forall x < \mathbf{s}yF$. Јасно је да ако је F $\Sigma-$формула односно $\Delta-$формула, онда су то и поменуте формуле.

Из теореме 1.17 следи да, ако је $F(\mathbf{x})$ $\Delta-$формула и i је $n-$торка природних бројева, онда је $\vdash F(\mathbf{i})$ или $\vdash \neg F(\mathbf{i})$. С обзиром да је $F(\mathbf{x})$ $\Delta-$формула, обе формуле $F(\mathbf{i})$ и $\neg F(\mathbf{i})$ су $\Sigma-$формуле. Према теореми 1.17, која год од ових да је тачна, теорема је у PA. Стога су сви примери $\Delta-$формула одлучиви.

1.3 Дељење, количник и остатак

Дефиниција 1.21
$d|x$ је формула $\exists q\ q \cdot d = x$.

$d|x$ је очигледно $\Sigma-$формула. Наредна теорема показује да је $d|x$ и $\Delta-$формула јер је еквивалентна формули изграђеној од атомских формула Буловим операцијама, ограниченим квантификаторима и заменом $\Sigma-$термова.

Докази следећих теорема су директни, те их нећемо експлицитно наводити.

Теорема 1.18
$\vdash \exists q\ q \cdot d = x \to \exists q(q \leq x \wedge q \cdot d = x)$.

Теорема 1.19
$\vdash d|d$.

Теорема 1.20
$\vdash d|x \wedge x|y \to d|y$.

Теорема 1.21
$\vdash d|x \to (d|(x+y) \leftrightarrow d|y)$.

Теорема 1.22
$\vdash d \neq 0 \to$
$\exists q \exists r(x = q \cdot d + r \wedge r < d\ \wedge \forall q' \forall r'(x = q' \cdot d + r' \wedge\ r' < d \to q = q' \wedge r = r'))$.

Дефинисаћемо остатак и означавати га Ost.

Дефиниција 1.22
$Ost(x, d, r)$ је формула

$$((r < d \wedge \exists q\ x = q \cdot d + r) \vee (d = 0 \wedge r = x)).$$

Видимо да је $Ost(x,d,r)$ $\Sigma-$формула, а из теореме 1.22 видимо и да је псеудотерм.

Сетимо се да одговарајућу функцију коју дефинише преудотерм F означавамо малим словом f, тј. функцију коју дефинише псеудотерм Ost означавамо ost.

Теорема 1.23
$\vdash ost(x,0) = x.$

Теорема 1.24
$\vdash d|x \leftrightarrow ost(x,d) = 0.$

Теорема 1.25
$\vdash ost(x+yd,d) = ost(x,d).$

Скуп природних бројева није затворен за операцију одузимања, стога уводимо псеудотерм који то јесте.

Теорема 1.26
$\vdash y \leq x \rightarrow \exists! z\ x = y + z$

Дефиниција 1.23
$Monus(x,y,z)$ је формула $(x = y + z \vee (x < y \wedge z = 0))$.

Очигледно је да је $Monus$ $\Sigma-$псеудотерм. Уместо $monus(x,y)$ пишемо $x \dot{-} y$ и ова функција представља замену за операцију одузимања.

Дефиниција 1.24
$Prost(p)$ је формула $(p \neq \mathbf{1} \wedge \forall d(d|p \rightarrow d = \mathbf{1} \vee d = p))$.

Није евидентно да је $Prost(p)$ $\Delta-$формула, али приметимо да, с обзиром да је $\vdash d|p \rightarrow d \leq p$, $Prost(p)$ је еквивалентно формули $p \neq \mathbf{1} \wedge \forall d \leq p(d|p \rightarrow d = \mathbf{1} \vee d = p)$, која јесте $\Delta-$формула јер је изграђена од $\Delta-$формула помоћу Булових операција и ограничених квантификатора.

Теорема 1.27
$\vdash$ *2 је најмањи прост.*

Теорема 1.28
$\vdash$ *Ако је $x > 1$, онда неки прост дели x.*

Дефиниција 1.25
$UzajamnoProsti(a,b)$ је формула

$$\forall d(d|a \wedge d|b \to d = \mathbf{1}).$$

$UzajamnoProsti(a, b)$ је $\Delta-$формула с обзиром да је еквивалентна формули $\forall d \leq a(d|a \wedge d|b \to d = \mathbf{1})$.

Теорема 1.29

$\vdash$ *a и b су узајамно прости ако и само ако ниједан прост не дели оба a и b.*

Доказ

Из теорема 1.20 и 1.28.□

Следи важно тврђење о узајамно простим бројевима.

Теорема 1.30

$\vdash$ *Ако су a и b већи од 1 и узајамно прости, онда за неке x и y важи* $ax + 1 = by$.

Доказ

Назовимо број i "добрим" ако и само ако $\exists x \exists y\ ax + i = by$. Полазећи од претпоставке да су a и b већи од 1 и узајамно прости, показаћемо да је 1 добар. Ако узмемо $x = b\dot{-}1$ и $y = a$, следи да је a добар, а ако је $x = 0$ и $y = 1$, следи да је b добар. Даље, ако је i добар, односно постоје x и y тако да је $ax + i = by$, онда је и qi добар, $x' = qx$ и $y' = qy$. Ако су i и i' добри и $i \geq i'$, онда је добар и $i\dot{-}i'$. Наиме, ако $ax + i = by$ и $ax' + i' = by'$, нека је $x'' = x + by' + (b\dot{-}1)x'$ и нека је $y'' = y + ax' + (a\dot{-}1)y'$. У том случају је $ax'' + (i\dot{-}i') = by''$. Нека је d најмањи позитиван добар број. Тада, ако је i добар, $d|i$ јер за неке $q, r, i = qd + r$ и $r < d$. Стога је qd добар и $i \geq qd$. Обзиром да $i\dot{-}qd = r$, r је добар, због тога што је d најмањи важи $r = 0$, а даље важи $i = qd$ и $d|i$. Имајући у виду да су a и b добри, следи да $d|a$, $d|b$, $d = 1$ и 1 је добар.□

Теорема 1.31

$\vdash$ *Ако је p прост и дели ab, онда p дели a или p дели b.*

Доказ

Претпоставимо да p дели ab. Ако p не дели a, онда су a и p узајамно прости. Према теореми 1.30, за неке $x, y, ax + 1 = py$ и онда је $abx + b = pby$. С обзиром да $p|ab$, $p|abx$ и $p|pby$, из теореме 1.21 следи $p|b$.□

1.4 Најмањи заједнички садржалац

У даљем тексту сматраћемо да су $M(x,y)$ и $H(x,y)$ произвољни псеудотермови.

Теорема 1.32

$\vdash$ *Ако је за све* $i<k, m(i)>0$, *онда постоји најмањи позитиван* l *такав да за све* $i<k$ *важи* $m(i)|l$.

Доказ

Индукцијом по k. Претпоставимо да је за све $i<k, m(i)>0$. Ако је $k=0$, онда је тражено l једнако 1. Претпоставимо да тврђење важи за k. За $k+1$ тражено l се добије када помножимо l које функционише за k са $m(k)$. Најзад, применимо принцип најмањег броја. $\square$

Дефиниција 1.26

$Nzs[m(i) : i<k](l)$ *је следећа формула*
$(\forall i<k\ m(i)>\mathbf{0}\wedge l>\mathbf{0}\wedge\forall i<k\ m(i)|l\wedge\forall j<l\neg[j>\mathbf{0}\wedge\forall i<k\ m(i)|j])\vee(\exists i<k\ m(i)=\mathbf{0}\wedge l=\mathbf{0})$, *која каже да је* l *најмањи заједнички садржалац низа елемената* $m(i)$, $i<k$.

Имајући у виду теорему 1.32, можемо да закључимо да је $Nzs[m(i) : i<k](l)$ псеудотерм. Уколико је $M(x,y)$ $\Sigma-$псеудотерм, онда је то и $Nzs[m(i) : i<k](l)$.

Теорема 1.33

$\vdash j<k\rightarrow m(j)|nzs[m(i) : i<k]$.

Теорема 1.34

$\vdash$ *Било који садржалац свих* $m(i)$, $i<k$, *садржи и* $nzs[m(i) : i<k]$.

Доказ

Претпоставимо да $m(i)|x$ за све $i<k$. Нека је $l=nzs[m(i) : i<k]$. Можемо претпоставити да је $l>0$. За неке $q,r, x=ql+r$ и $r<l$. С обзиром да $m(i)|l$ и $m(i)|x$, онда и $m(i)|r$ за све $i<k$, што је у супротности са тиме да је l минимално ако је $r>0$. Дакле $r=0$ и $l|x$. $\square$

Теорема 1.35

$\vdash$ *Ако је* p *прост и* $p|nzs[m(i) : i<k]$, *онда* $p|m(i)$ *за неко* $i<k$.

