Глава 7

Арифметика

τι εστιν αληθεια;

Ευαγγ. κατα Ιωαννην

7.a Функция следования

В этой главе мы изучаем структуры, образованные хорошо известными отношениями или операциями, определенными на множестве $\mathbb{N}$, обозначаемой также ω , натуральных чисел. Мы начинаем с изучением функции следования которая числу x сопоставляет число $x+1$; язык содержит символ s для обозначения этой функции, также символ константы 0 для обозначения наименьшего натурального числа.

Выражаем аксиомами, что s инъективно, и что каждый элемент, за исключением 0, является последователем:

$$(\forall x)(\forall y)(sx = sy \to x = y), \quad (\forall x)sx \neq 0$$

$$(\forall x)(\exists y)(x = 0 \vee x = sy) \ .$$

Какими будут модели теории, образованной из этих трех аксиом? Они содержат во-первых орбиту действия s на 0 : эта орбита $\{0, s(0), \dots, s^n(0), \dots\}$ является копией функции следования на натуральных числах. Ещё они могут содержать конечные, циклические орбиты или бесконечные орбиты копии функции следования $(\mathbb{Z}, s)$ на целых числах. Но наша функция следования не содержит циклов порядка n , что выражается аксиомой :

$$\neg(\exists x_1)\dots(\exists x_n)(x_2 = sx_1 \wedge \dots \wedge x_n = x_{n-1} \wedge x_1 = sx_n) \ .$$

Обозначим через S теорию, аксиоматизированную этим бесконечным списком аксиом. Легко видеть, что она не конечно аксиоматизируема: если мы выразим, что не имеется циклов порядка $1, 2, \dots, n$, то допускаем циклы порядка $n+1$. Я утверждаю, что эта теория полна, т.е. это теория функции следования, и что она допускает элиминацию кванторов (в языке s, 0).

Действительно, каждая модель S содержит копию $(\mathbb{N}, s)$, в которой можно выбирать элементы $a_1, \dots, a_n$, удаленных друг от друга на произвольно большие расстояния, таким образом, с теорией этой модели совместно утверждение, что существуют $a_1, \dots, a_n$, не удовлетворяющие никаким равенствам $a_i = s^k a_j$, и, следовательно, каждая ω-насыщенная модель S образована из копии $(\mathbb{N}, s)$ и из бесконечного числа копий $(\mathbb{Z}, s)$; тогда легко видеть, что в двух таких моделях, два кортежа, удовлетворяющие одним и тем же формулам без кванторов, ω-эквивалентны.

Мы могли бы также провести челнок Фраиссе в стиле главы 1: надо предварительно заменить функцию следования её графиком, то есть множеством пар $(n, n+1)$, называемым "бинарным отношением следования"; определение классов p-эквивалентности в этом случае не сложное. Можно также поступать немного по-другому, замечая, что с точностью до изоморфизма имеется ω счетных моделей S , смотря по тому сколько копий $(\mathbb{Z}, s)$ она имеет $0, 1, 2, \dots, n, \dots$ или ω , в то время как для каждого несчетного кардинала λ она имеет единственную модель в этой мощности, так как имеется только одна возможность λ копий $(\mathbb{Z}, s)$. Теория, которая так же, как S, имеет единственную модель в мощности λ , называется *λ-категоричной*, или еще *категоричной в λ*.

Теорема 7.1 *Если теория T не имеет конечных моделей, и категорична в мощности $\lambda \geq |T|$, то она полна.*

Доказательство. Предположим, что T имеет модель M, удовлетворяющую f, и другую N, удовлетворяющую $\neg f$. Тогда M и N бесконечны, и по теореме Левенгейма-Сколема, они имеют соответственно элементарно эквивалентные M_1 и N_1 мощности λ , которые должны быть изоморфны: это противоречие.

□

Таким образом, эта теорема также доказывает, что S полна; на практике, ее область применения гораздо более ограничена чем мы могли бы думать, так как часто λ-категоричность теории можно понять только с помощью челнока, который дает ее полноту непосредственно. Например, мы могли ее использовать, чтобы показать полноту теории алгебраически замкнутых полей данной характеристики, зная теорему Штейница о базе трансцендентности, и также, конечно, единственность алгебраического замыкания, доказанную без теорию моделей!

Для того, чтобы доказать элиминацию кванторов, зная, что S полна, достаточно отметить, что в несчетной модели S (и также в его ω-насыщенной счетной модели!) два кортежа, удовлетворяющие одним и тем же свободным формулам, переводятся автоморфизмом. Из всего этого заключаем, что теория следования очень проста и классификация его моделей непосредственна.

7.b Порядок

Порядок $(\mathbb{N}, \leq)$ натуральных чисел был тщательно изучен в первой главе: его теория является теорией дискретного порядка с наименьшим элементом и без наибольшего элемента, и мы знаем (см. описание типов в разделе 1.b, упражнение 1.10), что она имеет элиминацию кванторов, если добавить к языку символ 0 для обозначения наименьшего элемента и для каждого целого n , символ $d_n(x, y)$ для обозначения отношения "имеется n элементов между x и элементом y ".

Теперь, когда мы имеем некоторый опыт в обращении с бесконечным челноком, то, что мы имеем действительно полную теорию , и что порядок и "расстояния", а также "расстояние до 0 ", описывают типы, можно выяснить так :

- моделями обсуждаемой теории являются цепи вида $\mathbb{N} + \mathbb{Z} \times C$, где C является какой-нибудь цепью (здесь, в отличие от последователя, имеется связь между различными копиями $\mathbb{Z}$: они должны быть упорядочены одни по отношению к другим) ;

- в ω-насыщенной модели этой теории, цепь C плотна без концов: действительно, если $a < b$ и $d(a, b) = \infty$, то с теорией этой модели совместно утверждение, что существует x , $a < x < b$, на бесконечном расстоянии

как от a , так и от b ; и что существует элемент y , $y > b$, на бесконечном расстоянии от b ;

– возрастающие кортежи в двух таких моделях, имеющие одни и те же расстояния, ∞-эквивалентны.

Теория порядка натуральных чисел, которая конечно аксиоматизируема, также не доставляет больших проблем: её модели ясно описаны выражением $\mathbb{N} + \mathbb{Z} \times C$, если мы считаем, что понятие цепи является ясным. Она более сложна, чем теория следования, в следующем техническом смысле : отношение $y = sx$ *интерпретируемо* формулой $x < y \wedge (\forall z)(x \leq z \leq y \rightarrow x = z \vee z = y)$; говорят также, что следование *определимо* через порядок. Каждое предложение на языке следования можно таким образом заменить предложением на языке порядка: заменяем следование на его перевод; так что знание о теории порядка влечет знание теории следования.

Каждая модель теории следования получается из модели теории порядка: достаточно упорядочить различные копии $\mathbb{Z}$. Это – очень редкое явление.

7.c Сумма

Мы рассматриваем теперь структуру, образованную бинарной операцией суммы, определенной на универсуме натуральных чисел; она позволяет интерпретировать порядок, заменяя формулу $x \leq y$ на $(\exists z)(x + z = y)$. В этом случае, не каждая модель порядка получается из модели суммы: если эта модель содержит элемент x , больший всех чисел вида $0, 1, 1+1, \ldots, 1+\cdots+1, \ldots$ (в этом случае говорят, что x – *нестандартный*), то легко видеть, что $x + x$ на бесконечном расстоянии от x ; таким образом, необходимо, чтобы цепь C не имела наибольшего элемента.

Упражнение 7.2 *Счетная модель порядка получается из модели суммы тогда и только тогда, когда она имеет вид* ω *или* $\omega + \mathbb{Z} \times \mathbb{Q}$ *, где* $\mathbb{Q}$ *– цепь рациональных чисел.*

Мы собираемся теперь аксиоматизировать теорию суммы и описать её типы; для простоты, мы добавим к языку два символа константы для обозначения 0 и 1 : эти элементы определимы через сумму, $x = 0$ определяется через $x + x = x$, а $x = 1$ – через $x \neq 0 \wedge (\forall u)(\forall v)(u + v = x \rightarrow u = 0 \vee v = 0)$. Тогда, сумма удовлетворяет следующим аксиомам:

1. $(\forall x)(\forall y)(x + y = y + x)$ коммутативность,
2. $(\forall x)(\forall y)(\forall z)[(x + y) + z = x + (y + z)]$ ассоциативность,
3. $(\forall x)(x + 0 = x)$
4. $(\forall x)(x + 1 \neq x)$
5. $(\forall x)(\forall y)(x + y = 1 \rightarrow x = 0 \vee x = 1)$

6. $(\forall x)(\forall y)(\exists z)(x = y + z \vee y = x + z)$

7. $(\forall x)(\forall y)(\forall u)(\forall v)(x = y + u \wedge y = x + v \to x = y)$.

Эти аксиомы выражают, что отношение $(\exists z)(x+z = y)$ является линейным порядком (транзитивным по (2), рефлексивным по (3), антисимметричным по (7), линейным (6)), которое отныне обозначим через $\leq$; по (3) и (1) наименьшим элементом является 0, и по (4) и (5) его последователем является 1.

Они влекут также, что каждое ненулевое x , будучи больше чем 0 , имеет вид $y+1$ и $x+1$ является последователем x : по (4) $x+1 > x$ и, если $y > x$, то $y = x+z$ с $z \neq 0$, таким образом, $y = x+1+t$. Отметим, что они влекут также, что если $x \leq y$, то $x+z \leq y+z$, и если $x < y$, т.е. $x+1 \leq y$, то $x+z < y+z$. И обратно, рассматривая все случаи ($x < y$, $x = y$, $x > y$), мы видим, что они влекут следующие свойства *сократимости*: $x + z \leq y + z \to x \leq y$, $x + z = y + z \to x = y$, $x + z < y + z \to x < y$.

Теперь примем соглашения о сокращениях записи: если n – натуральное число, то мы обозначим через n , в качестве этого числа, терм $1+\cdots+1$, где сумма берется n раз; и мы обозначим через nx терм $x+\cdots+x$, где сумма берется n раз; не забываем, что, когда мы используем эти сокращения, произведение целых чисел не присутствует в нашем языке. В модели для аксиом (1) – (7), элементы вида $0, 1, 2, \ldots, n, \ldots$, образуют начальный сегмент, на котором сумма изоморфна сумме натуральных чисел; эти элементы называются *стандартными*; можно без помех отождествлять стандартное подмножество модели с соответствующими натуральными числами; их называют иногда также *настоящими* натуральными числами, контрастно с *нестандартными* элементами модели, которые, таким образом, больше, чем все стандартные элементы; модель сама называется *нестандартной*, если она содержит нестандартный элемент; таким образом, с точностью до изоморфизма существует единственная стандартная модель, состоящая из настоящих натуральных чисел.

Сумма удовлетворяет также свойствам евклидова деления, которые выражаются бесконечным списком следующих аксиом (одна аксиома для каждого ненулевого (стандартного!) натурального числа n) :

(8_n) $(\forall x)(\exists y)(x = ny \vee x = ny + 1 \vee \cdots \vee x = ny + (n-1))$,

что можно переписать также в виде

$(8'_n)$ $(\forall x)(\exists y)(\exists r)(x = ny + r \wedge r < n)$

Невозможно заменить список аксиом (8) единственной аксиомой так, как пытаются делать, универсально квантифицируя по n : в нашем языке произведения нет, ny есть не что иное, как сокращение для $y + \cdots + y$. И действительно не очень трудно видеть, что порожденная аксиомами $1, 2, \ldots, 7, 8_1, \ldots, 8_n, \ldots$ теория не конечно аксиоматизируема, т.е. конечное число аксиом евклидова деления никогда не может повлечь все остальные.

