Министерство высшего и среднего специального образования РСФСР
МОСКОВСКИЙ ИНСТИТУТ ЭЛЕКТРОННОГО МАШИНОСТРОЕНИЯ

Ю.И.Манин

ЛЕКЦИИ ПО МАТЕМАТИЧЕСКОЙ ЛОГИКЕ

Часть II

Учебное пособие для студентов
специальности 0647

Рекомендовано Редсветом института
в качестве учебного пособия

Москва - 1974

Содержание

§ I. Введение. Интуитивная вычислимость.

I.I. Мы продолжаем формализованное описание математики. Основным объектом первой части курса было математическое доказательство; было показано, что его подходящим формальным аналогом является понятие вывода в языке, после чего самые интересные результаты утверждали невыводимость содержательных математических утверждений (например, гипотезы континуума).

Основным объектом этой второй части курса будет детерминированный процесс вычисления, или переработки нечисловой информации, короче, алгоритм. Будет построено подходящее формальное описание алгоритмов (точнее, результатов их действий), и самые интересные результаты окажутся утверждениями о несуществовании алгоритмов, вычисляющих содержательно описываемые функции.

Обе теории - доказательства и вычисления - могут довольно длительное время излагаться независимо, и мы предпочли именно такое изложение, хотя оно не соответствует историческому ходу открытий. Когда же техника обеих теорий окажется уже достаточно развитой, можно будет эффективно применять каждую из них для исследования другой.

В этом параграфе мы наметим основные опорные точки теории вычислимости на совершенно неформальном уровне строгости, который можно назвать физическим. Характерной чертой нашего подхода будет аппеляция к интуитивному представлению читателя о том, что такое алгоритм, пользуясь которым очень удобно объяснить структуру основных понятий.

Однако при формализации этих понятий в следующем параграфе мы дадим точное описание не алгоритмов, а результатов их работы, то есть вычислимых функций. С нашей точки зрения, понятие алгоритма слишком много теряет при любой формализации, тогда как понятие алгоритмической вычислимости, насколько мы можем судить, не теряет ничего существенного.

I.2. Введем несколько простых основных понятий. Пусть X, Y – два множества. Частичной функцией (или отображением) из X в Y мы будем называть любую пару $(\mathcal{D}(f), f)$, состоящую из подмножества $\mathcal{D}(f) \subset X$ и отображения $f : \mathcal{D}(f) \to X$. Здесь $\mathcal{D}(f)$ называется областью определения f; f определена в точке $x \in X$, если $x \in \mathcal{D}(f)$; f нигде не определена, если $\mathcal{D}(f)$ пусто.

Через $Z^+ = \{1, 2, 3, \ldots\}$ будем обозначать множество натуральных чисел, исключая нуль. Если $n \geq 1$, через $(Z^+)^n$ мы обозначим n-кратное прямое произведение Z^+ на себя, то есть множество векторов $(x_1, \ldots, x_n)$, $x_i \in Z^+$. Удобно считать, что $(Z^+)^0$ – множество, состоящее из одного элемента. Нашим основным объектом будут частичные функции из $(Z^+)^m$ в $(Z^+)^n$ для различных m, n. В следующей ниже классификации этих функций по степени их вычислимости под словом "программа" читатель может представлять себе программу для универсальной вычислительной машины, написанную без учета ограничений на время и память. Подразумевается, что каждая программа для вычисления функции содержит специальное "пустое место" для ввода очередного значения аргумента.

1*-1978

I.3. Основное определение. а) Частичная функция f из $(Z^+)^m$ в $(Z^+)^n$, $n \neq 0$ называется вычислимой, если существует такая "программа", что при подаче на ее вход вектора $x \in (Z^+)^m$ мы получим на выходе

$$f(x) \quad , \text{если} \quad x \in D(f)$$
$$0 \quad , \text{если} \quad x \notin D(f)$$

(Здесь 0 - просто указатель того, что f не определена в X ; можно было бы разрешить в этом случае получить на выходе что угодно не из $(Z^+)^n$).

б) Частичная функция f из $(Z^+)^m$ в $(Z^+)^n$ называется полувычислимой, если существует такая "программа", что при подаче на ее вход $x \in (Z^+)^m$ мы получаем на выходе $f(x)$, если $x \in D(f)$; получаем на выходе 0 или же программа работает бесконечно долго, если $x \notin D(f)$.

В частности, вычислимые функции полувычислимы, а всюду определенные полувычислимые функции вычислимы.

в) Частичная функция f называется абсолютно невычислимой, если она не удовлетворяет условию б) и тем более а).

I.4. Пояснения. а) Из этих трех понятий основным является полувычислимость, ибо вычислимость сводится к нему. Действительно, для выделения вычислимых функций из полувычислимых можно поступить так.

Пусть $X \subset Y$ два множества. Назовем характеристической функцией подмножества X в Y такую функцию

$\chi_X : Y \to Z^+$, что

$$\chi_X(x) = \begin{cases} 1, \text{ если } & x \in X \\ 2, \text{ если } & x \notin X \end{cases}$$

Заметим, что χ_X определена всюду.

Теперь пусть f - полувычислимая функция из $(Z^+)^m$ в $(Z^+)^n$. Если она даже вычислима, то вычислима и характеристическая функция ее области определения $D(f)$: к вычисляющей f программе нужно добавить инструкции "перерабстать 0 в 2 , а не 0 в 1 и подать на выход". Наоборот, если вычислима $\chi_{D(f)}$, то вычислима и f : перед программой, полувычисляющей f , нужно написать программу, вычисляющую $\chi_{D(f)}$, и подавать на выход сразу 0, если $\chi_{D(f)}(x) = 2$, или передавать x в программу для f , если $\chi_{D(f)}(x) = 1$. Таким образом f вычислима $\Leftrightarrow$ f полувычислима и $\chi_{D(f)}$ полувычислима (и значит, автоматически вычислима, ибо всюду определена).

Правую часть этой импликации мы выберем в качестве формализации понятия вычислимости, когда полувычислимость будет формализована.

б) <u>Существуют абсолютно невычислимые функции</u>. действительно, каждая программа - это конечный текст под конечным алфавитом, так что множество программ счетно, тогда как множество всех функций $Z^+ \to Z^+$ несчетно.

(Критику этого рассуждения см. ниже).

Конкретный пример абсолютно невычислимой функции.

Рассмотрим язык арифметики $L_1 Ar$, списанный в главе I. Представим себе список всех замкнутых формул этого языка, записанных, скажем, в лексикографическом порядке (алфавит предполагается конечным и упорядоченным). Определим функцию f соглашением

$$f(k) = \begin{cases} \text{I, если } k\text{-я формула списка истинна в стандартной интерпретации;} \\ \text{не определена, если } k\text{-я формула ложна.} \end{cases}$$

Функция $f(k)$ абсолютно невычислима (теорема Тарского).

Иначе говоря, нельзя распознать (хотя бы в принципе) все теоретико-числовые теоремы, написав одну (хотя бы очень большую и сложную) программу для их распознавания по данной формулировке.

Доказательство этого результата, конечно, требует гораздо более глубокого анализа понятия вычислимости.

в) Существуют полувычислимые, но не вычислимые функции. Сначала приведем характерный пример полувычисляющей программы. Рассмотрим функцию f из Z^+ в Z^+, определенную через задачу Ферма.

$$\begin{cases} \text{I, если существуют } x, y, z \in Z^+ \\ \quad \text{с условием } x^{n+2} + y^{n+2} = z^{n+2} \\ \text{не определена иначе} \end{cases}$$

Вот программа, полувычисляющая f: после того, как на вход подано n, перебирать вектора (x, y, z) в

лексикографическом порядке и проверять для каждого вектора условие $x^{n+2} + y^{n+2} = z^{n+2}$. Если оно выполнено, подать на вход I. Иначе, переходить к следующему (x, y, z).

Значит, f полувычислима. Но мы до сих пор не знаем, вычислима ли f. Гипотеза Ферма состоит в том, что f нигде не определена (и, значит, вычислима!). Самые сильные теоретические результаты, известные относительно f, – так называемые критерии Куммера, Вифериха, Вандивера и др. – можно рассматривать как некоторое приближение <u>именно к доказательству вычислимости</u> f, <u>а не того, что она нигде не определена</u>. Поэтому для последующей проверки гипотезы Ферма для тех или иных значений f нужен еще (машинный) счет (объем которого быстро растет с ростом n) для вычисления $f_{\pi(f)}$ в точке n, когда оно возможно.

Аналогичную природу имеет пример полувычислимой функции, которая уже заведомо не является вычислимой: установлено, что существует такой многочлен $P(t, x_1, \ldots, x_n)$ с целыми коэффициентами, что функция.

$$g(t) = \begin{cases} \text{I, если уравнение } P(t, x_1, \ldots, x_n) = 0 \\ \quad \text{разрешимо с } x_1, \ldots, x_n \in \mathbb{Z}^+; \\ \text{не определена иначе} \end{cases}$$

не вычислима. Ее полувычислимость устанавливается точно также, как для функции f, связанной с уравнением Ферма.

I.5. <u>Критика предшествующих доказательств</u>.

Прежде чем двигаться дальше, рассмотрим более критически, скажем, рассуждение из п. I.4 а). Первое слабое место бро-

сается в глаза: мы не уточнили, что такое программа. Однако это не так существенно: при любом выбранном уточнении программа должна быть текстом над конечным алфавитом, чтобы удовлетворять интуитивным представлениям, а таких текстов счетное множество. Гораздо более сильное возражение состоит примерно в следующем: на каком основании мы можем работать с одним уточнением понятия программы? Возможно, существует все возрастающая иерархия точно описываемых " вычислительных средств", так что для каждой функции из Z^+ в Z^+ можно подобрать свою программу, которая может вычислять эту функцию?

Фундаментальным открытием теории вычисления было то обстоятельство, что на последний вопрос нужно дать отрицательный ответ. К настоящему времени мы обладаем единственным и окончательным формальным понятием, которое выдержало все проверки на его соответствие интуитивному представлению о полувычислимости, и которое конструируется так:

I.6. Тезис Черча (слабейшая форма). Можно явно указать

а) семейство простейших полувычислимых функций;

б) семейство элементарных операций, которые позволяют строить по одним полувычислимым функциям другие полувычислимые функции; с тем свойством, что любая полувычислимая функция получается за конечное число шагов, каждый из которых состоит в применении одной из элементарных операций к ранее построенным, либо к простейшим функциям.

I.7. Пояснение. В следующем параграфе тезису Черча будет придана точная формулировка: простейшие функции и

элементарные операции будут заданы явно. С этого времени начнется точная математическая теория вычислимости. Однако нам казалось важным отметить принципиальное значение того открытия, что семейства таких функций и операций вообще существуют и могут быть явно указаны, что далеко не очевидно.

Это - экспериментальный факт, возможно, важнейший из открытых логикой. Свидетельства в его пользу и его значение будут обсуждены несколько позже.

§ 2. Частично рекурсивные функции.

2.I. В этом параграфе мы изложим точное определение и первоначальные свойства класса функций, который считается адэкватной формализацией класса полувычислимых функций. Он будет описан тем способом, который указан в формулировке тезиса Черча в § I.

2.2. Простейшие функции.

$$\mathcal{SUC} : \mathbb{Z}^+ \to \mathbb{Z}^+, \quad \mathcal{SUC}(x) = x + 1$$

$$1^n : (\mathbb{Z}^+)^n \to \mathbb{Z}^+, \quad 1^{(n)}(x_1, \ldots, x_n) = 1 \quad n \geq 0$$

$$pr^{(n)}_{(i)} : (\mathbb{Z}^+)^n \to \mathbb{Z}^+, \quad pr^{(n)}_{(i)}(x_1, \ldots, x_n) = x_i, \quad n \geq 1$$

2.3. Элементарные операции над частичными функциями.

а) Композиция (или подстановка). Она ставит в соответствие паре функций f из $(\mathbb{Z}^+)^m$ в $(\mathbb{Z}^+)^n$ и g из $(\mathbb{Z}^+)^n$ в $(\mathbb{Z}^+)^p$. Функцию $h = g \circ f$ из $(\mathbb{Z}^+)^m$ в $(\mathbb{Z}^+)^p$, которая определяется так:

$$\begin{cases} \mathcal{D}(g\circ f) = f^{-1}(\mathcal{D}(g)) = \{x \in \mathcal{D}(f) \subset (\mathbb{Z}^+)^m \mid f(x) \in \mathcal{D}(g)\} \\ (g\circ f)(x) = g(f(x)) \end{cases}$$

б) <u>Соединение</u>. Эта операция ставит в соответствие k частичным функциям f_i из $(\mathbb{Z}^+)^m$ в $(\mathbb{Z}^+)^{n_i}$ $(i = 1, \ldots, k)$ функцию $(f_1, \ldots, f_k)$ из $(\mathbb{Z}^+)^m$ в $(\mathbb{Z}^+)^{n_1} \times \ldots \times (\mathbb{Z}^+)^{n_k}$, которая определяется так:

$$\mathcal{D}(f_1, \ldots, f_k) = \mathcal{D}(f_1) \cap \mathcal{D}(f_2) \cap \ldots \cap \mathcal{D}(f_k)$$

$$(f_1, \ldots, f_k)(x_1, \ldots, x_m) = (f_1(x_1, \ldots, x_m), \ldots, f_k(x_1, \ldots, x_m))$$

в) <u>Рекурсия</u>. Эта операция ставит в соответствие паре функций f из $(\mathbb{Z}^+)^n$ в $\mathbb{Z}^+$ и g из $(\mathbb{Z}^+)^{n+2}$ в $\mathbb{Z}^+$ функцию h из $(\mathbb{Z}^+)^{n+1}$ в $\mathbb{Z}^+$, которая определяется индукцией по последнему аргументу:

$$\begin{cases} h(x_1, \ldots, x_n, 1) = f(x_1, \ldots, x_n) \text{ (начальное условие)} \\ h(x_1, \ldots, x_n, k+1) = g(x_1, \ldots, x_n, k, h(x_1, \ldots, x_n, k)) \\ \qquad \text{при } k \geq 1 \text{ (индуктивный шаг)} \end{cases}$$

Область определения $\mathcal{D}(h)$ описывается также индуктивно:

$$(x_1, \ldots, x_n, 1) \in \mathcal{D}(h) \Longleftrightarrow (x_1, \ldots, x_n) \in \mathcal{D}(f),$$

$$(x_1, \ldots, x_n, k+1) \in \mathcal{D}(h) \Longleftrightarrow (x_1, \ldots, x_n, k) \in \mathcal{D}(h)$$

$$\text{и} \quad (x_1, \ldots, x_n, k, h(x_1, \ldots, x_n, k)) \in \mathcal{D}(g), \quad k \geq 1$$

г) <u>Операция μ</u>. Эта операция ставит в соответствие частичной функции f из $(\mathbb{Z}^+)^{n+1}$ в $\mathbb{Z}^+$ частичную функцию h из $(\mathbb{Z}^+)^n$ в $\mathbb{Z}^+$, которая определяется так:

$$\mathcal{D}(h) = \{(x_1, \ldots, x_n) \mid \exists x_{n+1} \geq 1, f(x_1, \ldots, x_n, x_{n+1}) = 1 \ \& \ (x_1, \ldots x_n, k) \in \mathcal{D}(f)$$

для всех $k \leq x_{n+1}\}$

$$h(x_1, \ldots, x_n) = \min\{y \mid f(x_1, \ldots x_n, y) = 1\}$$

В общих чертах μ вводит функции, заданные "неявно", как это часто делается во многих областях математики. Три особенности операции μ заслуживают быть отмеченными немедленно.

