5 НЕРАЗРЕШИМЫЕ ПРОБЛЕМЫ И НЕПОЛНОТА АРИФМЕТИКИ

5.1 Полусистемы Туэ

Пусть Δ - некоторый конечный алфавит. Через Δ^* обозначаем множество всех слов в алфавите Δ. Рассмотрим конечный список

$$(A_0, B_0), \ldots, (A_m, B_m) \tag{14}$$

пар непустых слов в алфавите Δ.

Определение 5.1.1. *Пусть A — произвольное слово из Δ^*. Если существуют такое i из $\{0, \ldots, m\}$ и такие слова U, V из Δ^*, что A графически совпадает с UA_iV, то скажем, что слово UB_iV получается из A применением правила (A_i, B_i).*

В этом случае также скажем, что UB_iV является непосредственным следствием A в полусистеме Туэ T, задаваемой алфавитом Δ и списком (14).

Слово B из Δ^* является следствием слова A из Δ^* в T, если существует такая конечная последовательность слов $D_0, \ldots, D_n$, что D_0 есть A, D_n есть B, а каждое слово этой последовательности, кроме начального, является непосредственным следствием в T предыдущего слова. При $n = 0$ это означает, что B совпадает с A. При $n > 0$ это означает, что для каждого i из $\{0, \ldots, n-1\}$ найдутся такие U, V из Δ^* и такое j из $\{0, \ldots, m\}$, что D_i графически совпадает с UA_jV, а D_{i+1} графически совпадает с UB_jV.

Если B является следствием слова A в T, то пишем: $A \longrightarrow_T B$.

Пример 5.1.1.

Рассмотрим алфавит $\Delta = \{0, 1\}$ и список

$$(01, 10), (00, 0), (11, 1). \tag{15}$$

Докажем индукцией по длине слова A, что для каждого A из Δ^* найдется такое B, что B является следствием A и B есть 0, либо B есть 1, либо B есть 10.

Действительно, если в слове A имеется подслово 00, то его можно заменить на подслово 0. Полученное непосредственное следствие имеет меньшую длину. Аналогично, подслово 11 можно заменить на подслово 1. Если 1 стоит в A после 0, то подслово 01 можно заменить на 10.

Например, из 001100 последовательно получаем 001100, 01100, 0100, 010, 100, 10.

При этом 1 есть следствие A, если A не содержит 0, 0 есть следствие A, если A не содержит 1, 10 есть следствие A, если A содержит и 0, и 1.

Пример 5.1.2.

Рассмотрим алфавит $\Delta = \{0.1\}$ и список

$$(01, 10), (10, 01), (00, 1) \tag{16}$$

Докажем, что для каждого непустого A из Δ^* найдется следствие вида 1^n или 01^n. Заменяя подслово 10 на подслово 01 последовательно несколько раз, получим следствие из A, в котором нули стоят раньше единиц, если в A вообще входят нули. Затем последние два нуля заменяем на 1 последовательно несколько раз. Например, из 01011010 последовательно получаем 00111010, 00111001, 1111001, 111111.

Если в A было n единиц и $2m$ нулей, то в полученном следствии нет нулей и $n + m$ единиц. Если в A было n единиц и $2m + 1$ нулей, то в полученном следствии один нуль и $n + m$ единиц.

Из примеров видно, что слово может иметь несколько разных непосредственных следствий. Например, в примере 15 непосредственными следствиями слова 001100 являются слова 11100 (заменяем первое вхождение 00 на 1), 010100 (заменяем вхождение 01 на 10), 001010 (заменяем вхождение 10 на 01), 00111 (заменяем второе вхождение 00 на 1) и другие.

Теорема 5.1. *По каждой МТ M можно построить такую полусистему Туэ $T(M)$, что M перерабатывает СП Π_1 в СП Π_2 или Π_1 совпадает с Π_2 тогда и только тогда, когда $\Pi_1 \longrightarrow_{T(M)} \Pi_2$. При этом каждое незаключительное СП для M имеет в $T(M)$ одно и только одно непосредственное следствие, а каждое заключительное СП для M не имеет в $T(M)$ ни одного непосредственного следствия.*

Доказательство. Пусть M — МТ с множеством состояний Q и внешним алфавитом E. Каждой паре $\langle s, q\rangle$ из $E \times Q$ сопоставляем 1, 7 или 49 правил полусистемы $T(M)$ в зависимости от $M(s, q)$.

Случай 1. $M(s, q) = s'Lr$, s' — непустой символ. Включаем в $T(M)$ правила:

(aqs, ras') для всех a из E,

$(hqs, hr \wedge s')$.

В этом случае включаем 7 правил в $T(M)$.

Случай 2. $M(s,q) = \wedge Lr$. Включаем в $T(M)$ правила:

$(aqsb, ra \wedge b)$ для всех a, b из E,

$(aqsh, rah)$ для всех a из E,

$(hqsb, hr \wedge \wedge b)$ для всех b из E,

$(hqsh, hr \wedge h)$.

В этом случае включаем 49 правил в $T(M)$.

Случай 3. $M(s,q) = s'Rr$, s' — непустой символ. Включаем в $T(M)$ правила:

$(qsa, s'ra)$ для всех a из E,

$(qsh, s'r \wedge h)$.

В этом случае включаем 7 правил в $T(M)$.

Случай 4. $M(s,q) = \wedge Rr$. Включаем в $T(M)$ правила:

$(bqsa, b \wedge ra)$ для всех a, b из E,

$(hqsa, hra)$ для всех a из E,

$(bqsh, b \wedge r \wedge h)$ для всех b из E,

$(hqsh, hr \wedge h)$.

В этом случае включаем 49 правил в $T(M)$.

Случай 5. $M(s,q) = s'Cr$. Включаем в $T(M)$ правило:

(qs, rs').

Правила $T(M)$ — это все включенные в $T(M)$ правила для всех пар $\langle s,q\rangle$ из $E \times Q$ и только они. Алфавит $T(M)$ — это $\{h, !\} \bigcup Q \bigcup E$.

Этим полусистема Туэ $T(M)$ полностью определяется.

Так как каждое незаключительное СП содержит точно одно вхождение символа из Q и левое слово каждого правила содержит точно одно вхождение символа из Q, то, сопоставляя определение $T(M)$ с определением работы МТ на СП из параграфа 4.7, получаем, что заключительное СП не имеет непосредственных следствий в $T(M)$, а незаключительное СП Π имеет одно и только одно непосредственное следствие Π' в $T(M)$ и при этом

$$\Pi \Longrightarrow^1_M \Pi'.$$

Для окончания доказательства осталось применить индукцию по числу непосредственных следствий при переходе от Π_1 к Π_2 или по числу тактов работы МТ M при переработке Π_1 в Π_2. ∎

Нумерация слов алфавита Δ — это отображение Δ^* во множество натуральных чисел ω, при котором разные слова имеют разные номера.

Рассмотрим теперь любую такую нумерацию слов в алфавите

$$\{h, !\} \bigcup Q \bigcup E,$$

что существует такая рекурсивная функция J, для которой $J(n)$ — это номер слова $hq \wedge |^n * h$, где q — начальное состояние МТ M.

Теорема 5.2. *Существует такая полусистема Туэ T, что не существует алгоритма, который бы по паре $\langle m, n \rangle$ натуральных чисел определял бы, являются ли m и n номерами таких слов, что слово номера n является следствием слова номера m в T.*

Доказательство. В качестве МТ M возьмем МТ, вычисляющую частично рекурсивную функцию ϕ', существование которой утверждается в теореме 4.43. Напомним, что область определения функции ϕ' не является рекурсивной, а множество значений этой функции является одноэлементным и состоит из числа 0. В качестве T возьмем $T(M)$. Пусть q — начальное состояние M. Из определений и теоремы 5.1 следует, что

$$hq \wedge |^n * h \longrightarrow_T h! \wedge *h$$

тогда и только тогда, когда ϕ' определено. Пусть $f(i,j) = 1$, если i и j являются номерами таких слов в алфавите полусистемы $T(M)$, что слово номера j является следствием в $T(M)$ слова номера i, и $f(i,j) = 0$ в остальных случаях. Пусть f — рекурсивная функция. Пусть m — номер слова $h! \wedge *h$.

Рассмотрим такую одноместную арифметическую функцию g, что $g(n) = f(J(n), m)$. Ясно, что g — рекурсивная функция.

Если $\phi'(n)$ определено, то

$$hq \wedge |^n * h \longrightarrow_T h! \wedge *h$$

и, значит, $f(J(n), m) = 1$. Поэтому $g(n) = 1$ для такого n. Если же $\phi'(n)$ не определено, то $h! \wedge *h$ не является следствием в $M(T)$ слова $hq \wedge |^n * h$ и, значит, $f(J(n), m) = 0$. Поэтому, $g(n) = 0$ в этом случае. Итак, существует алгоритм для определения по n, определено ли $\phi'(n)$, что противоречит выбору ϕ'. ∎

5.2 Соответствия Поста

Пусть Δ — некоторый конечный алфавит и

$$(A_0, B_0), \ldots, (A_m, B_m) \tag{17}$$

конечный список пар непустых слов в алфавите Δ. Скажем, что существует соответствие Поста для (17), если существует такая конечная непустая последовательность $i_1, \ldots, i_k$ натуральных чисел, не превосходящих m, что слово $A_{i_1} \ldots A_{i_k}$ графически совпадает с $B_{i_1} \ldots B_{i_k}$.

Теорема 5.3. *Не существует алгоритма, который бы по списку (17) определял бы, существует ли соответствие Поста для (17).*

Доказательство. В качестве МТ M возьмем МТ, вычисляющую частично рекурсивную функцию ϕ', существование которой утверждается в теореме 4.43. Пусть q — начальное состояние M.

Пусть $\Delta = \{h, !\} \bigcup Q \bigcup E$. Пусть $\bar{\Delta} = \{\bar{a} \mid a \in \Delta\}$. Для $A \in \Delta^*$ или $A \in (\bar{\Delta})^*$ через $\bar{A}$ обозначим $\bar{b}_1 \ldots \bar{b}_s$, если A есть $b_1 \ldots b_s$, и обозначим $b_1 \ldots b_s$, если A есть $\bar{b}_1 \ldots \bar{b}_s$.

Через $\Pi(M)$ обозначим объединение следующих пяти списков пар непустых слов в алфавите $\Delta \bigcup \bar{\Delta}$:

1. $\{(\bar{A}, B), (A, \bar{B}) \mid (A, B) \in T(M)\}$;
2. $\{(a, \bar{a}), (\bar{a}, a) \mid a \in \{h\} \bigcup E\}$;
3. $\{(hq \wedge |^n * h, hq \wedge |^n * h\bar{D})\}$, где D — непосредственное следствие $hq \wedge |^n * h$ в $T(M)$;
4. $\{(\bar{!}\bar{a}, !), (\bar{a}\bar{!}, !), (!a, \bar{!}), (a!, \bar{!}) \mid a \in E\}$;
5. $\{(\bar{h}\bar{!}\bar{h}\bar{!}, \bar{!}), (h!h!, !)\}$.