Как следствие этих аксиом, получаем единственность остатка и частного евклидова деления: если $ny + r = nz + s$, с r и s меньше n , тогда $y = z$ и $r = s$; действительно, если например $z \leq y$, $z = y+u$, то $ny+r = ny+nu+s$, упрощая получим $r = nu+s$, таким образом, $nu \leq r < n$: единственное число, меньшее r , которое имеет вид nu есть 0 , таким образом, $u = 0$. Мы обозначим через $[x/n]$ *"целую часть"* от деления x на n , т.е. единственный y, такое, что

$x = ny + r$ с $r < n$; r называется *остатком* от деления x на n .

Теорема 7.3 *Множество аксиом* $1, 2, \ldots, 7, 8_1, \ldots, 8_n, \ldots$ *образует полную теорию суммы натуральных чисел и допускает элиминацию кванторов в языке* $0, 1, \leq, +, [\ /2], \ldots, [\ /n], \ldots$.

Доказательство. В языке который мы рассматриваем, всякая подструктура содержит 0 и 1 , и замкнута относительно сложения и функций $[\ /n]$. Пусть нам даны ω-насыщенные модели M и M' этой теории, кортежи $\bar{a}$ и $\bar{b}$, порождающие в них изоморфные подструктуры A и B : мы должны показать что $\bar{a}$ и $\bar{b}$ ∞-эквивалентны. (Это покажет ещё, что теория полна, так как подструктура, порожденная пустым множеством, всегда изоморфна сложению настоящих натуральных чисел).

Добавим например элемент α к A ; я утверждаю что подструктура, порожденная A и α образована из элементов вида $a + k[\alpha/n]$, где a из A и k и n – натуральные числа. Действительно, 0 и 1 имеют такой вид; как считать сумму $a + k[\alpha/n]$ и $b + h[\alpha/m]$? Надо, очевидно, привести к общему знаменателю :

$$\begin{array}{lcllcl} \alpha & = & n[\alpha/n] + r_n \ , & \alpha & = & m[\alpha/m] + r_m \ , \\ \alpha & = & nm[\alpha/nm] + r_{nm} \ , & r_{nm} & = & np + r_n = mq + r_m \ , \end{array}$$

откуда

$$[\alpha/n] \ = \ m[\alpha/nm] + p \qquad [\alpha/m] \ = \ n[\alpha/nm] + q$$

и искомая сумма равна $a + b + pk + qh + (km + hn)[\alpha/nm]$. Отметим, что форма выражения зависит только от остатков α по модулю n , m , nm .

Как поделить $a + k[\alpha/n]$ на m ? Если $a = m[a/m] + r$, тогда

$$a + k[\alpha/n] = m([a/m] + k[\alpha/mn]) + r + kp \ ,$$

таким образом, частное равно $[a/m] + k[\alpha/nm] + [r + kp/m]$, и снова видим, что это вычисление зависит только от остатков α .

Следовательно, чтобы определить полностью структуру, порожденную A и α с точностью до изоморфизма, остается выяснить когда

$$a + k[\alpha/n] \leq b + h[\alpha/m] \ ;$$

(и в частности, когда $a + k[\alpha/n] = b + h[\alpha/m]$) ; это перепишется еще в виде $a + km[\alpha/nm] + kp \leq b + hn[\alpha/nm] + hq$, и умножая два числа на nm (аксиомы влекут $x \leq y \leftrightarrow kx \leq ky$) и добавляя $(km + hn)r_{nm}$ к обеим частям, получим

$$nma + nmkp + hnr_{nm} + km\alpha \leq nmb + nmhq + kmr_{nm} + hn\alpha \ ,$$

которое является неравенством вида $a' + k'\alpha \leq b' + h'\alpha$, способ получения a', b', k', h' из начальных данных a, b, k, h, m, n зависит только от остатков α по модулю n , m , nm .

Поманипулируем еще с этим неравенством, которое мы перепишем без штрихов, и предположим что $k \geq h$; заменяя k на $k - h$ получим : $a + k\alpha \geq b$, или $k[a/k] + r + k\alpha \leq k[b/k] + s$; если $r \leq s$, то это эквивалентно неравенству $[a/k] + \alpha \leq [b/k]$; если $r > s$, то это эквивалентно неравенству $[a/k] + \alpha < [b/k]$; случай $k < h$ разбирается подобным способом. В итоге, с точностью до изоморфизма подструктура, порожденная A и α, определяется :

1) последовательностью остатков α по модулю n ,

2) неравенствами вида $a+\alpha \leq b, a \leq \alpha+b$, с a и b в A , удовлетворяющимися элементом α .

Обозначим через A_1 множество, образованное из разностей пар элементов из A , и через B_1 – множество, образованное из разностей пар элементов из B: изоморфизм A на B продолжается до изоморфизма A_1 на B_1 , сохраняющего порядок (так как $a-b \leq c-d \leftrightarrow a+d \leq c+b$; на самом деле A_1 и B_1 – *подструктуры*, которые изоморфны).

Нам надо таким образом найти β , удовлетворяющий тем же конгруэнциям, что и α , и определяющий на B_1 сечение, соответствующее тому, что определяет α на A_1 ; различаем два случая:

– $\alpha \in A_1$; таким образом α имеет вид $a-b$; берем в качестве β соответствующую разность элементов B, и оставляем читателю проверку того, что β имеет тот же остаток по модулю n что и α

– $\alpha \notin A_1$; так как A_1 замкнуто относительно последователя и предшественника, если $a \in A_1$ и $a < \alpha$, тогда $a+1 < \alpha$, и если $b \in A_1$, $\alpha < b$, тогда $\alpha < b-1$; и мы хотим найти β в соответствующем сечении, удовлетворящий данные конгруэнции, т.е. удовлетворить список формул $\ldots, a \leq y, \ldots y \leq b, \ldots y \sim r_n(\mod n), \ldots$; так как для того, чтобы определять y по модулю $n_1, \ldots, n_s$, достаточно определить его по модулю их произведения (это является следствием аксиом!), конечная система, извлеченная этого списка, эквивалентна трем условиям :

$$a \leq y,\ y \leq b,\ y \sim r_n(\mod n) ,$$

которым удовлетворяет a, или $a+1$, или $a+2\ldots$ или $a+(n-1)!$. Эти условия таким образом совместны с теорией M , и по компактности и ω-насыщенности существует β в M , удовлетворяющий им всем.

□

Существует более естественный способ аксиоматизации суммы, состоящий в выражении свойства рекурсии натуральных чисел: если подмножество натуральных чисел содержит 0 , и если вместе с каждым x оно содержит $x+1$, тогда оно совпадает целиком с $\mathbb{N}$. Если мы вводим переменную X для подмножеств $\mathbb{N}$, это пишется так:

$$(\forall X)[(0 \in X \wedge (\forall x)(x \in X \to x+1 \in X)] \to (\forall x)(x \in X) .$$

Только вот это выражение не является разрешенной аксиомой в нашем языке; нам разрешаются квантификации по *индивидам* носителя рассматриваемой структуры, но не квантификации по его подмножествам; мы можем говорить о множестве, об отношении, о функции только если мы их вводим заранее специальным символом. Именно по этой причине наш язык называется языком первого порядка; языки, в которых определяют квантификацию также по подмножествам, отношениям и т.п., именуются языками второго порядка; они не позволяют развить теорию моделей подобно той, что первого порядка, как показывает следующее упражнение :

Упражнение 7.4 *Покажите, что язык второго порядка не обладает свойством компактности (заметьте, что в языке второго порядка сумма, или даже следование натуральных чисел характеризуется с точностью до изоморфизма).*

Но, хотя в нашем языке невозможно говорить во всей общности о подмножествах N , можно по крайней мере рассматривать те из них, которые определяются формулой $f(x)$ языка суммы, и сказать, что если 0 удовлетворяет f , и если вместе с каждым x $x+1$ так же удовлетворяет f, тогда каждый x удовлетворяет f. Для этого нужно добавить по одной аксиоме A_f для каждой формулы f ; но, так как все эти аксиомы имеют один и тот же вид, то иногда говорят, что A_f является *схемой аксиом* : чтобы получить аксиомы, которые описывает схема A_f , надо заменить f последовательно всеми формулами.

Аксиоматикой Пресбургера называются следующие аксиомы:

(I) $(\forall x)(x+1 \neq 0)$

(II) $(\forall x)(\forall y)(x+1 = y+1 \to x = y)$

(III) $(\forall x)(x+0 = x)$

(IV) $(\forall x)(\forall y)[x+(y+1) = (x+y)+1]$

(V_f) $(\forall \bar{x})\{[f(\bar{x},0) \wedge (\forall y)(f(\bar{x},y) \to f(\bar{x},y+1))] \to (\forall y) f(\bar{x},y)\}$.

Рекурсия (еще говорят: индукция) является движущей идеей этой аксиоматики, которая, очевидно, выполняется для суммы натуральных чисел; аксиома (IV) объясняет как можно считать $x+y$ последовательно начиная с $x+0$, $x+1$, $x+2$, и т.д. ; имеется по одной аксиоме (V_f) для каждой формулы f языка $(+,0,1)$ с $n+1$ свободными переменными: эта аксиома называется аксиомой индукции, относительно переменной x , в формуле $f(x_1,\ldots,x_n,x)$.

Теорема 7.5 *Аксиоматика Пресбургера аксиоматизирует теорию суммы натуральных чисел.*

Доказательство. Ясно, что эти аксиомы истинны для суммы натуральных чисел, и для доказательства полноты этой теории лучше всего вывести из них каждую аксиому предыдущего списка. Действительно, аксиоматика Пресбургера обязана своей элегантностью скорее метафизическому вдохновению, чем интуиции о том, что является типами. Мы здесь проделаем это быстро.

(2) Ассоциативность доказывается , индукцией по z :

$$x+(y+0) = x+y = (x+y)+0 \ ;$$

$$x+(y+(z+1)) = x+((y+z)+1) = (x+(y+z))+l =$$

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

(1) Коммутативность получается в три этапа ; индукцией по x : $0+x = x$, индукцией по x : $1+x = x+1$, индукцией по y : $x+y = y+x$.

(4) индукцией по x : $0+1 \neq 0$; $x \neq x+1$ влечет $x+1 \neq (x+1)+1$

(5) индукцией по x показываем, что каждое ненулевое число имеет вид $u+1$; если $(u+1)+y=1$, $0=u+y$, и ни u ни y не имеют вид $v+1$, таким образом, $u=0$

Аксиомы (6) , (7) , (8_n) оставляем читателю.

□

Отметим, что в доказательстве теоремы 7.5 используются только слабые версии, тем не менее бесконечное число, аксиом индукции.

Пример модели теории суммы Возьмите две упорядоченные группы : $\mathbb{Z}$ целых чисел и $\mathbb{Q}$ рациональных чисел; снабдите произведение групп $\mathbb{Z}\times\mathbb{Q}$ лексикографическим порядком. Тогда элементы, большие чем $(0,0)$ составляют модель теории суммы натуральных чисел.