Выбор <u>минимального</u> y с $f(x_1, \ldots, x_n, y) = 1$ делается, конечно, для обеспечения однозначности функции h.

Область определения h на первый взгляд представляется искусственно суженной: если, скажем, $f(x_1, \ldots x_n, 2) = 1$, а $f(x_1, \ldots x_n, 1)$ не определено, мы считаем $h(x_1, \ldots x_n)$ не определенной, а не равной 2. Причина этого состоит в желании сохранить интуитивную полувычислимость функции h и будет несколько подробнее прокомментировано ниже (см. п. 2.7 а).

Наконец, все описанные до μ операции, если их применять к всюду определенным функциям, дают в результате

всюду определенную функцию. Для μ это, очевидно, не так: это единственная операция, ответственная за возникновение частичных функций.

2.4. Определение. а) Последовательность частичных функций $f_1, \ldots, f_N$ называется частично рекурсивным (соотв. примитивно рекурсивным) описанием функции $f_N = f$, если

f_1 – одна из простейших функций;

f_i – для всех $i \geq 2$ либо является простейшей функцией, либо получается применением одной из элементарных операций к некоторым из функций $f_1, \ldots, f_N$ (соотв. одной из элементарных операций, кроме μ).

б) Функция f называется частично рекурсивной (соотв. примитивно рекурсивной), если она допускает частично рекурсивное (соотв. примитивно рекурсивное) описание.

(Аналогия с определением <u>вывода</u> в формальном языке бросается в глаза и может быть использована).

2.5. <u>Тезис Черча</u> (обычная форма).

а) Функция f полувычислима, если и только если она частично рекурсивна.

б) Функция f вычислима, если и только если f и $f_{\infty(f)}$ частично рекурсивны.

2.6. <u>Использование тезиса Черча</u>. Прежде чем обсуждать подробные аргументы в пользу тезиса Черча, укажем, как он используется в математической практике.

Два основных способа бросаются в глаза при изучении литературы.

а) Определение алгоритмической неразрешимости.

Пусть имеется счетная последовательность математических "задач" $P_1, P_2, \ldots, P_n, \ldots$. Предполагается, далее, что каждая задача имеет ответ "да" или "нет" и что по номеру n условие задачи P_n выписывается "эффективно". Такая последовательность $P = (P_n)$ называется "массовой проблемой". Свяжем с ней функцию f из Z^+ в Z^+:

$$\mathcal{D}(f) = \{ i \in Z^+ \mid P_i \text{ имеет ответ "да"} \}$$

$$f(i) = 1 \text{, если } i \in \mathcal{D}(f)$$

Массовая проблема P называется алгоритмически разрешимой, если функции f и $\chi_{\mathcal{D}(f)}$ частично рекурсивны. В противном случае P называется алгоритмически неразрешимой. Заметим, что в принципе возможно еще различать случаи, когда только $\chi_{\mathcal{D}(f)}$ не является частично рекурсивной или когда даже f не частично рекурсивна. Вторая неразрешимость еще "хуже" первой; примеры были указаны в § I.

Еще один известный пример массовой проблемы: проблема тождества слов в группах. Пусть G - некоторая группа, $a_1, \ldots, a_r \in G$ - некоторые элементы. "Приведенное слово" от $a_1, \ldots, a_r$ - это выражение вида $a_{i_1}^{\varepsilon_1} \ldots a_{i_k}^{\varepsilon_k}$, где $k \geq 1$, $\varepsilon_i = \pm 1$ и если $i_a = i_{a+1}$, то $\varepsilon_a = \varepsilon_{a+1}$. Расположим все приведенные слова в алфавитном порядке и поставим задачу P_n:

"Верно ли, что n-е слово представляет единичный элемент группы G?"

"Массовая проблема" (P_n) алгоритмически разрешима для одних групп G и элементов $a_1, \dots, a_r$ и неразрешима для других (Новиков, Бум). Функция f здесь всегда частично рекурсивна.

б) <u>Тезис Черча как эвристический принцип</u>. Интуитивно понятие "полувычислимости" представляется более широким, чем понятие "частичной рекурсивности", и многие задачи о частично рекурсивных функциях становятся значительно легче, если подставить в их формулировку неформальные представления и разрешить пользоваться ими в решении. Скажем, формула $e = \lim (1+\frac{1}{n})^n$ и алгоритм Эвклида делают интуитивно ясным, что функции $f, g : Z^+ \longrightarrow Z^+$:

$f(n) =$ n-й десятичный знак разложения

$g(n) =$ n-е простое число

вычислимы, тогда как проверка их рекурсивности требует довольно кропотливых конструкций.

Тезис Черча позволяет разбить решение таких задач на два этапа; I) отыскание неформального решения с использованием любых интуитивных алгоритмов; 2) последующая формализация. Второй этап предполагает известную опытность в отыскании частично рекурсивного описания самых разнообразных полувычислимых функций, а тезис Черча дает уверенность в том, что такое описание существует.

По мере накопления доказательств рекурсивности в литературе все чаще ограничиваются проведением лишь первого этапа решения: ярким примером тому служит книга Х.Роджерса "Теория рекурсивных функций и эффективная вычислимость", М., "Мир",

1972. К концу лекций мы также позволим себе ряд вольностей такого рода.

2.7. Аргументы в пользу тезиса Черча. а) Прежде всего, представляется ясным, что простейшие функции вычислимы. Далее, элементарные операции, примененные к полувычислимым функциям, снова дают полувычислимую функцию: программа, полувычисляющая ее, без труда компонуется из полувычисляющих программ для данных функций. Мы рассмотрим подробнее только случай μ -оператора, оставив легкую конструкцию остальных трех программ читателю.

В обозначениях п. 2.3. г. пусть f - полувычислимая функция из $(\mathbb{Z}^+)^{n+1}$ в $\mathbb{Z}^+$. Для вычисления $h(x_1, \ldots, x_n)$ будем перебирать в порядке возрастания последней координаты вектора $(x_1, \ldots, x_n, 1)$, $(x_1, \ldots, x_n, 2)$ и вычислять значения f в них. Если $(x_1, \ldots, x_n) \in \mathcal{D}(h)$, где h получается из f применением μ -оператора, то программа для f последовательно вычисляет $f(x_1, \ldots, x_n, 1)$, $\ldots, f(x_1, \ldots, x_n, y-1)$, и наконец, $f(x_1, \ldots, x_n, y)$; Наименьшее такое y , если оно существует, нужно подать на выход: это будет значение h в точке $(x_1, \ldots, x_n)$ Если же y не существует или хоть одно из значений f в точке $(x_1, \ldots, x_n, k)$ (до достижения f 1) окажется не определенным, то полувычисляющая f программа либо даст ответ не из $\mathbb{Z}^+$ - его нужно послать на выход, либо будет работать бесконечно долго; но по нашему соглашению h в точке $(x_1, \ldots, x_n)$ тогда не определена, и такое поведение программы для h согласуется с определением полувычислимости h .

2-1978

Из всего сказанного нужно сделать вывод, что частично рекурсивные функции полувычислимы. Наиболее сильное утверждение тезиса Черча состоит, таким образом, в том, что полувычислимые функции частично рекурсивны (определение вычислимости через полувычислимость мы просто перенесли без изменений из § I). Как было сказано, это экспериментальный факт. Экспериментальные свидетельства в его пользу делятся на несколько классов, которые мы рассмотрим последовательно в подпунктах б) - г).

б) В литературе имеется огромный набор рекурсивных описаний различных (полу) вычислимых функций. См., например, книгу Р.Петер "Рекурсивные функции", М., Ил, 1954. Часть этого списка мы приведем в следующем параграфе. Имеется также набор приемов составления рекурсивных описаний, применимых к целым классам (полу) вычислимых функций. Каждый раз, когда какой-нибудь автор пытался найти частично рекурсивное описание (полу) вычислимой функции, это описание находилось.

в) Тьюринг предложил математическое описание абстрактной вычислительной машины и сильные аргументы в пользу того, что эта машина является универсальной (то есть может (полу) вычислять все (полу) вычислимые функции), детально проанализировав характерные черты процесса детерминированного вычисления. (Обратите внимание, что мы совершенно не занимались формализацией процесса вычисления, а только его результатами!).

Оказалось, что класс функций, полувычисляемых машиной Тьюринга, в точности совпадает с классом частично рекурсивных функций.

г) Черч, Пост, Марков, Колмогоров, Успенский и др. предложили другие детерминированные схемы переработки информации (не обязательно числовой) общего характера. Во всех случаях оказалось, что при подходящей "эффективной" нумерации множеств входов и выходов эти способы приводят к такому классу отображений из Z^+ в Z^+, который совпадают с соответствующим подклассом частично рекурсивных функций.

За дальнейшим обсуждением тезиса Черча мы отсылаем читателя к литературе.

§ 3. Примеры рекурсивных функций

3.1. В этом параграфе будет приведен краткий список частично рекурсивных функций (почти все они будут даже примитивно рекурсивными) и выборка первоначальных приемов доказательств рекурсивности. В дальнейшем изложении этот список будет пополняться по мере надобности.

Вводя новые функции, мы будем все больше сокращать их рекурсивные описания, по мере увеличения опыта читателя.

3.2. а) $sum(X_1, X_2) = X_1 + X_2 : (Z^+)^2 \to Z^+$. Обычное индуктивное описание $X_1 + X_2$ индукций по второму аргументу таково:

начальное значение $(X_2 = 1): X_1 + 1 = suc(X_1)$

выражение $k+1$ -го

значения через $(k-e): X_1 + k + 1 = (X_1 + k) + 1 = suc(sum(X_1, k))$

Значит, sum получается рекурсией из функций (см. формулы из § 2):

$$f = suc : \mathbb{Z}^+ \longrightarrow \mathbb{Z}^+$$

$$g = suc \circ pr_3^{(3)} : (\mathbb{Z}^+)^3 \longrightarrow \mathbb{Z}^+$$

$$g(x_1, x_2, x_3) = x_3 + 1$$

Рекурсивным описанием sum является последовательность

$$f = suc, pr_3^{(3)}, \quad g = suc \circ pr_3^{(3)}, sum$$

б) $sum_n(x_1, x_2, \ldots, x_n) = x_1 + \quad + x_n \ , \ n \geq 3$

Так как $sum_n(x_1, \ldots x_n) =$

$$= sum(sum(x_1, \ldots, x_{n-1}), x_n)$$

(справа стоит композиция функций sum_{n-1} и соединения $sum_{n-1}, pr_3^{(3)}$, индукцией по n получаем, что эта сумма также примитивно рекурсивна).

3.3. а) $prod(x_1, x_2) = x_1 \cdot x_2$

Результат применения рекурсии к функции

$$f = pr_1^{(1)} \qquad Z^+ \to Z^+$$
$$g = sum \circ (pr_1^{(3)}, pr_3^{(3)}) \qquad (Z^+)^3 \to Z^+$$
$$g(x_1, x_2, x_3) = x_1 + x_3$$

б) $prod(x_1, \quad , x_n) = x_1 \cdot \ . \ x_n$

Индукция по n, как в предыдущем пункте.

3.4. а) $x \dot{-} 1 \ . \ Z^+ \longrightarrow Z^+$

$$X \dot{-} 1 = \begin{cases} X-1, & \text{если } X \geq 2 \\ 1, & \text{если } X = 1 \end{cases}$$

Рекурсия применяется к функциям

$$f : (Z^+)^0 \longrightarrow Z^+ \qquad (0) \longmapsto 1,$$

$$g = pr_1^{(2)} : (Z^+)^2 \longrightarrow Z^+ ; \; g(X_1, X_2) = X_1$$

(Заметим, что $X \dot{-} 1$ зависит от одного аргумента, так что f должна зависеть от 0 аргументов, а g – от двух, формула рекурсии превращается в $h(k+1) = g(k, h(k))$.