Доказ

Индукцијом по k. Ако је $k=0$, $nzs[m(i) : i<0]=1$ и p не дели $nzs[m(i) : i<0]$. Претпоставимо да $p|nzs[m(i) : i<k+1]$. С обзиром да свако $m(i), i<k+1$ дели

$nzs[m(i) : i < k] \cdot m(k)$, из теореме 1.34 следи $nzs[m(i) : i < k+1] | nzs[m(i) : i < k] \cdot m(k)$. Према теореми 1.31, или $p | nzs[m(i) : i < k]$, одакле по индукцијској хипотези p дели неко $m(i), i < k$, или $p | m(k)$. $\square$

Теорема 1.36 (Кинеска теорема о остацима)

$\vdash [\forall i < k\ (1 < m(i) \wedge h(i) < m(i)) \wedge \forall i, j (i < j < k \rightarrow m(i)$ *и* $m(j)$ *су узајамно прости)]* $\rightarrow \exists a < nzs[m(i) : i < k] \forall i < k\ ost(a, m(i)) = h(i)$. *Другим речима, за чланове неког низа* $m(i)$, $i < k$, *који су сви по паровима узајамно прости, и за све* $h(i)$ *такве да је* $1 < m(i) \wedge h(i) < m(i)$, *постоји* $a < nzs[m(i) : i < k]$ *за које важи да је* $h(i)$ *остатак при дељењу* a *са* $m(i)$.

Доказ

Претпоставимо да важи $\forall i < k (1 < m(i) \wedge h(i) < m(i)) \wedge \forall i, j (i < j < k \rightarrow m(i)$ и $m(j)$ су узајамно прости). Доказ изводимо индукцијом по k. Нека је $a = 0$ када је $k = 0$. $a < 1 = nzs[m(i) : i < 0]$. Претпоставимо да је за произвољно k, $a < nzs[m(i) : i < k]$, и $ost(a, m(i)) = h(i)$ за све $i < k$. Нека је $l = nzs[m(i) : i < k], m = m(k)$. l и m су узајамно прости, што видимо из следећег. Ако $p | l$, онда према теореми 1.35 за неко $i < k$, $p | m(i)$, а пошто су $m(i)$ и m узајамно прости, p не дели m.

Имајући у виду да су l и m узајамно прости, према теореми 1.30 за неке $x, y, lx + 1 = my$. Множењем обе стране са $a + (l \dot{-} 1)h(k)$ видимо да за неке друге $x, y, lx + a + (l \dot{-} 1)h(k) = my$. Нека је $a^* = l(x + h(k)) + a$. Онда $a^* = my + h(k)$. Ако је $i < k$, онда с обзиром да $m(i) | l$, $ost(a^*, m(i)) = ost(a, m(i)) = h(i)$ и $ost(a^*, m(k)) = ost(a^*, m) = h(k)$, с обзиром да је $h(k) < m(k) = m$. Нека је $l' = nzs[m(i) : i < k+1]$. Ако је $a^* < l'$, доказ је завршен. Ако је $a^* \geq l'$, онда нека је b највећи садржалац од l' које је $\leq a^*$, и нека је $a^{**} = a^* \dot{-} b$. Онда је $a^{**} < l'$, а с обзиром да $m(i) | l' | b$ за све $i < k+1$, $ost(a^{**}, m(i)) = ost(a^* \dot{-} b, m(i)) = ost(a^*, m(i)) = h(i)$. $\square$

Теорема 1.37

$\vdash$ *Низ елемената* $m(i), i < k$ *има јединствену највећу вредност.*

Дефиниција 1.27

$Max[m(i) : i < k](l)$ *је формула* $[\exists i < k\ m(i) = l \wedge \forall i < k\ m(i) \leq l]$, *односно* l *је члан низа* $m(i), i < k$ *који има највећу вредност.*

Јасно, $Max[m(i) : i < k](l)$ је $\Sigma-$псеудотерм.

Дефиниција 1.28

$Max(x,y,z)$ је $[(x \geq y \wedge\ z = x) \vee (x < y \wedge z = y)]$, односно формула која каже да је z максимум од x и y.

Max(x,y,z) је $\Sigma-$псеудотерм.

У наставку дефинишемо функцију *Beta* коју је Гедел дефинисао како би кодирао коначне низове природних бројева као парове бројева.

Дефиниција 1.29

$Beta(a,b,i,r)$ је $ost(a, \boldsymbol{1} + (\boldsymbol{i} + \boldsymbol{1}) \cdot b) = r$.

$Beta(a,b,i,r)$ је такође $\Sigma-$псеудотерм.

Теорема 1.38 (Геделова лема)

$\vdash$ За произвољан псеудотерм $H(i,y)$ и за свако k, постоје a и b такви да је за све $i < k, beta(a,b,i) = h(i)$. Дакле, за произвољан псеудотерм $H(i,y)$ постоје a и b такви да је остатак при дељењу a са $\boldsymbol{1} + (\boldsymbol{i}+1) \cdot b$ једнак $h(i)$, за свако $i < k$.

Још важи да, ако је $s = max(k, max[h(i) : i < k]) + 1$, a и b се могу одабрати тако да $b < nzs[i+1 : i < s] + 1$ и $a < nzs[1 + (i+1)b : i < k]$.

Доказ

Нека је s као што каже тврђење леме. Онда $s > k$ и за све $i < k, s > h(i)$. Нека је $b = nzs[i+1 : i < s]$. Претпоставимо да је $i < j < k$. Показаћемо да су $1 + (i+1)b$ и $1 + (j+1)b$ узајамно прости. Претпоставимо да $p|1 + (i+1)b$ и $p|1 + (j+1)b$. Онда p дели њихову разлику $(j \dot{-} i)b$, односно важи $p|j \dot{-} i$ или $p|b$. С обзиром да је $1 \leq j \dot{-} i < k < s$, важи и $j \dot{-} i|b$. У сваком случају, $p|b$ и према томе $p|(i+1)b$. Пошто важи $p|1+(i+1)b$, p дели њихову разлику 1, што је контрадикција. Према томе, ако $i < j < k, 1 + (i+1)b$ и $1 + (j+1)b$ су узајамно прости. Штавише, за све $i < k, h(i) < s \leq b < 1 + (i+1)b$ и $1 < 1 + (i+1)b$. Према Кинеској теореми о остацима, односно теореми 1.36, узимајући $m(i) = 1 + (i+1)b$, за неко $a < nzs[1 + (i+1)b : i < k]$, $beta(a,b,i) = h(i)$, за све $i < k$. $\square$

Приметимо да су псеудотермови који у Геделовој леми пружају везе између a и b $\Sigma-$псеудотермови. Они ће нам омогућити да видимо да су помоћу $\Delta-$формула дефинисани одређени појмови у вези са синтаксом PA, попут "Геделовог броја терма Пеанове аритметике" или "Геделовог броја формуле Пеанове аритметике".

Теорема 1.39

$\vdash$ За произвољне c,d,k,n постоје a и b такви да је $beta(a,b,k) = n$ и за свако $i < k, beta(a,b,i) = beta(c,d,i)$.

Доказ

Дефинишемо $H(i, y)$ где је $y = beta(c, d, i)$ ако је $i < k$, а иначе $= n$, и нека су a, b као у Геделовој леми. □

1.5 Увод у Геделове бројеве

Сада почињемо да развијамо синтаксу Пеанове аритметике у самој Пеановој аритметици. Развијање синтаксе неке теорије унутар те саме теорије може се назвати "доказивањем метатеорије у самој теорији".

Начин на који Пеанова аритметика доказује тврђења везана за своју синтаксу, тј. тврђења која граде њену метатеорију се разликује од начина на који доказује тврђења везана за природне бројеве. Да би Пеанова аритметика доказала тврђење о природним бројевима, довољно је да реченица или формула језика PA која исказује то тврђење буде теорема у PA. Шта реченица на језику PA изражава, зависи од тога из ког скупа њене променљиве узимају вредности, као и од тога шта означавају њени нелогички симболи.

Када је реч о скупу природних бројева, односно када променљиве узимају вредности из тог скупа, реченице PA могу изражавати тврђења само о природним бројевима и релацијама и операцијама које се могу дефинисати у том скупу на језику Пеанове аритметике. Стога није за очекивати да би Пеанова аритметика могла да докаже чак и неке најједноставније тврдње о својој синтакси, попут нпр. оне која каже да универзални квантификатор није променљива, а камоли нека значајнија тврђења. Ипак, из следећих разлога, чини се да је сасвим оправдано сматрати Пеанову аритметику способном за доказивање чињеница о својој сопственој синтакси.

Под "Синтаксом" ћемо сматрати неформалну математичку теорију синтаксе Пеанове аритметике, а објекти којима се она бави су основни симболи PA, као и уређени парови и коначни низови објеката.

Постоји двострука кореспонденција између Синтаксе и PA: најпре, између објеката Синтаксе и објеката PA, односно природних бројева, а друго, између имена и предиката језика Синтаксе и термова и формула језика PA. Бројеви који одговарају објектима Синтаксе се називају Геделови бројеви или кодови тих објеката.

Укратко ћемо описати систем Геделовог нумерисања.