Замечание . *Для теории суммы, число типов над $\emptyset$ есть 2^ω : имеется действительно 2^ω возможностей, чтобы выбрать остатки по модулю n (когерентным способом!) . Следовательно эта теория не может иметь счетную ω-насыщенную модель.*

7.d Сумма и произведение : кодирование конечных множеств

С этого момента, мы будем изучать структуру, образованную из натуральных чисел с суммой и произведением; теория этой структуры называется *арифметикой*. Мы предположим, что язык содержит $0,1,\leq,+,\cdot$, хотя $0,1,\leq$ необязательны, так как они определимы через сумму; тем не менее 0 и 1 очень удобны, так как они позволяют выразить каждое натуральное (стандартное!) число термом $n=1+\cdots+1$; и с другой стороны, порядок играет такую фундаментальную роль в классификации формул арифметики, что практически необходимо его выделять специальным символом.

Так же, как и для суммы, мы называем *стандартной моделью* модель $\mathbb{N}$ арифметики, образованную из настоящих натуральных чисел; так как каждый элемент стандартной модели выделен термом, его диаграмма (множество предложений, а не только предложений без кванторов, которым удовлетворяют его элементы) является частью арифметики, и каждая нестандартная модель является элементарным расширением стандартной модели, являющейся ее начальным сегментом.

В предыдущих параграфах, мы изучили некоторые частичные структуры арифметики, одна богаче другой, каждая из которых интерпретировалась в следующей. Мы смогли аксиоматизировать их теории, и описать некоторые нестандартные модели: это изучение от случая к случаю становилось все более деликатным. С суммой нам было труднее, чем с порядком или последователем, но мы вышли из положения почти тем же путем, преодолев осложнения только технического характера.

Но мы поймем, что со суммой и произведением мы делаем качественный

прыжок и мы входим в новую область; и теперь нам не удастся ни аксиоматизировать арифметику, ни строить нестандартные модели, так как мы увидим, что имеются теоретические препятствия против этих попыток: арифметика не может иметь ни аксиоматизацию, ни нестандартных моделей той же природы, присущей изученным до этого частичным структурам; конечно, нам надо уточнить, что мы понимаем под "природой" этих объектов.

Мы еще не готовы для этого и в этом параграфе мы лишь покажем, что арифметика содержит кодированную в ней самой *комбинаторику*, или теорию конечных множеств. Так как это кодирование очень существенно для изучения моделей арифметики и для того, чтобы оценить её выразительную силу, его нужно хорошо усвоить. Предположим, что мы хотим сказать "существует конечная последовательность из 10 элементов таких, что f " ; мы должны только написать $(\exists x_1)\dots(\exists x_{10})f$; мы можем делать это также для последовательности из миллиарда элементов ; но как сказать на нашем языке первого порядка "существует конечная последовательность из x элементов", где x – переменная ? Вот тут-то β-функция Геделя и дает искомое средство.

Функция $\beta(u,v,w)$ Геделя сопоставляет трем целым числам u,v,w последовательность целых чисел $a_0,\dots a_{w-1}$ длины w (если $w=0$, то $\beta(u,v,w)$ – пустая последовательность), определенную таким образом: a_i является остатком евклидова деления u на $(i+1)v+1$.

Теорема 7.6 *Функция $\beta(u,v,w)$ является сюръекцией $\mathbb{N}^3$ в множество конечных последовательностей элементов из $\mathbb{N}$.*

Доказательство. Натуральные числа удовлетворяют китайской лемме: если $d_0,\dots,d_{w-1}$ попарно взаимно просты, то для данных $a_0,\dots,a_{w-1}$ существует натуральное u , конгруэнтное a_0 по модулю d_0 , ... , конгруэнтное a_{w-1} по модулю d_{w-1} (чтобы доказать китайскую лемму, покажите, что

$$\mathbb{Z}/d_0\dots d_{w-1}\mathbb{Z} = \mathbb{Z}/d_0\mathbb{Z}\times\dots\times\mathbb{Z}/d_{w-1}\mathbb{Z}\ .$$

Нам остается найти u больше $a_0,\dots,a_{w-1}$ (чтобы эти натуральные числа были остатками по модулю для всех $(i+1)v+1)$), такое, что, если $i<j<w$, то $(i+1)v+1$ и $(j+1)v+1$ были взаимно простыми. Полагаем $v=n!$, где n больше $w,a_0,\dots,a_{w-1}$; если p является простым общим делителем $(i+1)n!+1$ и $(j+1)n!+1$, то он делит также $(j-i)n!$ и он делит таким образом $j-i$ или $n!$, и так как $j-i$ делит $n!$, он делит $n!$; но так как p делит $(i+1)n!+1$, он должен делить 1, это абсурд.

□

Свет проник в разум читателя: для того, чтобы сказать "существует конечная последовательность, у которой i-ый член ... " скажем "существует u,v,w такие, что остаток деления u на $(i+1)v+1$ ... "; и все это – на языке арифметики, так как формула $(\exists y)(a=yb+c\wedge c<b)$ выражает, что c является остатком деления a на b.

В качестве иллюстрации определим в арифметике показательную функцию x^y . Прежде всего заметим, что сумма получается итерацией следования, произведение – итерацией суммы, и показательная функция – итерацией произведения : сумма – это единственная функция f такая, что $(\forall x)f(x,0)=x$,

$(\forall x)(\forall y)f(x,y+1) = f(x,y)+1$; произведение – это единственная функция f такая, что $(\forall x)f(x,0) = 0$, $(\forall x)(\forall y)f(x,y+1) = f(x,y)+x$; показательная функция – единственная f такая, что $(\forall x)f(x,0) = 1$, $(\forall x)(\forall y)f(x,y+1) = f(x,y)\cdot x$. Но эти определения, содержащие квантификацию по функции ("единственная функция"), для нас запрещены. Кажется, что градация структур становится все более и более сложной: следование, сумма, сумма и произведение; за ним следует структура: сумма, произведение, показательная функция. Ничего подобного, мы укажем формулу первого порядка языка суммы и произведения, определяющего график показательной функции – отношение $z = x^y$.

Введем сокращение: $r(u,v)$ обозначает остаток от деления u на $v+1$; мы уже отметили, что эта функция определяется через сумму и произведение. Наша формула $f(x,y,z)$, определяющая отношение $z = x^y$, следующая:

$$(\exists u)(\exists v)(r(u,v) = 1 \wedge r(u,(y+1)v) = z \wedge$$

$$\wedge\ (\forall i)(1 \le i \le y \to r(u,(i+1)v) = x \cdot r(u,iv))) \ .$$

Почему это то, что нужно ? Предположим что x,y,z удовлетворяют формуле; рассмотрим последовательность

$$a_0 = r(u,v), \ldots, a_i = r(u,(i+1)v), \ldots, a_y = r(u,(y+1)v) \ ;$$

так как $a_0 = 1$, и $a_{i+1} = a_i \cdot x$, обязательно получим $a_y = x^y$, и, кстати, формула утверждает, что $z = a_y$! Обратно, если $z = x^y$, то по теореме 7.6 последовательность $a_0 = 1, \ldots, a_i = x^i, \ldots, a_y = x^y$ имеет вид $\beta(u,v,y+1)$, откуда следует существование u и v и формула действительно удовлетворяется.

Идея этого доказательства заключается в том, что определение рекурсией благодаря функция β превращается в нечто выразимое на языке арифметики; теперь читателю предлагается определить через сумму и произведение любую функцию из $\mathbb{N}$ в $\mathbb{N}$, которая приходит ему на ум (например, ту, которая x сопоставляет x-ое простое число); если в некоторых случаях он потерпит неудачу, то это из-за недостатка опыта в управлении функцией β или, возможно, у него больное воображение; иначе, он установит, несколько неожиданно для себя, что каждая "естественная" функция из $\mathbb{N}$ в $\mathbb{N}$ определима в арифметике. Пока все это выглядит немного кустарно, и теперь мы покажем метод более систематического исследования, состоящий в интерпретации "теории конечных множеств" (или комбинаторики) внутри арифметики.

Все, или по крайней мере каждый читатель математической литературы знает как писать числа в десятичной системе счисления посредством десяти цифр; и выпускники средней школы знают также как писать число в двоичной системе счисления посредством двух цифр 0 и 1 : оно состоит в том, чтобы его представить в виде $\sum \varepsilon_i 2^i$, с $\varepsilon_i = 0$ или 1 , причем ε_i все нули начиная с некоторого номера. Мы нуждаемся в нескольких элементарных леммах о нумерации.

Лемма 7.7 *Каждое число обладает одним единственным разложением в двоичном основании.*

Доказательство. Покажем сначала единственность; мы используем формулу $\sum_{0\le i\le k} 2^i = 1+2+\cdots+2^k = 2^{k+1}-1$, которую легко показать индукцией по k ; итак, предположим, что $\sum \varepsilon_i 2^i = \sum \eta_i 2^i$ – два разложения одного и того же числа; ε_i как и η_i нули начиная с некоторого места, существует наибольший индекс k такой, что $\varepsilon_k \neq \eta_k$, предположим например, что $\varepsilon_k = 0, \quad \eta_k = 1$; отбрасывая то, что соответствует индексам, большим k , получаем равенство: $\sum_{0\le i\le k-1} \varepsilon_i 2^i = \sum_{0\le i\le k-1} \eta_i 2^i + 2^k$, которое невозможно, так как левый член мажорируется $2^k - 1$.

Покажем теперь, что каждое число x имеет требуемое разложение; мы не делаем это индукцией по x из-за проблемы сложения с "записью в уме". Проще заметить, что имеются 2^k различных разложений $\sum_{0\le i\le k-1} \varepsilon_i 2^i$, в которых все цифры являются нулями начиная с k ; мы уже поняли, что числа, которые они представляют, все различные, и они кроме того мажорируются $\sum_{0\le i\le k-1} 2^i = 2^k - 1$: это – все числа от 0 до $2^k - 1$.

□

Лемма 7.8 *Функция $\gamma(x,i)$, сопоставляющая паре (x,i) $(i+1)$-ую цифру разложения x в двоичном основании, определима через сумму и произведение.*

Доказательство. Отношение $y = \gamma(x,i)$ определяется следующей формулой, которая может выражена только через сумму и произведение, так как, как мы уже знаем, показательная функция определяется через них:

$$(\exists u)(\exists v)(\exists w)\{[r(u,v) = 1 \vee r(u,v) = 0] \wedge$$

$$\wedge\ (\forall j)[1 \le j \le w \to (r(u,jv) = r(u,(j+1)v) \vee 2^j + r(u,jv) =$$

$$= r(u,(j+1)v))] \wedge x = r(u,(w+1)v) \wedge (i > w \to y = 0) \wedge$$

$$\wedge\ (i = 0 \to y = r(u,v)) \wedge (((1 \le i \le w) \wedge r(u,iv) = r(u,(i+1)v)) \to y = 0) \wedge$$

$$\wedge\ [((1 \le i \le w) \wedge r(u,iv) \neq r(u,(i+1)v)) \to y = 1]\} .$$

Это – то, что надо, потому что последовательность $\beta(u,v,w+1)$, представленная тройкой $u, v, w+1$, дает в точности частичные суммы разложения x по основанию два.

□

Мы вводим теперь бинарное отношение "принадлежности" между целыми числами: говорим, что $x \in y$, если $x+1$-ая цифра разложения y по основанию два равна 1; если она равна 0, то $x \notin y$. По лемме 7.8 отношение $x \in y$ определимо в арифметике формулой $\gamma(y,x) = 1$. Это бинарное отношение принадлежности определяет модель "теории множеств" с носителем $\mathbb{N}$; очевидно, чтобы дать смысл этому утверждению, надо было бы уточнить аксиомы этой теории, чего автор этих строк абсолютно избегает. Будет проще, если читатель убедится, что натуральные числа, снабженные этой принадлежностью,

имеют формальные свойства множеств, с которыми они упражнялись школе, и которые в течение века служат жизненной средой для развития математики.