б) $X_1 \dot{-} X_2 : (Z^+)^2 \to Z^+$

$$X_1 \dot{-} X_2 = \begin{cases} X_1 - X_2, & \text{если } X_1 \geq X_2 + 1 \\ 1, & \text{если } X_1 < X_2 + 1 \end{cases}$$

Эта "усеченная разность" получается применением рекурсии к функциям:

$$f(X_1) = X_1 - 1 \; ;$$

$$g(X_1, X_2, X_3) = X_3 - 1$$

Теперь мы в состоянии доказать уже общий результат, который часто будет полезен:

3.5. <u>Предложение</u>. Пусть $F(X_1 \dots X_n)$ – многочлен с целыми значениями, который при всех $(X_1 \dots X_n) \in (Z^+)^n$ принимает значения ≥ 1. Пусть далее $f_1, \dots, f_n$ – любые частично рекурсивные функции (от каких угодно аргументов).

Тогда композиция $F(f_1, \ldots, f_n)$ является частично рекурсивной функцией. Она примитивно рекурсивна, если $f_1, \ldots, f_n$ примитивно рекурсивны.

<u>Доказательство</u>. Достаточно проверить, что $F(X_1, \ldots, X_n)$ примитивно рекурсивна.

Если все коэффициенты F неотрицательны, то F является суммой произведений X_i. Из 3.2. и 3.3. легко следует, что F примитивно рекурсивны (например, $X_1^2 X_3$ есть композиция $prod \cdot (pr_1^{(3)}, pr_1^{(3)}, pr_3^{(3)})$).

В общем случае представим F в виде $F^+ - F^-$, где у F^+ и F^- – все коэффициенты неотрицательны. Из 3.4 б) мы можем заключить, что <u>усеченная</u> разность $F^+ \dot{-} F^-$ является примитивно рекурсивной функцией; но так как, по предложению, для всех допустимых значений аргументов $F^+ - F^- \geq 1$, эта усеченная разность совпадает с обыкновенной.

Вот типичная ситуация, в которой мы будем использовать предложение 3.5. Пусть $f, g : (Z^+)^n \to Z^+$ две частично рекурсивные функции. Предположим, что нас интересует множество точек, где $f = g$. Оно совпадает с множеством точек, где функция $(f-g)^2 + 1$ принимает значение I. Последняя функция частично рекурсивна, по предложению 3.5, и поэтому такое описание часто бывает удобнее предыдущего.

Продолжим наш список рекурсивных функции.

3.6.

$$\chi_{(1)}(x) = \begin{cases} 1 & \text{при } x = 1 \\ 2 & \text{при } x \geq 2 \end{cases}$$

Рекурсия к $f(\cdot) = 1$ и $g(x, X_2) = 2$.

Аналогично описывается любая функция h $Z^+ \to Z^+$, принимающая в точке I значение a, в точках ≥ 2 значение b.

3.7.

$$\psi_1(x) = \begin{cases} \text{I при } X = 1 \\ \text{не определена при } X \geq 2 \end{cases}$$

Эта функция, конечно, не может быть примитивно рекурсивной, потому что она не всюду определена.

Ее можно получить, например, применяя μ - оператор к функции $(\psi_{(1)}(X_1) + X_2) \dot{-} 1$, которая примитивно рекурсивна по предыдущему:

$$\psi_{(1)}(X) = \min y / (\psi_{(1)}(X) + y) \dot{-} 1 = 1$$

3.8. $rem(x, y) =$

$$rem(x,y) = \begin{cases} \text{остаток от деления } y \text{ на } x, \\ \text{если он не нулевой;} \\ x, \text{ если } y \text{ делится на } x. \end{cases}$$

На этом примере можно продемонстрировать искусственный прием, полезный при отыскании рекурсивных описаний. Напишем сначала очевидную индуктивную формулу:

$$rem(X, 1) = 1$$

$$rem(x, y+1) = \begin{cases} suc(rem(x,y)), \text{ если } rem(x,y) \neq x \\ \text{I, если } rem(x,y) = x \end{cases}$$

Нам нужно теперь показать примитивную рекурсивность функции справа, заданной "кусочно".

Заметим прежде всего, что если определить примитивно рекурсивную функцию φ формулой

$$\varphi(x,y) = \psi((rem(x,y)-x)^2+1), \text{ где } \psi(z) = \begin{cases} 2 \text{ при } z = 1 \\ 1 \text{ при } z \geq 2 \end{cases}$$

то мы получим

$$rem(x,y) \neq x \Leftrightarrow \varphi(x,y) = 1$$

$$rem(x,y) = x \Leftrightarrow \varphi(x,y) = 2$$

Отсюда находим:

$$rem(x, y+1) = 2\, suc(rem(x,y)) \dot{-} \varphi(x,y) \cdot suc(rem(x,y)),$$

что немедленно доставляет способ описать rem рекурсией.

3.9. Опишем этот прием в достаточно общем виде. Допустим, что функция $f(x_1, \ldots, x_n)$ задана предписанием:

$$f(x_1, \ldots, x_n) = \begin{cases} g_1(x_1, \ldots x_n), \text{ если } \varphi_1(x_1, \ldots, x_n) = 1 \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ g_m(x_1, \ldots x_n), \text{ если } \varphi_m(x_1, \ldots x_n) = 1 \end{cases}$$

Мы будем считать, что "множества I-уровней" $\varphi_i = 1$ попарно не пересекаются. Кроме того, можно считать, что φ_i принимает значения только I или 2: если это не так, то нужно заменить φ_i на $\psi((\varphi_i - 1)^2 + 1)$, где $\psi(x) = 2$ при $x = 1$, $\psi(x) = 1$ при $x \geq 2$.

Тогда

$$\varphi_1(x_1 \ldots x_n) = 2\sum_{i=1}^{m} g_i(x_1 \ldots x_n) \dot{-} \sum g_i(x_1 \ldots x_n)\varphi_2(x_1 \ldots x_n)$$

Если, скажем, все g_i и φ_i примитивно рекурсивны, то отсюда видно, что и φ примитивно рекурсивна. Заметим, что в п. 3.8., а также ниже, в пунктах 3.10 и 3.11 этот способ нужно применять для доказательства рекурсивности вспомогательной функции, к которой затем применяется рекурсия.

3.10.

$$qt(x,y) = \begin{cases} \text{целая часть } \frac{y}{x}, & \text{если } \frac{y}{x} \geq 1 \\ 1, & \text{если } \frac{y}{x} < 1 \end{cases}$$

Очевидно, имеем

$$qt(x,y+1) = \begin{cases} qt(x,y), & \text{если } rem(x,y+1) \neq x \\ qt(x,y)+1, & \text{если } rem(x,y+1) \neq x,\ y+1 \neq x \\ 1, & \text{если } y+1 = x \end{cases}$$

Поэтому можно применить прием, описанный в пп. 3.8 и 3.9. Читателю будет полезно восстановить детали.

3.11. $\quad rad(x) =$ целая часть $\sqrt{x}$.

Имеем: $\quad rad(1) = 1$;

$$rad(x+1) = \begin{cases} rad(x), & \text{если } qt(rad\,x+1, x+1) < rad\,x+1 \\ rad\,x+1, & \text{если } qt(rad\,x+1, x+1) = rad\,x+1 \end{cases}$$

2^{xx}-1978

Прежний прием позволяет показать после этого, что rad примитивно рекурсивна.

3.12. $min(x,y)$, $max(x,y)$.

Доказательство оставляется читателю в качестве упражнения.

§ 4. Перечислимые множества

4.1. Определение. Множество $E \subset (Z^+)^n$ называется перечислимым, если существует такая частично рекурсивная функция f, что $E = \mathcal{D}(f)$ (область определения f).

Обсуждение в § 1 и § 2 показывает, что интуитивный смысл перечислимости E таков: существует программа, которая распознает элементы x, принадлежащие E, но, возможно, не умеет распознавать элементы, не принадлежащие E. Позже будет дано другое интуитивное описание перечислимых множеств, более ясно указывающее на происхождение названия: это множества, все элементы которых могут быть получены (возможно, с повторениями и в неизвестном порядке) с помощью некоторой "порождающей" их программы.

Понятие перечислимого множества, наряду с понятием частично рекурсивной функции, занимает центральное место во всей теории. Из дальнейших результатов будет видно, что любое из них может быть сведено к другому, однако, в доказательствах необходимую гибкость дает лишь использование обоих понятий.

Начнем со следующего простого факта.

4.2. Предложение. Класс перечислимых множеств совпадает с классом множеств уровней (и даже I-уровней) частично рекурсивных функций.

Доказательство. Напомним, что множеством m -уровня (или просто m -уровнем) функции f из $(Z^+)^n$ в Z^+ называется множество $E \subset \mathcal{D}(f)$,

$$x \in E \Leftrightarrow f(x) = m$$

а) Пусть E перечислимо, $E = \mathcal{D}(f)$, где f частично рекурсивна. Тогда

$E = 1$ I-уровень функции $(f - m)^2 + 1$

Функция $(f - m)^2 + 1$ частично рекурсивна в силу предложения 3.5.

б) Пусть E I-уровень частично рекурсивной функции $f(x_1, \dots, x_n)$. Положим

$$g(x_1, \dots, x_n) = \min y \,|\, (f(x_1, \dots x_n) - 1)^2 + y = 1$$

Очевидно, g частично рекурсивна и $E = \mathcal{D}(g)$ ■

Основной теоремой этого параграфа будет следующее гораздо более трудное утверждение и его следствия:

4.3. Теорема. Следующие два класса множеств совпадают:

а) Перечислимые множества.

б) Проекции множеств уровня примитивно рекурсивных функций.

4.4. Первая часть доказательства. Напомним прежде всего, что если дано некоторое множество $E \subset (Z^+)^{n+m}$, то его проекцией ("на первые n координат") называется множество $F \subset (Z^+)^n$, которое определяется так:

$$(x_1, \ldots, x_n) \in F \Leftrightarrow \exists\, (y_1, \ldots, y_n) \in (Z^+)^m \mid (x_1, \ldots, y_m) \in E$$

Аналогично определяется проекция "на координаты о номерами $(i_1, \ldots, i_k) \subset (1, \ldots, n)$". Число m удобно называть <u>коразмерностью</u> проекции. Каноническое отображение проекции $E \to F$ также принято называть проекцией; это не может привести к путанице.

Назовем временно проекции уровней примитивно рекурсивных функций <u>примитивно перечислимыми</u> множествами.

Первая часть доказательства будет состоять в установлении того факта, что примитивно перечислимые множества перечислимы; вторая - в проверке обратного включения.

Итак, пусть $f(x_1, \ldots, x_n, x_{n+1}, \ldots, x_{n+m})$ - некоторая примитивно рекурсивная функции, E - проекция ее I-уровня на первые n -координат. (I-уровнями можно ограничиться в силу уже использованного соображения: K -уровень f совпадает с I-уровнем $f' = (f - K)^2 + 1$. Построим явно такую частично рекурсивную функцию g, что $E = \mathcal{D}(g)$

Разберем отдельно три случая, в зависимости от коразмерности проекции: $m = 0, 1$, или ≥ 2.

<u>Случай а</u>) $m = 0$. Тогда $E = 1$ - уровень $f \Rightarrow E$ перечислимо по предложению 4.2) g построена тем явно).

<u>Случай б</u>) $m = 1$. Положим

$$g(x_1, \ldots x_n) = \min x_{n+1} \mid f(x_1, \ldots, x_n, x_{n+1}) = 1$$

Очевидно, g частично рекурсивна и $\mathcal{D}(g) = E$ (обратите внимание на то, как здесь используется обстоятельство $\mathcal{D}(f) = (\mathbb{Z}^+)^{n+1}$).

Случай в) $m \geq 2$. Мы сведем этот случай к предыдущему с помощью следующей леммы, важной во многих других вопросах и имеющей принципиальный интерес. (Отсутствие понятия размерности в "рекурсивной геометрии"):

4.5. Лемма. Для всех $m \geq 1$ существует такое взаимно однозначное отображение $t^{(m)} : \mathbb{Z}^+ \to (\mathbb{Z}^+)^m$, что

а) функции $t_i^{(m)} = pr_i^{(m)} \circ t^{(m)}$ примитивно рекурсивны, $1 \leq i \leq m$;

б) обратная функция $\sigma^{(m)} : (\mathbb{Z}^+)^m \to \mathbb{Z}^+$ примитивно рекурсивна.

4.6. Использование леммы. Предположим, что лемма верна. Применим ее к ситуации п. 4.4, случай в) так: положим при $m \geq 2$

$$g(x_1, \quad x_n, y) = f(x_1, \quad x_n, t_1^{(m)}(y), \quad t_m^{(m)}(y))$$

Очевидно, g примитивно рекурсивна вместе с f . Легко проверяется, что E совпадает с проекцией I-уровня функции g на первые n координат. Так как это проекция коразмерности I, мы свели этот случай к уже разобранному.

4.7. Доказательство леммы. Случай $m = 1$ тривиален. Проведем индукцию по m , начиная с $m = 2$.

Конструкция $t^{(2)}$. Сначала построим явно $\sigma^{(2)}$:

$\mathcal{T}^{(2)}:(\mathbb{Z}^+)^2 \to \mathbb{Z}^+$, положив

$$\mathcal{T}^{(2)}(x_1, x_2) = \frac{1}{2}\left((x_1 + x_2)^2 - x_1 - 3x_2 + 2\right)$$

Легко проверяется, что если перенумеровать пары $(x_1, x_2) \in (\mathbb{Z}^+)^2$ в "канторовоком порядке", расположив их по возрастанию $x_1 + x_2$, а внутри группы с данными $x_1 + x_2$ – по возрастанию x_1, то $\mathcal{T}^{(2)}(x_1, x_2)$ будет как раз номером пары (x_1, x_2) в этом списке. Тем самым, $\mathcal{T}^{(2)}$ взаимно однозначна и примитивнс рекурсивна (использовать предложение 3.5 и рекурсивность qt, п. 3.10 для учета $\frac{1}{2}$).