Терм Пеанове аритметике који одговара имену у Синтакси представља Геделов број објекта означеног тим именом (нпр. ако симбол $\forall$ има Геделов број 5,

онда име "за сваки" језика Синтаксе које се односи на симбол $\forall$ одговара терму **ssssss0** језика аритметике, који означава број 5). Формула Пеанове аритметике која одговара предикату у Синтакси је тачна само за оне објекте Синтаксе за које предикат важи. Даље, постоје разне везе између термова, формула, реченица и доказа у Пеановој аритметици, које мање или више одговарају по-стојећим везама између имена, предиката, реченица и доказа у Синтакси. Кореспонденција између имена и предиката Синтаксе и термова и формула Пеанове аритметике природно се проширује на ону између реченица Синтаксе и реченица PA изграђених од термова и формула који одговарају именима и предикатима од којих су поменуте реченице Синтаксе формиране. Имајући у виду ту кореспонденцију, реченице PA су доказиве у PA само ако су њихови пандани доказиви у Синтакси. Ипак, реченице Синтаксе које изражавају познате и елементарне (и неке не толико елементарне) синтактичке истине, биће пандани доказивих реченица у PA. Штавише, кореспонденција се шири на дефиницију комплексних појмова: дефиниције комплексних формула Пеанове аритметике, састављених од једноставнијих, често личе на неформалне дефиниције помоћу којих су њихови одговарајући предикати Синтаксе дефинисани један помоћу другог. Коначно, кореспонденција се шири, мада грубље, на ону између неформалних доказа у Синтакси и доказа у PA. Наиме, низовима реченица које у Синтакси изражавају неформалне доказе синтактичких чињеница ће често одговарати докази реченица у Пеановој аритметици чије пандане у језику Синтаксе те чињенице формулишу.

Сваком основном симболу Пеанове аритметике додељујемо природан број, који се у том случају назива Геделов број или код, на следећи начин:

$\perp$	$\rightarrow$	$\forall$	$=$	**0**	**s**	$+$	$\cdot$
1	3	5	7	9	11	13	15

Променљивој v_i додељујемо број $2i + 17$. Дакле, сваки основни симбол има непаран Геделов број.

Дефинишемо $\pi(i, j) = 2((i + j)(i + j) + i + 1)$. Ако објекти x и y (било да су симболи или уређени парови) имају Геделове бројеве i и j, онда ће уређени пар $\langle x, y\rangle$ имати Геделов број $\pi(i, j)$. С обзиром да је $\pi(i, j)$ паран број, он сигурно није Геделов број основног симбола.

Знамо, сваки терм и формула је неки уређени пар тј. уређена тројка, а свака уређена тројка је по дефиницији уређени пар, па су заиста сви објекти неки уређени парови, те смо им на претходни начин доделили код, односно дефинисали смо Геде-

лове бројеве за све термове и формуле у PA. Пре него што почнемо да доказујемо синтаксу PA у PA, развићемо зачетке теорије коначних низова природних бројева у PA. Да бисмо то урадили, најпре морамо у PA развити теорију уређених парова природних бројева. Почећемо дефиницијом $\Sigma-$псеудотерма за који ћемо моћи да покажемо у PA закон уређених парова.

Дефиниција 1.30
$Par(x, y, z)$ је формула $2((x + y)(x + y) + x + 1) = z$ која каже да је z код пара објеката чији су кодови x и y.

$Par(x, y, z)$ је $\Sigma-$псеудотерм. Писаћемо (x, y) уместо $par(x, y)$. Дакле, (x, y) је код пара објеката чији су кодови x и y.

У наставку текста, тамо где будемо били у могућности даваћемо експлицитне дефиниције псеудотермова помоћу идентитета, као нпр. у следећој дефиницији.

Дефиниција 1.31
$(x, y) = 2((x + y)(x + y) + x + 1)$.

Теорема 1.40
$\vdash$ *Ако $(x, y) = (x', y')$, онда је $x = x'$ и $y = y'$.*

Доказ
Претпоставимо да важи $(x, y) = (x', y')$. Тада је $(x+y)(x+y)+x+1 = (x'+y')(x'+y')+x'+1$. Ако $x+y < x'+y'$, онда $(x+y)(x+y)+x+1 \leq (x+y+1)(x+y+1) \leq (x'+y')(x'+y') < (x'+y')(x'+y')+x'+1$, што није могуће. Слично, ако $x'+y' < x+y$, онда $(x', y') < (x, y)$, што је такође немогуће. Дакле, $x + y = x' + y'$, односно $x = x'$ и $y = y'$. $\square$

Сваки терм или формула у PA имају непаран Геделов број, или паран облика $\pi(i, j)$, где су i и j непарни.

Теорема 1.41
$\vdash x, y < (x, y)$.

Приметимо да претходна теорема каже да је Геделов број терма већи од Геделовог броја сваког његовог подтерма, да је Геделов број атомске формуле $t = t'$ већи од Геделовог броја термова t и t', Геделов број формуле је већи од Геделових бројева њених подформула, као и да је Геделов број формуле $\forall vF$, већи од Геделовог броја промењљиве v.

Теорема 1.42
$\vdash x < x' \to (x, y) < (x', y), \quad y < y' \to (x, y) < (x, y').$

Дефиниција 1.32
$Prvi(z, w)$ је формула

$$(\exists y < z(w, y) = z \vee (\neg\exists x, y < z(x, y) = z \wedge w = \boldsymbol{0})),$$

која каже да је w код прве координате пара чији је код z или је $w = 0$ ако такав пар не постоји.

Дефиниција 1.33
$Drugi(z, w)$ је формула

$$(\exists x < z(x, w) = z \vee (\neg\exists x, y < z(x, y) = z \wedge w = \boldsymbol{0})),$$

која каже да је w код друге координате пара чији је код z или је $w = 0$ ако такав пар не постоји.

$Prvi(z,w)$ и $Drugi(z,w)$ су $\Sigma-$псеудотермови.

Теорема 1.43
$\vdash prvi((x, y)) = x,\ drugi((x, y)) = y.$

За уређену тројку $\langle i, j, k\rangle$ дефинишемо следећи псеудотерм.

Дефиниција 1.34
$(x, y, z) = (x, (y, z)).$

Дефиниција 1.35
$pr(w) = prvi(w);\ dr(w) = prvi(drugi(w));\ tr(w) = drugi(drugi(w)).$

Теорема 1.44
$\vdash pr((x, y, z)) = x;\ dr((x, y, z)) = y;\ tr((x, y, z)) = z.$

Теорема 1.45
$\vdash x, y, z < (x, y, z).$

1.6 Кодирање коначних низова

Као што је већ познато, уређени пар је одређен својом првом и другом компонентом. Слично, коначан низ $h_0, h_1, ..., h_{k-1}$ је одређен својом дужином k, те вредностима h_i, за свако $i < k$. Уколико су низови исте дужине, а различити, то значи да имају различите вредности h_i за неко $i < k$.

До сада смо постигли да ниједна формула у PA осим $\perp$ нема исти Геделов број као неки основни симбол у PA. Имајући у виду да ће докази бити дефинисани као коначни низови одређене врсте, желимо да им доделимо Геделове бројеве који се разликују од оних који су додељени основним симболима и формулама. С обзиром на то да сваки основни симбол има непаран Геделов број, а свака формула, осим $\perp$, Геделов број облика $\pi(i, \pi(a, b))$, где је i непаран, а $\pi(a, b)$ паран, жељени резултат постижемо тиме што ћемо Геделове бројеве коначних низове дефинисати да буду облика $\pi(\pi(a, b), k)$, где за свако c, d за које важи $\pi(c, d) < \pi(a, b)$, постоји $i < k$, тако да је $Beta(c, d, i) \neq Beta(a, b, i)$. Наиме, прво сваком члану низа, тј. свакој формули која је члан низа, додељујемо код на претходно описан начин, те добијамо низ кодова на који затим применимо Геделову лему, односно проналазимо a и b такве да је код i-тог члана низа једнак са $Beta(a, b, i)$. Најзад, Геделов број низа је $\pi(\pi(a, b), k)$, где је k дужина низа, а a и b знамо да постоје на основу Геделове леме, и бирамо их такве да за свако c, d за које важи $\pi(c, d) < \pi(a, b)$, постоји $i < k$, тако да је $Beta(c, d, i) \neq Beta(a, b, i)$, односно ни за једно i није $Beta(c, d, i)$ једнако коду i-тог члана низа, те је Геделов број низа, одређен на овај начин, јединствен.

Дефиниција 1.36

$KonNiz(s)$ је формула $\exists a < s \exists b < s \exists k < s(s = ((a, b), k) \wedge \forall c < s \forall d < s((c, d) < (a, b) \rightarrow \exists i < k\ beta(c, d, i) \neq beta(a, b, i))$, односно s је Геделов број коначног низа који се добија на горепоменути начин.

Дефиниција 1.37

$dn(s) = drugi(s)$, тј. дужина низа чији је код s је друга координата пара помоћу којег добијамо s.

Дефиниција 1.38

$vredn(s, i) = beta(prvi(prvi(s)), drugi(prvi(s)), i)$, односно код i-тог члана низа је једнак Beta функцији, као што смо претходно и описали.

$KonNiz$ је $\Delta-$формула, а $dn(s)$ и $vredn(s, i)$ су $\Sigma-$псеудотермови. Писаћемо s_i уместо $vredn(s, i)$.

Јасно је да је закон коначних низова доказив у PA.

Теорема 1.46

$\vdash (KonNiz(s) \wedge KonNiz(s') \wedge dn(s) = dn(s') \wedge \forall i < dn(s) s_i = s_{i'}) \rightarrow s = s'$.

Теорема 1.47

$\vdash \exists! s\ (KonNiz(s) \wedge dn(s) = \boldsymbol{0})$.

Доказ

$((0,0),0)$ је коначан низ дужине 0. Његова јединственост следи из теореме 1.46. □

Дефиниција 1.39

$[\,] = ((\boldsymbol{0}, \boldsymbol{0}), \boldsymbol{0})$.