Например, одним из принципов этой теории множеств является аксиома экстенсиональности: "два множества, которые имеют одни и те же элементы, равны"; она здесь выполняется, так как два числа, имеющие одно и то же разложение по основанию два, равны! Мы имеем пустое множество, являющееся числом 0; для данных двух чисел a и b , мы можем образовать пару $\{a,b\}$, которая равна одноэлементному множеству $\{a\} = 2^a$, если $a = b$, и $2^a + 2^b$, если a и b – различные. Вообще, в этой модели для данных n различных чисел $a_0, \ldots, a_{n-1}$ можно образовывать множество $\{a_0, \ldots, a_{n-1}\}$, являющийся числом $2^{a_0} + \cdots + 2^{a_{n-1}}$.

Если $x \in y$, то $x < y$ так как $i < 2^i$. Поэтому наше отношение принадлежности *фундировано*, т.е. не существует последовательности $x_1, \ldots, x_n$ с $x_1 \in x_2 \in \cdots \in x_n \in x_1$. В частности, элементы a все строго меньше a. Теперь легко видеть, что если имеется два множества a и b , то можно образовывать их объединение, совпадающее с числом $a + b$, если a и b дизъюнктны; аксиома суммы также истинна: можно образовывать объединение элементов a ; как и аксиома множества всех подмножеств: можно образовать множество чисел, являющихся подмножествами a ; схема аксиом замещения также верна (это последнее "темное" утверждение адресована ученым: если Вам не хватает науки, и если Вы хотите блистать в обществе, пролистайте учебник по теории множеств).

В модели $(\mathbb{N}, \in)$ имеются только конечные множества; здесь "конечность" – внешнее свойство относительно модели: для данного числа a, множество x, таких, что $x \in a$, конечно; как мы заметили, любое конечное множество чисел имеет вид $\{x/x \in a\}$. В предыдущей фразе, слова "множество", "конечный" необходимо понимать в естественном, неформальном, интуитивном смысле (если считать множества естественными объектами, о которых можно иметь интуицию!), а не в техническом смысле модели $(\mathbb{N}, \in)$; но также можно показать, что эта модель удовлетворяет аксиоме "каждое множество конечно" или еще "для каждого a существует натуральное число n и биекция n на a".

Как в теории множеств, представляются натуральные числа ? Число 0 представляется множеством $\emptyset$; 1 представляется , одноэлементным множеством содержащим $\{\emptyset\}$, 2 есть $\{\emptyset, \{\emptyset\}\}$, и т.д. Если n^* обозначает множество, представляющее число n , то $n + 1$ представляется $n^* \cup \{n^*\}$. Таким образом, натуральное число становится множеством предшествующих ему натуральных чисел. Мы видим, что натуральное число n^* транзитивно (если $x \in y$ и $y \in n^*$, тогда $x \in n^*$), и что отношение принадлежности определяет на элементах n^* (строгий) линейный порядок: читатель может проверить что только элементы вида n^* модели $(\mathbb{N}, \in)$ обладают этими двумя свойствами; они составляют множество N^* ("множество", не представимое в модели $(\mathbb{N}, \in)$!) натуральныХ чисел в смысле модели $(\mathbb{N}, \in)$.

Мы уже отметили, что если x и y дизъюнктны относительно $\in$, $x \cap y = \emptyset$, т.е. x и y не имеют общих разрядов, равных 1, тогда $x \cup y = x + y$; и что $\{x\} = 2^x$; кроме того $x \notin x$ (так как если $x \in y$, то $x < y$); следовательно, отображение, которое x сопоставляет x^* определяется законом следующей индукции: $0^* = 0$,

$(x+1)^* = x^* + 2^{x^*}$. Наш читатель не будет более удивлен, узнав, что функция $y = x^*$ определяется в арифметике формулой:

$$(\exists u)(\exists z)(r(u,v) = 0 \wedge r(u,(x+1)v) = y \wedge$$

$$\wedge\ (\forall i)(1 \leq i \leq x \to r(u,(i+1)v) = r(u,iv) + 2^{r(u,iv)}))\ .$$

Следовательно, мы можем переложить, посредством отображения $*$, которое определимо, структуру $\mathbb{N}$ на его образ N^* . Что мы выигрываем при этом ? То, что теперь N^* вся покрыта комбинаторикой, что все то что будет говорить о конечных подмножествах N^* , конечных множествах конечных подмножеств N^* , и т.д. может быть выражено с помощью $\in$. Что такое пара (x,y) ? Это – множество $\{\{x\},\{x,y\}\}$; Что такое произведение множеств $x \times y$? Это – множество пар, у которых первая координата является элементом x и вторая элемент y . Что такое отображение x в y ? Это – подмножество $x \times y$, являющееся графиком функции. Что такое конечная последовательность элементов x ? Это – отображение n^* в x для некоторого n^* . Короче, все теоретико-множественные понятия, например бинарного отношения на x , группы на x и т.д., которые не выходят за рамки конечных множеств, непосредственно переводимы благодаря отношению $\in$.

Таким образом, если для доказательства свойства натуральных чисел нужны комбинаторные понятия, то вместо того чтобы использовать функцию β , которая была полезной на техническом этапе для определения отношения $\in$, мы можем использовать наше отображение $*$, чтобы свободно работать с N^* в нашей комбинаторике $(\mathbb{N},\in)$, и вернуться в $\mathbb{N}$ обратным отображением из N^* в $\mathbb{N}$.

Например, предположим что мы хотим определить функцию $y = p_x$, отображающую x на x-ое простое число; читатель это умеет с помощью функции β , как в предыдущих примерах; но можно также перейти в N^* и выразить, что y^* – простое число (в смысле N^*), такое, что существует биекция между x^* и множеством простых чисел, меньших числа y^* .

Здесь, экономия времени не фантастическая; она становится таковой если необходимо ввести множества множеств, функций, и т.д. Управление функцией β , чтобы закодировать все эти понятия, становится сложной манипуляцией, в то время как в $(\mathbb{N},\in)$ все происходит естественно : достаточно выразить нашу интуицию. Тем не менее читателю, у которого интуиция ещё недостаточно сформирована (или искажена теоретико-множественной практикой, приведшей к потере доверия этому отношению $\in$) нужно время от времени проводить тяжелые, но более осязаемые доказательства посредством этой функции β : понимание значения этого кодирования конечных множеств в арифметике очень важно.

Мы заключим этот параграф несколькими тонкими рассмотрениями. Мы сейчас работали в стандартной модели $\mathbb{N}$; что произойдет, если мы заменим $\mathbb{N}$ на одно из его нестандартных элементарных расширений N_1 ? Формула, определяющая отношение $\in$ на $\mathbb{N}$ определяет бинарное отношение также на N_1 , которое мы обозначим тем же символом, и $(N_1,\in)$ является, очевидно, элементарным расширением $(\mathbb{N},\in)$, так как каждое свойство $\in$ выражается через сумму и произведение.

Подмножества A из N_1 , соответствующие множествам в смысле этой комбинаторики, то есть подмножества A из N_1 , соответствующие некоторому a из N_1 такому, что для каждого x из N_1 , $x \in a$ тогда и только тогда, когда x в A , будут называться *"множествами, кодированными в модели N_1"*, или еще *"конечными множествами в смысле N_1"*. Все действительно конечные подмножества N_1 кодируются таким образом, так как следующее предложение является теоремой арифметики:

$$(\forall x_1)\dots(\forall x_n)(\exists y)(\forall x)(x \in y \leftrightarrow (x = x_1 \vee \dots \vee x = x_n)) \ ;$$

Но следующая аксиома также истинна в арифметике, которая говорит, что для любого x сегмент $[0, x]$ закодирован:

$$(\forall x)(\exists y)(\forall z)(z \in y \leftrightarrow z < x) \ .$$

Следовательно, среди этих конечных в смысле N_1 множеств, находятся и те, у которых число элементов x (более точно, x^*) нестандартное; Значит, рассматриваемые вне модели, они бесконечны, но что касается свойств, выразимых на нашем языке, они ведут себя точно так же, как конечные множества. Кроме того, модель $(N_1, \in)$ удовлетворяет аксиоме "каждое множество конечно", то есть "каждое множество находится в биекции с натуральным числом" !

Понятие стандартного или нестандартного числа ощутимо только если рассматривать нашу модель извне или на более мощном языке. Каждая модель арифметики живет с мыслью, что она составлена из настоящих натуральных чисел: только внешний наблюдатель лишен этой иллюзии.

7.e Кодирование формул, теорема Тарского

Так как мы располагаем комбинаторикой, мы можем кодировать формулы языка $(0, 1, \leq, +, \cdot)$, то есть их представлять числами и так, чтобы манипуляции на формулах становились определимыми операциями в арифметике. Мы хотим, таким образом, инъективно сопоставить каждой формуле свой код; для этого сначала упорядочим все символы языка : скобки $(,)$, логические символы $\neg, \vee, \wedge, \exists, \forall$ сигнатурные символы $=, 0, 1, \leq, +, \cdot$, символы переменных $x_1, x_2, x_3 \dots$, и в этом порядке им сопоставим числа $0, 1, 2, 3, 4 \dots$. Слово является конечной последовательностью $a_0, \dots, a_n$ этих символов; его можно представлять, например, числом $p_0^{a_o+1} \cdot \dots \cdot p_n^{a_n+1}$, где p_i обозначает i-ое простое число: символ, который находится в i-ом месте, – это степень p_i минус один. Видно сразу, что множество кодов слов легко определимо в арифметике: это множество таких чисел x , что если простое число p делит x , то каждое простое число, меньшее p, делит x . Более сложно, но можно определить множество кодов формул благодаря функции β.

Вот почему мы откажемся от этого кодирования в пользу нашей комбинаторики $(\mathbb{N}, \in)$; действительно, слово есть не что иное как конечная последовательность символов, то есть отображение n^* в конечное подмножество нашего

списка символов из $\mathbb{N}$ (можно брать и N^*): это непосредственно выражается в структуре $(\mathbb{N}, \in)$. Слова являются таким образом конечными последовательностями в смысле $(\mathbb{N}, \in)$. Как отличить формулы от других слов? Вводя список их подформул: слово m является формулой, если существует конечная последовательность $m_0, \ldots, m_n$ слов, такая, что последнее есть m и каждая m_i либо атомна, либо является конъюнкцией или дизъюнкцией двух предшествующих слов этой последовательности, либо является отрицанием или квантификацией предыдущего слова. Все это непосредственно выразимо в $(\mathbb{N}, \in)$ как только покажут, как определяются атомные формулы: это слова такого-то или такого вида.

Все понятия которые касаются формул и которые не выходят за комбинаторику (т.е. которые включают только конечные множества) определимы в арифметике: это понимается единообразно в модели $(\mathbb{N}, \in)$; если вы не хотите её использовать, то надо будет каждый раз манипулировать функцией β . Например функции, которые формуле или, более точно, её коду, сопоставляют её сложность, её ранг квантификации, код множества её подформул, код множества её свободных переменных и т.д., определимы. Значит, можно выразить в арифметике, что формула является предложением, то есть она не содержит свободных переменных.