Восстановление пары (x_1, x_2) по ее номеру y является элементарной задачей и приводит к следующим формулам для обратной функции $t^{(2)}$:

$$t_1^{(2)}(y) = y - \frac{1}{2}\left[\sqrt{2y - \frac{7}{4}} - \frac{1}{2}\right]\left(\left[\sqrt{2y - \frac{7}{4}} - \frac{1}{2}\right] + 1\right)$$

$$t_2^{(2)}(y) = \left[\sqrt{2y - \frac{7}{4}} - \frac{1}{2}\right] - t_1^{(2)}(y) + 2$$

Здесь $[z]$ означает целую часть z. Проверку примитивной рекурсивности этих функций с помощью результатов (и приемов) § 3 мы оставляем читателю в качестве упражнения.

Конструкция $t^{(m)}$, $m \geq 3$. Предположим, что $t^{(m-1)}$, $\mathcal{T}^{(m-1)}$ уже построены и проверены их свойства. Положим прежде всего

$$\mathcal{T}^{(m)}(X_1, \dots, X_m) = \mathcal{T}^{(2)}(\mathcal{T}^{(m-1)}(X_1, \dots X_{m-1}), X_m)$$

Ясно, что $\mathcal{T}^{(m)}$ примитивно рекурсивна и взаимно однозначна. Решая уравнение $\mathcal{T}^{(2)}(\mathcal{T}^{(m-1)}(X_1, \dots X_{m-1}), X_m) = y$ в два приема, получим для обратной функции $t^{(m)}$ формулы:

$$t_m^{(m)}(y) = t_2^{(2)}(y)$$

$$t_i^{(m)}(y) = t_i^{(m-1)}(t_1^{(2)}(y)) \qquad 1 \le i \le m-1$$

По индуктивному предположению, $t_i^{(m)}$ примитивно рекурсивны.

Этим завершается доказательство леммы и вместе с ним первая часть доказательства теоремы 4.3.

<u>Вторая часть доказательства</u>. Теперь мы должны установить, что всякое перечислимое множество примитивно перечислимо.

Начнем со следующего свойства класса примитивно перечислимых множеств.

4.8. <u>Лемма</u>. Класс примитивно перечислимых множеотв замкнут относительно следующих операций: конечное прямое произведение, конечное пересечение, конечное объединение, проекция.

<u>Доказательотво</u>. Пусть $E, E' \subset (\mathbb{Z}^+)^n$, $E_1 \subset (\mathbb{Z}^+)^2$ - три примитивно перечислимых множества, проекции I-уровней примитивно рекурсивных функций f, f' и f_1 соответственно:

$$x = (x_1, \ldots, x_n) \in E \Leftrightarrow \exists\, y = (y_1, \ldots, y_m) \mid f(x, y) = 1$$
$$x = (x_1, \ldots, x_n) \in E' \Leftrightarrow \exists\, z = (z_1, \ldots, z_q) \mid f'(x, y) = 1$$
$$u = (u_1, \ldots, u_n) \in E_1 \Leftrightarrow \exists\, v = (v_1, \ldots, v_s) \mid f_1(x, y) = 1$$

Тогда имеем:

$E \times E_1$ проекция I-уровня функции $(f \cdot f_1)(x, u; y, v)$

$E \cup E'$ проекция I-уровня функции $(f - 1)(f' - 1) + 1$

$E \cap E'$ проекция I-уровня функции $(f \cdot f')(x, y, z)$

Устойчивоость относительно проекций заложена в определение.

Пусть теперь E - некоторое перечислимое множество. Реализуем его как I-уровень частично рекурсивной функции f из $(\mathbb{Z}^+)^n$ в $\mathbb{Z}^+$ по предложению 4.2 и заметим, что для доказательства примитивной перечислимости E достаточно проверить примитивную перечислимость <u>графика</u> $\Gamma_f \subset (\mathbb{Z}^+)^n \times \mathbb{Z}^+$. Действительно, ясно, что E = I-уровень f = проекция на первые n координат множества $\Gamma_f \cap [(\mathbb{Z}^+)^n \times \{1\}]$. Кроме того, множество $\{1\} \subset \mathbb{Z}^+$ примитивно перечислимо, например, по п. 3.6. Если мы докажем, что Γ_f примитивно перечислимо, из леммы 4.6 будет следовать то же самое для E. Итак, окончательная редукция нашей задачи выглядит так: <u>доказать, что графики частично рекурсивных функций f примитивно перечислимы</u>. С этой целью мы проверим, что а) графики простейших функций примитивно перечислимы; б) если даны функции с примитивно перечислимыми графиками, то у функции, которая получается из них применением одной из элементарных операций, также примитивно перечислимый график.

Графики простейших функций.

$\Gamma_{suc} \subset (\mathbb{Z}^+)^2 =$ I-уровень $(x_1 + 1 - x_2)^2 + 1$

$\Gamma_{1^{(n)}} \subset (\mathbb{Z}^+)^{n+1} =$ I-уровень x_{n+1}

$\Gamma_{pr^{(n)}} \subset (\mathbb{Z}^+)^{n+1} =$ I-уровень $(x_1 - x_{n+1})^2 + 1$

Устойчивость относительно соединения.

Пусть f, g – частичные отображения из $(\mathbb{Z}^+)^m$ в $(\mathbb{Z}^+)^p$ и $(\mathbb{Z}^+)^q$ соответственно. Предположим, что Γ_f и Γ_g примитивно перечислимы. Тогда $\Gamma_{(f,g)} \subset (\mathbb{Z}^+)^m \times (\mathbb{Z}^+)^p \times (\mathbb{Z}^+)^q$ совпадает с пересечением

$$(\Gamma_f \times (\mathbb{Z}^+)^q) \cap perm(\Gamma_g \times (\mathbb{Z}^+)^p)$$

Здесь $perm : (\mathbb{Z}^+)^m \times (\mathbb{Z}^+)^q \times (\mathbb{Z}^+)^p \simeq (\mathbb{Z}^+)^m \times (\mathbb{Z}^+)^p \times (\mathbb{Z}^+)^q$ – операция, которая меняет местами два последних сомножителя:

$$(x^{(m)}, y^{(q)}, z^{(p)}) \longmapsto (x^{(m)}, z^{(p)}, y^{(q)})$$

Из леммы 4.6 видно, что $\Gamma_{(f,g)}$ примитивно перечислим.

Устойчивость относительно композиции. Пусть g – частичное отображение на $(\mathbb{Z}^+)^n$ в $(\mathbb{Z}^+)^m$, f – то же из $(\mathbb{Z}^+)^m$ в $(\mathbb{Z}^+)^p$, $h = f \circ g$. Тогда Γ_h – проекция множества $(\Gamma_g \times (\mathbb{Z}^+)^p) \cap ((\mathbb{Z}^+)^n \times \Gamma_f)$ на $(\mathbb{Z}^+)^n \times (\mathbb{Z}^+)^p$

Как выше, если Γ_f и Γ_g примитивно перечислимы, то же верно для Γ_h по лемме 4.6.

Устойчивость относительно рекурсии и μ – оператора является значительно более тонким фактом. Нам понадобиться следующая красивая и полезная лемма.

4.9. Лемма. Существует примитивно рекурсивная функция $Gd(k,t)$ (функция Геделя) со следующим свойством:

для любого $N \in \mathbb{Z}^+$ и любой конечной последовательности $a_1, \ldots, a_N \in (\mathbb{Z}^+)$ длины N существует такое $t \in \mathbb{Z}^+$, что $Gd(k,t) = a_k$ при всех $1 \le k \le N$

(Иными словами, $Gd(k,t)$ – это такая последовательность функций от аргумента k, пронумерованная значениями параметра t, что любая функция от k на сколь угодно большом интервале $1, \ldots, N$ может быть имитирована подходящим членом последовательности).

Доказательство. Сначала положим

$$gd(k;u,t) = rem(1+kt, u)$$

и покажем, что gd обладает тем же свойством, что и Gd, если разрешить подбирать $(u,t) \in (\mathbb{Z}^+)^2$. После этого можно будет положить $Gd(k,y) = gd(k; t_1^{(2)}(y), t_2^{(2)}(y))$, где $t^{(2)}: \mathbb{Z}^+ \to (\mathbb{Z}^+)^2$ – изоморфизм из леммы 4.5. (Избавление от лишнего параметра несущественно, но в дальнейшем укоротит формулы).

Итак, пусть даны $a_1, \ldots, a_N \in \mathbb{Z}^+$. Сначала выберем $X \in \mathbb{Z}^+$ с условиями $X \ge N$, $1 + kX' > a$ для всех $1 \le k \le N$. Далее, положим $t = X'$. Легко видеть, что если $k_1 \ne k_2$, $k_1, k_2 \le N$, то $1 + k_1 X'$ и $1 + k_2 X'$ взаимно просты: их общий делитель должен был бы делить $(k_1 - k_2)X'$, то есть состоять из простых чисел $\le X$, но ни одно из

них не делит $1 + k_1 X'$!

По элементарной теореме теории чисел, существует решение $u \in Z^+$ системы сравнений

$$u \equiv a_k \mod (1 + kX'), \quad 1 \le k \le N$$

Очевидно, отсюда вытекает, что

$$gd(k, u, t) = rem(1 + kt, u) = a_k, \quad 1 \le k \le 1$$

Теперь продолжим доказательство теоремы 4.3.

4.10. <u>Устойчивость относительно μ - операции.</u>

Пусть f - частичная функция из $(Z^+)^{n+1}$ в Z^+, и пусть

$$g(X_1, \dots, X_n) = \min y \,/\, f(X_1, \dots, X_n, y) = 1$$

Напомним, что область определения g состоит из тех $(X_1, \dots, X_n)$, для которых $\min y$ существует и $(X_1, \dots, X_n, k) \in D(f)$ для всех k, меньших этого $\min y$.

Мы хотим доказать, что если Γ_f примитивно перечислим, то Γ_g также примитивно перечислим.

Пусть Γ_f является проекцией 1-уровня (на первые $n+1$ координат) примитивно рекурсивной функции F:

$$f(X_1, \dots, X_{n+1}) = \varphi \iff \exists (y_1, \dots, y_m) \,/\, F(X_1, \dots, X_{n+1}, \varphi, y_1, \dots, y_m) = 1$$

(буквой φ мы обозначили тот аргумент F, который становится значением f). Как в п. 4.4 достаточно рассмотреть случай $m = 1$: если $m \geq 2$, то воспользоваться леммой 4.5 для замены вектора $(y_1, \ldots, y_n)$ одним числом y, а если $m = 0$, то ввести "фиктивный аргумент" y, от которого F на самом деле не зависит.

Итак, пусть $m = 1$. Введем функцию G от аргументов $x_1, \ldots, x_n, j, y, t, t_1$, положив

$$\psi(1) = 2, \quad \psi(x) = 1 \quad \text{при} \quad x \geq 2$$

$$F_k = F(x_1, \ldots, x_n, k, Gd(k,t), Gd(k,t_1)), \quad k \geq 1$$

$$G = F(x_1, \ldots, x_n, j, 1, y) \prod_{k=1}^{j-1} \psi(Gd(k,t))\, F$$

Здесь $\prod_{k=1}^{0} = 1$ по определению.

Легко убедиться, что G примитивно рекурсивна; она получается рекурсией по аргументу j из двух других функций, примитивная рекурсивность которых очевидна.

Мы покажем, что Γ_g является проекцией на координаты $(x_1, \ldots, x_n, j)$ I-уровня функции G.

<u>Включение $pr\,(G=1) \subset \Gamma_g$</u>. Пусть $(x_1, \ldots, x_n, j, y, t, t_1)$ – фиксированная точка на I-уровне G. Мы должны проверить, что $(x_1, \ldots, x_n) \in \mathcal{D}(g)$ и что $j = g(x_1, \ldots, x_n)$

Иными словами, нужно установить, что

$$f(x_1, \ldots, x_n, j) = 1$$

$$f(x_1, \ldots, x_n, k) \text{ определена и } > 1$$

для всех $k \leq j-1$

Так как $G = 1$ в данной точке, все сомножители G равны I в этой точке. В частности, $F(x_1, \ldots, x_n, \gamma, 1, y) = 1$, откуда и следует, что $f(x_1, \ldots, x_n, y) = 1$, ибо Γ_f есть проекция I-уровня F. Если $\gamma = 1$ больше проверять нечего.

Пусть $\gamma > 1$. Обращение в I k-го сомножителя в $\prod_{k=1}^{\gamma-1}$ дает тогда:

$$\psi(Gd(k,t)) = 1 \Rightarrow Gd(k,t) \geq 2$$

$$F_k = 1 \Rightarrow Gd(k,t) = f(x_1, \ldots x_n, k) \geq 2$$

Это доставляет треубемое.

<u>Включение $\Gamma_g \subset pr(G=1)$</u>. Пусть $(x_1, \ldots, x_n, \gamma) \in \Gamma_g$ Мы должны подобрать значения остальных координат y, t, t_1 так, чтобы следать все сомножители в соответствующей точке равными I.

Прежде всего, $(x_1, \ldots, x_n, \gamma, 1) \in \Gamma_f$ согласно определению g. Поднимая эту точку с Γ_f на I-уровень F, найдем нужное значение y. В случае $\gamma = 1$ значения t, t_1 можно взять любыми.

Пусть $\gamma > 1$. Наидем тогда t из системы уравнений

$$Gd(k,t) = f(x_1, \ldots, x_n, k); \quad 1 < k \leq \gamma - 1$$

(Правые части существуют в силу спределения $\mathcal{D}(g)$).