Теорема 1.48

$\vdash dn(s) = k \rightarrow \exists! s'(KonNiz(s') \wedge dn(s') = \boldsymbol{s}k \wedge \forall i < k\ s_{i'} = s_i \wedge s'_k = n)$.

Доказ

Претпоставимо да $dn(s) = k$. Нека је $c = prvi(prvi(s)),\ d = drugi(prvi(s))$. Према теореми 1.39, постоје a и b такви да је $beta(a,b,k) = n$ и за све $i < k, beta(a,b,i) = beta(c,d,i)$. Нека је $s' = ((a,b), sk)$. Тада је $dn(s') = sk, s'_i = beta(a,b,i) = beta(c,d,i) = s_i$, за све $i < k$, и $s'_k = beta(a,b,k)$. Према принципу најмањег броја, можемо да претпоставимо да је (a,b) најмањи. □

Теорема 1.49

За било који псеудотерм $H(i,j)$, $\vdash \exists! s\ (KonNiz(s) \wedge dn(s) = k \wedge \forall i < k\ s_i = h(i))$.

Доказ

Индукцијом по k, користећи теорему 1.47 када је $k = 0$ и позивајући се на теорему 1.48 са $n = h(k)$ када је k позитивно. □

Следеће две теореме су нам неопходне да бисмо могли да уведемо операције издвајања подниза и конкатенације, које нам омогућују да користећи постојеће, дефинишемо нове термове, формуле и доказе.

Теорема 1.50

$\vdash\ e \leq j < k \wedge dn(s) = k \rightarrow \exists! s'(KonNiz(s') \wedge dn(s') = j \dot{-} e \wedge \forall i < j \dot{-} e\ s'_i = s_{e+i})$, *односно, ако имамо коначан низ дужине* k, *постоји тачно један коначан низ дужине* $j \dot{-} e$, *где је* $e \leq j < k$, *чији сваки члан има код* $s'_i = s_{e+i}$.

Доказ

Индукцијом по $j \dot{-} e$. Ако је $j = e$, $[\,]$ нам даје решење. Ако је $e < j + 1 < k$ и s_i функционише за j, онда према теореми 1.48, нека је s'' такво такво да је $dn(s'') = j \dot{-} e + 1,\ s''_i = s'_i$ за $i < j \dot{-} e$ и $s''_{j \dot{-} e} = s_j$. Тада s'' функционише за $j + 1$. □

Теорема 1.51

$\vdash dn(s) = k \wedge dn(s') = k' \wedge j \leq k + k' \rightarrow \exists s''(KonNiz(s'') \wedge dn(s'') = j) \wedge \forall i < j(i < k \rightarrow s''_i = s_i) \wedge k \leq i < j \rightarrow s''_i = s'_{i \dot{-} k})$, *односно, за два коначна низа дужине* k *и* k', *постоји коначан низ дужине* j, $j \leq k + k'$, *за који важи* $s''_i = s_i$ *за* $i < k$, *односно* $s''_i = s'_{i \dot{-} k}$ *за* $k \leq i < j$.

Доказ

Слично као и у претходном доказу, индукцијом по j. Користимо [ ] када је $j = 0$, а даље теорему 1.48. □

Теорема 1.52

$\vdash dn(s) = k \wedge dn(s') = k' \rightarrow \exists s''(KonNiz(s'') \wedge dn(s'') = k + k' \wedge \forall i < k\ s''_i = s_i \wedge \forall i < k'\ s''_{k+i} = s'_i)$, *mj. за два коначна низа дужине* k *и* k', *постоји коначан низ дужине* $k + k'$ *за који је* $s''_i = s_i$, $i < k$ *и* $s''_{k+i} = s'_i$, $i < k'$.

Доказ

Према теореми 1.51. □

Подниз коначног низа $h_0, ..., h_e, ..., h_j, ...$ од e до j је низ $h_e, ..., h_{j-1}$. У случају $j \leq e$, то је [ ].

Конкатенацијом коначног низа $a, ..., b$ дужине k са низом $c, ..., d$ дужине k', добија се коначан низ $a, ..., b, c, ..., d$ дужине $k + k'$. $[n]$ је коначан низ дужине 1 за који је $[n]_0 = n$.

Дефиниција 1.40

$Podniz(s, e, j, s')$ *је формула* $(\neg e \leq j < dn(s) \wedge s' = [\,]) \vee (e \leq j < dn(s) \wedge KonNiz(s') \wedge dn(s') = j \dot{-} e \wedge \forall i < j \dot{-} e\ s'_i = s_{e+i})$, *која каже да је низ чији је код* s', *подниз коначног низа чији је код* s, *његова дужина је* $j \dot{-} e$, $e \leq j < dn(s)$, *а код сваког члана* $s'_i = s_{e+i}$, $i < j \dot{-} e$.

Podniz(s, e, j, s') је $\Sigma-$псеудотерм. Пишемо $s_{[e,j)}$ уместо podniz(s,e,j).

Дефиниција 1.41

$Konkat(s, s', s'')$ *је формула* $(KonNiz(s'') \wedge dn(s'') = dn(s) + dn(s') \wedge \forall i < dn(s)\ s''_i = s_i \wedge \forall i < dn(s')s''_{dn(s)+i} = s'_i)$, *која каже да је коначан низ чија је дужина једнака збиру дужина низова са кодовим* s *и* s', *низ чији чланови имају кодове* $s''_i = s_i$, $i < dn(s)$ *и* $s''_{dn(s)+i} = s'_i$, $i < dn(s')$.

Konkat(s, s', s'') је $\Sigma-$псеудотерм. Пишемо $s * s'$ уместо konkat(s, s').

Дефиниција 1.42
$Niz(s,n)$ је формула $KonNiz(s) \wedge dn(s) = 1 \wedge s_0 = n$.

Niz(n,s) је $\Sigma-$псеудотерм. Пишемо $[n]$ уместо niz(n).

Теорема 1.53
$\vdash$ *Ако је s коначан низ, онда $[\,] * s = s = s * [\,]$.*

Теорема 1.54
$\vdash$ *Ако су s, s' и s'' коначни низови, онда је $s * (s' * s'') = (s * s') * s''$.*

Доказ
Нека су k, k' и k'' дужине низова s, s' и s''. Нека је $u = s' * s''$, $u' = s * s', v = s * u$ и $v' = u' * s''$. Тада, користећи асоцијативност сабирања, видимо да су v и v' коначни низови дужине $k + k' + k''$, као и да за све $i < k + k' + k'', v_i = v'_i$. Применом закона коначних низова следи тврђење.□

1.7 Термови и формуле PA у PA

Ако је σ терм или формула PA, или неки од симбола $\bot, \to, \forall, =, \mathbf{0}, \mathbf{s}, +, \cdot$, а i његов Геделов број, онда ћемо писати $\ulcorner\sigma\urcorner$ уместо $\mathbf{i}$.

Дефиниција 1.43
$\ulcorner\bot\urcorner, \ulcorner\to\urcorner, \ulcorner\forall\urcorner, \ulcorner=\urcorner, \ulcorner\boldsymbol{0}\urcorner, \ulcorner\boldsymbol{s}\urcorner, \ulcorner+\urcorner, \ulcorner\cdot\urcorner$ *су термови* ***1,3,5,7,9,11,13*** *и* ***15***.

Дефиниција 1.44
Promenljiva(v) је $\Delta-$формула $\exists i < v\ v = \boldsymbol{2} \cdot \boldsymbol{i} + \boldsymbol{17}$.

Теорема 1.55
$\vdash \neg Promenljiva(\ulcorner\forall\urcorner)$.

Претходно смо поменули како делује да PA не може да докаже чак ни врло једноставно тврђење које каже да $\forall$ није променљива. Сада видимо да може.

Подсетимо се дефиниције терма у PA коју смо на почетку дали: t је терм ако и само ако постоји коначан низ чија је последња вредност t, а свака претходна вредност низа је $\mathbf{0}$, променљива, уређени пар симбола $\boldsymbol{s}$ и претходне вредности низа, уређена тројка $+$ и две претходне вредности низа или уређена тројка $\cdot$ и две претходне вредности низа.

Дефиниција 1.45

Term(t) је формула

$\exists s[KonNiz(s) \wedge dn(s) > \boldsymbol{0} \wedge s_{dn(s)\dot{-}1} = t \wedge \forall i < dn(s)(s_i = \ulcorner \boldsymbol{0} \urcorner \vee Promenljiva(s_i) \vee$
$\exists j, k < i[s_i = (\ulcorner \boldsymbol{s} \urcorner, s_j) \vee s_i = (\ulcorner + \urcorner, s_j, s_k) \vee s_i = (\ulcorner \cdot \urcorner, s_j, s_k)])]$.

Нека је "A(s,t)" скраћеница за израз "$[KonNiz(s) \wedge ...)])$]" у дефиницији Term(t). A(s,t) је очигледно $\Delta-$формула, па је Term(t) очигледно $\Sigma-$формула. Међутим, због квантификатора "$\exists s$" који није ограничен, остаје да се покаже да је Term(t) $\Delta-$формула. Наредна теорема нам даје то тврђење.

Теорема 1.56

$\vdash \exists s\ A(s,t) \leftrightarrow \exists b < nzs[i+1 : i < t+2] + 1$
$\exists a < nzs[1 + (i+1)b : i < t+1] \exists s \leq ((a,b), t+1) A(s,t)$.