Но как определить то, что формула $f(\bar{x})$ удовлетворяется кортежем $\bar{a}$? Индукцией по сложности f ? Конечно, но индукция имеет дело с парой (f, A) , где A является множеством кортежей, удовлетворяющих f . Так как это множество A может быть бесконечным и убежать из нашей комбинаторики, то непонятно, как проводить это определение индукцией. Невозможность этого утверждается следующей теоремой, которая выдвинута вперед, так как она очень точно указывает пределы выразительной силы арифметики:

Теорема 7.9 (Тарский) *Множество кодов предложений,истинных в арифметике, не определимо арифметической формулой.*

Доказательство. Итак допустим, что существует формула $V(x)$ с одной свободной переменной x , такая, что числа n , удовлетворяющие ей, были точно кодами истинных предложений. Множество A кодов формул с единственной свободной переменной x определимо, так же как и функция φ , сопоставляющая паре (n, m) , где n в A , код предложения, полученного заменой в формуле с кодом n переменной x числом m .

Тогда обозначим через $V(x, y)$ формулу $V(\varphi(x, y))$; мы видим, что эта формула удовлетворяется такими парами (n, m), что n – код формулы, имеющей единственную свободную переменную x , такой, что предложение, полученное из неё заменой x на m, было истинным. Пусть тогда n_0 – код формулы $\neg V(x, x)$; мы не сможем выйти из следующей дилеммы :

– если $V(n_0, n_0)$ истинно, то $\neg V(n_0, n_0)$ истинно ,

– если $V(n_0, n_0)$ ложно, $\neg V(n_0, n_0)$ ложно.

□

Замечание. Мы должны были выбрать вполне определенное кодирование, но ясно, что в этом выборе имеется большой произвол: его можно модифицировать, но сущность от этого не изменится; необходимо только, чтобы оно позволило арифметически выразить "обычные" операции на формулах (например замена переменной величины константой, отрицание, и т.д.). Если четные номера сопоставим истинным предложениям, а нечетные номера – ложным предложениям, то у нас нет никаких шансов доказать теорему Тарского.

7.f Иерархия арифметических множеств

Говорят, что подмножество $\mathbb{N}^n$ – *арифметическое*, если оно образовано из n-ок, удовлетворяющих некоторой формуле $f(x)$ в языке арифметики; говорят ещё, что подмножество определимо в арифметике. Мы приступаем к классификации арифметических формул и множеств, которые они определяют, по числу кванторов этих формул в пренексной форме. Мы уже говорили в разделе 2.a о приведении к пренексной форме в общих чертах; здесь мы собираемся определить специальные пренексные формы в арифметике, вводя понятие "ограниченных квантификаций".

В формулах вида $(\exists y)(y \leq x \wedge f(x,y))$ или $(\forall y)(y \leq x \to f(x,y))$ со свободной переменной x указанные кванторы называются ограниченными: чтобы понять истинна ли формула на n , достаточно проверить только те y , которые меньше n ; как только известно n , нужно сделать лишь конечное число проверок; вполне понятно, что такого рода квантификации гораздо более простой природы, чем неограниченные кванторы, и что надлежит их различать. Итак, введем обозначения: $(\exists y \leq x)f$, $(\forall y \leq x)f$ как сокращения $(\exists y)(y \leq x \wedge f)$, $(\forall y)(y \leq x \to f)$; в формулах $(\exists y < x)f$, $(\forall y < x)f$ *переменная* x *– свободная*, даже если она не свободна в f .

Формула называется Δ_0-формулой, или еще с *ограниченной квантификацией*, если все его кванторы ограничены; точно так же, как формула приводится к пренексной форме, легко видеть, что Δ_0-формула эквивалентна Δ_0-формуле, у которой все кванторы стоят впереди.

Σ_1-*формула* есть формула, имеющая вид $(\exists x)f$, где f есть Δ_0-формула ; Π_1-*формула* имеет вид $(\forall x)f$ для некоторой Δ_0-формулы f. И индукцией по n определим классы Σ_n- и Π_n-формул для $n > 1$: Σ_{n+1}-*формула* имеет вид $(\exists x)f$, где f есть Π_n-формула; Π_{n+1}-*формула* имеет вид $(\forall x)f$, где f есть Σ_n-формула. Индекс n означает таким образом, что перед формулой имеется n кванторов, поочередно $\exists$ и $\forall$; Σ означает что формула начинается с $\exists$, и Π , что она начинается $\forall$.

Теорема 7.10 *В арифметике, конъюнкция или дизъюнкция двух* Σ_n*- формул эквивалентна* Σ_n*-формуле; ограниченная квантификация, или экзистенциальная квантификация, примененная к* Σ_n*-формуле дает формулу, эквивалентную* Σ_n*-формуле; отрицание* Σ_n*-формулы эквивалентна* Π_n*-формуле.*

Конъюнкция или дизъюнкция двух Π_n*-формул эквивалентна* Π_n*-формуле; ограниченная квантификация, или универсальная квантификация, применен-*

ная к Π_n*-формуле, дает формулу, эквивалентную* Π_n*-формуле; отрицание* Π_n*-формулы эквивалентна* Σ_n*-формуле.*

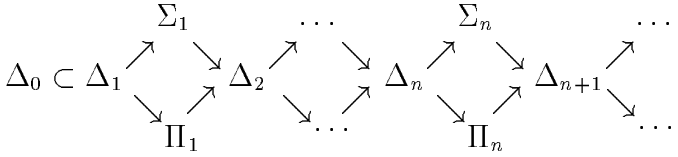
Доказательство. Индукцией по n: Σ_{n+1}-формула имеет вид $(\exists x)f$, где f есть Δ_0- или Π_n-формула в зависимости от значения n; $(\exists x)f \wedge (\exists y)g$, $(\exists x)f \vee (\exists y)g$ эквивалентны соответственно $(\exists x)(\exists y)(f \wedge g)$, $(\exists x)(\exists y)(f \vee g)$, при условии, что в первом случае в случае необходимости изменяются имена связанных переменных так, чтобы x не была свободной в g , а y – в f ; $(\exists y)(\exists x)f$ эквивалентна $(\exists z)(\exists y \leq z)(\exists x \leq z)f$. Формула вида $(\exists y \leq u)(\exists x)f$ эквивалентна формуле $(\exists z)(\exists y \leq u)(\exists x \leq z)f$; $(\forall y \leq u)(\exists x)f$ эквивалентна $(\exists z)(\forall y \leq u)(\exists x \leq z)f$, действительно, каждому y, меньшему, чем u, соответствует x , и так как этих x конечное число, они мажорируются некоторым z . Наконец $\neg(\exists x)f$ эквивалентна $(\forall x)\neg f$. Для Π_{n+1} рассуждения аналогичны. □

Из теоремы 7.10 следует, что каждая формула эквивалентна Σ_n- или Π_n-формуле для некоторого n. Будем говорить, что формула есть "Σ_n- формуле", когда она эквивалентна, очевидным образом, Σ_n-формуле; например, скажем, что отрицание Σ_n-формулы есть Π_n-формула, хотя, формально, это не так; скажем так же, что Σ_n-формула есть также Σ_{n+1}- и Π_{n+1}-формула (квантифицируйте по переменной, не содержащейся в формуле).

Теперь будем говорить, что $A \subset N^k$ есть Σ_n-множество, если оно имеет Σ_n-определение, то есть если оно составлено из множества кортежей, удовлетворяющих некоторой Σ_n-формуле, и что оно есть Π_n–множество, если имеет Π_n-определение. Естественно, если множество определяется Σ_n-формулой для некоторого n, то возможно, что эта формула эквивалентна гораздо более низкой формуле в этой иерархии.

Σ_n-множество, являющееся одновременно Π_n-множеством, называется Δ_n–множеством, т.е. если его дополнение – Σ_n-множество. У нас нет Δ_n-формул: задание Δ_n-множества – это задание Σ_n-определения этого множества и Π_n-определения этого множества, эквивалентных,следовательно, в арифметике. Классы Σ_n-множеств и Σ_n-формул будем часто отождествлять и обозначать просто через Σ_n. Аналогично обозначаем класс Π_n- и Δ_n-множеств.

Как следствие теоремы 7.10 для классов Δ_n , Σ_n , Π_n получаем следующую диаграмму включений, обозначенных стрелками :



Мы увидим, что каждое из этих включений строгое, то есть что иерархия не обрывается с некоторого n . Вкратце, классы Δ_n являются алгебрами Буля относительно $\vee, \wedge, \neg$, замкнутыми относительно ограниченных квантификаций; классы Σ_n и Π_n замкнуты относительно $\vee, \wedge$ и ограниченных квантификаций; классы Σ_n замкнуты относительно $\exists$, классы Π_n – относительно $\forall$, дополнение Σ_n-множества принадлежит классу Π_n, а дополнение Π_n-множества – классу Σ_n . Отметим мимоходом, что в теоретико-множественных терминах экзистенциальная квантификация A называется проекцией A из ω^{k+1} на ω^k .

В действительности оказывается, чтобы установить эту иерархию введение ограниченных кванторов необязательно. Назовем *диофантовым* множество, определимое формулой вида $(\exists y_1)\dots(\exists y_n)f$, где число кванторов $\exists$ необязательно равно 1, а f является конъюнкцией уравнений $P(x,y)=Q(x,y)$, где P и Q – многочлены с натуральными коэффициентами. Так как такое уравнение является формулой без кванторов, ясно, что каждое диофантово множество есть Σ_1 , но так же истинно, что каждое Σ_1-множество диофантово; это теорема Матиясевича, которая позволяет ответить на знаменитую проблему Гильберта; я не буду здесь рассматривать эту теорему.

Прежде чем продолжить, мы проведем несколько классических манипуляций на множествах Σ_n и Π_n. Мы говорим, что функция из ω^k в $\omega^{k'}$ есть Σ_n-функция, если её график является Σ_n-подмножеством в $\omega^{k+k'}$; здесь, функция *всюду определена*: каждому $\bar{x}$ из ω^k соответствует один и единственный $\bar{y}$ из $\omega^{k'}$. Если f является функцией из ω^k в $\omega^{k'}$, а g – функцией из ω^k в $\omega^{k''}$, то *склейкой* f и g называется функция из ω^k в $\omega^{k'+k''}$, которая кортежу $\bar{x}$ сопоставляет сочленение $f(\bar{x})g(\bar{x})$; если f является функцией из ω^k в $\omega^{k'}$, то её *координаты* - композиция f с одной из k' канонических проекций $\omega^{k'}$ в ω .

Лемма 7.11 *График Σ_n-функции есть Π_n-множество; композиция двух Σ_n-функций является также Σ_n-функцией; обращение Σ_n-биекции и также склейка двух Σ_n-функций является Σ_n-функцией; наконец, функция есть Σ_n-функция тогда и только тогда, когда каждая из её координат есть Σ_n-функция.*

Доказательство. Поскольку f – всюду определенная функция, отношение $\bar{y}\neq f(\bar{x})$ определяется формулой $(\exists\bar{z})(\bar{z}=f(\bar{x})\wedge\bar{z}\neq\bar{y})$ из класса Σ_n, если такова формула $\bar{z}=f(\bar{x})$; если h – композиция f и g , то отношение $\bar{z}=h(\bar{x})$ определяется через $(\exists\bar{y})(\bar{z}=g(\bar{y})\wedge\bar{y}=f(\bar{x}))$; биекция и обратное для неё отображение имеют один и тот же график (поменяйте ролями $\bar{x}$ и $\bar{y}$).