Список $\Pi(M)$ есть объединение пяти множеств. Если для списка $\Pi(M)$ существует соответствие Поста, то оно не начинается парой, входящей в первые два и в последние два множества этого объединения.

Если последовательность пар из $\Pi(M)$ уже выбрана и конкатенация левых слов этих пар имеет вид C, а конкатенация правых слов этих пар имеет вид CD_1 или $C\bar{D}_1$, где D_1 — незаключительное СП для M, то дальше надо дописать несколько пар из (2), потом одну пару из (1), и затем опять несколько пар из (2), в результате получив конкатенацию левых слов CD_1 или $C\bar{D}_1$ и конкатенацию правых слов $CD_1\bar{D}_2$ или $C\bar{D}_1D_2$, где D_2 — непосредственное следствие D_1 в $T(M)$, либо дописать пару из (3) с тем же результатом.

Если $\phi'(n)$ не определено, то всегда конкатенация правых слов длиннее конкатенации левых слов, и для $\Pi(M)$ не существует соответствия Поста. Иначе мы приходим к случаю, когда D_1 — заключительное слово Поста. Используя пары из (4), (5), (2), найдем соответствие Поста для $\Pi(M)$.

Итак, для $\Pi(M)$ существует соответствие Поста тогда и только тогда, когда $\phi'(n)$ определено. ■

5.3 Ассоциативные исчисления

Пусть Δ - некоторый конечный алфавит и

$$(A_0, B_0), \ldots, (A_m, B_m) \tag{18}$$

конечный список пар непустых слов в алфавите Δ.

Определение 5.3.1. *Если существуют такое $i \in \{0, \ldots, m\}$ и такие слова U, V из Δ^*, что A графически совпадает с UB_iV, то скажем, что слово UA_iV получается из A обратным применением правила (A_i, B_i). В этом случае также скажем, что A и UA_iV непосредственно эквивалентны в ассоциативном исчислении, заданном алфавитом Δ и списком правил (18). Если B — непосредственное следствие из A в полусистеме Туэ, заданной алфавитом Δ и списком (18), то A и B непосредственно эквивалентны в ассоциативном исчислении, заданном алфавитом Δ и списком правил (18).*

Слова A и B эквивалентны в ассоциативном исчислении, заданном алфавитом Δ и списком правил (18), если существует такая конечная последовательность слов $D_0, \ldots, D_n$, что D_0 есть A, D_n есть B, и для $i \in \{0, \ldots, n-1\}$ слово D_{i+1} непосредственно эквивалентно слову D_i в рассматриваемом ассоциативном исчислении. При $n = 0$ это означает, что A есть B, а при $n > 0$ это означает, что для каждого $i \in \{0, \ldots, n-1\}$ найдутся такие $U, V \in \Delta^*$ и такое $j \in \{0, \ldots, m\}$, что либо D_i графически совпадает с UA_jV, а D_{i+1} графически совпадает с UB_jV, либо D_{i+1} графически совпадает с UA_jV, а D_i графически совпадает с UB_jV.

Если A и B эквивалентны в ассоциативном исчислении S, то пишем: $A \longleftrightarrow_S B$.

Теорема 5.4. *Отношение $\longleftrightarrow_S$, заданное на множестве Δ^* ассоциативным исчислением S с алфавитом Δ и списком правил (18), является рефлексивным, симметричным и транзитивным.*

Доказательство. Очевидно. ∎

Теорема 5.5. *Существует такое ассоциативное исчисление S, что не существует алгоритма, который по паре $\langle m, n\rangle$ натуральных чисел определял бы, являются ли m и n номерами эквивалентных в S слов.*

Доказательство. В качестве МТ M возьмем МТ, вычисляющую частично рекурсивную функцию ϕ', существование которой утверждается в теореме 4.43. Напомним, что область определения функции ϕ' не является рекурсивной, а множество значений этой функции является одноэлементным и состоит из числа 0. В качестве T возьмем полусистему Туэ $T(M)$, построенную в доказательстве теоремы 5.1, а в качестве S возьмем ассоциативное исчисление, алфавит которого совпадает с алфавитом полусистемы $T(M)$, а список правил которого совпадает со списком правил полусистемы $T(M)$.

Из доказательства теоремы 5.2 следует, что доказательство теоремы закончится, если будет доказана следующая лемма.

Лемма 5.6. *Пусть* Π_1 *— незаключительное СП, а* Π_2 *— заключительное СП.* $\Pi_1 \longrightarrow_T \Pi_2$ *тогда и только тогда, когда* $\Pi_1 \longleftrightarrow_S \Pi_2$.

Доказательство. Ясно, что из $\Pi_1 \longrightarrow_T \Pi_2$ следует, что $\Pi_1 \longleftrightarrow_S \Pi_2$. Пусть $\Pi_1 \longleftrightarrow_S \Pi_2$. Тогда существует такая конечная последовательность $D_0, \ldots, D_m$ слов в алфавите Δ, что D_0 есть Π_1, D_m есть Π_2 и для каждого $i \in \{0, \ldots, m-1\}$ слова D_i и D_{i+1} непосредственно эквивалентны в S. Утверждение $\Pi_1 \longrightarrow_T \Pi_2$ будем доказывать индукцией по m. Если $m = 1$, то D_1 является заключительным СП и не может получаться из D_0 обратным применением правила (в каждом правиле $T(M)$ левое слово не содержит заключительного состояния !).

Если в последовательности $D_0, \ldots, D_m$ каждое следующее слово получается из предыдущего прямым применением правила, то $\Pi_1 \longrightarrow_T \Pi_2$.

Если в последовательности $D_0, \ldots, D_m$ некоторое слово получается из предыдущего обратным применением правила ,то таким словом не может быть D_m, так как левое слово каждого правила не содержит заключительного состояния. Поэтому найдется такое $i \in \{0, \ldots, m-1\}$, что D_i получается из D_{i-1} обратным применением правила, а D_{i+1} получается из D_i прямым применением правила. Тогда D_{i-1} и D_{i+1} являются непосредственными следствиями D_i в $T(M)$. Так как D_i имеет только одно непосредственное следствие в $T(M)$, то D_{i-1} и D_{i+1} графически совпадают. Поэтому вместо последовательности $D_0, \ldots, D_m$ можно взять более короткую последовательность $D_1, \ldots, D_{i-1}, D_{i+2}, \ldots, D_m$, если $m \geq i+2$, или $D_1, \ldots, D_{i-1}, D_m$, если $m = i+1$. ∎

Теорема 5.5 тоже доказана. ∎

Определение 5.3.2. *Алгебраическая система сигнатуры* $\langle * \rangle$, *в которой истинна формула*

$$(\forall x)(\forall y)(\forall z)(x * (y * z)) = ((x * y) * z),$$

называется полугруппой.

Определение 5.3.3. *По ассоциативному исчислению* S *заданному алфавитом* Δ *и списком правил (18) следующим образом построим полугруппу. Основным множеством этой полугруппы будет множество всех классов эквивалентности, на которое отношение* $\longleftrightarrow_S$ *разбивает* *множество Δ^*. Операция на множестве классов задается следующим образом:*

если ζ и θ — классы эквивалентности по $\longleftrightarrow_S$, то выбираем произвольным образом слова $A \in \zeta$ и $B \in \theta$ и через $\zeta * \theta$ обозначаем класс, содержащий слово AB.

Говорят,что полученная полугруппа задается множеством образующих Δ и множеством определяющих соотношений (18).

Теорема 5.7. *Построенная в определении 5.3.3 алгебраическая система определена корректно: класс $\zeta * \theta$ определяется однозначно и не зависит от выбора $A \in \zeta$ и $B \in \theta$. Полученная алгебраическая система является полугруппой.*

Доказательство. Пусть $A_1 \longleftrightarrow_S A_2$ и $B_1 \longleftrightarrow_S B_2$. Надо доказать, что $A_1B_1 \longleftrightarrow_S A_2B_2$. Рассмотрим такую последовательность $D_0, \ldots, D_m$, что D_0 есть A_1, D_m есть A_2 и для каждого $i \in \{0, \ldots, m-1\}$ слова D_i и D_{i+1} непосредственно эквивалентны в S. Рассмотрим такую последовательность $E_0, \ldots, E_l$, что E_0 есть B_1, E_l есть B_2 и для каждого $i \in \{0, \ldots, l-1\}$ слова E_i и E_{i+1} непосредственно эквивалентны в S. Рассмотрим теперь последовательность

$$D_0E_0, D_1E_0, \ldots, D_mE_0, D_mE_1, \ldots, D_mE_l.$$

Легко заметить, что начало этой последовательности — это слово A_1B_1, конец этой последовательности — это слово A_2B_2, а каждые два соседних слова этой последовательности непосредственно эквивалентны в S. Это и доказывает эквивалентность в S слов A_1B_1 и A_2B_2.

Итак, в определении 5.3.3 корректно определяется алгебраическая система.

Эта алгебраическая система является полугруппой. Действительно, если $A \in \zeta$, $B \in \theta$ и $C \in \gamma$, то $\zeta * \theta$ содержит слово AB, а $(\zeta * \theta) * \gamma$ содержит слово ABC. Класс же $\theta * \gamma$ содержит слово BC и, значит, класс $\zeta * (\theta * \gamma)$ содержит слово ABC. Так как классы $(\zeta * \theta) * \gamma$ и $\zeta * (\theta * \gamma)$ имеют общий элемент, то они совпадают. ∎

Пусть теперь $\langle G; * \rangle$ — произвольная полугруппа. Пусть f — некоторое отображение Δ в G. Если $s > 1$ и $a_1, \ldots, a_s \in \Delta$, то $f(a_1 \ldots a_s)$ — это $f(a_1) \ldots f(a_s)$. Индукцией по длине слова A тем самым $f(A)$ определено для всех непустых $A \in \Delta^*$.

Теорема 5.8. $f(AB) = f(A) * f(B)$ *для любых непустых* $A, B \in \Delta^*$.