Доказ

Смер $\leftarrow$ је очигледан, а за смер $\rightarrow$ дајемо само нацрт.

Ако је s коначан низ који показује да је t терм, онда постоји неки коначан низ s' чија је свака вредност $\leq t$. Наиме, претпоставимо да важи $A(s,t)$. Онда постоји низ s' такав да $A(s',t)$ и $(*)$ за све $i < dn(s'), s'_i = t$. (Интуитивно, s' добијемо од s индуктивним брисањем вредности већих од t сдесна на лево.) Индукцијом по j, постоји низ s' такав да је $A(s',t)$ и $(^*j)$ ако је $j \leq dn(s') = k'$, онда за све i, ако је $k' \dot{-} j \leq i < k'$, тада $s'_i \leq t$. Уврштавањем $j = dn(s')$ у $(^*j)$ добијемо s' такво да је $A(s',t)$ и за које важи $(*)$. Сличан аргумент нам показује да такође смемо претпоставити да за све i, j, ако је $i < j < dn(s')$, онда $s'_i \neq s'_j$. Поновним постављањем s' као s, смемо да претпоставимо да за све $i < dn(s), s_i \leq t$, и за све $i < j < dn(s), s_i \neq s_j$.

Применом Дирихлеовог принципа (који тврди да ако m места садрже у себи n слова и $n > m$, онда неко место садржи бар два слова) следи да је $dn(s) \leq t+1$.

За све коначне низове s, ако за све $i \leq t+1, s_i \leq t$, онда за неке i, j, $i < j \leq t+1$ и $s_i = s_j$. Ово доказујемо индукцијом по t.

Закључујемо да за неке коначне низове s, $A(s,t)$, $dn(s) \leq t+1$ и за свако $i < dn(s)$, $s_i \leq t$. Према Геделовој леми, постоје a, b такви да за све $i < t+1$, $Beta(a,b,i) = s_i$, $b < nzs[i+1 : i < max(t+1, max[s_i : i < t+1]) + 1] + 1 = nzs[i+1 : i < t+2] + 1$, и $a < nzs[1 + (i+1)b : i < t+1]$. Следи да за неке коначне низове важи $s' \leq ((a,b), t+1)$, $A(s',t)$. $\square$

Претходно смо дефинисали атомске формуле у PA као изразе облика $t = t'$ и $\perp$.

Дефиниција 1.46
$Atformula(x)$ је формула
$(\exists t < x\ \exists t' < x[Term(t) \wedge Term(t') \wedge x = (\ulcorner = \urcorner, t, t')] \wedge x = \ulcorner \bot \urcorner)$.

$Atformula(x)$ је $\Delta-$формула, с обзиром да је $Term(t)$ $\Delta-$формула.

Дефиниција 1.47
Formula(x) је формула
$\exists s[KonNiz(s) \wedge dn(s) > \boldsymbol{0} \wedge s_{dn(s)\dot{-}1} = x \wedge \forall i < dn(s)(Atformula(s_i) \vee$
$\exists j, k < i\ s_i = (\ulcorner \rightarrow \urcorner, s_j, s_k) \vee \exists j < i\ \exists v[Promenljiva(v) \wedge s_i = (\ulcorner \forall \urcorner, v, s_k)])]$.

Појављују се неограничени квантификатори $\exists s$ и $\exists v$ као и у дефиницији Formula(x). Доказ да се они могу ограничити помоћу "$\leq x$" је сличан оном који смо дали за теорему 1.56, стога ћемо га овде изоставити.

Претпостављамо да постоји $\Delta-$формула $Ax(x)$ која означава да је нешто аксиома Пеанове аритметике. Такође, претпостављамо да је дат $\Sigma-$псеудотерм $sub(t, i, x)$ који даје код формуле која се добије када се у формули која има код x, сва слободна појављивања променљиве која има код i замене термом који има код t.
Нпр. $sub(\ulcorner 0 \urcorner, \ulcorner 1 \urcorner, \ulcorner v_0 + v_1 = v_2 \urcorner) = \ulcorner v_0 + 0 = v_2 \urcorner$.

Дефиниција 1.48
PosledModPon(x,y,z) је формула

$$Formula(x) \wedge Formula(z) \wedge y = (\ulcorner \rightarrow \urcorner, z, x),$$

односно y је код формуле која је добијена modus ponens-ом од формула са кодовима x и z.

Дефиниција 1.49
PosledGen(x,y) је формула

$$\exists v < x(Formula(y) \wedge Promenljiva(v) \wedge x = (\ulcorner \forall \urcorner, v, y)),$$

односно, x је код формуле која је добијена генерализацијом од формула са кодовима y и v.

Обе наведене формуле су $\Delta-$формуле, као и она што следи у наредној дефиницији.

Дефиниција 1.50
$Dok(y,x)$ је формула
$(KonNiz(y) \wedge s_{dn(y)\dot{-}1} = x \wedge \forall i < dn(y)\dot{-}1[Ax(y_i) \vee$
$\exists j < i\ \exists k < i\ PosledModPon(y_i, y_j, y_k) \vee\ \exists j < iPosledGen(y_i, y_j)])$, *односно y је код низа који представља доказ за формулу чији је код x.*

Дефиниција 1.51
$Bew(x)$ је формула $\exists yDok(y,x)$, односно $Bew(x)$ значи да је x доказива у PA.

Јасно је да је Bew(x) $\Sigma-$формула, али није и $\Delta-$формула (осим уколико PA није неконзистентна).

Сада можемо да истражујемо шта Пеанова аритметика доказује о доказивости у PA.

1.8 Основне особине Bew(x)

С обзиром да је Bew(x) $\Sigma-$формула, онда је за сваку реченицу S Пеанове аритметике и Bew$(\ulcorner S \urcorner)$ $\Sigma-$реченица, тј. доказано је тврђење (iv) са почетка овог поглавља. Још важи да ако је S реченица и $\vdash S$, онда Bew$(\ulcorner S \urcorner)$ је тачна $\Sigma-$реченица, а према теореми 1.17, $\vdash$ Bew$(\ulcorner S \urcorner)$, тј. важи (i).

Теорема 1.57
Нека су S и T реченице Пеанове аритметике. Тада
$\vdash Bew(\ulcorner (S \to T) \urcorner) \to (Bew(\ulcorner S \urcorner) \to Bew(\ulcorner T \urcorner))$.

Доказ
Довољно је уочити да $\vdash Dok(y, \ulcorner (S \to T) \urcorner) \wedge Dok(y', \ulcorner S \urcorner) \to Dok(y * y' * [\ulcorner T \urcorner], \ulcorner T \urcorner)$. (Интуитивно, с обзиром да је *modus ponens* једно од два правила закључивања Пеанове аритметике, доказ за T је коначан низ који чине докази тврђења $S \to T$, S, и најзад сама реченица T).□

С обзиром да (iii) лако следи из (v), остаје да се покаже (v). Морамо показати да $\vdash S \to Bew(\ulcorner S \urcorner)$ за било коју $\Sigma-$реченицу S. Најпре морамо да покажемо да је функција која сваком броју i додељује Геделов број нумерала $\mathbf{i}$, дефинисана $\Sigma-$псеудотермом.

Дефиниција 1.52
$Num(x,y)$ је формула $\exists s(dn(s) = x + \mathbf{1} \wedge s_0 = \ulcorner \mathbf{0} \urcorner \wedge \forall i < x\ s_{i+1} = (\ulcorner \boldsymbol{s} \urcorner, s_i) \wedge s_x = y)$, односно y је код нумерала у којем се $\boldsymbol{s}$ појављује x пута.

Потребан нам је и $\Sigma-$псеудотерм за функцију која сваком i додељује Геделов број $i-$те променљиве.

Дефиниција 1.53
$prom(x) = \boldsymbol{2} \cdot x + \boldsymbol{17}$.

Дефиниција 1.54
$su(x, y, z) = sub(num(x), prom(y), z)$.

Вредност функције дефинисане $\Sigma-$псеудотермом $su(x, y, z)$ за било које i, j, k је резултат, $F_{v_j}(\mathbf{i})$, замене $\mathbf{i}$ за $j-$ту променљиву v_j у формули са Геделовим бројем k. Тако је нпр.

Теорема 1.58
$\vdash su(\boldsymbol{3}, \boldsymbol{4}, \ulcorner v_4 = v_1 \urcorner) = \ulcorner \boldsymbol{3} = v_1 \urcorner$.

Сада морамо објаснити једну врсту нотације: $'Bew[F]'$. Претпоставимо да је F формула Пеанове аритметике у којој је тачно m променљивих слободно и то су променљиве $v_{k_1}, ..., v_{k_m}$, где је $k_1 < ... < k_m$. Тада је $Bew[F]$ формула $Bew(su(v_{k_m}, \mathbf{k}_m, ..., su(v_{k_2}, \mathbf{k}_2, su(v_{k_1}, \mathbf{k}_1, \ulcorner F \urcorner))...))$. Приметимо да $Bew[F]$ има исте слободне променљиве $v_{k_1}, ..., v_{k_m}$ као и F. $Bew[F]$ је тачно за бројеве $i_1, ..., i_m$ (када су они додељени $v_{k_1}, ..., v_{k_m}$ редом) ако и само ако је

$$F_{v_{k_1}}(\mathbf{i}_1)...{}_{v_{k_m}}(\mathbf{i}_m)$$

односно, резултат замене нумерала $\mathbf{i}_1, ..., \mathbf{i}_m$ који означавају те бројеве за променљиве $v_{k_1}, ..., v_{k_m}$ у F, теорема Пеанове аритметике. У случају да је F реченица, тј. нема слободних променљивих, $Bew[F]$ је у ствари $Bew(\ulcorner F \urcorner)$.