Граф склейки h функций f и g определяется формулой $\bar{y}_1=f(\bar{x})\wedge\bar{y}_2=g(\bar{x})$; каноническая проекция ω^k на его i-ую координату определяется Δ_0-формулой без квантора $y=x_i$, следовательно, если f есть Σ_n-функция, то такова же и её композиция с проекцией; обратно, любая функция f является склейкой своих координат. □

Лемма 7.12 *Пусть $f(\bar{x})$ – Σ_n-функция; если $\varphi(\bar{y})$ – Σ_n-формула, то такова и $\varphi(f(\bar{x}))$; и если $\varphi(\bar{y})$ – Π_n-формула, то такова и $\varphi(f(\bar{x}))$.*

Доказательство. Формула $\varphi(f(\bar{x}))$ может быть записана по выбору как $(\exists\bar{y})(\bar{y}=f(\bar{x})\wedge\varphi(\bar{y}))$ или $(\forall\bar{y})(\bar{y}\neq f(\bar{x})\vee\varphi(\bar{y}))$!

□

То же самое можно сказать по-другому:

Лемма 7.13 *Прообраз Σ_n-множества относительно Σ_n-функции является Σ_n-множеством; прообраз Π_n-множества относительно Σ_n-функции является Π_n-множеством.*

Доказательство. Записываем $\bar{x}\in f^{-1}(A)$ по нашему желанию в виде $(\exists\bar{y})(\bar{y}=f(\bar{x})\wedge\bar{y}\in A)$ или $(\forall\bar{y})(\bar{y}\neq f(\bar{x})\vee\bar{y}\in A)$.

□

Лемма 7.14 *Образ Σ_n-множества при Σ_n-функции является Σ_n-множеством.*

Доказательство. Запишем $\bar{x} \in f(A)$ в виде $(\exists \bar{y})(\bar{x} = f(\bar{y}) \wedge \bar{y} \in A)$.

□

Характеристическая функция множества A отображает x на 1 , если $x \in A$, и отображает x на 0, если $x \notin A$.

Лемма 7.15 *Δ_n-множества и только они имеют характеристическую Σ_n-функцию.*

Доказательство. Пусть f – характеристическая функция A ; если $A \in \Delta_n$, то график f определяется Σ_n-формулой: $(\bar{x} \in A \wedge y = 1) \vee (\bar{x} \notin A \wedge y = 0)$; и если f – Σ_n-функция, A определяется формулой $f(\bar{x}) = 1$, а его дополнение определяется формулой $f(\bar{x}) = 0$.

□

Лемма 7.16 *Для любых k и h , существует Σ_1-биекция между ω^k и ω^h .*

Доказательство. Рассмотрим биекцию f из ω в $\omega \times \omega$, состоящую в перечислении ω^2 по возрастанию $x + y$, затем по возрастанию y : разбиваем четверть плоскости $\omega \times \omega$ на отрезки, параллельные второй диагонали, помещаем их впритык один за другим и пронумеруем. В n первых отрезках, соответствующих $x + y = 0$, $x + y = 1$, ..., $x + y = i$, ..., $x + y = n - 1$, содержится $1 + 2 + \cdots + n = n(n + 1)/2$ пар; следовательно, функция g , обратная к f , определяется формулой $g(x, y) = (x + y)(x + y + 1)/2 + y$; g – Σ_1-биекция ω^2 на ω (если вас геометрия не убеждает, то вы можете всегда доказывать биективность индукцией по x и y), так как её график определяется Δ_0-формулой $2z = (x + y)(x + y + 1) + 2y$. Функция, которая $(x_1, \ldots, x_k, x_{k+1})$ сопоставляет $(x_1, \ldots, g(x_k, x_{k+1}))$, является Σ_1-биекцией ω^{k+1} на ω^k, откуда с помощью композиции следует общий результат.

□

Так как можно свести ω^k к ω всегда Σ_1-биекцией, сохраняющей иерархию, в основном говорят, когда речь идет об арифметических множествах, только о подмножествах ω , или функциях из ω в ω : введение ω^k не является большим обобщением. Например, с помощью биекции из ω^2 в ω докажем следующую лемму, которая будет полезна впоследствии:

Лемма 7.17 (Принцип Σ_n-выбора) *Пусть $R(x, y)$ – бинарное Σ_n-отношение на натуральных числах, такое, что для каждого x существует такой y , что (x, y) удовлетворяет R. Тогда существует Σ_n-функция f из ω в ω, такая, что для каждого x пара $(x, f(x))$ удовлетворяет R .*

Доказательство. Если бы мы попытаемся сопоставить x наименьшее y, такое, что $N \vdash R(x, y)$, то чтобы выражение "для каждого $z < y$, $(x, z) \notin R$" было Σ_n-формулой, необходимо Π_n-определение для R. Лучше мы перепишем R в виде $(\exists t)S(x, y, t)$, где S есть Δ_0 или Π_{n-1} в зависимости от значения n , и берем y из пары (y, t) с наименьшим номером. Пусть π – каноническая Σ_1-биекция ω^2 на ω и пусть π_1 и π_2 – две Σ_1-проекции обращения π : для каждого

x пара $(\pi_1(x), \pi_2(x))$ – единственная такая, что $x = \pi(\pi_1(x), \pi_2(x))$; Рассмотрим функцию $y = f(x)$, график которой определяется следующей Σ_n-формулой:

$$(\exists z)(S(x, \pi_1(z), \pi_2(z)) \wedge (\forall u < z)\neg S(x, \pi_1(u), \pi_2(u)) \wedge y = \pi_1(z)) \ .$$

□

Лемма 7.18 *Непустое подмножество ω есть Σ_n-множество если и только если оно образ Σ_n-отображения из ω в ω ; оно есть Δ_n-множество если и только если оно образ возрастающего Σ_n-отображения из ω в ω .*

Доказательство. Множество ω всех натуральных чисел определяется Δ_0-формулой $x = x$; таким образом, по 7.14 образ Σ_n-функции есть Σ_n-множество. Обратно, предположим, что A содержит a и определяется формулой $(\exists y)f(x, y)$, где f из Π_{n-1} или Δ_0 в зависимости от значения n. Рассмотрим функцию g из ω^2 в ω , которая пару (x, y) отображает на x если $f(x, y)$ удовлетворяется, и отображает на a иначе; её график $z = g(x, y)$ определяется Δ_0-формулой $(f(x, y) \wedge z = x) \vee (\neg f(x, y) \wedge z = a)$, и образ g есть в точности A ; остается брать композицию g с Σ_1-биекцией ω на ω^2.

Предположим теперь, что f – возрастающая Σ_n-функция из ω^2 в ω ; таким образом, имеем $f(x+1) \geq f(x)$ для каждого x . Если её образ конечен, то есть если f постоянна начиная с некоторого числа, то он множество $\{a_0, \ldots, a_s\}$, определимое формулой $x = a_0 \vee \cdots \vee x = a_s$; иначе дополнение образа f , которое не ограничено в ω , определяется следующей Σ_n-формулой : $x < f(0) \vee (\exists y)(f(y) < x < f(y+1))$; значит, этот образ является Δ_n-множеством.

Пусть f – перечисление непустого множества A натуральных чисел: $f(0)$ есть наименьший элемент A, $f(1)$ – его второй элемент, ... , $f(n)$ – его $(n+1)$-ый элемент ($f(0)$ считается первым, а не нулевым элементом !); если A бесконечно, то f – возрастающая инъекция, биекция между ω и A ; если A конечно, то договоримся, что f повторяет наибольший элемент A : в этом последнем случае график f определяется следующей Δ_0-формулой:

$$(x = 0 \wedge y = a_0) \vee \cdots \vee (x = m-1 \wedge y = a_{m-1}) \vee (x \geq m \wedge y = a_m) \ ;$$

Если A – бесконечное Δ_n-множество, то $y = f(x)$ определяется следующей Σ_n-формулой, где функция β должна служить для того, чтобы кодировать последовательность $f(0)$, $f(1)$, ... ,$f(x)$:

$$(\exists u)(\exists v)\{[r(u, v) \in A \wedge ((\forall t \leq v)(t < r(u, v) \to t \notin A)] \wedge$$

$$\wedge (\forall i \leq x)(r(u, iv) \in A \wedge r(u, (i+1)v) \in A \wedge r(u, iv) < r(u, (i+1)v) \wedge$$

$$\wedge ((\forall t \leq y)(r(u, iv) < t < r(u, (i+1)v) \to t \notin A))) \wedge r(u, (x+1)v) = y\},$$

поскольку отношения $w = r(u, v)$, эквивалентные $w < v \wedge (\exists z \leq u)u = zv + w$, и отношения $t \in A$, $t \notin A$ выразимы Σ_n-формулами.

□

Лемма 7.19 *Если A является Σ_n-подмножеством в ω и если $f_1, \ldots, f_s$ являются Σ_n-функциями из ω^{m_i} в ω , то замыкание A этими функциями есть также Σ_n-множество.*

Доказательство. Элемент этого замыкания получается из элементов A итерацией композиций f_i ; если выберем какой-либо способ такого получения элемента a , то получаем конечную последовательность $a_0, \ldots, a_n$ с $a_n = a$, и такую, что каждый a_j либо лежит в A , либо получается как f_i от предыдущих элементов: закодируем эту последовательность посредством функции β .

□

В двух предыдущих леммах, мы закодировали рекурсивные определения с помощью функции β; поймем, что такие действия не выводят за класс функций Σ_n (это позволяет понять, что все "обычные" функции лежат в Σ_1); более точно, мы говорим, что функция f из ω^{k+1} в ω определена через функцию g из ω_k в ω (g имеет на одну переменную меньше, чем f ; если $n = 0$, то это константа) и функцию h из ω^{k+2} в ω (h имеет, таким образом, на одну переменную больше, чем f) индукцией (говорят также, рекурсией) относительно переменной y , если f – функция (обязательно единственная), определенная следующими условиями :

$$f(x_1, \ldots, x_k, 0) = g(x_1, \ldots, x_k) \ ,$$

$$f(x_1, \ldots, x_k, y+1) = h(x_1, \ldots, x_k, y, f(x_1, \ldots, x_n, y)) \ .$$

Функция g называется функцией *начальных данных*, равной $f(\bar{x}, 0)$; а функция h – *функцией перехода*, позволяющей вычислить $f(\bar{x}, y+1)$ зная значение $f(\bar{x}, y)$.

Лемма 7.20 *Если g и h – Σ_n-функции, то функция f, определенная индукцией через них, также является Σ_n-функцией.*

Доказательство. Чтобы определить отношение $z = f(x_1, \ldots, x_k, y)$, закодируем последовательность $f(x, 0), f(x, 1), \ldots, f(x, y)$ с помощью функции β .

□

Класс Δ_0 , служащий началом иерархии, создан искусственно, и его элементы трудно характеризуемы; многое не изменилось бы, если рассматривать квантификации типа $(\exists y \leq 2x)$, $(\forall y \leq 2x)$, или даже $(\exists y \leq 2^x)$, $(\forall y \leq 2^x)$, но однако эти очень простые квантификации выводят за класс Δ_0 . Напротив, видно, что если f – Σ_n-функция и φ – формула, то формулу $(\exists y \leq f(x))\varphi$ можно переписать по выбору $(\exists z)(\exists y \leq z)(z = f(x) \wedge \varphi)$ или $(\forall z)(\exists y \leq z)(z \neq f(x) \vee \varphi)$, в то время как $(\forall y \leq f(x))\varphi$ можно переписать по выбору $(\exists z)(\forall y \leq z)(z = f(x) \wedge \varphi)$ или $(\forall z)(\forall y \leq z)(z \neq f(x) \vee \varphi)$, так, что *квантификации, ограниченные Σ_n-функциями, не выводят за класс Σ_n , ни за класс Π_n*, ни, следовательно, за класс Δ_n . Эта надежность классов Δ_n , Σ_n , Π_n показывает, что они создают очень естественную иерархию для арифметических множеств, и мы увидим в конце этого параграфа, что более высокое место в этой иерархии действительно означает большую сложность определения.