Доказательство. Индукцией по длине слова A. Если длина A равна 1, то утверждаемое равенство следует из определения f. Пусть

$$f(AB) = f(A) * f(B).$$

Тогда

$$f(aAB) = f(a) * f(AB) = f(a) * (f(A) * f(B)) = f(aA) * f(B).$$

∎

Теорема 5.9. *Пусть $\langle G; * \rangle$ — полугруппа и f — такое отображение Δ в G, что $f(A_i) = f(B_i)$ для всех $i \in \{0, \dots, m\}$. Пусть S — ассоциативное исчисление, заданное алфавитом Δ и списком правил (18). Если $A, B \in \Delta^*$ и $A \longleftrightarrow_S B$, то $f(A) = f(B)$.*

Доказательство. Пусть $D_0, \dots, D_m$ — такая последовательность слов в алфавите Δ, что D_0 есть A, D_m есть B и каждые два соседние слова этой последовательности непосредственно эквивалентны. Равенство $f(A) = f(B)$ будем доказывать индукцией по m. Пусть D' получается из D прямым применением правила (A_i, B_i). Тогда существуют такие $U, V \in \Delta^*$, что D есть UA_iV, а D' есть UB_iV. По теореме 5.8,

$$f(D) = f(U) * (f(A_i) * f(V)) = f(U) * (f(B_i) * f(V)) = f(D').$$

Теперь $f(D_0) = f(D_1)$ и $f(D_1) = f(D_m)$. Поэтому $f(A) = f(B)$. ∎

Теорема 5.10. *Пусть $A, B \in \Delta^*$ и $f(A) = f(B)$ для любой полугруппы $\langle G; * \rangle$ и любого такого отображения f алфавита Δ в G, что $f(A_i) = f(B_i)$ для всех $i \in \{0, \dots, m\}$.*

Тогда $A \longleftrightarrow_S B$ для ассоциативного исчисления S заданного алфавитом Δ и списком правил (18).

Доказательство. Так как $A_i \longleftrightarrow_S B_i$, то, взяв для любого $D \in \Delta^*$ за $f(D)$ класс эквивалентности по S, содержащий D, получим, что в полугруппе классов эквивалентности по S выполнены равенства $f(A_i) = f(B_i)$ для всех $i \in \{0, \dots, m\}$. Поэтому $f(A) = f(B)$ в этой полугруппе. Значит, $A \longleftrightarrow_S B$. ∎

Пусть S — ассоциативное исчисление, заданное алфавитом $\Delta = \{a_0, \dots, a_l\}$ и списком правил (18). Пусть g — одно-однозначное отображение Δ в переменные. Пусть $g(aA) = (g(a) * g(A))$ для любых $a \in \Delta$

и непустого $A \in \Delta^*$. Эти правила каждому непустому слову из Δ^* ставят в соответствие терм сигнатуры $\langle * \rangle$. Обозначим через ϕ формулу

$$((\forall x)(\forall y)(\forall z)(((x * y) * z) = (x * (y * z)) \to (\forall g(a_0)) \dots (\forall g(a_l))$$
$$(((\dots (g(A_0) = g(B_0) \& g(A_1) = g(B_1)) \dots) \& g(A_m) = g(B_m))$$
$$\to g(A) = g(B))). \quad (19)$$

Теорема 5.11. *Формула ϕ тогда и только тогда тождественно истинна, когда $A \longleftrightarrow_S B$.*

Доказательство. Пусть формула ϕ тождественно истинна. Рассмотрим произвольную полугруппу $\langle G; * \rangle$. Формула ϕ истинна в этой полугруппе. Выберем произвольные $b_0, \dots, b_l$ в G. Рассмотрим такое отображение f алфавита Δ в G, что $f(a_i) = b_i$ для $i \in \{0, \dots, l\}$. Из истинности ϕ в рассматриваемой полугруппе следует, что если $f(A_i) = f(B_i)$ для всех $i \in \{0, \dots, l\}$, то $f(A) = f(B)$. По теореме 5.10, $A \longleftrightarrow_S B$.

Пусть, наоборот, $A \longleftrightarrow_S B$. ϕ есть импликация $(\phi_1 \to \phi_2)$. Рассмотрим произвольную систему $\langle G; * \rangle$ сигнатуры $\langle * \rangle$. Если эта система не является полугруппой, то ϕ в ней истинна, так как ϕ_1 в ней ложна. Пусть эта система — полугруппа. Надо доказать, что ϕ_2 истинна в этой полугруппе. Рассмотрим произвольное отображение f алфавита Δ в G. Это отображение приписывает значения переменным $g(a_0), \dots, g(a_l)$: значение $g(a_i)$ есть $f(a_i)$ для $i = 0, 1, \dots, l$. Формула ϕ_2 начинается кванторной приставкой. Если отбросить эту кванторную приставку, то получим матрицу этой формулы. Надо доказать, что матрица формулы ϕ_2 при этих значениях переменных истинна. Если хотя бы одно из равенств $f(A_i) = f(B_i)$ не выполняется для $i = 0, 1, \dots, l$, то матрица формулы ϕ_2 истинна при этих значениях переменных. Пусть теперь

$$f(A_0) = f(B_0), \dots, f(A_m) = f(B_m).$$

По теореме 5.9, $f(A) = f(B)$, а это говорит об истинности матрицы формулы ϕ_2 при этих значениях переменных. ∎

Нумерация формул логики предикатов некоторой сигнатуры — это такое отображение, которое каждой формуле этой сигнатуры ставит в соответствие непустое множество натуральных чисел — номеров этой формулы так, что никакое натуральное число не является номером двух разных формул.

Пусть рассматриваемая сигнатура содержит символ $*$ двухместной операции. Выберем в качестве M МТ, вычисляющую функцию ϕ', существование которой утверждается в теореме 4.43, в качестве T — полусистему Туэ $T(M)$, в качестве S — ассоциативное исчисление с тем же алфавитом и с тем же списком правил, что и у $T(M)$, в качестве A — слово $h! \wedge *h$, в качестве B — слово $hq \wedge |^n * h$, и обозначим формулу (19) через ϕ_n. Рассмотрим теперь любую такую нумерацию формул логики предикатов рассматриваемой сигнатуры, что, при некотором g, существует такая рекурсивная функция J, для которой $J(n)$ — это номер формулы ϕ_n.

Теорема 5.12. *Не существует алгоритма, который бы по натуральному числу n определял бы, является ли n номером тождественно истинной формулы логики предикатов рассматриваемой сигнатуры.*

Доказательство. Пусть f — рекурсивная функция такая, что $f(i) = 1$, если i — номер тождественно истинной формулы, и $f(i) = 0$ в остальных случаях. Рассмотрим такую функцию g, что $g(n) = f(J(n))$ для всех натуральных n. Функция g рекурсивна. Если $\phi'(n)$ определено, то

$$hq \wedge |^n * h \longleftrightarrow_S h! \wedge *h$$

по теореме 5.2 и лемме 5.6. По теореме 5.11, $J(n)$ в этом случае — номер тождественно истинной формулы. Значит $g(n) = 1$. Если же $\phi'(n)$ не определено, то $J(n)$ не является номером тождественно истинной формулы и $g(n) = f(J(n)) = 0$. Это противоречит выбору ϕ'. ∎

5.4 Тезис Черча

Мы заканчиваем формальное изложение теории алгоритмов. Но прежде, чем поставить последнюю точку, хотелось бы обсудить некоторые содержательные вопросы.

С алгоритмами математики сталкивались испокон веков. Вспомним хотя бы алгоритм Евклида для нахождения общего наибольшего делителя двух натуральных чисел или общего наибольшего делителя двух многочленов. Изложенный в главе 3 способ определения тождественной истинности формулы логики высказываний, состоящий в приведении этой формулы к КНФ и проверке, каждая ли эд полученной КНФ содержит в качестве члена одновременно и некоторое высказывание, и отрицание этого высказывания, тоже, разумеется, является алгоритмом. В главе 4 фактически приводится алгоритм, который по последовательности, задающей частично рекурсивную функцию, строит программу, вычисляющую эту же функцию. В главе 3 строится алгоритм, который по формуле логики предикатов строит эквивалентную ей предваренную формулу. Этот список алгоритмов можно продолжать.

До тех пор, пока мы приводим конкретные алгоритмы для решения каких-то задач, мы фактически не нуждаемся в формальном уточнении, что же такое алгоритм вообще. Обычно либо все соглашаются, что приводимая процедура действительно позволяет эффективно вычислить нужную величину по заданным, либо всем сразу ясно, что приводимое рассуждение на самом деле не позволяет фактически вычислить результат, а является чистой теоремой существования.

Дело однако меняется, если мы хотим доказать отсутствие алгоритма для решения какой-то массовой задачи, например ,отсутствие алгоритма, который по формуле логики предикатов определяет, является ли эта формула тождественно истинной. В таком случае необходимо формальное (математическое) определение алгоритма.

Такое формальное определение было разработано в 30-х годах нашего века. Оно было предложено параллельно несколькими авторами в разных терминах. Одним из таких уточнений понятия эффективно вычислимой функции является понятие частично рекурсивной функции, другим — понятие функции, вычислимой по Тьюрингу, третьим — программно вычислимой функции. Были предложены четвертое, пятое и т.д. уточнения.

Насколько предложенные уточнения удовлетворительны? Ответ на такой вопрос не может быть математической теоремой, так как само понятие алгоритма не является математическим. Ответ на этот вопрос может дать только практика. Более подробно, все функции, которые считаются эффективно вычислимыми, должны удовлетворять формальному определению, а все, которые не считаются эффективно вычислимыми, должны не удовлетворять ему.

Если принять этот критерий, то предложенные уточнения хороши. Косвенным подтверждением этого является и тот факт, что все упомянутые уточнения, хотя они и формулируются в различных терминах, определяют один и тот же класс функций.

Поэтому общепринят сейчас следующий тезис Черча: функция тогда и только тогда эффективно вычислима, когда она частично рекурсивна.

Этот тезис, как уже упоминалось, не может быть доказан. Его надо воспринимать, как экспериментальный факт, который подтверждается обширной практикой.

Даже, если принять тезис Черча, при рассмотрении функций, аргументы которых пробегают не натуральные числа, а другие конструктивные объекты, например, слова некоторого алфавита, программы или формулы, возникает проблема кодировки этих объектов натуральными числами. Обычно предлагают какую-то конкретную кодировку, но тогда остается досада от сомнения, не изменится ли все при другой кодировке. Кроме того, описание кодировки обычно громоздко, а явное выписывание последовательностей, доказывающих частичную рекурсивность нужных функций, хотя и рутинно, но нудно.

По этой причине мы не стали явно описывать нужные кодировки, а наоборот акцентировали внимание на свойствах, которые от такой кодировки требуются, оставляя читателю самому придумать одну из кодировок, удовлетворяющую требуемым свойствам. Во всех случаях придумать такую кодировку просто, а требуемые свойства естественны.

5.5 Формулировка формальной арифметики

В этой главе мы будем рассматривать сигнатуру Ω_1, содержащую символы операций двухместных $+$ и $*$ и нульместных 0, 1.

Определение 5.5.1 (ФА). *Аксиомами формальной арифметики (ФА) являются все аксиомы исчисления предикатов, другими словами, все секвенции видов:*

а) $\Phi \vdash \Phi$,

б) $\vdash x = x$,

в) $x = y\ (\Phi)^z_x \vdash (\Phi)^z_y$,

а так же все секвенции следующих видов:

г) $\vdash \neg 0 = (x+1)$,

д) $\vdash (x+0) = x$,

е) $\vdash (x+(y+1)) = ((x+y)+1)$,

ж) $\vdash (x*0) = 0$,

з) $\vdash (x*(y+1)) = ((x*y)+x)$,

и) $(x+1) = (y+1) \vdash x = y$,

к) $(\Phi)^x_0\ (\forall x)(\Phi \to (\Phi)^x_{x+1}) \vdash \Phi$,

где Φ *— формула, а* x, y, z *— переменные. В в), как обычно, предполагается, что* $(\Phi)^z_x$ *и* $(\Phi)^z_y$ *определены. ФА может иметь и другие аксиомы.*

Правилами вывода в ФА являются все правила вывода исчисления предикатов и только они. Определения доказательства и дерева доказательства совпадают с соответствующими определениями для исчисления предикатов из главы 3.