Теорема 1.59 ("Доказивост *modus ponens*−ом")
За било које формуле F, G језика PA,
$\vdash Bew[(F \to G)] \to (Bew[F] \to Bew[G])$.

Доказ
Да бисмо учинили доказ прегледнијим, претпоставимо да су слободне променљиве у F v_2 и v_3, а у G v_1 и v_3. Тада
Bew[F] је $Bew(su(v_3, \mathbf{3}, (su(v_2, \mathbf{2}, \ulcorner F \urcorner))))$,
Bew[G] је $Bew(su(v_3, \mathbf{3}(su(v_1, \mathbf{1}, \ulcorner G \urcorner))))$, и
$Bew[(F \to G)]$ је $Bew(su(v_3, \mathbf{3}, su(v_2, \mathbf{2}, su(v_1, \mathbf{1}, \ulcorner (F \to G) \urcorner))))$.
Посматрајмо сад да

$\vdash su(v_3, \mathbf{3}, su(v_2, \mathbf{2}, su(v_1, \mathbf{1}, \ulcorner(F \to G)\urcorner))) =$
$(\ulcorner\to\urcorner, su(v_3, \mathbf{3}, (su(v_2, \mathbf{2}, \ulcorner F\urcorner))), su(v_3, \mathbf{3}, (su(v_1, \mathbf{1}, \ulcorner G\urcorner))))$. Тада, као и у доказу теореме 1.57,
$\vdash Dok(y, su(v_3, \mathbf{3}, su(v_2, \mathbf{2}, su(v_1, \mathbf{1}, \ulcorner(F \to G)\urcorner)))) \wedge Dok(y', su(v_3, \mathbf{3}, (su(v_2, \mathbf{2}, \ulcorner F\urcorner))))$
$\to Dok(y * y' * [su(v_3, \mathbf{3}, (su(v_1, \mathbf{1}, \ulcorner G\urcorner)))], su(v_3, \mathbf{3}, (su(v_1, \mathbf{1}, \ulcorner G\urcorner))))$. $\square$

Аналогно тврђењу (i) важи:

Теорема 1.60
За сваку формулу F Пеанове аритметике, ако $\vdash F$, *онда* $\vdash Bew[F]$.

Доказ
Претпоставимо, опет ради једноставности, да је $m = 2$ и да су у F две слободне променљиве v_3 и v_5. Онда је формула $Bew[F]$ једнака формули
$Bew(su(v_5, \mathbf{5}, su(v_3, \mathbf{3}, \ulcorner F\urcorner)))$. Нека формула G буде $\forall v_3 \forall v_5 F$. Онда је G реченица и према (i), $\vdash Bew(\ulcorner G\urcorner)$. Нека је H $\forall v_5 F$. Хоћемо да видимо да важи $\vdash Bew(\ulcorner G\urcorner) \to Bew[H]$. (Интуитивно, $(G \to H_{v_3}(\mathbf{i}))$ је свакако доказиво у логици и свакако је аксиома многих формулација логике. Према томе, да бисмо добили доказ H_{v_3}, додајемо доказ тврђења $(G \to H_{v_3}(\mathbf{i}))$ доказу формуле G и примењујемо *modus ponens*.)
Према томе, с обзиром да $\vdash \exists y\, Dok(y, (\ulcorner\to\urcorner, \ulcorner G\urcorner, su(v_3, \mathbf{3}, \ulcorner H\urcorner)))$ и
$\vdash Dok(y, (\ulcorner\to\urcorner, \ulcorner G\urcorner, su(v_3, \mathbf{3}, \ulcorner H\urcorner))) \wedge Dok(y', \ulcorner G\urcorner) \to$
$Dok(y' * y * [su(v_3, \mathbf{3}, \ulcorner H\urcorner)], su(v_3, \mathbf{3}, \ulcorner H\urcorner))$, егзистенцијалним квантификовањем имамо да $\vdash Bew(\ulcorner G\urcorner) \to Bew(su(v_3, \mathbf{3}, \ulcorner H\urcorner))$, тј. $\vdash Bew(\ulcorner G\urcorner) \to Bew[H]$. Слично, $\vdash Bew[H] \to Bew[F]$, па је стога $\vdash Bew[F]$. $\square$

Сада ћемо доказати да за било коју $\Sigma-$формулу F, $\vdash F \to Bew[F]$. (v) је специјалан случај овог резултата у којем је F реченица. Специјално, с обзиром да је Bew($\ulcorner S\urcorner$) $\Sigma-$реченица, $\vdash$ Bew($\ulcorner S\urcorner$) $\to$Bew($\ulcorner$Bew($\ulcorner S\urcorner)\urcorner$), односно важи (iii).

Теорема 1.61 ("Доказива Σ_1-комплетност")
За било коју $\Sigma-$*формулу,* $\vdash F \to Bew[F]$.

Доказ
Почињемо уочавањем да можемо претпоставити да је F стриктна $\Sigma-$формула, јер ако је $\Sigma-$формула, онда за неку стриктну $\Sigma-$формулу G, F је еквивалентно са G, тј. $\vdash F \to G$ и $\vdash G \to F$, одакле према теореми 1.60, $\vdash Bew[G \to F]$. Међутим, онда према теореми 1.59, $\vdash Bew[G] \to Bew[F]$, и онда ако $\vdash G \to Bew[G]$, $\vdash F \to Bew[F]$.

Најпре разматрамо случај у којем је F нека формула $u+v=w$. Претпоставимо да је F нека формула$v_5+v_2=v_3$. Хоћемо да видимо да $\vdash v_5+v_2=v_3 \to Bew[v_5+v_2=v_3]$.

Овде има аргумент, који може да се формализује у PA, који ово показује. Аргумент није ништа друго до разрађивање доказа теореме 1.7.

Нека је i_5 произвољно. (У формализацији, променљива v_5 игра улогу i_5 у садашњем аргументу.)

Претпоставимо да за произвољно i_3 важи $i_5+0=i_3$. (У формализацији, аксиома (3) је записана негде у овој тачки отприлике.) Тада $i_5=i_3$ и $\mathbf{i}_5$ је $\mathbf{i}_3$. (Овде би биле употребљене аксиоме идентитета из логике.) $v_0+\mathbf{0}=v_0$ је аксиома PA, дакле доказива је. Онда према правилу генерализације, $\forall v_0\ v_0+\mathbf{0}=v_0$ је доказиво. $\forall v_0\ v_0+\mathbf{0}=v_0 \to \mathbf{i}_5+\mathbf{0}=\mathbf{i}_5$ је логичка аксиома. Одатле следи да је $\mathbf{i}_5+\mathbf{0}=\mathbf{i}_5$, тј. $\mathbf{i}_5+\mathbf{0}=\mathbf{i}_3$ је доказиво. Дакле, за све i_3 је $\mathbf{i}_5+\mathbf{0}=\mathbf{i}_3$ доказиво ако $i_5+0=i_3$.

Нека је i_2 произвољно. Претпоставимо да је за све $\mathbf{i}_3$, $\mathbf{i}_5+\mathbf{i}_2=\mathbf{i}_3$ доказиво ако је $i_5+i_2=i_3$. Нека је $i_4=i_2+1$. Показаћемо да за све $\mathbf{i}_3$, $\mathbf{i}_5+\mathbf{i}_4=\mathbf{i}_3$ доказиво ако $i_5+i_4=i_3$. Нека је сада i_3 произвољно и претпоставимо $i_5+i_4=i_3$. Тада је $i_5+(i_2+1)=(i_5+i_2)+1=i_3$. С обзиром да 0 није следбеник, $i_3\neq 0$ и за неки број i_1, $i_3=i_1+1$. Дакле, $(i_5+i_2)+1=i_1+1$ и $i_5+i_2=i_1$. Према претпоставци, $\mathbf{i}_5+\mathbf{i}_2=\mathbf{i}_1$ је доказиво. Следећи аксиому (4), $\forall v_0\forall v_1\ v_0+\mathbf{s}v_1=\mathbf{s}(v_0+v_1)$ је доказиво, па је то и $\mathbf{i}_5+\mathbf{si}_2=\mathbf{si}_1$. Међутим, $\mathbf{si}_2$ је $\mathbf{i}_4$, а $\mathbf{si}_1$ је $\mathbf{i}_3$. Дакле, $\mathbf{i}_5+\mathbf{i}_4=\mathbf{i}_3$ је доказиво. Стога, за све i_3, $\mathbf{i}_5+\mathbf{i}_4=\mathbf{i}_3$ је доказиво ако $i_5+i_4=i_3$. Следи да је за све i_2, ако је за све i_3, $\mathbf{i}_5+\mathbf{i}_2=\mathbf{i}_3$ доказиво ако је $i_5+i_2=i_3$, онда, где је $i_4=i_2+1$, за све i_3, $\mathbf{i}_5+\mathbf{i}_4=\mathbf{i}_3$ је доказиво ако $i_5+i_4=i_3$.