Наконец, при каждом $k \le y-1$ поднимем точку

$$(x_1, \ldots, x_n, k, Gd(k,t)) \in \Gamma_f$$

до точки на $F=1$ с дополнительной координатой $y^{(k)}$, после чего найдем t_1 из системы уравнений

$$Gd(k,t) = y^{(k)}, \quad 1 \le k \le y-1$$

Это обратит в единицу все сомножители в $\prod_{k=1}^{y-1}$.

$\psi(Gd(k,t)) = 1$, потому что $Gd(k,t) = f(x_1, \ldots x_n, k) \geqslant 2$ при $k \le y-1$

$$F_k = F(x_1, \ldots, x_n, k, Gd(k,t), Gd(k,t_1)) = 1$$

по определению t, t_1.

4.II. Устойчивость относительно рекурсии.

Нам осталось провести последний этап доказательства теоремы 4.3.

Пусть f, g – частичные функции от n, $n+2$ переменных соответственно, а h – функция от $n+1$ переменной, которая получается из них с помощью рекурсии:

$$h(x_1, \ldots, x_n, 1) = f(x_1, \ldots x_n)$$
$$h(x_1, \ldots x_n, k+1) = g(x_1, \ldots, x_n, k, h(x_1, \ldots x_n, k))$$

Мы должны установить, что если Γ_f, Γ_g примитивно перечислимы, то и Γ_h примитивно перечислим.

Пусть F, G – примитивно рекурсивные функции, I-уровни которых проектируются на Γ_f, Γ_g соответственно:

$$\varphi = f(x_1, \dots, x_n) \Longleftrightarrow \exists y / F(x_1, \dots, x_n, \varphi, y) = 1$$

$$\psi = g(x_1, \dots, x_{n+2}) \Longleftrightarrow \exists z / G(x_1, \dots, x_{n+2}, \psi, z) = 1$$

(как в п. 4.10 достаточно ограничиться случаем, когда коразмерность проекции равна I).

Построим явно функцию H, I-уровень которой проектируется на Γ_h. Ее аргументами будут $x_1, \dots, x_{n+1}, \eta$; t, t_1 (η – аргумент, который станет значением h). Положим:

$$\chi(1) = 1, \quad \chi(x) = 2 \quad \text{при} \quad x \geq 2$$

$$G_k = G(x_1, \dots, x_n; k-1; Gd(k-1, t)\, Gd(k, t)\, Gd(k, t_1))$$

$$H = F(x_1, \dots, x_n, Gd(1, t), y) \cdot \chi\left[\left(\eta - Gd(x_{n+1}, t)\right)^2 + 1\right] \prod_{k=2}^{x_{n+1}} G_k$$

(Мы считаем, что $\Pi = 1$, если $x_{n+1} = 1$). Как в п. 4.10 легко проверяется, что H примитивно рекурсивна.

Включение $pr(H=1) \subset \Gamma_h$. Пусть $(x_1, \ldots, x_{n+1}, \eta, y, t, t_1)$ – точка на $H=1$. Мы должны проверить, что $h(x_1, \ldots, x_{n+1}) = \eta$.

Так как второй сомножитель равен I, получаем прежде всего: $\eta = Gd(x_{n+1}, t)$.

Если к тому же $x_{n+1} = 1$, то равенство 1 первого сомножителя H дает с учетом предыдущего:

$$\eta = Gd(1,t) = f(x_1, \ldots x_n) = h(x_1, \ldots, x_n, 1)$$

Пусть теперь $x_{n+1} > 1$. В таком случае из равенства $G_k = 1$ находим при всех $2 \le k \le x_{n+1}$

$$Gd(k,t) = g(x_1, \ldots, x_n, k-1, Gd(k-1,t))$$

а из равенства $F=1$ и определения h

$$Gd(1,t) = f(x_1, \ldots x_n) = h(x_1, \ldots, x_n, 1)$$

Поднимаясь по k от $k=1$ до $k = x_{n+1}$ и пользуясь рекурсивным определением h, убеждаемся индукцией по k, что $Gd(k,t) = h(x_1, \ldots, x_n, k)$ и, в частности,

$$\eta = Gd(x_{n+1}, t) = h(x_1, \ldots, x_{n+1})$$

Включение $\Gamma_h \subset pr(H=1)$. Дана точка

$$(x_1, \ldots, x_{n+1}, \eta = h(x_1, \ldots x_{n+1})) \in \Gamma_h$$

Мы должны подобрать такие значения y, t, t_1, чтобы обратить H в I.

Если $x_{n+1} = 1$, выберем t так, чтобы $Gd(1,t) = h(x_1, \ldots, x_n, 1) = f(x_1, \ldots x_n)$. После этого поднимем точку $(x_1, \ldots, x_n, Gd(1,t)) \in \Gamma_f$ до точки на $F = 1$; это даст нужное значение y; t_1 можно выбирать как угодно.

Пусть, наконец, $x_{n+1} > 1$. Сначала выберем как решение системы уравнений:

$$Gd(1,t) = f(x_1, \ldots, x_n) = h(x_1, \ldots, x_n, 1)$$

$$Gd(k,t) = h(x_1, \ldots x_n, k) - g(x_1, \ldots x_n, k-1, Gd(k-1,t))$$

$$2 \le k \le x_{n+1}$$

Затем, подняв точку $(x_1, \ldots, x_n, Gd(1,t)) \in \Gamma_f$ на I-уровень F, отыщем y. Это обратит в I первые два сомножителя H.

После этого поднимем точки $(2 \le k \le x_{n+1})$

$$(x_1, \ldots, x_n, k-1, Gd(k-1,t), Gd(k,t)) \in \Gamma_g$$

на уровень G, дооавив координаты $z^{(k)}$, и решим относительно t_1 систему уравнений

$$Gd(k_1, t_1) = z^{(k)}, \quad 2 \le k \le x_{n+1}$$

3-1978

Это обеспечивает обращение в I сомножителей G_K.

Доказательство теоремы 4.3. окончено.

4.12. Объяснение термина "перечислимое множество".

Теорема 4.3. показывает, что если E перечислимо, то существует программа, "порождающая E" (ср. п. 4.1). Действительно, пусть E – проекция на первые n координат I-уровня примитивно рекурсивной функции $F(x_1, \ldots x_n, y)$. Порождающая E программа должна перебирать векторы $(x_1, \ldots x_n, y)$ в каком-нибудь порядке, вычислять F и подавать на выход $(x_1, \ldots, x_n)$ в том и только том случае, когда значение F равно I. В отличие от "распознавающей" программы, типа описанной в § I, которая может навечно застрять на элементе, не принадлежащем E, порождающая программа рано или поздно выпишет любой элемент E и ничего кроме них. Однако, если E пусто или конечно, мы может никогда этого не узнать.

В заключение этого параграфа мы обсудим свойства так называемых разрешимых множеств.

4.13. Определение. Множество $E \subset (Z^+)^n$ называется разрешимым, если оно перечислимо и его дополнение перечислимо.

(Одним из центральных результатов теории состоит в доказательстве того, что существуют перечислимые, но не разрешимые множества. Мы не успеем привести доказательство по недостатку времени; но этот результат тесно связан с теоремой Гёделя о неполноте, которая будет доказана довольно подробно).

4.14. Теорема. Следующие три класса множеств совпадают:

а) множества, характеристическая функция которых (частично) рекурсивна;

б) множества уровня всюду определенных частично рекурсивных функций;

в) разрешимые множества.

Доказательство. Соотношения а) = б) $\subset$ в) очевидны из уже доказанного. Поэтому остается проверить включение в) $\subset$ а).

Пусть $E \subset (Z^+)^n$ – разрешимое множество, E' – его дополнение. По определению, $E = \Phi(f)$, $E' = \Phi(f')$ для некоторых частично рекурсивных функций f, f'. Можно даже считать, что $f = 1$, $f' = 2$ (там, где они определены). Рассмотрим $\Gamma_f \cup \Gamma_{f'} \subset (Z^+)^n \times (Z^+)$ Очевидно, это объединение является графиком Γ_g характеристической функции g множества E. Из леммы 4.8 и дальнейшего обсуждения ясно, что Γ_g перечислим вместе с Γ_f и $\Gamma_{f'}$. Поэтому частичная рекурсивность g будет вытекать из следующего результата, который представляет самостоятельный интерес.

4.15. Предложение. Для того, чтобы частичная функция g из $(Z^+)^n$ в Z^+ была частично рекурсивной, необходимо и достаточно, чтобы ее график Γ_g был перечислим.

Доказательство. Необходимость уже установлена.

Проверим достаточность. Так как Γ_g перечислим, существует такая примитивно рекурсивная функция $G(x_1, \ldots x_n, y, z)$ (см. п. 4.10), что

Γ_g = проекция на $(x_1, \dots, x_n, y)$ I-уровня G.

Положим $H(x_1, \dots, x_n, u) = G(x_1, \dots, x_n, t_1^{(2)}(u), t_2^{(2)}(u))$

где $u \longmapsto (t_1^{(2)}(u), t_2^{(2)}(u))$ - примитивно рекурсивный изоморфизм $\mathbb{Z}^+ \xrightarrow{\sim} (\mathbb{Z}^+)^2$, описанный в пп. 4.5. и 4.7. Очевидно, H примитивно рекурсивна. Наконец, положим

$$h(x_1, \dots, x_n) = \min u \mid H(x_1, \dots, x_n, u) = 1$$

Это частично рекурсивная, область определения которой совпадает с $\mathcal{D}(g)$ и которая, как легко видеть, позволяет вычислить g

$$g(x_1, \dots, x_n) = t_1^{(2)}(h(x_1, \dots, x_n))$$

Тем самым, g достаточно рекурсивна, чем завершается доказательство предположения 4.I5 и теоремы 4.I4.

4.I6. <u>Следствие</u>. Для любой частично рекурсивной функции g существует описание, в котором операция μ применяется один раз.

4.I7. <u>Следствие</u>. Если частично рекурсивная функция g всюду определена, то существует ее описание $g_1, \dots, g_N = g$ в котором все функции всюду определены.

Действительно, описание, конец которого (начиная с G), построен в п. 4.I5, обладает этим свойством.

§ 5. <u>Формализация арифметики (результаты)</u>.

5.I. Ближайшие параграфы будут посвящены классической теореме логики - теореме Геделя о неполноте формальных систем.

В ней органически сочетаются идеи теории формальных языков и теории рекурсивных функций. Чтобы возможно более выпукло показать идею теоремы Геделя, мы проведем изложение по следующему плану:

а) <u>формализация арифметики</u>. Мы напомним структуру языка арифметики $L_1 A_2$ и сформулируем основной результат об описании разрешимых множеств на этом языке.

б) <u>Арифметизация формализма</u>. Мы опишем геделевскую нумерацию формул, термов и выводов в языке $L_1 A_2$ и сформулируем основной результат о разрешимости множества пар номеров (формула - ее вывод) специального вида.

в) <u>Теорема Геделя</u>. Мы сформулируем и докажем эту теорему, опираясь на результаты а) и б).

После этого доказательствам а) и б) будут посвящены отдельные параграфы.

5.2. <u>Алфавит $L_1 A_1$</u>. Он состоит из счетного множества символов переменных $X_1, X_2, \ldots$ константы $\bar{0}$; символов операций $', +, \cdot,$ и символа отношения $=$; скобок, связок и кванторов.

Стандартная интерпретация в $\mathbb{Z}$: интерпретируем $\bar{0}$ как 0 , штрих как прибавление единицы; остальное ясно.

Удобные сокращения:

$$\bar{n} := \text{терм}((\bar{0})', \ldots,)' \quad (\underline{\underline{n}} \text{ штрихов}, \ n \in \mathbb{Z}^+)$$

$$s \neq t := \neg(s = t)$$

$$t \leq s := \exists u \, (t + u = s)$$

Аксиомы A_1 A_2. Это логические аксиомы A_{x_0} и A_{x_1}, аксиомы равенства (см. первую часть курса), а также следующие собственные аксиомы.

А. Аксиома сложения и умножения (ср. 3.2 и 3.3).

$$x_1' = x_2' \longrightarrow x_1 = x_2 \;;$$

$$\bar{0} \neq x_1' \;;$$

$$x_1 + \bar{0} = x_1 \;;$$

$$x_1 + x_2' = (x_1 + x_2)' \;;$$

$$x_1 \cdot \bar{0} = \bar{0} \;;$$

$$x_1 \cdot (x_2') = (x_1 \cdot x_2) + x_1 \;;$$

Б. Схема аксиом индукции.

$$P(\bar{0}) \longrightarrow (\forall X (P(X) \rightarrow P(X')) \rightarrow \forall X\, P(X))$$

где $P(X)$ – любая формула со свободной переменной X.

Напомним, что если $P(X)$ интерпретировать как " обладает свойством P ", то формальная аксиома индукции будет относиться лишь к счетному множеству свойств, выразимых на языке $L_1 A_2$, тогда как в интуитивной математике аксиома индукции относится к любому из $2^{\aleph_0}$ свойств (т.е. подмножеств $\mathbb{Z}^+ \cup \{0\}$).

За остальными определениями общих понятий, относящихся к языкам L_1, мы отсылаем читателя к первой части курса.

5.3. Определение. Множеотво $E \subset (\mathbb{Z}^+)^n$ называется выразимым (в $L_1 A_2$), если существует такая формула $P(X_1, \ldots, X_n)$ с $\underline{\underline{n}}$ свободными переменными, что для любых

целых $k_1, \dots, k_n \geq 0$ имеем:

$$(k_1, \dots, k_n) \in E \Leftrightarrow A_1 A_2 \vdash P(\bar{k}_1, \dots, \bar{k}_n)$$

$$(k_1, \dots, k_n) \notin E \Leftrightarrow A_1 A_2 \vdash \neg P(\bar{k}_1, \dots, \bar{k}_n)$$

5.4. Лемма о выразимости. Следующие два класса множеств $E \subset (\mathbb{Z}^+)^n$ (всевозможные n) совпадают:

а) Разрешимые.