Теоремы 3.2 и 3.3 и следствие из этой теоремы 3.3 справедливы и для формальной арифметики.

Ясно, что все секвенции, доказуемые в исчислении предикатов, доказуемы и в ФА. Ясно также, что теоремы 3.20 и 3.21 и теорема 3.23 справедливы и для ФА. Доказательства этих утверждений, приведенные ранее, дословно годятся и для ФА. В частности, из определения 5.5.1 и теоремы 3.21 получается

Теорема 5.13. *Для любых термов t и s доказуемы секвенции:*
1) $\vdash \neg 0 = (t+1)$,
2) $\vdash (t+0) = t$,
3) $\vdash (t+(s+1)) = ((t+s)+1)$,
4) $\vdash (t*0) = 0$,
5) $\vdash (t*(s+1)) = ((t*s)+t)$,
6) $\vdash (t+1) = (s+1) \to t = s$.

Теорема 5.14 (о формальной индукции). *Пусть Γ — любая конечная или пустая последовательность формул, Φ и x — любые формула и переменная. Если секвенции $\Gamma \vdash (\Phi)^x_0$ и $\Gamma \vdash (\forall x)(\Phi \to (\Phi)^x_{(x+1)})$ доказуемы в ФА, то секвенции $\Gamma \vdash (\forall x)\Phi$ и $\Gamma \vdash \Phi$ тоже доказуемы в ФА.*

Доказательство. Обозначим формулу

$$(\forall x)(\Phi \to (\Phi)^x_{(x+1)})$$

через Ψ. В дереве

$$\frac{\Gamma \vdash (\forall x)\Phi}{\dfrac{\Gamma \vdash ((\Phi)^x_0 \to (\forall x)\Phi)}{\dfrac{\Gamma\ (\Phi)^x_0 \vdash (\forall x)\Phi}{\Gamma\ (\Phi)^x_0 \vdash (\Psi \to (\forall x)\Phi) \quad \Gamma\ (\Phi)^x_0 \vdash \Psi}\ \to -\text{уд}}\ \to -\text{вв} \quad \Gamma \vdash (\Phi)^x_0}$$

корень получается по правилу удаления импликации, а все висячие вершины доказуемы. Секвенция $\Gamma \vdash \Phi$ доказывается аналогично. ∎

Теорема 5.15. *Для любых термов t, r, s доказуемы секвенции:*
1) $\vdash (t+r) = (r+t)$,
2) $\vdash (t+(r+s)) = ((t+r)+s)$,
3) $\vdash (t*r) = (r*t)$,
4) $\vdash (t*(r*s)) = ((t*r)*s)$,
5) $\vdash (t*(r+s)) = ((t*r)+(t*s))$,
6) $\vdash ((r+s)*t) = ((r*t)+(s*t))$,
7) $(t+s) = (r+s) \vdash t = r$.

Доказательство. 1). По теореме 3.21, достаточно доказать секвенцию $\vdash (x+y) = (y+x)$, где x, y — переменные. По теореме 5.14, достаточно доказать секвенции $\vdash (0+y) = (y+0)$ и

$$\vdash (x+y) = (y+x) \to ((x+1)+y) = (y+(x+1)).$$

Докажем эти секвенции.

Докажем сначала $\vdash (0+y)=(y+0)$. Обозначим через Φ формулу

$$((0+y)=y \to (0+y)=(y+0))$$

и через Ψ формулу

$$(y=(y+0) \to (0+y)=(y+0)).$$

Рассмотрим дерево:

$$\dfrac{\vdash (0+y)=(y+0)}{\vdash (0+y)=y \qquad \dfrac{\vdash \Phi}{\dfrac{(0+y)=y \vdash (0+y)=(y+0)}{(0+y)=y \vdash \Psi \quad (0+y)=y \vdash y=(y+0)}\;\to\!-\text{уд}}\;\to\!-\text{вв}}$$

Используя правило введения импликации и транзитивность равенства (пункт в) теоремы 3.23), доказываем секвенцию

$$(0+y)=y \vdash (y=(y+0) \to (0+y)=(y+0)).$$

Используя правило утончения, симметричность равенства (пункт б) теоремы 3.23) и схему аксиом д), доказываем секвенцию

$$(0+y)=y \vdash y=(y+0).$$

Осталось доказать секвенцию

$$\vdash (0+y)=y.$$

По теореме 5.14, надо доказать секвенции $\vdash (0+0)=0$ и

$$\vdash ((0+y)=y \to (0+(y+1))=(y+1)).$$

Первая из этих секвенций есть 2) теоремы 5.13, когда t есть 0.

Докажем вторую. Пусть Θ обозначает формулу

$$(0+(y+1))=((0+y)+1).$$

В дереве

$$\dfrac{\vdash ((0+y)=y \to (0+(y+1))=(y+1))}{\dfrac{(0+y)=y \vdash (0+(y+1))=(y+1)}{\dfrac{(0+y)=y \vdash (\Theta \to (0+(y+1))=(y+1))}{(0+y)=y \quad \Theta \vdash (0+(y+1))=(y+1)}\;\to\!-\text{вв} \quad (0+y)=y \vdash \Theta}\;\to\!-\text{уд}}$$

две висячие вершины. Левая доказана по теореме 3.21, так как

$$x = y \ \ (0 + (y + 1)) = (x + 1) \vdash (0 + (y + 1)) = (y + 1)$$

является аксиомой в) при Φ равном $(0 + (y + 1)) = (z + 1)$. Правая доказуема по теореме 5.13.

Итак, секвенция $\vdash (0 + y) = (y + 0)$ доказуема. Докажем вторую секвенцию.

Достаточно доказать секвенцию

$$(x + y) = (y + x) \vdash ((x + 1) + y) = ((x + y) + 1).$$

Действительно, в этом случае секвенция

$$(x + y) = (y + x) \vdash ((x + 1) + y) = (y + (x + 1)) \tag{20}$$

получается по правилам удаления импликации и введения импликации из секвенции

$$(x + y) = (y + x) \ \ ((x + 1) + y) = ((x + y) + 1) \vdash \\ ((x + 1) + y) = (y + (x + 1)) \tag{21}$$

и доказуемой секвенции. Так как секвенция

$$\vdash (y + (x + 1)) = ((y + x) + 1)$$

доказуема (схема аксиом е)), то секвенция (21) получается из доказуемой секвенции и секвенции

$$(x + y) = (y + x) \ \ ((x + 1) + y) = ((x + y) + 1) \\ (y + (x + 1)) = ((y + x) + 1) \vdash \\ ((x + 1) + y) = (y + (x + 1)) \tag{22}$$

по правилам утончения (дважды примененным), удаления импликации и введения импликации. Так как

$$z_1 = z_2 \ \ ((x + 1) + y) = (z_1 + 1) \vdash ((x + 1) + y) = (z_2 + 1)$$

является аксиомой, то секвенция

$$(x + y) = (y + x) \ \ ((x + 1) + y) = ((x + y) + 1) \vdash \\ ((x + 1) + y) = ((y + x) + 1) \tag{23}$$

доказуема (теорема 3.21). Секвенция (22) получается из секвенции (23) и секвенции

$$((x+1)+y) = ((y+x)+1) \;\; (y+(x+1)) = ((y+x)+1) \vdash \\ ((x+1)+y) = (y+(x+1)) \quad (24)$$

по правилам утончения, введения и удаления импликации. Так как секвенция

$$u = w \;\; v = w \vdash u = v$$

доказуема для любых переменных u, v, w (теорема 3.23), то секвенция (24) тоже доказуема (теорема 3.21). Поэтому секвенции (22), (21) и (20) доказуемы. Осталось доказать секвенцию

$$\vdash ((x+1)+y) = ((x+y)+1).$$

По теореме 5.14, достаточно доказать секвенции

$$\vdash ((x+1)+0) = ((x+0)+1),$$

$$((x+1)+y) = ((x+y)+1) \vdash ((x+1)+(y+1)) = ((x+(y+1))+1).$$

Докажем первую секвенцию. Обозначим $((x+1)+0) = ((x+0)+1)$ через Θ. В дереве

$$\frac{\vdash ((x+1)+0) = ((x+0)+1)}{\vdash (((x+1)+0) = (x+1) \to \Theta) \quad \vdash ((x+1)+0) = (x+1)}$$

корень получается по правилу удаления импликации, а вторая висячая вершина доказуема по теореме 5.13, пункт 2). Для доказательства первой висячей вершины достаточно доказать секвенции

$$((x+1)+0) = (x+1) \vdash ((x+0)+1) = (x+1), \quad (25)$$

$$((x+1)+0) = (x+1) \vdash \\ (((x+0)+1) = (x+1) \to ((x+1)+0) = ((x+0)+1)) \quad (26)$$

(правила удаления импликации и введения импликации). Дерево

$$\cfrac{((x+1)+0) = (x+1) \vdash ((x+0)+1) = (x+1)}{\cfrac{\vdash ((x+0)+1) = (x+1)}{\vdash (x+0) = x \quad \vdash (x+0) = x \to ((x+0)+1) = (x+1)}\;\to\!-\text{уд}}\;\text{ут}$$

доказывает (25). Первая висячая вершина этого дерева является аксиомой, а вторая доказуема по теореме 3.21. Секвенция (26) получается по правилу введения импликации из доказуемой по теореме 3.21 секвенции

$$((x+1)+0)=(x+1)\ ((x+0)+1)=(x+1)\vdash((x+1)+0)=((x+0)+1).$$

Докажем вторую секвенцию. Достаточно доказать секвенции

$$((x+1)+y)=((x+y)+1)\vdash((x+1)+y)=(x+(y+1)), \tag{27}$$

$$((x+1)+y)=(x+(y+1))\vdash \\ ((x+1)+(y+1))=((x+(y+1))+1). \tag{28}$$

Так как

$$\vdash (x+(y+1))=((x+y)+1)$$

является аксиомой, то для доказательства (27) достаточно доказать

$$((x+1)+y)=((x+y)+1)\quad (x+(y+1))=((x+y)+1)\vdash \\ ((x+1)+y)=(x+(y+1)). \tag{29}$$

Секвенция (29) доказуема (теорема 3.21).

Для доказательства (28) достаточно доказать

$$\vdash ((x+1)+(y+1))=(((x+1)+y)+1), \tag{30}$$

$$((x+1)+y)=(x+(y+1)) \\ ((x+1)+(y+1))=(((x+1)+y)+1)\vdash \\ ((x+1)+(y+1))=((x+(y+1))+1). \tag{31}$$

(30) доказуема по теореме 5.13, а (31) доказуема по теореме 3.21.