Према индукцији (у формализацији се на овом месту појављује аксиома), за све i_3, $\mathbf{i}_5+\mathbf{i}_2=\mathbf{i}_3$ је доказиво ако $i_5+i_2=i_3$. Стога, ако $i_5+i_2=i_3$, онда је $\mathbf{i}_5+\mathbf{i}_2=\mathbf{i}_3$ резултат замене друге, треће и пете променљиве у $v_5+v_2=v_3$ уместо $\mathbf{i}_2,\mathbf{i}_3$ и $\mathbf{i}_5$ доказив.

Слично је за све друге изборе променљивих и слично, ако је F формула $u=v,\mathbf{0}=u,\mathbf{s}u=v$ или $u\cdot v=w$.

Да бисмо доказали теорему, довољно је показати да $\vdash F \to Bew[F]$, ако је F формула која се добија конјункцијом, дисјункцијом, егзистенцијалним квантификатором или ограниченим егзистанцијалним квантификатором од формуле G за коју важи $\vdash G \to Bew[G]$.

Конјункција: претпоставимо да је F формула $(G\wedge H)$,

$\vdash G \to Bew[G]$ и
$\vdash H \to Bew[H]$. Онда
$\vdash F \to (Bew[G] \wedge Bew[H])$. Сада
$\vdash G \to (H \to F)$. Према теореми 1.60,
$\vdash Bew[(G \to (H \to F))]$. Међутим, према теореми 1.59,
$\vdash Bew[(G \to (H \to F))] \to (Bew[G] \to Bew[(H \to F)])$ и
$\vdash Bew[(H \to F)] \to (Bew[H] \to Bew[F])$,
$\vdash F \to Bew[F]$.

Аргумент за дусјункцију је сличан, али чак једноставнији.

Егзистенцијални квантификатор: Претпоставимо да је F формула $\exists x G$ и
$\vdash G \to Bew[G]$. Према логици,
$\vdash G \to F$. Према теореми 1.59 и 1.60,
$\vdash Bew[G] \to Bew[F]$. Стога,
$\vdash G \to Bew[F]$. Променљива x није слободна у F, па није ни у $Bew[F]$, која има исте слободне променљиве као и F. По логици,
$\vdash \exists x G \to Bew[F]$, тј.
$\vdash F \to Bew[F]$.

Ограничени квантификатор је мало компликованији. Нека је H произвољна формула. Желимо да докажемо да су $Bew[H_y(\mathbf{s}y)]$ и$Bew[H]_y(\mathbf{s}y)$ еквивалентне. Претпоставимо да је y v_k, $k-$та променљива и нећемо помињати друге променљиве осим y и бројеве осим оних чији је нумерал замена за y. Тада, према формализацији доказа тврђења да за било који број i, резултат замене $\mathbf{s}i$ за y у H је резултат замене $\mathbf{i}$ за y у $H_y(\mathbf{s}y)$,
$\vdash su(y, \mathbf{k}, \ulcorner H_y(\mathbf{s}y) \urcorner) = su(\mathbf{s}y, \mathbf{k}, \ulcorner H \urcorner)$. Сада
$Bew[H_y(\mathbf{s}y)]$ је $Bew(su(y, \mathbf{k}, \ulcorner H_y(\mathbf{s}y) \urcorner))$ и
$Bew[H]_y(\mathbf{s}y)$ је $Bew(su(\mathbf{s}y, \mathbf{k}, \ulcorner H \urcorner))$, стога
$\vdash Bew[H_y(\mathbf{s}y)] \leftrightarrow Bew[H]_y(\mathbf{s}y)$.

Слично, с обзиром да у није слободна у $H_y(\mathbf{0})$,
$\vdash su(y, \mathbf{k}, \ulcorner H_y(\mathbf{0}) \urcorner) = \ulcorner H_y(\mathbf{0}) \urcorner = su(\mathbf{0}, \mathbf{k}, \ulcorner H \urcorner)$ и
$\vdash Bew[H_y(\mathbf{0})] \leftrightarrow Bew[H_y](\mathbf{0})$.

Сада претпоставимо да је F формула $\forall x < y G$ и
$\vdash G \to Bew[G]$. Стога, $F_y(\mathbf{0})$ је $\forall x(x < \mathbf{0} \to G_y(\mathbf{0}))$. С обзиром на
$\vdash \neg x < \mathbf{0}$,
$\vdash F_y(\mathbf{0})$,

$\vdash Bew[F_y(\mathbf{0})]$ према теореми 1.60,

$\vdash Bew[F]_y(\mathbf{0})$ према претходном, и

$\vdash F_y(\mathbf{0}) \to Bew[F]_y(\mathbf{0})$, тј.

$\vdash (F \to Bew[F])_y(\mathbf{0})$. Тада, с обзиром

$\vdash x < \mathbf{s}y \leftrightarrow x < y \vee x = y$,

$\vdash F_y(\mathbf{s}y) \leftrightarrow (F \wedge G)$, одакле према теоремама 1.59 и 1.60,

$\vdash Bew[F] \wedge Bew[G] \to Bew[F_y(\mathbf{s}y)]$. С обзиром на

$\vdash G \to Bew[G]$,

$\vdash (F \to Bew[F]) \to (F_y(\mathbf{s}y) \to Bew[F] \wedge Bew[G])$. Имајући у виду

$\vdash Bew[F_y(\mathbf{s}y)] \leftrightarrow Bew[F]_y(\mathbf{s}y)$,

$\vdash (F \to Bew[F]) \to (F_y(\mathbf{s}y) \to Bew[F]_y(\mathbf{s}y))$, тј.

$\vdash (F \to Bew[F]) \to (F \to Bew[F])_y(\mathbf{s}y)$ и стога

$\vdash \forall y((F \to Bew[F]) \to (F \to Bew[F])_y(\mathbf{s}y))$. По индуктивној аксиоми,

$\vdash F \to Bew[F]$.

Стога, за сваку $\Sigma-$формулу F, $\vdash F \to Bew[F]$. $\square$

2 Непотпуност Пеанове аритметике и Лебова теорема

2.1 Лема о дијагонализацији

Генерализована лема о дијагонализацији

Претпоставимо да су $y_0, ..., y_n, z_1, ..., z_m$ *различите променљиве и да су* $P_0(y_0, ..., y_n, \boldsymbol{z}), ..., P_n(y_0, ..., y_n, \boldsymbol{z})$ *формуле на језику* PA *у којима се све слободне променљиве налазе међу* $y_0, ..., y_n, \boldsymbol{z}$*.(*$\boldsymbol{z}$ *је скраћеница за* $z_1, ..., z_m$*). Тада постоје формуле* $S_0(\boldsymbol{z}), ..., S_n(\boldsymbol{z})$ *на језику* PA *у којима су све променљиве међу* $\boldsymbol{z}$ *и важи*
$\vdash S_0(\boldsymbol{z}) \leftrightarrow P_0(\ulcorner S_0(\boldsymbol{z})\urcorner, ..., \ulcorner S_n(\boldsymbol{z})\urcorner, \boldsymbol{z}), ...,$ *као и*
$\vdash S_n(\boldsymbol{z}) \leftrightarrow P_n(\ulcorner S_0(\boldsymbol{z})\urcorner, ..., \ulcorner S_n(\boldsymbol{z})\urcorner, \boldsymbol{z})$.

Доказ

Нека је $Su(w, x_0, ..., x_n, y)$ један $\Sigma-$псеудотерм за $(n+2)-$арну функцију *subst* чија је вредност за $a, b_0, ..., b_n$ Геделов број израза који се добија респективном заменом променљивих $x_0, ..., x_n$ у формули која има Геделов број a, нумералима $\mathbf{b}_0, ..., \mathbf{b}_n$. Нека је за свако $i \leq n$, k_i Геделов број за

$$P_i(su(x_0, x_0, ..., x_n), ..., su(x_n, x_0, ..., x_n), \mathbf{z}),$$

а нека је $S_i(\mathbf{z})$ следећа формула

$$P_i(su(\mathbf{k}_0, \mathbf{k}_0, \mathbf{k}_1, ..., \mathbf{k}_n), ..., su(\mathbf{k}_n, \mathbf{k}_0, ..., \mathbf{k}_n), \mathbf{z}).$$

Једино што треба да покажемо је

$$\vdash su(\mathbf{k}_i, \mathbf{k}_0, ..., \mathbf{k}_n) = \ulcorner S_i(\mathbf{z})\urcorner.$$

Респективном заменом променљивих $x_0, ..., x_n$, нумералима $\mathbf{k}_0, ..., \mathbf{k}_n$ у формули која има Геделов број k_i, тј. у формули

$$P_i(su(x_0, x_0, ..., x_n), ..., su(x_n, x_0, ..., x_n), \mathbf{z}),$$

добија се формула $S_i(\mathbf{z})$, те је $subst(k_i, k_0, ..., k_n)$ једнако Геделовом броју израза $S_i(\mathbf{z})$. Дакле, $\Sigma-$реченица

$$su(\mathbf{k}_i, \mathbf{k}_0, ..., \mathbf{k}_n) = \ulcorner S_i(\mathbf{z})\urcorner$$

је тачна, а из доказивости тачних $\Sigma-$реченица следи

$$\vdash su(\mathbf{k}_i, \mathbf{k}_0, ..., \mathbf{k}_n) = \ulcorner S_i(\mathbf{z}) \urcorner. \square$$

Приметимо да, ако су све формуле $P_0(y_0, ..., y_n, \mathbf{z}), ..., P_n(y_0, ..., y_n, \mathbf{z})$, $\Sigma-$формуле или $\Delta-$формуле, онда су и све формуле $S_0(z), ..., S_n(z)$ такође $\Sigma-$формуле или $\Delta-$формуле, респективно.