Функции из Σ_1 называются также *рекурсивными функциями*, так как определение рекурсией является одним из главных способов, который позволяет их получить; иногда их называют также *эффективно вычислимыми функциями*, так как они являются выражением на математических терминах немного туманной идеи "функций, вычислимых чисто механическим способом" (говорят также: вычислимый алгоритмом). Множества Σ_1 , являющиеся их образами, называются *рекурсивно*, или еще *эффективно, перечислимыми* множествами; что касается Δ_1-множеств, у которых характеристическая функция рекурсивна, они называются *рекурсивными* или еще *разрешимыми*.

Под алгоритмом для механического вычисления функции f понимают задание программы или списка инструкций, которую вычислитель, начиная с данного x , осуществляет шаг за шагом, обладающее следующим свойством: каково бы ни было число x , данное вначале, через некоторое время вычислитель получит приказ остановиться и выводить число $f(x)$. Вычислитель, который может быть, например, тем, что называют в коммерции компьютером, не имеет никакую самостоятельность, и никакую интеллектуальную инициативу: он умеет только придерживаться инструкций данного списка; но в этом чисто теоретическом подходе к вычислимости мы не заботимся о возможности выполнения вычислений реальным механическим устройством и, в частности, мы пренебрегаем временем и пространством необходимыми для вычислений, лишь бы только они завершались.

Поймем сначала, что Σ_1-функция f вполне вычислима существом с самыми ограниченными интеллектуальными возможностями, но которое имеет беспредельную любовь к вычислениям совершенно идиотских, механических операций. Отношение $y = f(x)$ имеет вид $(\exists z)\varphi(x, y, z)$, где φ – Δ_0-формула; однако проверка выполнимости бесквантворной формулы$\varphi(\bar{x})$ на кортеже $\bar{a}$ доступно любому ученику начальной школы: достаточно уметь складывать, умножать и вычитать (для проверки: $a \leq b$?) Если даны m, n, p , то проверку истинности предложения $\varphi(m, n, p)$ можно осуществить дебильным методом: так как все кванторы ограничены числом $\max(m, n, p)$, то необходимо проверить лишь конечное число значений для связанных переменных, и достаточно запрограммировать наш оператор так, чтобы он проводил все испытания с числами меньшими $max(m, n, p)$. Очевидно, этот алгоритм непрактичен: рост времени вычислений вместе с увеличением данных состарит благородного программиста, но он совершенно удовлетворяет нас, живущих в рае объектов, которые существуют только в теории. И вот инструкции, которые мы даем нашему оператору: начинай с данного x ; нумеруй все пары (y, z) натуральных чисел посредством канонической Σ_1-биекции ω^2 на ω ; для каждой пары (y, z) проверь истинность формулы $\varphi(x, y, z)$; остановись как только ты найдешь такое истинное предложение; выводи значение y соответствующей пары.

А что насчет обратного утверждения? Для этого нужно поразмышлять немного о том, что может быть механической процедурой; нашим исполнителем может быть вычислитель с ластиком и карандашом, пишущий на листе бумаги, или более современно, читающая (и пишущая) головка с лентой, разбитой на ячейки, намагниченные или размагниченные; его программа состоит из списка инструкций $I_0, \ldots, I_n$, каждая из которых следующего типа: если ты обнаружил то-то (например, перед тобой находится намагниченная ячей-

ка), то осуществляй такую-то операцию (например, размагничивай ячейку, или перемещайся на одну ячейку налево, или направо, и т.д.) и затем перейди к i-ой инструкции; иначе (ячейка перед тобой – не намагниченная) осуществляй такую-то операцию, и перейди к j-ой инструкции. Мы можем закодировать числом, благодаря нашей комбинаторике, состояние листа бумаги, или магнитной ленты, перед нашим оператором так же, как и инструкцию, которую он должен осуществить: это число, которое называют "этапом вычисления", кодирует положение, где находится оператор. Задание программы есть не что иное, как задание "функции перехода", позволяющей переходить от этапа к следующему этапу. Должно быть ясно ввиду элементарности тестов и операций, выполняемых нашим оператором, что эта функция перехода будет иметь график, определенный формулой с квантификациями, ограниченными не очень страшной рекурсивной функцией. В этих условиях, по 7.20 функция, сопоставляющая паре (x, z) код z-ого этапа вычисления, полученного от начального данного x , с I_0 в качестве начальной инструкции, также рекурсивна. Функция $y = f(x)$, вычисленная этим способом, определяется Σ_1-формулой : "существует момент времени z, такой, что оператор, начиная с данного x , после z этапов получил приказ остановиться, и выводить x". Запомним интерпретацию неограниченного экзистенциального квантора в этой формуле: он по сути соответствует длительности вычисления.

Предыдущие рассуждения выглядели бы более строгими, если бы мы дали математическое определение "процедур механических вычислений"; по этому поводу, высказывание "функция вычислима если и только если она рекурсивна" известна под именем *тезиса Чёрча*: говорят тезис, а не теорема Чёрча, потому что, в отсутствии точного определения вычислимости, это мнение, правдоподобность которого можем подтверждать только аргументами такого же типа, что мы наметили. Этот тезис поддерживается тем, что все многочисленные формальные подходы к вычислимости (один из них через *машины Тьюринга*, которые можно рассматривать как абстрактные эквиваленты наших компьютеров; фактически, они являются их весьма далекими прародителями и, впрочем, именно компьютеры надо было бы скорее рассматривать в качестве конкретных реализаций машин Тьюринга, изобретенных до компьютеров!), предпринятые до сих пор, определяют один и тот же класс Σ_1-функций. Кроме того этот тезис не без пользы: часто, чтобы найти Σ_1-формулу, определяющую график функции, кодируют в арифметике естественный способ её вычисления.

И даже тезис Чёрча допускает следующее усиление: "каждая функция из $\mathbb{N}$ в $\mathbb{N}$ есть Σ_1-функция, если только она не является специально построенным контрпримером"! Вот это совершенно парадоксальное высказывание, так как имеется только счетное число Σ_1-функций (не более, чем формул), и они составляют таким образом совсем незначительное множество среди всех функций из $\mathbb{N}$ в $\mathbb{N}$. Но, однако, опыт показывает, что функции и множества, которые появляются "естественно" в математическом контексте, лежат в классе Σ_1 , за очень редкими исключениями (например проблема Гильберта, решенная Матиясевичем), и кроме того, это даже легко доказывается.

Фактически, все функции, о которых может думать нормальный математик принадлежат к еще более ограниченному классу – классу примитивно рекур-

сивных функций. Это – функции, которые получаются из функций $x \mapsto 0$, $x \mapsto x$, $x \mapsto x+1, \ldots, (x_1, \ldots, x_i, \ldots x_n) \mapsto x_i, \ldots$ композициями, склейками и определениями рекурсией. Это – не очень естественный класс функций, и если Σ_1-функцию в общем легко выявить (при наличии небольшого опыта, в конце концов находят Σ_1-формулу её графика), то часто трудно доказать, что она примитивно рекурсивна: нет другого способа, кроме последовательного построения, начиная с базисных функций. Так как эти функции имеют свойства, касающиеся аксиоматизации арифметики, а также в качестве примера, мы покажем, что функция γ леммы 7.8 примитивно рекурсивна :

Лемма 7.21 *Функция $\gamma(x,y)$ примитивно рекурсивна .*

Доказательство.

1° Функция $Min(1,x)$ примитивно рекурсивна :
$Min(1,0) = 0$, $Min(1,x+1) = 1$,

2° Полагаем $x \dot{-} y = 0$ если $y > x$, $x \dot{-} y = x - y$, если $x \geq y$; функция $x \dot{-} 1$ примитивно рекурсивна : $0 \dot{-} 1 = 0$, $(x+1) \dot{-} 1 = x$,

3° Функция $x \dot{-} y$ примитивно рекурсивна : $x \dot{-} 0 = x$, $x \dot{-} (y+1) = (x \dot{-} y) \dot{-} 1$,

4° Пусть $f(x,y)$ – частичная сумма разложения по основанию 2 числа x до y : если $x = \varepsilon + \varepsilon_1 2 + \cdots + \varepsilon_k 2^k$, тогда $f(x,y) = \varepsilon + \varepsilon_1 2 + \cdots + \varepsilon_y 2^y$; это примитивно рекурсивная функция: $f(0,y) = 0$; $f(x+1,y) = f(x,y) + 1$, если $f(x,y) + 1 < 2^{y+1}$, и $f(x+1,y) = 0$ если $f(x,y) + l = 2^{y+1}$; или еще $f(x+1,y) = Min(1, 2^{y+1} \dot{-} (f(x,y)+1)) \cdot (f(x,y)+1)$, и функция перехода примитивно рекурсивна, так как таковы сумма, произведение и показательная функция.

5° Тогда $\gamma(x,0) = f(x,0)$, $\gamma(x,y+1) = Min(1, f(x,y+1) \dot{-} f(x,y))$.

□

После рассмотрения этого примера, читатель должен быть теперь убежден что все введенные в разделе 7.f функции о формулах (сопоставляющая формуле её ранг квантификации, или код множеств её свободных переменных, и т.д.), в определении которых рекурсия играла главную роль, рекурсивны и даже примитивно рекурсивны; и что такие множества, как множества предложений, множества Σ_n-предложений и т.п., все лежат Δ_1. Это можно принять только слепой верой в обобщенный тезис Чёрча или проверкой каждого отдельного случая, которую мы оставим подозрительному читателю. После этого, мы можем уточнить теорему Тарского следующим образом :

Теорема 7.22 *Множество кодов Σ_n-предложений, истинных в арифметике является Σ_n-множеством вне Π_n; множество кодов предложений, истинных в арифметике является Π_n-множеством вне Σ_n.*

Доказательство. Покажем сначала положительную часть теоремы, и прежде всего, что множество кодов Δ_0-предложений, истинных в арифметике, есть Δ_1-множество. Действительно, в Δ_0-формуле $f(a_1, \ldots, a_n)$ все связанные переменные ограничены числом $max(a_1, \ldots, a_n)$, и истинность этого предложения определяется индукцией по парам, образованным подформулой g в f и множеством кортежей ограниченных $max(a_1, \ldots, a_n)$ и удовлетворяющих g. Так как множества таких кортежей конечны, они соответствуют объектам, кодированным в нашей комбинаторике, и высказывание "x является кодом истинного Δ_0-предложения" выражается Σ_1-формулой; таково же и высказывание "x является кодом ложного Δ_0-предложения" , так как преобразование,состоящее в том, чтобы брать отрицание формулы соответствует рекурсивной операции на кодах. Высказывание "x не является кодом Δ_0-предложения, или является кодом ложного Δ_0-предложения", таким образом, есть Σ_1-формула и определяет дополнение нашего множества.