Доказательства 2)—7) проводятся аналогично и предоставляются читателю. ∎

5.6 Представимые в формальной арифметике функции

Зафиксируем переменные x_0, x_1, x_2, ... Вместо

$$(\Phi)^{x_0,x_1,\ldots,x_n}_{t_0,t_1,\ldots,t_n}$$

будем писать

$$\Phi(t_0,t_1,\ldots,t_n).$$

Определение 5.6.1 (нумералов). *0 есть 0. Если $\overline{n}$ определено, то $\overline{(n+1)}$ есть $(\overline{n}+1)$.*

Определение 5.6.2. *Арифметическая функция $f : \omega^n \to \omega$ называется представимой в ФА формулой Φ, если:*

а) для каждых таких натуральных

$$m, m_1, \ldots, m_n,$$

что

$$f(m_1, \ldots, m_n) = m,$$

в ФА доказуема секвенция

$$\vdash \Phi(\overline{m}, \overline{m_1}, \ldots, \overline{m_n});$$

б) в ФА доказуема секвенция

$$\Phi(x_{n+1}) \quad \Phi(x_{n+2}) \vdash x_{n+1} = x_{n+2};$$

в) переменные x_0, $x_1, \ldots, x_n$ не встречаются в Φ связанно; переменные x_{n+1}, $x_{n+2}, \ldots$ не встречаются в Φ свободно.

Целью этого параграфа является доказательство теоремы о том, что всякая рекурсивная функция представима в ФА.

По теореме 4.38, достаточно доказать, что простейшие функции представимы в ФА, а суперпозиции, примитивные рекурсии и дающие всюду определенные функции минимизации не выводят из класса представимых в ФА функций.

Лемма 5.16. *Формула $x_0 = 0$ представляет в ФА функцию одного аргумента, равную нулю при любом значении своего аргумента (эта функция в главе 4 обозначалась через θ).*

Доказательство. Очевидно. ∎

Лемма 5.17. *Формула $x_0 = (x_1 + 1)$ представляет в ФА функцию $'$.*

Доказательство. Очевидно. ∎

Лемма 5.18. *Формула $x_0 = x_j$ представляет в ФА функцию η^i_j.*

Доказательство. Очевидно. ∎

Лемма 5.19. *Пусть переменные*

$$y_1, \ldots, y_s$$

попарно различны, не встречаются в формулах

$$\Phi_0, \Phi_1, \ldots, \Phi_s$$

и отличны от $x_0, x_1, \ldots$.

Если формулы

$$\Phi_0, \Phi_1, \ldots, \Phi_s$$

представляют в ФА всюду определенные функции

$$\phi_0, \phi_1, \ldots, \phi_s,$$

то формула Ψ, *равная*

$$(\exists y_1) \ldots (\exists y_s)((\ldots(\Phi_1(y_1) \& \ldots) \& \Phi_s(y_s)) \& \Phi_0(x_0, y_1, \ldots, y_s)),$$

представляет в ФА

$$[\phi_0; \phi_1, \ldots, \phi_s].$$

Доказательство. а). Пусть

$$\phi_i(m_1, \ldots, m_n) = a_i,$$

$$\phi_0(a_1, \ldots, a_s) = b.$$

Тогда

$$[\phi_0; \phi_1, \ldots, \phi_s](m_1, \ldots, m_n) = b.$$

В этом случае секвенции

$$\vdash \Phi_i(\overline{a_i}, \overline{m_1}, \ldots, \overline{m_n}),$$

$$\vdash \Phi_0(\overline{b}, \overline{a_1}, \ldots, \overline{a_s})$$

доказуемы. Поэтому доказуема секвенция

$$\vdash ((\ldots(\Phi_1(\overline{a_1}, \overline{m_1}, \ldots, \overline{m_n}) \& \ldots) \& \Phi_s(\overline{a_s}, \overline{m_1}, \ldots, \overline{m_n})) \& \Phi_0(\overline{b}, \overline{a_1}, \ldots, \overline{a_s})).$$

По правилу $\vdash \exists$, доказуема и секвенция

$$\vdash \Psi(\overline{b}, \overline{m_1}, \ldots, \overline{m_n}).$$

б). Для доказательства

$$\Psi(x_{n+1}) \quad \Psi(x_{n+2}) \vdash x_{n+1} = x_{n+2},$$

по лемме 3.26, достаточно выбрать не встречающиеся в

$$\Phi_0, \Phi_1, \ldots, \Phi_s$$

попарно различные переменные $z_1, \ldots, z_s$, отличные от

$$y_1, \ldots, y_s, x_0, \ldots, x_{n+2},$$

и доказать секвенцию

$$\begin{aligned}&\Psi(x_{n+1})\\ &\quad (\exists z_1)\ldots(\exists z_s)((\ldots(\Phi_1(z_1)\&\ldots)\&\Phi_s(z_s))\&\Phi_0(x_{n+2}, z_1, \ldots, z_s)) \vdash\\ &\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad x_{n+1} = x_{n+2}.\end{aligned}$$

Для этого достаточно доказать

$$\begin{aligned}&\Phi_1(z_1) \quad \Phi_1(y_1)\ldots\Phi_s(z_s) \quad \Phi_s(y_s)\\ &\qquad\qquad \Phi_0(x_{n+1}, y_1, \ldots, y_s) \quad \Phi_0(x_{n+2}, z_1, \ldots, z_s) \vdash x_{n+1} = x_{n+2}.\end{aligned}$$

Для этого достаточно доказать

$$\begin{aligned}&y_1 = z_1 \ldots y_s = z_s\\ &\qquad\qquad \Phi_0(x_{n+1}, y_1, \ldots, y_s) \quad \Phi_0(x_{n+2}, z_1, \ldots, z_s) \vdash x_{n+1} = x_{n+2}.\end{aligned}$$

Для этого достаточно доказать секвенцию

$$\Phi_0(x_{n+1}, z_1, \ldots, z_s) \quad \Phi_0(x_{n+2}, z_1, \ldots, z_s) \vdash x_{n+1} = x_{n+2},$$

доказуемость которой следует из б) определения 5.6.2 для Φ_0. ■

Лемма 5.20. *Пусть u, y, z — попарно различные переменные, отличные от $x_0, x_1 \ldots, x_n$ и не входящие в Φ. Если формула Φ представляет в ФА всюду определенную функцию ϕ от $n+1$ аргумента, то формула Ψ, равная*

$$\begin{aligned}&(\exists y)((\Phi(0, x_1, \ldots, x_n, y)\&\\ &\qquad (\forall z)((\exists u)(z + (u+1)) = y \to \neg\Phi(0, x_1, \ldots, x_n, z)))\&\\ &\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad x_0 = y),\end{aligned}$$

представляет минимизацию функции ϕ.

Доказательство. а). Пусть

$$\phi(a_1, \dots, a_n, 0) \neq 0, \dots, \phi(a_1, \dots, a_n, i-1) \neq 0,$$
$$\phi(a_1, \dots, a_n, i) = 0.$$

Тогда доказуемы секвенции

$$\vdash \neg\Phi(0, \overline{a_1}, \dots, \overline{a_n}, \overline{j})$$

для $j = 0, 1, \dots, i-1$.

В самом деле, пусть

$$\phi(a_1, \dots, a_n, j) = b.$$

Тогда доказуема

$$\vdash \Phi(\overline{b}, \overline{a_1}, \dots, \overline{a_n}, \overline{j}).$$

Поэтому доказуема секвенция

$$\Phi(\overline{0}, \overline{\mathrm{a}_1}, \dots, \overline{\mathrm{a}_n}, \overline{j}) \vdash \overline{0} = \overline{b}.$$

Однако $\overline{b}$ есть $(\overline{(b-1)} + 1)$. По теореме 5.13, доказуема секвенция

$$\vdash \neg\overline{0} = \overline{b}.$$

Покажем теперь, что доказуема секвенция

$$(\exists u)(z + (u+1)) = \overline{i} \vdash (\dots(z = 0 \vee \dots) \vee z = \overline{i-1}) \qquad (32)$$

для $i > 0$ и доказуема секвенция

$$\vdash \neg(\exists u)(z + (u+1)) = 0.$$

Сначала докажем последнюю секвенцию. По лемме 3.27.а), достаточно доказать секвенцию

$$\vdash (\forall u)\neg(z + (u+1)) = 0,$$

а, значит, секвенцию

$$\vdash \neg(z + (u+1)) = 0$$

(правило $\vdash \forall$). Доказуемость последней секвенции следует из того, что

$$\vdash (z + (u+1)) = ((z+u) + 1)$$

является аксиомой, а секвенция

$$\vdash \neg((z+u)+1)=0$$

доказуема.

Для $i>0$ докажем секвенцию

$$(\exists u)(z+(u+1))=\bar{i} \vdash ((\exists v)(z+(v+1))=\overline{i-1} \vee z=\overline{i-1}). \tag{33}$$

Из доказуемости этой секвенции доказуемость секвенции (32) следует содержательной индукцией по i.

Для доказательства секвенции (33) предварительно докажем

$$\neg u=0 \vdash (\exists w)u=(w+1). \tag{34}$$

Из доказуемости (34) доказуемость (33) легко следует. Действительно, надо доказать

$$(z+(u+1))=(\overline{i-1})+1 \vdash ((\exists v)(z+(v+1))=\overline{i-1} \vee z=\overline{i-1}).$$

Так как

$$(z+(u+1))=\overline{i-1}+1 \vdash (z+u)=\overline{i-1}$$

доказуема, а

$$(z+u)=\overline{i-1}\ \ u=0 \vdash z=\overline{i-1}$$

тоже доказуема, то достаточно доказать секвенцию

$$z+u=\overline{i-1}\ \ u=(w+1) \vdash z+(w+1)=\overline{i-1},$$

которая доказуема по теореме 3.23.

Секвенцию (34) доказываем формальной индукцией по u, заменяя ее на секвенцию

$$\vdash (\neg u=0 \to (\exists w)u=(w+1)).$$

Так как

$$\vdash 0=0$$

доказуема, то секвенция

$$\vdash (\neg 0=0 \to (\exists w)0=(w+1))$$

тоже доказуема. Осталось доказать секвенцию

$$(\neg u=0 \to (\exists w)u=(w+1)) \vdash (\neg(u+1)=0 \to (\exists w)(u+1)=(w+1)).$$

Для этого достаточно доказать секвенцию

$$\vdash (\exists w)(u+1) = (w+1),$$

которая получается из доказательства секвенции

$$\vdash (w+1) = (w+1)$$

по правилу $\vdash \exists$.

Итак, секвенции (32) доказаны для всех $i > 0$.