Последица 1

Претпоставимо да су $P_0(y_0, ..., y_n), ..., P_n(y_0, ..., y_n)$ формуле на језику PA, чије су све слободне променљиве међу променљивима $y_0, ..., y_n$. Тада постоје реченице $S_0, ..., S_n$ на језику PA такве да

$\vdash S_0 \leftrightarrow P_0(\ulcorner S_0 \urcorner, ..., \ulcorner S_n \urcorner), ...,$ *и*

$\vdash S_n (\leftrightarrow P_n(\ulcorner S_0 \urcorner, ..., \ulcorner S_n \urcorner)$.

Доказ

Ово је специјални случај генерализоване леме о дијагонализацији, када је $m = 0$. $\square$

Последица 2 (Лема о дијагонализацији)

Претпоставимо да је $P(y)$ формула на језику PA у којој је y једина слободна променљива. Тада постоји реченица S на језику PA таква да $\vdash S \leftrightarrow P(\ulcorner S \urcorner)$.

Доказ

Ово је специјални случај Последице 1, када је $n = 0$. $\square$

2.2 Лебова теорема и теорема о непотпуности PA

Леон Хенкин 1952. године поставља питање да ли је реченица S, добијена из леме о дијагонализацији када се уместо $P(x)$ стави $Bew(x)$, доказива или не. За такво S важи $\vdash S \leftrightarrow Bew(\ulcorner S \urcorner)$. Мартин Хуго Леб је 1954. година одговорио на ово питање показавши да за све реченице S, ако $\vdash Bew(\ulcorner S \urcorner) \rightarrow S$, онда $\vdash S$. Данас је ово тврђење познато као Лебова теорема. Она одмах даје одговор на Хенкиново питање, јер ако $\vdash S \leftrightarrow Bew(\ulcorner S \urcorner)$, онда $\vdash Bew(\ulcorner S \urcorner) \rightarrow S$, стога је $\vdash S$.

Значај Лебове теореме је вишеструк, а огледа се, између осталог, и у следећим ситуацијама.

Често није једноставно схватити колико је велики јаз, у математичком смислу, између тачности и доказивости. Наиме, уколико се не схвата разлика између ова два појма, може се чинити да је формула $Bew(\ulcorner S \urcorner) \rightarrow S$, за коју претпоставка Лебове теореме тврди да је доказива, тривијално тачна у сваком случају, независно

од тога да ли је S тачна или не, односно доказива или не. Међутим, ако је S нетачна, не би било добро да је и доказива, јер би се тада чинило да S не би требало увек да буде доказиво, већ само под условом да је $Bew(\ulcorner S \urcorner) \to S$ доказиво.

Можда делује као да $Bew(x)$ у Лебовој теореми функционише као негација. Знамо, ако је $\neg S \to S$ доказиво, доказиво је и S, а доказивање формуле S на овај начин назива се *reductio ad absurdum*. Међутим, доношење закључака о S само на основу чињенице да је $(S \to S)$ доказиво, је логичка грешка која се назива *petitio principii*. Уколико се не разликују појмови тачне и доказиве формуле, може се чинити да Лебова теорема тврди да је *petitio principii* допуштено у Пеановој аритметици.

Можда би било за очекивање да ће PA бар повремено тврдити да је исправна с обзиром на недоказиву реченицу S, тј. тврдити да ако доказује S, онда S важи. Међутим, Лебова теорема нам говори да то никада није тако. PA тврди $Bew(\ulcorner S \urcorner) \to S$, што је исправно с обзиром на S само када је очигледно да јесте, односно када је S заиста доказива.

Коначно, може изгледати врло чудно да тврђење које каже да ако је S доказиво, онда је S тачно, није само по себи доказиво. Чини се да је сасвим очигледно да за било које S важи да, ако је S тачно, онда је S и доказиво. Зашто се уопште бавити Пеановом аритметиком ако њене теореме нису тачне, и како је могуће да било која таква очигледна истина није доказива?

У наставку наводимо Лебову теорему, као и њен доказ.

Теорема 2.1 (Лебова теорема)
Ако $\vdash Bew(\ulcorner S \urcorner) \to S$, *онда* $\vdash S$.

Доказ
Нека је $Q(x)$ формула $(Bew(x) \to S)$. Према дијагоналној леми, постоји реченица I за коју важи: $\vdash I \leftrightarrow Q(\ulcorner I \urcorner)$, тј. $\vdash I \leftrightarrow (Bew(\ulcorner I \urcorner) \to S)$. Ради лакшег читања, скратићемо "$Bew(I)$" на "PI". Даље имамо
(1) $\vdash I \leftrightarrow (PI \to S)$. Одавде следи
(2) $\vdash I \to (PI \to S)$, а онда по услову (i) из претходног поглавља о Пеановој аритметици,
(3) $\vdash P(I \to (PI \to S))$, а по услову (ii) из претходног поглавља
(4) $\vdash P(I \to (PI \to S)) \to (PI \to P(PI \to S))$. Из (3) и (4) следи
(5) $\vdash PI \to P(PI \to S)$. Поново према услову (ii) из претходног поглавља имамо
(6) $\vdash P(PI \to S) \to (PPI \to PS)$, а према (5) и (6) следи

(7) $\vdash PI \to (PPI \to PS)$. Према услову (iii) из претходног поглавља,
(8) $\vdash PI \to PPI$, а из (7) и (8) следи
(9) $\vdash PI \to PS$.
Сада претпоставимо да је $\vdash Bew(\ulcorner S \urcorner) \to S$, односно
(10) $\vdash PS \to S$. Према (9) и (10) имамо
(11) $\vdash PI \to S$, а из (1) и (11) следи
(12) $\vdash I$. Из (i) претходног поглавља, следи
(13) $\vdash PI$, а онда из (11) и (13) следи
(14) $\vdash S$.$\square$

Теорема 2.2 (Прва теорема непотпуности *PA*)
Нека је $\vdash S \leftrightarrow \neg Bew(\ulcorner S \urcorner)$. *Онда ако је PA конзистентна,*
(а) $\nvdash S$;
(б) ако $\vdash Bew(\ulcorner S \urcorner) \to \vdash S$, *онда* $PA \nvdash \neg S$.

Доказ
(а) Имамо из (i) ако $\vdash S$ онда $\vdash Bew(\ulcorner S \urcorner)$, односно $\vdash \neg S$. С обзиром да је PA конзистенстна, добијамо $\nvdash S$;
(б) Ако $\vdash \neg S$, онда $Bew(\ulcorner S \urcorner)$, одакле по претпоставци следи $\vdash S$. Из конзистентности PA добијамо $\nvdash \neg S$. $\square$

Теорема 2.3 (Друга теорема о непотпуности *PA*)
Ако је PA конзистентна, онда $PA \nvdash \neg Bew(\ulcorner \bot \urcorner)$.

Доказ
Контрапозицијом, ако $\vdash \neg Bew(\ulcorner \bot \urcorner)$, онда $\vdash Bew(\ulcorner \bot \urcorner) \to \bot$, одакле из Лебове теореме следи $\vdash \bot$, односно PA није конзистентна. $\square$

2.3 Последице Лебове теореме

Контрапозицијом, из Лебове теореме имамо да, ако P није доказиво у PA, онда "ако је P доказиво у PA, онда је P тачно" није доказиво у PA. Уз претпоставку да је PA конзистентна, дајемо примере реченица које нису доказиве у PA.

Пример 1
С обзиром да "$1 + 1 = 3$" није доказиво у PA, онда ни "ако је $1 + 1 = 3$ доказиво у PA, онда $1 + 1 = 3$ " није доказиво у PA.

Пример 2
Дајемо пример тачне реченице која није доказива у PA.

Јака коначна Ремзијева теорема тврди да за било које природне бројеве n, k, m веће од нуле постоји N такво да ако обојимо било који подскуп од n елемената скупа $S = \{1, 2, 3, ..., N\}$ једном од k боја, онда постоји подскуп Y скупа S који има најмање m елемената, за који важи да су сви његови подскупови од n елемената исте боје, а број елемената скупа Y је мањи или једнак најмањем елементу скупа Y.

Парис-Харингтонова теорема каже да јака коначна Ремзијева теорема није доказива у PA. Дакле, из Лебове теореме следи да "ако је јака коначна Ремзијева теорема доказива у PA, онда је јака коначна Ремзијева теорема тачна" није доказива у PA.

Литература

[1] George Boolos, The Logic of Provability, Cambridge University Press, 1993.

[2] Raymond M. Smullyan, Logicians who reason about themselves

[3] Жарко Мијајловић, Зоран Марковић, Коста Дошен, Хилбертови проблеми и логика, Завод за уџбенике и наставна средства - Београд, 1986.

[4] https://en.wikipedia.org/wiki/Kurt_G%C3%B6del

[5] https://en.wikipedia.org/wiki/Martin_L%C3%B6b

[6] https://en.wikipedia.org/wiki/L%C3%B6b%27s_theorem

[7] https://en.wikipedia.org/wiki/Paris%E2%80%93Harrington_theorem#The_strengthened_finite_Ramsey_theorem

[8] http://www-groups.dcs.st-and.ac.uk/history/Biographies/Lob.html