б) Выразимые в $L_1 A_2$.

Доказательство мы отложим до § 8. Вот интуитивные пояснения.

б) $\subset$ а). Пусть E – множество, P – выражающая его формула. Мы хотим написать программу, распознающую элементы из E и из дополнения к E. Она может быть устроена так: после подачи на вход $(k_1, \dots, k_n)$ программа перебирает (скажем, в алфавитном порядке) конечные последовательности символов языка с пробелами; проверяет их на свойство "быть выводом $P(\bar{k}_1, \dots, \bar{k}_n)$ или $\neg P(\bar{k}_1, \dots, \bar{k}_n)$" и подает на выход I или 2, когда добирается до такого вывода.

а) $\subset$ б). Это – просто утверждение о том, что наш формальный язык настолько богат, что процесс вычисления рекурсивной функции f в точке $(k_1, \dots, k_n)$, приводящий к равенству $f(k_1, \dots, k_n) = 1$, можно превратить в формальный вывод некоторой формулы $P(\bar{k}_1, \dots, \bar{k}_n)$.

Для доказательства теоремы Геделя нужна только вторая часть леммы.

§ 6. Арифметизация формализма (результаты).

6.I. Пусть M - некоторое множество. Нумерацией мы назовем взаимно однозначное соответствие между M и некоторым подмножеством $\mathcal{Z}^+$; элементу $m \in M$ ставится в соответствие его номер. В важных для нас случаях M будет состоять из последовательностей символов языка $L_1 A_2$ (или выражений языка). Тогда имеет смысл говорить о вычислимой нумерации, подразумевая под этим существование программы, которая по выражению вычисляет его номер, а по целому числу узнает, является ли оно номером выражения, и если да, то какого.

Мы считаем в этом параграфе, что раз навсегда выбраны и зафиксированы три вычислимых нумерации:

в) символов языка $L_1 A_2$;

б) выражений (конечных последовательностей символов)

в) конечных последовательностей выражений.

Их реальная конструкция будет дана в § 9.

6.2. Определение. Пусть $a \in \mathcal{Z}^+$ - такое целое число, что выражением с номером $\underline{\underline{a}}$ является некоторая формула $P(X_1)$ языка $L_1 A_2$, содержащая фиксированную переменную X_1 в качестве единственной свободной переменной.

Тогда "диагонализацией формулы номер $\underline{\underline{a}}$ " называется формула $P(\bar{a})$.

(Напомним, что $\bar{a}$ - "цифра" в языке $L_1 A_2$, обозначающая число $\underline{\underline{a}}$).

6.3. Лемма о разрешимости. Пусть $\mathfrak{S}$ – некоторое множество формул языка $L_1 A_2$, содержащее A_1 A_2 и имеющее разрешимое множество номеров. Тогда следующее множество $G \subset \mathcal{X}^+ \times \mathcal{X}^+$ разрешимо:

$$(a, b) \in G \Leftrightarrow \left\{ \begin{array}{l} b \text{ есть номер вывода из } \mathfrak{S} \\ \text{диагонализации формулы номер } \underline{\underline{a}} \end{array} \right\}$$

Интуитивные пояснения. Программа, распознающая элементы из G, может работать так.

После подачи на вход $(a, b) \in (\mathcal{X}^+)^2$ программа выписывает выражение номер $\underline{\underline{a}}$ и проверяет, формула ли это (возможность автоматического синтаксического анализа заложена в определение формул), если да, входит ли туда свободно только X_1; если да, строит диагонализацию формулы.

Затем программа выписывает последовательность выражений номер $\underline{\underline{b}}$, проверяет, является ли последнее выражение построенной ранее диагонализацией. Если да, она проверяет, являются ли все остальные выражения формулами. Если и это так, остается проверить, является ли эта последовательность выводом из $\mathfrak{S}$. Для этого нужно перебирать все формулы последовательности по очереди. Синтаксический анализ покажет, получается ли очередная формула применением MP или Gen из предыдущих, если нет, остается лишь проверить, принадлежит ли она $\mathfrak{S}$, для этого нужно вычислить ее номер, пользуясь вычислимостью номеров $\mathfrak{S}$.

§ 7. Теорема Геделя о неполноте.

7.1. Система аксиом арифметики, формализованная в $L_1 A_2$, была результатом длительного анализа наших представлений о целых числах. Долгое время казалось естественным, что она содержит всю "интуитивно очевидную" информацию, из которой дедуктивными рассуждениями можно получить любую теорему теории чисел. Отголоском этих представлений остаются непрекращающиеся в среде специалистов по теории чисел попытки получить "элементарно" различные результаты, которые формулируются элементарно, но доказываются, скажем, аналитически (с помощью дзета-функции, модулярных форм ...) или вообще "не финитно" (оценки чисел решения сравнений по А.Веймо). Хотя время от времени такие попытки удаются, теорема Геделя показывает, что по крайней мере некоторые теоретико-числовые истины нельзя получить таким путем: существуют замкнутые формулы $L_1 A_2$, истинные в стандартной интерпретации, но не выводимые из $A_x A_2$.

Кстати, тот же результат остается верным, если как угодно расширить систему аксиом, лишь бы аксиомы оставались алгоритмически распознаваемыми (иначе можно было бы взять в качестве аксиом все формулы, истинные в стандартной интерпретации).

7.2. Чтобы точно сформулировать теорему Геделя, рассмотрим множество $\mathcal{E} \supset A_x A_2$ формул языка $L_1 A_2$, обладающее двумя свойствами:

а) Множество номеров $\mathcal{E}$ разрешимо.

б) Если $P(X)$ – такая формула, что $\mathcal{E} \vdash \exists X \neg P(X)$, то какая-нибудь из формул $P(\bar{n})$ $(n = 0, 1, 2, 3, \ldots)$ невыводима из $\mathcal{E}$.

Свойство б) называется ω - непротиворечивостью. Если $\mathcal{E} \supset A_x A_2$ ω - непротиворечиво, то и $\mathcal{E}$ непротиворечиво. Действительно, все формулы $\neg(\bar{0} = \bar{n}')$ выводимы из $A_x A_2$; значит формула $\exists x(\bar{0} = \bar{x}')$ не может быть выводима из $\mathcal{E}$ в силу ω - непротиворечивости, а если бы $\mathcal{E}$ было противоречиво, из него можно было бы вывести что угодно.

С другой стороны, ω - непротиворечивость - вполне естественное свойство любой приличной системы аксиом: произвольное множество формул, истинных в стандартной интерпретации, очевидно, ω - непротиворечиво.

7.3. Теорема. Если множество формул $\mathcal{E} \supset A_x A_2$ удовлетворяет условиям п. 7.2 а), б), то существует такая замкнутая формула $\mathcal{U}$, что как $\mathcal{U}$, так и $\neg\mathcal{U}$ невыводимы из $\mathcal{E}$.

Кроме того, $\mathcal{U}$ истинна в стандартной интерпретации.

Доказательство. а) Конструкция $\mathcal{U}$. Рассмотрим множество $G \subset \mathbb{Z}^+ \times \mathbb{Z}^+$, построенное в лемме о разрешимости 6.3 :

$(a, b) \in G \Leftrightarrow$ " b есть номер вывода из $\mathcal{E}$ диагонализации формулы номер a ".

В силу леммы о выразимости 5.4 существует такая формула $Q(x_1, x_2)$ с двумя свободными переменными, что

$$(a, b) \in G \Leftrightarrow A_x A_2 \vdash Q(\bar{a}, \bar{b})$$

$$(a, b) \notin G \Leftrightarrow A_x A_2 \vdash \neg Q(\bar{a}, \bar{b})$$

Рассмотрим формулу $\forall x_2 \neg Q(x_1, x_2)$ и обозначим через c – ее номер. Наконец, положим:

$\mathcal{U}$: формула $\forall x_2 \neg Q(\bar{c}, x_2) =$

= диагонализация формулы номер $\underline{\underline{c}}$.

б) <u>Стандартная интерпретация $\mathcal{U}$</u> . По определению стандартной интерпретации имеем:

$\mathcal{U}$ истинна в стандартной интерпретации $\Leftrightarrow$

- нет такого d , что $Q(\bar{c}, \bar{d})$ истинна
- нет такого d , что $Q(\bar{c}, \bar{d})$ выводима из $A_x A_2$
- нет такого d , что $(c\, d) \in G$ (по определению G
- нет вывода из $\mathcal{E}$ диагонализации формулы номер $\underline{\underline{c}}$
- нет вывода $\mathcal{U}$ из $\mathcal{E}$.

(Обратите внимание на эквивалентность второй и третьей строк: если все $Q(\bar{c}, \bar{d})$ не выводимы из A_2 , то все $(\bar{c}, \bar{d}) \notin G$ так что $\neg Q(\bar{c}, \bar{d})$ выводимы из A_2 , и значит, $Q(\bar{c}, \bar{d})$ не истинны.

Итак, формула $\mathcal{U}$ утверждает: "я невыводима!". Следовательно, когда мы докажем, что она действительно не выводима, мы убедимся, что она истинна в стандартной интерпретации.

в) <u>$\mathcal{U}$ невыводима</u>. Действительно, предположим, что $\mathcal{U}$ выводима из $\mathcal{E}$; пусть k – номер вывода.

Тогда $(c, k) \in G \Rightarrow \mathcal{E} \vdash Q(\bar{c}, \bar{k})$

Кроме того, $\mathcal{E} \vdash \forall x_2 \neg Q(\bar{c}, x_2)$ откуда по МР и логической аксиоме $\forall x\, P(x) \rightarrow P(t)$ получим $\mathcal{E} \vdash \neg Q(\bar{c}, \bar{k})$. Но $Q(\bar{c}, \bar{k})$ и $\neg Q(\bar{c}, \bar{k})$ не могут быть выводимы из $\mathcal{E}$ одновременно, ибо $\mathcal{E}$ непротиворечива.

г) $\neg \mathcal{U}$ невыводима. Действительно, предположим, что $\mathcal{E} \vdash \neg \mathcal{U}$. Пользуясь явным видом $\mathcal{U}$ и аксиомой о перестановке $\neg$ и $\forall$, получаем $\mathcal{E} \vdash \exists x_2 Q(\bar{c}, x_2)$

С другой стороны, мы уже знаем, что $\mathcal{U}$ невыводима, так что $(c, n) \in G$ для всех n (ибо $\mathcal{U}$ - диагонализация формулы номер $\underline{c}$). Поэтому $A_x A_2 \vdash \neg Q(\bar{c}, \bar{n})$ для всех n. Поскольку $\mathcal{E} \supset A_x A_2$, одновременная выводимость $\exists x_2 Q(\bar{c}, x_2)$ и $\neg Q(\bar{c}, \bar{n})$ противоречит ω - непротиворечивости $\mathcal{E}$.

7.4. Одной из самых удивительных особенностей формулы Геделя $\underline{\mathcal{U}}$ является то обстоятельство, что хотя мы устанавливаем ее невыводимость из наличного запаса аксиом $\mathcal{E}$, ее содержательная истинность для нас очевидна. Мы готовы присоединить ее к $\mathcal{E}$ в качестве новой аксиомы; но это изменит $\mathcal{E}$, увеличит количество выводимых из $\mathcal{E}$ формул, изменит тем самым G, а вместе с G и формулу Q и, значит, определяемую по Q формулу $\mathcal{U}$: появится новая формула $\mathcal{U}'$, невыводимая из $\mathcal{E} \cup \{\mathcal{U}\}$, в содержательной истинности которой, однако, мы по-прежнему не сомневаемся.

Принятие стандартной интерпретации есть неформальный акт мышления, с помощью которого мы каждый раз "угадываем" (не выводим!) истинность формулы Геделя. Если записать $\mathcal{U}$ в виде обычного утверждения о целых числах, это будет очень длинная арифметическая теорема странного вида, прямое доказательство которой, скорее всего, представит огромные трудности и заведомо потребует введения новых (по сравнению с $\mathcal{E}$) принципов.

Можно думать, что типологически такой акт мышления родствен тем, с которыми связаны все вообще крупные математические открытия (в том числе открытие Геделя). Феферман доказал замечательный результат о том, что <u>все</u> истинные формулы арифметики можно вывести из аксиом и формул геделевского типа.

§ 8. <u>Формализация арифметики (доказательства)</u>.

8.1. Этот параграф посвящен (сокращенному) доказательству леммы о **выразимости**, точнее, той ее части, которая нужна для теоремы Геделя: <u>разрешимые множества выразимы</u>.

В доказательстве удобнее рассматривать вместо множеств функции, так что мы начнем с формулировки параллельного свойства для функции.

8.2. <u>Определение</u>. Всюду определенная функция $f: (\mathbb{Z}^+)^n \to \mathbb{Z}^+$ называется представимой (в $L_1 A_2$), если существует такая формула $P(x_1, \ldots, x_{n+1})$, что

$$(k_1, \ldots, k_{n+1}) \in f \Leftrightarrow \begin{cases} A_2 A_2 \vdash P(\bar{k}_1, \ldots, \bar{k}_n, \bar{k}_{n+1}); \\ A_2 A_2 \vdash \exists! x_{n+1} P(\bar{k}_1, \ldots, \bar{k}_n, x_{n+1}) \end{cases}$$

Здесь $\exists! x P x$ ("существует единственный x со свойством P") есть сокращенная запись для формулы

$$\exists x P(x) \wedge \forall x \forall y (P(x) \wedge P(y) \to x = y)$$

8.3. <u>Предложение</u>. Рекурсивные функции представимы в $L_1 A_2$.