Докажем теперь

$$\vdash \Psi(\overline{i}, \overline{a_1}, \ldots, \overline{a_n}).$$

Достаточно доказать секвенции

$$\vdash \Phi(0, \overline{a_1}, \ldots, \overline{a_n}, \overline{i}),$$

$$(\exists u)(z + (u+1)) = \overline{i} \vdash \neg\Phi(0, \overline{a_1}, \ldots, \overline{a_n}, z).$$

Первая секвенция доказуема по условию. В случае, когда $i = 0$, рассуждение очевидно. Пусть $i > 0$. Используя доказуемость (32) и применяя $i-2$ раза правило удаления дизъюнкции, сведем дело к доказательству секвенций

$$z = \overline{j} \vdash \neg\Phi(0, \overline{a_1}, \ldots, \overline{a_n}, z)$$

для $j = 0, \ldots, i-1$. Но уже было замечено, что секвенции

$$\vdash \neg\Phi(0, \overline{a_1}, \ldots, \overline{a_n}, \overline{j})$$

доказуемы.

а) доказано.

б). Надо доказать

$$\Psi(x_{n+1}) \quad \Psi(x_{n+2}) \vdash x_{n+1} = x_{n+2}.$$

Сначала докажем секвенцию

$$\vdash (((\exists u)(x + (u+1)) = y \vee (\exists u)(y + (u+1)) = x) \vee x = y). \qquad (35)$$

Эту секвенцию будем доказывать формальной индукцией по x.

Секвенцию

$$\vdash (((\exists u)(0 + (u+1)) = y \vee (\exists u)(y + (u+1)) = 0) \vee 0 = y) \qquad (36)$$

будем доказывать формальной индукцией по y.

Секвенция

$$\vdash (((\exists u)(0 + (u + 1)) = 0 \vee (\exists u)(0 + (u + 1)) = 0) \vee 0 = 0)$$

доказуема.

Секвенция

$$(((\exists u)(0 + (u + 1)) = y \vee (\exists u)(y + (u + 1)) = 0) \vee 0 = y) \vdash$$
$$(((\exists u)(0 + (u + 1)) = (y + 1) \vee (\exists u)((y + 1) + (u + 1)) = 0) \vee 0 = (y + 1))$$

доказывается с помощью правил удаления дизъюнкции. Доказательство сводится к доказательству трех секвенций. Для доказательства первой надо доказать

$$(u + 1) = y \vdash ((u + 1) + 1) = (y + 1),$$

для доказательства второй надо доказать

$$\vdash \neg(\exists u)(y + (u + 1)) = 0,$$

для доказательства третей надо доказать

$$0 = y \vdash (0 + (0 + 1)) = (y + 1).$$

Итак, (36) доказана.

Секвенцию

$$(((\exists u)(x + (u + 1)) = y \vee (\exists u)(y + (u + 1)) = x) \vee x = y) \vdash$$
$$(((\exists u)((x + 1) + (u + 1)) = y \vee (\exists u)(y + (u + 1)) = (x + 1)) \vee (x + 1) = y)$$

будем доказывать с использованием правил удаления дизъюнкции. Доказательство сведется к доказательству трех секвенций. Доказательство второй и третьей достаточно очевидно. Докажем первую секвенцию. Достаточно доказать

$$(\exists u)(x + (u + 1)) = y \vdash ((\exists u)((x + 1) + (u + 1)) = y \vee (x + 1) = y).$$

Используя (34), сведем дело к доказательству секвенций

$$(x + (u + 1)) = y \quad u = 0 \vdash (x + 1) = y,$$

$$(x + (u + 1)) = y \quad u = w + 1 \vdash ((x + 1) + (w + 1)) = y,$$

доказательство которых легко получается с использованием теоремы 3.23. Итак (35) доказана.

В (35) вместо x подставляем x_{n+1}, а вместо y подставляем x_{n+2}. Для доказательства

$$\Psi(x_{n+1}) \quad \Psi(x_{n+2}) \vdash x_{n+1} = x_{n+2},$$

используя (35), достаточно доказать

$$\Psi(x_{n+1}) \quad \Psi(x_{n+2}) \quad (\exists u)(x_{n+1} + (u+1)) = x_{n+2} \vdash x_{n+1} = x_{n+2}. \tag{37}$$

Для доказательства (37) достаточно доказать

$$\begin{gathered}\Phi(0, x_1, \ldots, x_n, x_{n+1}) \quad \Phi(0, x_1, \ldots, x_n, x_{n+2}) \quad (x_{n+1} + (u+1)) = x_{n+2} \\ ((\exists u)(x_{n+1} + (u+1)) = x_{n+2} \to \neg\Phi(0, x_1, \ldots, x_n, x_{n+1})) \vdash \\ x_{n+1} = x_{n+2}.\end{gathered}$$

Доказательство последней секвенции очевидно.

б) доказано. ■

Напомним, что $\mathrm{rest}(x, y)$ обозначает остаток от деления x на y. Обозначим через γ следующую трехместную арифметическую функцию:

$\gamma(a, b, c) = \mathrm{rest}(a, (1 + ((c+1) * b)))$ для любых натуральных a, b, c.

Ясно, что γ — рекурсивная функция. Эта функция называется функцией Гёделя.

Лемма 5.21. *Функция γ представляется в ФА формулой*

$$\begin{aligned}(\exists y)(\exists z)(x_1 = (((1 + ((x_3 + 1) * x_2)) * y) + x_0) \& \\ (x_0 + (z+1)) = (1 + ((x_3 + 1) * x_2))).\end{aligned}$$

Доказательство. а). Пусть $\gamma(a, b, c) = i$. Тогда для подходящего d

$$a = (((1 + ((c+1) * b)) * d) + i),$$

где $i < (1 + ((c+1) * b))$. Поэтому существует натуральное e такое, что

$$(i + (e+1)) = (1 + ((c+1) * b)).$$

Достаточно доказать секвенции

$$\vdash \overline{a} = (((\overline{1} + ((\overline{c} + \overline{1}) * \overline{b})) * \overline{d}) + \overline{i}), \tag{38}$$

$$\vdash (\bar{i} + (\bar{e} + \bar{1})) = (\bar{1} + ((\bar{c} + \bar{1}) * \bar{b})). \tag{39}$$

Секвенции (38) и (39) будут доказаны, если для любых натуральных m и n будут доказаны секвенции

$$\vdash \overline{m+n} = (\overline{m} + \overline{n}), \tag{40}$$

$$\vdash \overline{m*n} = (\overline{m} * \overline{n}). \tag{41}$$

(40) доказываем содержательной индукцией по n. При $n = 0$ секвенция (40) доказуема (теоремы 3.23 и 5.13). Пусть

$$\vdash \overline{m+n} = (\overline{m} + \overline{n})$$

доказуема. Секвенция

$$\vdash (\overline{m} + \overline{n+1}) = ((\overline{m} + \overline{n}) + 1)$$

доказуема по теореме 5.13, так как, по определению, $(\overline{n} + 1)$ есть $\overline{n+1}$. Теперь доказуема секвенция

$$\vdash (\overline{m} + \overline{n+1}) = (\overline{m+n} + 1).$$

Однако $(\overline{m+n} + 1)$ есть $\overline{m+n+1}$.

(41) доказываем содержательной индукцией по n. При $n = 0$ секвенция (41) доказуема (теоремы 3.23 и 5.13). Пусть

$$\vdash \overline{m*n} = (\overline{m} * \overline{n})$$

доказуема. Секвенция

$$\vdash (\overline{m} * \overline{n+1}) = ((\overline{m} * \overline{n}) + \overline{m})$$

доказуема по теореме 5.13. Теперь доказуема секвенция

$$\vdash (\overline{m} * \overline{n+1}) = (\overline{m*n} + \overline{m}).$$

Однако, по 40, $(\overline{m*n} + \overline{m})$ есть $\overline{m*(n+1)}$.

Итак, а) доказано.

б). Достаточно доказать секвенцию

$$x_1 = (((1+((x_3+1)*x_2))*y_1)+x_4) \;\; x_1 = (((1+((x_3+1)*x_2))*y_2)+x_5)$$
$$(x_4 + (z_1 + 1)) = (1 + ((x_3 + 1) * x_2))$$
$$(x_5 + (z_2 + 1)) = (1 + ((x_3 + 1) * x_2)) \vdash x_4 = x_5.$$

Эта секвенция будет доказана, если будет доказана секвенция

$$x_1 = ((u_1 * y_1) + x_4) \;\; x_1 = ((u_1 * y_2) + x_5)$$
$$(x_4 + (z_1 + 1)) = u_1 \;\; (x_5 + (z_2 + 1)) = u_1 \vdash x_4 = x_5$$

(теорема 3.21). Используя (35), достаточно доказать секвенцию

$$x_1 = ((u_1 * y_1) + x_4) \;\; x_1 = ((u_1 * y_2) + x_5)$$
$$(x_4 + (z_1 + 1)) = u_1 \;\; (x_5 + (z_2 + 1)) = u_1$$
$$(x_4 + (z + 1)) = x_5 \vdash x_4 = x_5.$$

Доказательство этой секвенции сводится к доказательству трех секвенций, если использовать (35).

Секвенция

$$x_1 = ((u_1 * y_1) + x_4) \;\; x_1 = ((u_1 * y_1) + x_5) \vdash x_4 = x_5$$

легко доказывается с использованием теоремы 5.15.7).

Доказательство секвенции

$$x_1 = ((u_1 * y_1) + x_4) \;\; x_1 = ((u_1 * (y_1 + (z_3 + 1))) + x_5)$$
$$(x_4 + (z_1 + 1)) = u_1 \;\; (x_5 + (z_2 + 1)) = u_1$$
$$(x_4 + (z + 1)) = x_5 \vdash x_4 = x_5$$

сводится к доказательству секвенции

$$x_1 = ((u_1 * y_1) + x_4)$$
$$x_1 = ((u_1 * (y_1 + (z_3 + 1))) + (x_4 + (z + 1))) \vdash x_4 = x_5,$$

доказательство которой, по теореме 5.15, сводится к доказательству секвенции

$$0 = (((u_1 * (z_3 + 1)) + z) + 1) \vdash x_4 = x_5,$$

доказательство которой легко получается с использованием теоремы 5.13.1). Остается доказать секвенцию

$$x_1 = ((u_1 * (y_2 + (z_3 + 1))) + x_4)$$
$$x_1 = ((u_1 * y_2) + (x_4 + (z + 1)))$$
$$((x_4 + (z + 1)) + (z_2 + 1)) = u_1 \vdash x_4 = x_5,$$

доказательство которой, опять по теореме 5.15, сводится к доказательству секвенции

$$u_1 * (z_3 + 1) = (z + 1) \ \ ((x_4 + (z + 1)) + (z_2 + 1)) = u_1 \vdash x_4 = x_5.$$

Для доказательства последней секвенции достаточно доказать

$$0 = (((x_4 + (z_2 + 1)) * (z_3 + 1)) + ((z + 1) * z_3)) \vdash x_4 = x_5$$

или, по теореме 5.15,

$$0 = (((((x_4 + (z_2 + 1)) * z_3) + (x_4 + z_2)) + ((z + 1) * z_3)) + 1) \vdash x_4 = x_5,$$

что легко получается с использованием теоремы 5.13.1). ∎

Лемма 5.22. *Для любых натуральных $d_0, \ldots, d_m$ найдутся такие натуральные a, b, что $\gamma(a, b, i) = d_i$ для $i = 0, 1, \ldots, m$.*

Доказательство. В качестве b возьмем

$$(1 + m + d_0 + \cdots + d_m)!$$

(напомним, что $l! = 1 * 2 * \cdots * l$). Пусть

$$n_i = (1 + ((i + 1) * b)).$$

Заметим, что числа n_i и n_j взаимно простые при $i \neq j; i, j = 0, \ldots, m$.
Действительно, если $i > j$ и простое q делит n_i и n_j, то q делит $(i - j) * b$ и, значит, делит b (так как $i - j$ делит b). Но тогда q делит 1.
Пусть

$$M = n_0 * n_1 * \cdots * n_m$$

и $M_i = M/n_i$. Ясно, что числа M_i и n_i взаимно простые. Поэтому найдутся такие натуральные u_i и v_i, что

$$M_i u_i - n_i v_i = 1.$$

Пусть

$$a = d_0 u_0 M_0 + \cdots + d_m u_m M_m.$$

Найдем $\mathrm{rest}(a, n_i)$. Имеем

$$\mathrm{rest}(a, n_i) = \mathrm{rest}(d_i u_i M_i, n_i) = d_i.$$

∎

Лемма 5.23. *Пусть формула* Γ *представляет* γ, *а формулы* Φ *и* Ψ *представляют рекурсивные функции* ϕ *местности* n *и* ψ *местности* $n+2$ *в ФА. Тогда формула* Υ, *равная*

$$(\exists y)(\exists z)(((\exists w)(\Gamma(w,y,z,0)\&\Phi(w))\&\Gamma(x_0,y,z,x_{n+1}))\&$$
$$(\forall w)((\exists u)(w+(u+1))=x_{n+1}\to(\exists v_1)(\exists v_2)((\Gamma(v_1,y,z,w)\&$$
$$\Gamma(v_2,y,z,w+1))\&\Psi(v_2,x_1,\ldots,x_n,w,v_1)))),$$

представляет $R(\phi,\psi)$ *в ФА.*

Доказательство. а). Пусть

$$R(\phi,\psi)(a_1,\ldots,a_n,b)=d_b,$$

$$R(\phi,\psi)(a_1,\ldots,a_n,0)=d_0,\ldots,R(\phi,\psi)(a_1,\ldots,a_n,b-1)=d_{b-1}.$$

Выберем такие c_1 и c_2, что

$$\gamma(c_1,c_2,i)=d_i$$

для $i=0,\ldots,b$. Тогда доказуемы секвенции

$$\vdash\Gamma(\overline{d_i},\overline{c_1},\overline{c_2},\overline{i})$$

для $i=0,\ldots,b$ и секвенции

$$\vdash\Phi(\overline{d_0},\overline{a_1},\ldots,\overline{a_n}),$$

$$\vdash\Psi(\overline{d_{i+1}},\overline{a_1},\ldots,\overline{a_n},\overline{i},\overline{d_i})$$

для $i=0,\ldots,b-1$. Так как, по (32),

$$(\exists u)(w+(u+1))=b\vdash(\ldots(w=0\vee\ldots)\vee w=b-1)$$

доказуема, то

$$\vdash\Upsilon(\overline{d_b},\overline{a_1},\ldots,\overline{a_n},\overline{b})$$

доказуема.

б). Надо доказать секвенцию

$$\Upsilon(x_{n+2})\quad\Upsilon(x_{n+3})\vdash x_{n+2}=x_{n+3}.$$

Выберем Υ' так, что Υ есть

$$(\exists y)(\exists z)\Upsilon'.$$

Достаточно доказать секвенцию

$$\Upsilon'(x_{n+2}) \;\; \Upsilon''(x_{n+3}) \vdash x_{n+2} = x_{n+3},$$

где Υ'' есть $(\Upsilon')^{y,z}_{y_1,z_1}$.

Формальной индукцией по i докажем секвенцию

$$\begin{aligned}&\Upsilon'(x_{n+2}) \;\; \Upsilon''(x_{n+3}) \vdash \\ &\quad((\exists u)(i + (u + 1)) = x_{n+1} \to (\exists w)(\Gamma(w, y, z, i)\&\Gamma(w, y_1, z_1, i))). \quad (42)\end{aligned}$$

Заменяя в правой части этой секвенции i на 0, сведем дело к доказательству секвенции

$$\Gamma(w, y, z, 0) \;\; \Phi(w) \;\; \Gamma(w_1, y_1, z_1, 0) \;\; \Phi(w_1) \vdash \Gamma(w, y_1, z_1, 0),$$

которая легко доказывается с использованием теоремы 3.23 и доказуемости секвенции

$$\Phi(w_1) \;\; \Phi(w_2) \vdash w_1 = w_2.$$

Обозначим правую часть секвенции (42) через Δ. Осталось доказать секвенцию

$$\Upsilon'(x_{n+2}) \;\; \Upsilon''(x_{n+3}) \;\; \Delta \vdash (\Delta)^i_{i+1}.$$

Используя правило $\forall\vdash$, сведем дело к доказательству секвенции

$$\begin{aligned}&\Gamma(w, y, z, i) \;\; \Gamma(w, y_1, z_1, i) \;\; \Gamma(w_1, y, z, i) \;\; \Gamma(w_2, y, z, i + 1) \\ &\qquad \Psi(w_2, x_1, \ldots, x_n, i, w_1) \;\; \Gamma(v_1, y_1, z_1, i) \;\; \Gamma(v_2, y_1, z_1, i + 1) \\ &\qquad\qquad\qquad \Psi(v_2, x_1, \ldots, x_n, i, v_1) \vdash v_2 = w_2,\end{aligned}$$

которое легко получается из определения Γ и Ψ.

Итак, (42) доказана. Доказательство нужной секвенции сводится к доказательству двух секвенций.

Секвенция

$$\Upsilon'(x_{n+2}) \;\; \Upsilon''(x_{n+3}) \;\; x_{n+1} = 0 \vdash x_{n+2} = x_{n+3}$$

сразу доказывается, так как доказуемы

$$\Upsilon'(x_{n+2}) \;\; x_{n+1} = 0 \vdash \Phi(x_{n+2}),$$

$$\Upsilon''(x_{n+3}) \;\; x_{n+1} = 0 \vdash \Phi(x_{n+3}),$$

$$\Phi(x_{n+2}) \;\; \Phi(x_{n+3}) \vdash x_{n+2} = x_{n+3}.$$

Для доказательства

$$\Upsilon'(x_{n+2}) \;\; \Upsilon''(x_{n+3}) \;\; \neg x_{n+1} = 0 \vdash x_{n+2} = x_{n+3}$$

используем (34) и (42) и доказываем последовательно секвенции

$$\Upsilon'(x_{n+2}) \;\; \Upsilon''(x_{n+3}) \;\; (w + (0+1)) = x_{n+1} \vdash \\ (\exists w_1)(\Gamma(w_1, y, z, w) \& \Gamma(w_1, y_1, z_1, w)),$$

$$\Upsilon'(x_{n+2}) \;\; \Upsilon''(x_{n+3}) \;\; (w+(0+1)) = x_{n+1} \;\; \Gamma(w_1, y, z, w) \;\; \Gamma(w_1, y_1, z_1, w) \vdash \\ (((\Gamma(x_{n+2}, y, z, x_{n+1}) \& \Gamma(x_{n+3}, y_1, z_1, x_{n+1})) \& \\ \Psi(x_{n+2}, x_1, \ldots, x_n, w, w_1)) \& \Psi(x_{n+3}, x_1, \ldots, x_n, w, w_1)).$$

∎

Как уже отмечалось, из доказанных лемм следует

Теорема 5.24. *Каждая рекурсивная функция представима в ФА.*

5.7 Неполнота формальной арифметики

Определение 5.7.1. *Скажем, что ФА непротиворечива, если секвенции* $\vdash \Phi$ *и* $\vdash \neg\Phi$ *не доказуемы одновременно в ФА ни для какой формулы* Φ.

Предположение 1. *Рассмотрим теперь такую нумерацию формул сигнатуры* Ω_1, *что каждое число является номером некоторой формулы, каждая формула имеет только один номер, разные формулы имеют разные номера, и существует такая двухместная рекурсивная функция* D, *что* $D(m, n)$ *есть номер формулы*

$$(\Phi)^{x_1, x_2}_{\overline{m}, \overline{m}},$$

если n *является номером формулы* Φ.

Как обычно, формула Φ называется доказуемой в ФА, если секвенция $\vdash \Phi$ доказуема в ФА.

Определение 5.7.2. *Скажем, что ФА разрешима, если существует алгоритм, который по натуральному* n *определяет, доказуема ли формула номера* n *в ФА.*

Теорема 5.25. *Если ФА непротиворечива, то ФА неразрешима.*

Доказательство. От противного. Пусть такой алгоритм существует. Тогда рекурсивна следующая функция ϕ :

$$\phi(m) = \begin{cases} 1, & \text{если } m \text{ является номером доказуемой в ФА формулы,} \\ 0 & \text{в остальных случаях.} \end{cases}$$

Пусть функция ϕ представляется в ФА формулой Φ. Тогда $\Phi(\overline{1}, \overline{n})$ доказуема в ФА, если n — номер доказуемой в ФА формулы, $\Phi(0, \overline{n})$ доказуема в ФА в остальных случаях.

Заметим,что $\neg\Phi(\overline{1}, \overline{n})$ доказуема в ФА, если n не является номером доказуемой в ФА формулы.

Действительно, в этом случае доказуемы секвенции

$$\neg\neg\Phi(\overline{1}, \overline{n}) \vdash \Phi(0, \overline{n}),$$

$$\neg\neg\Phi(\overline{1}, \overline{n}) \vdash (\Phi(0, \overline{n}) \to \overline{1} = 0).$$

Значит, доказуема секвенция

$$\neg\neg\Phi(\overline{1}, \overline{n}) \vdash \overline{1} = 0.$$

Так как секвенция

$$\vdash \neg\overline{1} = 0$$

тоже доказуема, то доказуема секвенция

$$\vdash \neg\Phi(\overline{1}, \overline{n}).$$

Пусть формула Δ представляет в ФА функцию D. Рассмотрим следующую формулу Ψ:

$$(\forall x_0)(\Delta \to \neg\Phi(\overline{1}, x_0)).$$

Пусть эта формула имеет номер m. Рассмотрим формулу

$$\Psi(x_0, \overline{m}, \overline{m}).$$

Пусть эта формула имеет номер k. Тогда доказуема $\vdash \Delta(\overline{k}, \overline{m}, \overline{m})$.