8.4. <u>Вывод леммы о выразимости из предложения 8.3</u>.

Пусть $E \subset (\mathbb{Z}^+)^n$ – некоторое разрешимое множество. По предложению 4.13 его характеристическая функция g рекурсивна и, значит, по предложению 8.3. она представлена некоторой формулой $P(x_1, \dots, x_{n+1})$

Положим $Q(x_1, \dots, x_n) = P(x_1, \dots, x_n, \bar{1})$ и покажем, что E представлено формулой Q. Для этого достаточно доказать, что

$$(k_1, \dots, k_n) \in E \Rightarrow A_x A_2 \vdash Q(\bar{k}_1, \dots, \bar{k}_n)$$

$$(k_1, \dots, k_n) \notin E \Rightarrow A_x A_2 \vdash \neg Q(\bar{k}_1, \dots, \bar{k}_n)$$

Первая импликация немедленно следует из первой импликации в определении представимости g. Вторая требует более окольных рассуждений:

$$(k_1, \dots, k_n) \notin E \Rightarrow g(k_1, \dots, k_n) = 2 \Rightarrow$$
$$A_x A_2 \vdash P(\bar{k}_1, \dots, \bar{k}_n, 2)$$

Кроме того, по второму условию представимости и транзитивности

$$Q \wedge R \to Q$$

$$A_x A_2 \vdash \forall x \forall y \, (P(\bar{k}_1, \dots, \bar{k}_n, x) \wedge P(\bar{k}_1, \dots, \bar{k}_n, y) \to x = y)$$

Дважды применяя аксиому $\forall x G(x) \to G(t)$ и MP, получаем

$$A_x \vdash P(\bar{k}_1, \dots, \bar{k}_n, \bar{1}) \wedge P(\bar{k}_1, \dots, \bar{k}_n, \bar{2}) \to$$
$$\to \bar{1} = \bar{2}$$

Тавтология $(Q \to R) \to (\neg R \to \neg Q)$ и МР дают

$$A_x A_2 \vdash \neg(\bar{1} = \bar{2}) \to \neg(P(\ ,\bar{1}) \wedge P(\ ,\bar{2}))$$

Формула $\neg(\bar{1} = \bar{2})$ выводима из аксиом; кроме того, имеется тавтология $\neg(P \wedge Q) \to (P \to \neg Q)$; наконец, мы уже знаем, что $P(\ ,\bar{2})$ выводима из $A_x A_2$

Окончательно получаем

$$A_x A_2 \vdash \neg P(\bar{k}_1, \ldots, \bar{k}_n, \bar{1})$$

что и является вторым условием выразимости. ■

Мы провели эту часть доказательства довольно подробно, чтобы напомнить читателю о технике формального вывода. Если в формулировке предыдущих определений и лемм заменить выводимость из $A_x A_2$ содержательной истинностью (в стандартной интерпретации), то все доказательство стало бы интуитивно прозрачнее и короче; основной технической работы требует перевод этого доказательства на формальный язык.

Мы опустим такой перевод в оставшейся части параграфа, отсылая читателя за подробностями к книге Мендельсона (стр. 133 и дальше).

8.5. <u>Доказательство предложения 8.3 (план)</u>.

Мы покажем, что простейшие функции представимы и что применение элементарных операций сохраняет представимость. Напомним, что согласно следствию 4.14 из рекурсивной функции имеется описание, состоящее из всюду определенных функций. Поэтому все фигурирующие ниже функции предполагаются всюду определенными.

а) Простейшие функции — Представляющие формулы

$SUC\ x_1$	$x_2 = x_1'$
$1^{(n)}$	$(x_1 = x_1) \wedge \ldots \wedge (x_n = x_n) \wedge (x_{n+1} = 1)$
$pr_i^{(n)}$	$(x_1 = x_1) \wedge \ldots \wedge (x_n = x_n) \wedge (x_{n+1} = x_i)$

б) Устойчивость относительно композиции. Пусть даны

Функции	Представляющие формулы
$f(X_1, \ldots, X_m)$	$Q(X_1, \ldots, X_m, X_{m+1})$
$g_1(X_1, \ldots, X_n)$	$P_1(X_1, \ldots, X_n, X_{n+1})$
$\vdots$	$\vdots$
$g_m(X_1, \ldots, X_n)$	$P_m(X_1, \ldots, X_n, X_{n+1})$

Тогда функция $f(g_1, \ldots, g_m)$ представлена формулой

$$\exists y_1, \ldots, \exists y_m (P_1(X_1, \ldots, X_n, y_1) \wedge \ldots \wedge P_m(X_1, \ldots, X_n, y_m) \wedge$$
$$\wedge\ Q(y_1, \ldots, y_m, X_{n+1})$$

здесь связанные переменные $y_1, \ldots, y_m$ суть "временные обозначения" для значений $g_1, \ldots, g_m$ в точке $x_1, \ldots, x_n$, которые нужно вычислить, прежде чем подставить их в f в качестве аргументов.

4-1978

(Мы обозначаем одними и теми же буквами аргументы функций f, g: в метаязыке и переменные в L, H_2 ; в этом контексте не может возникнуть путаницы).

в) <u>Устойчивость относительно μ -операции</u>.

Пусть функция $f(x_1, \ldots, x_{n+1})$ представлена формулой $P(x_1, \ldots, x_{n+2})$. Тогда функция

$$g(x_1, \ldots x_n) = \min x_{n+1} \mid f(x_1, \ldots, x_{n+1}) = 1$$

представлена формулой

$$P(x_1, \ldots, x_{n+1}, \bar{1}) \wedge \forall y (y < x_{n+1} \rightarrow \neg P(x_1, \ldots x_n, y$$

г) <u>Устойчивость относительно рекурсии</u>. Формальные выводы в этой части доказательства особенно длинны и нетривиальны, да и структура представляющей формулы не очевидна. Пусть функция $h(x_1, \ldots, x_{n+1})$ определена рекурсией по последнему аргументу, исходя из функций $f(x_1, \ldots, x_n)$ и $g(x_1, \ldots, x_n, x_{n+1}, x_{n+2})$. Тогда для вычисления мы должны вычислить <u>переменное количество</u> $x_{n+2} - 1$ промежуточных значений $h(x_1, \ldots, x_n, k)$, $k < x_{n+2}$ Непосредственно ввести для них вспомогательные обозначения, как в пункте б), мы поэтому не можем.

Естественная идея состоит в том, чтобы воспользоваться для имитации последовательности $h(x_1, \ldots, x_n, k)$, $k < x_{n+2}$ функцией Геделя $\text{чет}(1 + x_2 x_3, x_1)$.

Итак, пусть f представлена формулой P ; g - формулой Q ; можно проверить, что $\text{чет}(1 + x_2 x_3, x_1)$ представлена формулой

$$R_k(x_1, x_2, x_3, x_4) := \exists w\,(x_1 = (1 + x_2 x_3)w +$$
$$+ x_4 \wedge (1 \le x_4) \wedge x_4 \le 1 + x_2 x_3)$$

Формула, представляющая g, выглядит так:

$$\exists u\, \exists v\, [(\exists \omega\, R_m(u, v, 1, \omega) \wedge P(x_1, \ldots, x_n, \omega)) \wedge$$
$$\wedge R_m(u, v, x_{n+1}, x_{n+2}) \wedge \forall \omega (\omega < x_{n+1} \to \exists y\, \exists z\, (R_m(u, v, \omega, y) \wedge$$
$$\wedge R_m(u, v, \omega', z) \wedge Q(x_1, \ldots, x_n, \omega, y, z)$$

Читателю следует, по крайней мере, проверить, что эта формула становится содержательно истинной после подстановки в нее $(\bar{K}_1, \ldots, \bar{K}_{n+1}) \in \Gamma_h$

Указания. (u, v) – параметры в функции Геделя, позволяющие имитировать ее промежуточные значения h; w – имя переменной, по которой происходит рекурсия.

§ 9. Нумерация.

9.I. В этом параграфе мы проведем подготовку к конструкции конкретной нумерации алфавита, выражений и последовательностей выражений языков L_1, свойства которой будут использованы в § I0 для доказательства леммы о разрешимости и дальнейших выводов из возможности арифметизации.

9.2. Пусть A – некоторое счетное множество. Положим $S(A) = A \cup A^2 \cup A^3 \ldots$. Элементы из $A^p \subset S(A)$ мы отождествляем с последовательностью $(a_1, \ldots, a_p)$ элементов A длины p.

Напомним, что нумерацией A называется взаимно одно-

значное соответствие $N : A \to Z^+$: $N(a)$ есть <u>номер</u> a ; $N_1^{-1}(n)$ есть элемент A с номером n . В дальнейшем мы ограничимся рассмотрением таких нумераций, для которых $N(A) = Z^+$

9.3. <u>Конструкция нумерации $S(A)$ по нумерации A</u> .

Построим отображение $N_1 : S(A) \to Z^+$, положив

$$N_1(a_1, \ldots, a_p) = \sigma^{(2)}(p, \sigma^{(p)}(N(a_1), \ldots, N(a_p))).$$

Нетрудно убедиться, что N_1 является нумерацией (см. а. 4.7). Пусть, далее, $(a_1, \ldots, a_p)$ и $(b_1, \ldots, b_q)$ - два элемента $S(A)$. N_1 - номер последовательности $(a_1, \ldots, a_p, b_1, \ldots, b_q) \in S(A)$ однозначно определяется N_1 -номерами $(a_1, \ldots, a_p)$ и $(b_1, \ldots, b_q)$. Поэтому существует функция $Z^+ \times Z^+ \to Z^+ : (m, n) \mapsto m * n$ со свойствами

$$N_1(a_1, \ldots, a_p, b_1, \ldots, b_q) = N_1(a_1, \ldots, a_p) * N_1(b_1, \ldots, b_q).$$

9.4. <u>Предложение</u>. а) Функция $m * n$ рекурсивна.

б) $m * n > \max(m, n)$

<u>Доказательство.</u> а) Начиная с этого места, мы будем ограничиваться установлением того, что многие интересующие нас функции вычислимы в интуитивном смысле слова, оставляя техническую проверку их рекурсивности читателю. Для $m * n$ вычислимость легко установить. В самом деле, будем считать для сокращения записи, что A отождествлено с Z^+ посредством N . Положим также, что для $a_1, \ldots, a_p \in Z^+$

$$\sigma^{(\infty)}(a_1, \ldots, a_p) = \sigma^{(2)}(p, \sigma^{(p)}(a_1, \ldots, a_p))$$

Тогда имеем в обозначениях п. 4.7 :

$$m = \sigma^{(\infty)}(a_1, \ldots, a_p) \Leftrightarrow a_i = t_i^{(t_1^{(2)}(m))}(m), \quad i = 1, \ldots, t_1^{(2)}(m)$$

$$n = \sigma^{(\infty)}(b_1, \ldots, b_q) \Leftrightarrow b_j = t_j^{(t_1^{(2)}(n))}(n), \quad j = 1, \ldots, t_1^{(2)}(n)$$

откуда $m * n = \sigma^{(2)}\left(t_1^{(2)}(m) + t_1^{(2)}(n), \sigma^{(t_1^{(2)}(m) + t_1^{(2)}(n))}\left(t_1^{(t_1^{(2)}(m)}(m), \ldots, t_{t_1^{(2)}(m)}^{(t_1^{(2)}(m)}(m), t_1^{(t_1^{(2)}(n)}(n), \ldots, t_{t_1^{(2)}(n)}^{(t_1^{(2)}(n)}(n)\right)\right)$

и вычислимость $m * n$ становится очевидной.

б) Для доказательства неравенства $m * n > \max(m, n)$ достаточно ограничиться случаем, когда длина $\underline{\underline{m}}$ или $\underline{\underline{n}}$ равна I. Заметим прежде всего, что $\sigma^{(2)}(x, y) \geq \max(x, y)$ и что функции $\sigma^{(i)}$, $i = 1, 2, \ldots \infty$ являются строго возрастающими по любому из своих аргументов.

<u>Неравенство</u> $\sigma^{(\infty)}(a_1, \ldots, a_p, b) > \sigma^{(\infty)}(a_1, \ldots, a_p)$

Имеем

$$\sigma^{(\infty)}(a_1, \ldots, a_p, b) = \sigma^{(2)}(p+1, \sigma^{(p+1)}(a_1, \ldots, a_p, b))$$

$$\sigma^{(\infty)}(a_1, \ldots, a_p) = \sigma^{(2)}(p, \sigma^{(p)}(a_1, \ldots, a_p))$$

Так как $p + 1 > p$ и $\sigma^{(p+1)}(a_1, \ldots, a_p, b) = \sigma^{(2)}(\sigma^{(p)}(a_1, \ldots, a_p), b) \geq \sigma^{(p)}(a_1, \ldots, a_p)$.

получаем требуемое.

<u>Неравенство</u> $\sigma^{(\infty)}(b, a_1, \ldots, a_p) > \sigma^{(\infty)}(a_1, \ldots, a_p)$

Достаточно ограничиться случаем $b = 1$. Имеем:

$$\mathcal{T}^{(\infty)}(1, a_1, \ldots, a_p) = \mathcal{T}^{(2)}(p+1, \mathcal{T}^{(p+1)}(1, a_1, \ldots, a_p))$$

$$\mathcal{T}^{(\infty)}(a_1, \ldots, a_p) = \mathcal{T}^{(2)}(p, \mathcal{T}^{(p)}(a_1, \ldots, a_p))$$

Поэтому достаточно проверить, что $\mathcal{T}^{(p+1)}(1, a_1, \ldots, a_p) \geq \mathcal{T}^{(p)}(a_1, \ldots$
Выражая $\mathcal{T}^{(p+1)}, \mathcal{T}^{(p)}$ **через** $\mathcal{T}^{(2)}$ и $\mathcal{T}^{(p)}, \mathcal{T}^{(p-1)}$ без труда получаем возможность провести индукцию по p. Первый шаг $\mathcal{T}^{(2)}(1, a) \geq a$, очевидно, обоснован. ■

Свойство 9.4 б) будет использоваться всегда так: если последовательность $(a_1, \ldots, a_p)$ входит в $(b_1, \ldots, b_q)$ как часть, то есть если для некоторого i имеем $b_i = a_1$, $b_{i+1} = a_2, \ldots, b_{i+p-1} = a_p$, то N_1 -номер $(b_1, \ldots, b_q)$ строго больше N_1 -номера $(a_1, \ldots, a_p)$

§ 10. Арифметизация формализма (доказательства).