Если формула $\Psi(x_0, \overline{m}, \overline{m})$ доказуема в ФА, то, кроме того, доказуема $\vdash \Phi(\overline{1}, \overline{k})$. Значит, доказуемы секвенции

$$\vdash (\Delta(\overline{k}, \overline{m}, \overline{m}) \to \neg\Phi(\overline{1}, \overline{k})),$$

$$\vdash \neg\Phi(\overline{1}, \overline{k})).$$

Это противоречит непротиворечивости ФА.

Итак,

$$\Psi(x_0, \overline{m}, \overline{m})$$

не доказуема в ФА. Поэтому

$$\vdash \neg\Phi(\overline{1}, \overline{k})$$

доказуема в ФА.

Но тогда секвенции

$$\vdash (\Delta(\overline{k}, \overline{m}, \overline{m}) \to \neg\Phi(\overline{1}, \overline{k})),$$

$$\vdash (\Delta(x_0, \overline{m}, \overline{m}) \to \neg\Phi(\overline{1}, x_0))$$

доказуемы в ФА. Для доказательства последней секвенции достаточно доказать секвенции

$$x_0 = \overline{k} \vdash (\Delta(x_0, \overline{m}, \overline{m}) \to \neg\Phi(\overline{1}, x_0)),$$

$$\neg x_0 = \overline{k} \vdash (\Delta(x_0, \overline{m}, \overline{m}) \to \neg\Phi(\overline{1}, x_0)).$$

Первая из них доказывается очевидным образом, а вторая доказывается с использованием доказуемой секвенции

$$\neg x_0 = \overline{k} \vdash \neg\Delta(x_0, \overline{m}, \overline{m}).$$

Получается, что

$$\Psi(x_0, \overline{m}, \overline{m})$$

доказуема в ФА, а это противоречит условию. ■

Распространим рассматриваемую нумерацию формул на нумерацию секвенций.

Предположение 2. *Будем теперь предполагать, что существуют такие рекурсивные функции D_1, J, μ и Θ_j для $j = 1, \ldots, 15$, что $D_1(n)$ задает номер формулы $\neg\Phi$, если n является номером формулы Φ, и выполняются следующие условия:*

а) $J(n, 0)$ задает число формул в левой части секвенции номера n;

$J(n, i)$ для $0 < i \leq J(n, 0)$ задает номер i-той формулы в левой части секвенции номера n;

$J(n, J(n, 0) + 1)$ задает номер формулы в правой части секвенции номера n;

б) $\mu(n) = 1$, если n — номер аксиомы ФА; $\mu(n) = 0$, если n не является номером аксиомы из ФА;

в) если j-тая схема правил вывода имеет одну посылку и секвенция номера m получается из секвенции номера n по этой схеме, то $m = \Theta_j(n)$, если же из секвенции номера n нельзя получить никакой секвенции по этой схеме, то $\Theta_j(n) = n$;

если j-тая схема правил вывода имеет две посылки и секвенция номера m получается из секвенций номеров n_1 и n_2 по этой схеме, то $m = \Theta_j(n_1, n_2)$, если же из секвенций номеров n_1 и n_2 нельзя получить никакой секвенции по этой схеме, то $\Theta_j(n_1, n_2) = n_1$;

если секвенция номера m получается из секвенций номеров n_1, n_2, n_3 по правилу удаления дизъюнкции, то $m = \Theta_6(n_1, n_2, n_3)$, если же из секвенций номеров n_1, n_2, n_3 нельзя получить никакой секвенции по правилу удаления дизъюнкции, то $\Theta_6(n_1, n_2, n_3) = n_1$.

Определение 5.7.3. *ФА полна, если для каждой замкнутой формулы Φ сигнатуры Ω_1 хотя бы одна из формул Φ и $\neg\Phi$ доказуема в ФА.*

Теорема 5.26. *Если ФА непротиворечива, то ФА неполна.*

Доказательство. Заметим сначала, что существует такая рекурсивная функция ϕ, что для любого натурального i число $\phi(i)$ есть номер теоремы ФА и для каждого номера m теоремы ФА найдется такое i, что $m = \phi(i)$. Другими словами,

$$\{\phi(0), \phi(1), \dots\}$$

содержит все номера теорем ФА и только номера теорем. Менее формально, существует алгоритм, перечисляющий все теоремы ФА.

Заметим, что m является номером теоремы ФА тогда и только тогда, когда существует такая последовательность $m_0, m_1, ..., m_s$, что m_i есть либо номер аксиомы ФА и, значит, $\mu(m_i) = 1$, либо

$$m_i = \Theta_j(m_k)$$

для $k < i$ и

$$j \in \{2, 3, 4, 5, 7, 10, 11, 12, 13, 14, 15\},$$

либо

$$m_i = \Theta_j(m_{k_1}, m_{k_2})$$

для $k_1, k_2 < i$ и $j = \{1, 8, 9\}$, либо

$$m_i = \Theta_j(m_{k_1}, m_{k_2}, m_{k_3})$$

для $j = 6$ и $k_1, k_2, k_3 < i$.

Используя это замечание, можно доказать, что является рекурсивной такая функция ψ_1, что $\psi_1(a, b, s) = 1$, если

$$m_0 = \gamma(a, b, 0), \ldots, m_s = \gamma(a, b, s)$$

является такой последовательностью номеров секвенций, что последовательность самих этих секвенций является доказательством, и

$$\psi_1(a, b, s) = 0$$

в остальных случаях. Напомним, что γ обозначает функцию Гёделя. Доказательство рекурсивности ψ_1 просто, хотя и несколько громоздко, и предоставляется читателю.

Обозначим

$$\gamma(exp(m, 0), exp(m, 1), exp(m, 2))$$

через $\psi_2(m)$,

$$\psi_1(exp(m, 0), exp(m, 1), exp(m, 2))$$

через $\psi_3(m)$ и номер секвенции $0 = 0 \vdash 0 = 0$ через ℓ.

Ясно, что в качестве ϕ можно взять следующую функцию:

$$\phi(m) = \begin{cases} \psi_2(m) & \text{если } \psi_3(m) = 1, \\ \ell & \text{в остальных случаях.} \end{cases}$$

Действительно, все значения ϕ являются номерами доказуемых в ФА секвенций. Обратно, пусть задана такая последовательность номеров секвенций

$$m_0, m_1, ..., m_s,$$

что последовательность этих секвенций является доказательством. Используя лемму 5.22, найдем такие a, b, что
$\gamma(a, b, i) = m_i$ для $i = 0, 1, ..., s$.
Рассмотрим число $m = 2^a * 3^b * 5^s$. Ясно, что $\phi(m) = m_s$.

Условие

$$J(\phi(m), 0) + |n - J(\phi(m), 1)| = 0$$

выполняется тогда и только тогда, когда теорема номера $\phi(m)$ имеет вид $\vdash \Phi$ и n является номером формулы Φ. Пусть

$$\psi_4(n, m) = J(\phi(m), 0) + |n - J(\phi(m), 1)|.$$

Опираясь на эти предварительные замечания, докажем, что если ФА — полна, то она разрешима.

Пусть ФА полна и непротиворечива. Рассмотрим следующую функцию ψ_5:

$$[*; \psi_4, [\psi_4; [D_1; \eta_1^2], \eta_2^2]].$$

Пусть ψ_6 является минимизацией ψ_5. Ясно, что $\psi_6(n)$ — это наименьший из таких m, что теорема номера $\phi(m)$ имеет вид $\vdash \Phi$ или $\vdash \neg\Phi$, где Φ — формула номера n. Если ФА полна, то ψ_6 — рекурсивная функция. Теперь

$$\overline{sg}(|n - J(\phi(\psi_6(n)), 1)|) = 1,$$

если формула номера n доказуема в ФА, и

$$\overline{sg}(|n - J(\phi(\psi_6(n)), 1)|) = 0,$$

если формула номера n не доказуема в ФА.

Менее формально, перебирая теоремы ФА, в случае полноты ФА, найдем первую теорему вида $\vdash \Phi$ или $\vdash \neg\Phi$, где Φ — заданная формула. Если теорема имеет вид $\vdash \Phi$, то Φ доказуема в ФА. Если же она имеет вид $\vdash \neg\Phi$, то Φ не доказуема в ФА.

Это означает, что ФА разрешима. А это противоречит теореме 5.25. ∎

Для завершения надо построить нумерации формул и секвенций, удовлетворящих предположениям 1 и 2.

Упражнения к §§5.1—5.7

Упражнение 5.7.1. *Для машин Тьюринга M, построенных в пунктах 4), 5), 6), 8) доказательства теоремы 4.18, построить полусистемы Туэ $T(M)$.*

Упражнение 5.7.2. *Для машин Тьюринга , построенных в пунктах 4), 5), 6), 8) доказательства теоремы 4.18, построить списки $\Pi(M)$.*

Упражнение 5.7.3. *Пусть ассоциативное исчисление задается алфавитом $\{0,1\}$ и списком правил $(00,0), (11,1), (011,10)$. Построить алгоритм,который по двум словам в этом алфавите определяет, эквивалентны или нет эти слова в этом исчислении.*

Упражнение 5.7.4. *Пусть ассоциативное исчисление задается алфавитом $\{0,1,2\}$ и списком правил*

$$(1, 022), (20, 0222), (111, 1), (000, 0), (22222, 2).$$

Построить алгоритм, который по двум словам в этом алфавите определяет, эквивалентны или нет эти слова в этом исчислении.

Упражнение 5.7.5. *Построить формулы, представляющие в ФА следующие функции:*

а) $3 * (x!)$;

б) $2 + (x!)$;

в) целая часть кубического корня плюс один;

г) целая часть квадратного корня минус три, если это число неотрицательно, или нуль;

д) наибольшее из квадрата первого числа и корня квадратного из второго;

е) наименьшее из двух чисел;

ж) равной $x!$, *если* $x < y$, *и* $y!$ *в остальных случаях;*

з) равной 0, если $x < y$, *и* 1, *если* $x \geq y$;

и) равной $|x - y|$, *если* x *четно, и* $2 * x$ *в остальных случаях;*

к) равной 2, *если* $x > 5$, *и* y *в остальных случаях;*

л) равной разности x *и* y, *если* $x > y$ *и* x *— простое число, нулю, если* $x \leq y$ *и* x *— простое число,* x *в остальных случаях;*

м) целая часть корня седьмой степени из произведения x *и* y;

н) равной x, *если* y *— простое число, и 2 в остальных случаях;*

о) $R(\eta_1^1, [*; \eta_3^3, \eta_1^3])$;

п) $R(\eta_1^1, [+; \eta_3^3, \eta_2^3])$;

р) $R(\eta_1^2, [*; \eta_3^4, \eta_4^4])$.

Упражнение 5.7.6. *Привести формальные доказательства секвенций 2)–7) теоремы 5.15.*

Упражнение 5.7.7. *Построить нумерации формул и секвенций, удовлетворяющих предположениям 1 и 2.*

Предметный указатель