10.1. Пусть L_1 - произвольный формальный язык первого порядка с условием: количество символов операций и отношений в L_1 конечно. Языки $L_1 A_z$ и $L_1 Set$ удовлетворяют этому условию; но его можно было заменить более общим ценой несущественных технических усложнений (доказательств), которые читатель без труда сможет провести сам. Пусть A - алфавит L_1.

Фиксируем нумерацию $N : A \to \mathbb{Z}^+$. Потребуем, чтобы символ $N^{-1}(1)$ был связкой и чтобы множества номеров символов переменных и констант были разрешимы. Построим по N нумерацию N_1 множества выражений $S(A)$ и затем по N_1

нумерацию N_2 множества конечных последовательностей выражений $S(S(A))$ как в § 9.

Мы покажем в этом параграфе возможность "автоматического синтаксического анализа" для языка L_1. Для этого мы будем последовательно строить такие рекурсивные функции, что по их значению на номере выражения мы сможем установить, является ли это выражение термом или формулой, входит ли туда свободно переменная с данным номером и т.п. В конце конструкции мы, в частности, сможем доказать лемму о разрешимости.

10.2. Переменные и константы. Положим прежде всего:

$$Var(k) = \begin{cases} 1, & \text{если } N_1^{-1}(k) \text{ не является выражением, состоящим из одной переменной,} \\ 2 & \text{иначе.} \end{cases}$$

$$Const(k) = \begin{cases} 1, & \text{если } N_1^{-1}(k) \text{ не является выражением, состоящим из одной константы,} \\ 2 & \text{иначе.} \end{cases}$$

Эти функции рекурсивны в силу предположения о нумерации N. Действительно, $N_1^{-1}(k) = \{\text{переменная } x\} \Leftrightarrow k = \sigma^{(\infty)}(1, N(x)) = \frac{1}{2}(N(x)^2 - N(x) + 2)$, а множество N -номеров переменных $\{N(x)\}$ рекурсивно по предположению.

10.3. Термы. Мы покажем, что существует рекурсивная функция $Term(k)$ со свойством:

$$Term(k) = 1 \Leftrightarrow N_1^{-1}(k) \text{ не терм.}$$

Следующий план конструкции с теми или иными вариациями

будет многократно повторяться в дальнейшем. Из определения терма и свойства 9.4 б) ясно, что

$$N_1^{-1}(k) \text{ не терм} \Longleftrightarrow \begin{cases} N_1^{-1}(k) \text{ не терм-константа } (\alpha); \\ \text{не терм-переменная } (\beta); \\ \text{не выражение вида} \\ f(t_1, \ldots, t_r), \text{ где} \\ f \text{ – символ операции ранга } r, \\ t_1, \ldots, t_r \text{ – термы с} \\ N_1\text{-номерами} \leq k-1 \ (\gamma) \end{cases}$$

Мы построим для каждого из условий $(\alpha), (\beta), (\gamma)$ такую функцию от k, что ее обращение в I будет равносильно выполнению соответствующего условия, а затем перемножим все эти функции.

Для условий (α) и (β) достаточно взять $Const(k)$ и $Var(k)$ соответственно. Для условия (γ) положим:

$$T_f(i_1, \ldots, i_r, k) = \min\{(Term(i_1)-1)\ldots(Term(i_r)-1)+1, \\ \delta[(N_1(f) * N_1(() * i_1 * \ldots * i_r * N_1(\,)) - k)^2 + 1]\}$$

где $\delta(1) = 2$, $\delta(X) = 1$ при $X \geq 2$.

Окончательно положим:

$$Term(1) = 1$$

$$Term(k) = Const(k)\, Var(k) \prod_{r \geq 1} \prod_{f \text{ ранга } r} \prod_{\substack{(i_1, \ldots, i_r) \\ i_j \leq k-1}} T_f(i_1, \ldots, i_r, k) \quad \text{при } k \geq 2$$

Вычислимость $Term(k)$ очевидна. Рекурсивность, однако, требует дальнейшей работы, ибо для вычисления $Term(k)$ мы пользуемся <u>всеми</u> вычисленными ранее значениями $Term(1)$, ..., $Term(k-1)$, а не только одним предыдущим. Мы опускаем эту часть.

10.4. <u>Атомарные формулы</u>. Построим рекурсивную функцию $At(k)$ со свойством:

$$At(k) = 1 \Leftrightarrow N_1^{-1}(k) \text{ не атомарная формула.}$$

Атомарные формулы имеют вид $p(t_1, \ldots, t_r)$, где p – отношение ранга r, а $t_1, \ldots, t_r$ – термы. Поэтому, как в предыдущем пункте, достаточно положить:

$$At(1) = 1;$$

$$At(k) = \prod_{r} \cdot \prod_{p \text{ ранга } r} \cdot \prod_{i_j = k-1} \min\{(Term(i_1) - 1) \cdot$$

$$\cdot (Term(i_r) - 1) + 1, \mathcal{L}[(N_1^{-1}(p) * N_1(\,)) * i_1 * i_2 N_1(\,) - k$$

Как и выше, вычислимость ясна, а рекурсивность требует аналогичной проверки.

10.5. <u>Формулы</u>. Построим рекурсивную функцию $Form(k)$ со свойством:

$$Form(k) = 1 \Leftrightarrow N_1^{-1}(k) \text{ не формула.}$$

Имеем:

$$P \text{ не формула} \Leftrightarrow \begin{cases} P \text{ не атомарная формула;} \\ P \text{ не имеет вида } \neg(Q), \ (Q_1)\cdot(Q_2), \\ \quad \text{где } \cdot \text{ – одна из связок;} \\ \text{не } \forall X Q, \ \exists X Q, \text{ где } Q, \\ Q_1, Q_2 \text{ – формулы с меньшими номе-} \\ \text{рами, а } \underline{\underline{X}} \text{ – переменная с меньшим} \\ \text{номером.} \end{cases}$$

Положим $Form(1) = 1$ и для каждого из условий за фигурными скобками построим соответствующую функцию от k, считая, что $Form(1), \ldots, Form(k-1)$ уже вычислены. Читателю уже должно быть ясно, как это делать. Ограничимся двумя конструкциями.

P не имеет вида $(Q_1) \longrightarrow (Q)$ (, где $A(1) = 1$) $\Leftrightarrow A(k) = 1$,

$$A(k) = \prod_{i_1, i_2 \le k-1} \min\{(Form(i_1)-1)(Form(i_2)-1)+1, \mathcal{L}[(N(\text{(})*$$
$$*\,\vartheta_1 * N(\text{)}) * N(\rightarrow) * N(\text{(}) * i_1 * N(\text{)}) - k)^2 + 1]\} \text{ при } k \ge 2$$

P не имеет вида $\forall X \ Q \Leftrightarrow B(k) = 1$, где $B(1) = 1$

$$B(k) = \prod_{i,j \le k-1} \min\{Form(i), Var(j), \mathcal{L}[(N_1(\vee) * i * j - k)^2 + 1]\}$$

10.6. <u>Подстановка терма в терм</u>. Построим рекурсивную функцию от трех переменных

$$Sub\ t(k, \ell, \vartheta) = \begin{cases} N_1 \text{ –номер мерта, результата} \\ \quad \text{подстановки терма } N_1^{-1}(k) \\ \quad \text{в терм } N_1^{-1}(\ell) \text{ вместо} \\ \quad \text{переменной } N_1^{-1}(\vartheta) \\ 1, \text{ если предыдущий рецепт не} \\ \quad \text{применим.} \end{cases}$$

(Так как, по соглашению, $N^{-1}(1)$ – связка, $N_1^{-1}(1)$ – выражение длины I, состоящее из этой связки и, значит, не терм, так что значение I для $Subt(k, l, \vartheta)$ не может быть смешано с номером терма).

Как выше, начнем со словесного описания. Буквами α, β, γ, δ обозначим фигурирующие в нем условия.

Имеем: $Subt(k, l, \vartheta) =$

$= I$, если (α): $N_1^{-1}(k)$ не терм или $N_1^{-1}(l)$ не терм или $N_1^{-1}(\vartheta)$ не переменная;

$= k$, если (β):

$= l$, если (γ): не (α) и $l \neq \vartheta$ и $N_1^{-1}(l)$ есть терм-константа или терм-переменная;

$= N_1(f) * N_1(() * Subt(k, l_1, \vartheta) * \ldots * Subt(k, l_r, \vartheta) * N_1())$

если (δ): не (α) и существуют термы $t_1, \ldots, t_r$ с N_1 номерами $l_1, \ldots, l_r$ и знак операции f такие, что $N_1^{-1}(l) = f(t_1, \ldots, t_r)$

Заметим, что (δ) зависит от чисел $N(f_1), l_1, \ldots, l_r$, не превосходящих 2.

Допустим теперь, что мы построим функции от $k, l, \vartheta, l_1, \ldots, l_r, \ldots$: $F_\alpha, F_\beta, F_\gamma, F_\delta$, которые вычислимы, принимают лишь значения 1 и 2 такие, что

$F_\alpha = 1 \Leftrightarrow$ выполняется условие (α)

$F_\beta = 1 \Leftrightarrow$ выполняется условие (β) ... и т.д.

Тогда по аналогии с приемами, описанными в п.9.9, мы сможем положить:

$$\mathcal{S}ubt(k,\ell,\vartheta) = 2(V_\alpha + V_\beta + V_\gamma + \sum_\delta V_\delta) \dot{-}$$
$$\dot{-}\,(F_\alpha V_\alpha + F_\beta V_\beta + F_\gamma V_\gamma + \sum_\delta F_\delta V_\delta)$$

(суммирование по δ относится к $\ell_1, \ldots, \ell_2, N_1(f) \leq k$).
Это будет <u>индуктивное</u> правило для вычисления $\mathcal{S}ubt$; рекурсивность, как выше, должна будет проверяться дополнительно.

Остается построить F . Нетрудно проверить, что годятся следующие формулы. Пусть $\mathcal{S}(1) = 1$, $\mathcal{S}(X) = 2$ при $X \geq 2$; $\tilde{\mathcal{S}}(1) = 2$, $\tilde{\mathcal{S}}(X) = 1$ при $X \geq 2$. Тогда:

$$F_\alpha = \mathcal{S}(\min(Term(k), Term(\ell), Var(\vartheta)) .$$

$$F_{1\alpha} = \beta \dot{-} F_\alpha$$

$$F_\beta = \mathcal{S}(F_{1\alpha} \cdot (\ell - \vartheta)^2 + 1)$$

$$F_\gamma = \mathcal{S}[F_{1\alpha} \cdot \tilde{\mathcal{S}}((\ell - \vartheta)^2 + 1) \cdot \min(\tilde{\mathcal{S}}(Const(\ell), \tilde{\mathcal{S}}(Var(\ell))]$$

$$F_\delta = \mathcal{S}[(k - N_1(f) * N_1(C) * \ell_1 * \quad * \ell_2 * N_1(\,))^2 + 1]$$

10.7. <u>Подстановка терма в формулу</u>. Совершенно аналогично строится рекурсивная функция:

$$Subf(k,\ell,\vartheta) \begin{cases} \text{номер формулы, результата подстановки терма } N_1^{-1}(k) \text{ вместо всех свободных вхождений переменной } N_1^{-1}(\vartheta) \text{ в формулу } N_1^{-1}(\ell) \text{ ;} \\ \text{I , если этот рецепт не применим.} \end{cases}$$

Мы опускаем подробности.

10.8. Читателю уже должен быть ясен принцип дальнейших конструкций, и мы ограничимся лишь несколькими краткими замечаниями.

а) Мы должны проверить, что множество (номеров) аксиом арифметики разрешимо, чтобы гарантировать применимость теоремы Геделя в простейшем интересном случае. Для этого следует перебрать по очереди (конечное) множество аксиом и схем аксиом, логических и собственных, и для каждой из них построить свою рекурсивную функцию от номера, равную 2, если под этим номером стоит частный случай данной схемы и 1 иначе, после чего перемножить эти функции.

Для индуктивной конструкции как раз и придется пользоваться функциями, которые распознают термы, формулы, вычисляют результат подстановки и т.п.

б) Нужно построить рекурсивную функцию

$$Diag(k) = \begin{cases} N_1 & \text{(диагонализация формулы } N_1^{-1}(k)\text{)} \\ 1, & \text{если этот рецепт не применим.} \end{cases}$$

в) Нужно построить рекурсивную функцию

$$Pr(i,k) = \begin{cases} 1, & \text{если } N_2^{-1}(k) \text{ есть вывод формулы } N_1^{-1}(i), \\ 2 & \text{иначе.} \end{cases}$$

г) Наконец, нужно заметить, что множество Геделя G является 1-уровнем функции $Pr(Diag(a), l)$:

$$(a,b) \in G \Longleftrightarrow Pr(Diag(a), b) = 1$$

Подп к печати 25.12.73. Л 77363 Ф 60x90/16.
Физ п л 4,5. Уч-изд л 3,0.
Заказ 1978. Тираж 500 ЭКЗ.Цена 9 коп

Типография Изд-ва МГУ Москва, Ленгоры