Когда Σ_1-предложение $(\exists x)f(x)$, где f является Δ_0-формулой, истинно? Если существует a, такой, что Δ_0-предложение $f(a)$ истинно. Как только заметим, что функция, которая коду Δ_0-формулы со свободной переменной x и числу a сопоставляет код Δ_0-предложения, полученного заменой x на a в формуле, является рекурсивной, и зная что истинность Δ_0-предложения выражается Σ_1-формулой, видим, что "существует a такой, что $f(a)$ истинно" есть Σ_1-формула. Так как истинные Π_1-предложения соответствуют отрицаниям ложных Σ_1-предложений, они образуют Π_1-множество. Индукцией по n , видим точно так же, что истинные Σ_n-предложения образуют множество, определенное Σ_n-формулой $V\Sigma_n(x)$; что истинные Π_n-предложения образуют множество, определенное Π_n-формулой $V\Pi_n(x)$.

Для отрицательной части, предположим, что существует Π_n-формула $V(x)$, определяющая множество кодов истинных Σ_n-предложений. Рассмотрим формулу $V(x, y) = V(\varphi(x, y))$, определяющую множество пар, у которых первый элемент формула Σ_n с одной свободной переменной, таких, что предложение, полученное заменой этой переменной на y истинна; здесь φ – Σ_1-функция замены переменной на константу. $V(x, y)$ есть Π_n-формула; таким образом, формула $\neg V(x, x)$ эквивалентна Σ_n-формуле с кодом n_0 и мы получаем то же противоречие, что в теореме Тарского.

□

Эта теорема доказывает, что все включения вида $\Delta_n \subset \Sigma_n \subset \Delta_{n+1}$, а также $\Delta_n \subset \Pi_n \subset \Delta_{n+1}$ – строгие. Мы видим, что каждое Σ_n-множество получается просто от "Σ_n-истинности", множества, определенного формулой $V\Sigma_n(x)$. Чтобы проверить, что b принадлежит a-ой Σ_n-формуле (т.е. множеству, определенному Σ_n-формулой с кодом a), надо проверить, что $\varphi(a, b) \in V\Sigma_n(x)$; по этой причине, это множество $V\Sigma_n(x)$, которое сложнее всех множеств Σ_n , называется "Σ_n-универсальным множеством".

Можно также релятивизировать иерархию и определять рекурсивность или Σ_n-множества относительно множества A. Тогда каждое Σ_n-множество рекурсивно в $V\Sigma_n(x)$. Если A и B взаимно рекурсивны по отношению друг к другу, то говорят, что они имеют одну и ту же степень, и изучение этих степеней, которые мы только упоминаем, составляет теорию рекурсивности.

7.g Некоторые аксиомы, модели фрагментов арифметики

Мы собираемся в этом параграфе рассматривать некоторые аксиомы, которым удовлетворяют сумма и произведение натуральных чисел, и мы поймем, в какой мере результаты предыдущих параграфов остаются в силе для структур, являющихся моделями только некоторого фрагмента арифметики. Назовем *минимальной арифметикой* следующее конечное множество аксиом A_0 :

$$(\forall x)(x+1 \neq 0) \qquad (\forall x)(\forall y)(x+1=y+1 \to x=y)$$
$$(\forall x)(0 \leq x) \qquad (\forall x)(\forall y)(y \leq x+1 \leftrightarrow y \leq x \vee y = x+1)$$
$$(\forall x)(x=0 \vee \neg(x \leq 0)) \qquad (\forall x)(\forall y)(x+1 \leq y \leftrightarrow x \leq y \wedge y \neq x)$$
$$(\forall x)(x+0=x) \qquad (\forall x)(\forall y)[x+(y+1)=(x+y)+1]$$
$$(\forall x)(x \cdot 0 = 0) \qquad (\forall x)(\forall y)[x \cdot (y+1) = x \cdot y + x]$$

Аксиомы A_0 определяют поведение 0 по отношению к арифметическим операциям так же, как и поведение $x+1$, предполагая знание поведения x. Выбор такой системы, образованной из конечного числа универсальных аксиом, не без произвола; мы могли бы например коммутировать переменные x и y в аксиомах, описывающих связи суммы и произведения с последователем.

В модели M системы A_0 отображение $s(x) = x+1$ инъективно; 0 лежит вне образа s , но там могут быть другие точки не-последователи. Для натурального числа n обозначим тем же символом n n-ого последователя 0 в M. Мы видим, что аксиомы A_0 говорят, что элементы, меньшие или равные n, – это $0, \ldots, n-1, n$, а все элементы M , за исключением $0, \ldots, n-1$, больше или равны n . Эти последователи 0 будут называться *стандартными* числами (или элементами) модели M ; это *стандартное подмножество* M является начальным сегментом, каждое стандартное число меньше каждого нестандартного числа (естественно, это использование слова "начальный сегмент" немного противозаконно, так как не можем вывести из A_0 , что $\leq$ есть порядок) ; и кроме того легко видеть, что это стандартное подмножество является ограничением M , изоморфным настоящим натуральным числам, с суммой и произведением. Это влечет, и является первопричиной существования A_0 , что каждое Σ_1-предложение арифметики является следствием A_0 .

Но в остальном A_0 является чрезвычайно слабой теорией, допускающей нестандартные числа с самым фантастическим поведением. Одно из редких не Σ_1-ограничений то, что функция следования не имеет циклов, так как в A_0 можно доказать , что, если $n > 1$, то $(\forall x)(x \leq x+n \wedge \neg(x+n \leq x))$. Вот модель, носитель которой состоит из её стандартного подмножества $0, 1, 2, \ldots$ и второй копии ω : $0', 1', 2', \ldots$; отношение $x \leq y$ выполняется на следующих парах: во всех случаях $n \leq m'$; если n меньше m , то $n' \leq m'$; и если $n+m$ является суммой n и m , то $n'+m = (n+m)'$, $n'+m' = n+m' = m'$; если $n \cdot m$ является произведением n и m , то $n \cdot m' = (n \cdot m)'$, $n' \cdot m = n' \cdot m' = n'$.

Однако, если мы добавим к A_0 следующую аксиому второго порядка :

$$(\forall X)((0 \in X \wedge (\forall x)(x \in X \to x+1 \in X)) \to (\forall x)(x \in X)) \ ,$$

то можем показать, что модель сводится к своему стандартному подмножеству, т.е. структура, образованная суммой и произведением настоящих натуральных чисел, характеризуется с точностью до изоморфизма. Это было замечено в начале этого века итальянским математиком Пеано; по этой причине называют *"арифметикой Пеано"* множество аксиом, образованное из A_0 и всех следующих "аксиом индукции" (по одной аксиоме для каждой формулы f):

$$I(f) \qquad (\forall \bar{x})\{[f(\bar{x},0) \wedge (\forall y)(f(\bar{x},y) \to f(\bar{x},y+1))] \to (\forall y) f(\bar{x},y)\} \ .$$

Этот список аксиом основывается на той же метафизике, что и аксиоматика Пресбургера (см. 7.c) для суммы натуральных чисел. Так как мы не имеем права выражать аксиому индукции, действительную для всех подмножеств модели, мы делаем это по крайней мере для любого подмножества, доступного в нашем языке, то есть определимого формулой арифметики.

Если мы добавим к A_0 аксиомы индукции только для формул из Δ_0 , Σ_n или Π_n, то говорим соответственно о теории Δ_0-индукции, Σ_n-индукции или Π_n-индукции. Отметим мимоходом, что аксиома Δ_0-индукции лежит одновременно в Σ_2 и Π_2 , а аксиома Σ_n или Π_n-индукции является $\Sigma_{n+2}-$ и Π_{n+2}-предложением (замените $f \to g$ на $\neg f \vee g$).

Добавление некоторых аксиом индукции делает множество A_0 более осмысленным; с $I(y = 0 \vee (\exists z \leq y) y = z + 1)$, мы доказываем, что каждое ненулевое число является последователем; мы видим также, простой проверкой доказательства теоремы 7.5, что теория суммы является следствием Δ_0-индукции (и даже конечного числа аксиом Δ_0-индукции, так как свойства евклидова деления доказываются с единственной аксиомой индукции, говорящей о произведении). Мы также доказываем при помощи Δ_0-индукции, что $(\forall x)(\forall y)(x \leq y \leftrightarrow (\exists z) x + z = y)$, из чего следует, что теория порядка полностью выводится также из Δ_0-индукции. При помощи Δ_0-индукции доказывают также, что произведение ассоциативно, коммутативно (и даже верно, что теория произведения, т.е. множество предложений, истинных для натуральных чисел и говорящих только о произведении, является следствием Δ_0-индукции) и дистрибутивно по сложению.

Однако Δ_0-индукция также слаба. Например, из Δ_0-индукции можно вывести теорему "для каждого x, существует простое число, которое не делит x": доказываем индукцией по формуле

$$(\forall x' \leq x)(x' \leq 1 \vee (\exists y \leq x)(\exists z \leq x)(y \geq 2 \wedge$$

$$\wedge (\forall u \leq x)(\forall v \leq x)(y = uv \to u = 1 \vee v = l) \wedge x' = yz)) \ ,$$

что каждое число имеет простой делитель; потом берем простой делитель $x+1$. Но позволяет ли Δ_0-индукция доказать, что "для каждого x существует простое число больше x", т.е. бесконечность множества простых чисел, – это сегодня открытая проблема. Обычно этот элементарный факт доказывают так: рассматривают множество простых чисел меньших x , и берут простой делитель последователя произведения. Чтобы провести это доказательство формально, надо доказать существование кода для множества простых чисел меньших числа x , что не обеспечивается Δ_0-индукцией.

Так как принадлежность, $x \in y$, есть Δ_1-отношение, надо ожидать, что Δ_0-индукция допускает абсурдное поведение для комбинаторики, присоединенной к арифметике. Например, Δ_0-индукция не позволяет доказать, что каждое множество действительно конечно, ни даже, что каждое одноэлементное множество кодируется: действительно, легко видеть, что начальный сегмент модели арифметики, замкнутый относительно суммы и произведения, является моделью Δ_0-индукции; если этот сегмент не замкнут относительно отображения $x \mapsto 2^x$, найдутся одноэлементные множества без кодов; этот метод не может быть приложен к предыдущей проблеме, так как известно, что между x и $2x$ всегда имеется простое число.

Напротив, следствием Σ_1-индукции является :

$$(\forall x_1)\dots(\forall x_n)(\exists x)(\forall y)[y \in x \leftrightarrow (y = x_1 \vee \dots \vee y = x_n)] \ ;$$

здесь можно даже доказать, что добавив элемент к кодированному множеству получаем снова кодированное множество :

$$(\forall x)(\forall y)(\exists z)(\forall t)(t \in z \leftrightarrow t \in x \vee t = y) \ .$$

Это заставляет думать, что Σ_1-индукция является достаточно сильной теорией, не искажающая нашу интуицию об арифметике, и остаток этого раздела будет посвящен доказательству приемлемости этой теории. Мы её берем, таким образом, как основу аксиоматического подхода к арифметике, еще раз отмечая между прочим, что специалисты в данной области её рассматривают как слишком сильную теорию. Они довольствуются добавлением нескольких аксиом к Δ_0-индукции, гарантирующих хорошее поведение показательной функции, то есть комбинаторики, и показывают, что эта система достаточна для доказательства всех обычных арифметических теорем, то есть всё кроме искусственных логических контрпримеров.

Но прежде чем продолжить, сделаем два замечания об аксиоме индукции. Студенты всегда обнаруживают с ужасом, что она имеет два вида: слабая форма, для которой рекурсия должна начинаться от 0 , и переходить от x к $x+1$, то что мы уже использовали ; и сильная форма, в которой переходят от всех z строго меньших y к y , то есть :

$$I'(f) \qquad (\forall \bar{x})\{[(\forall y)((\forall z < y)f(\bar{x}, z) \to f(\bar{x}, y))] \to (\forall y)f(\bar{x}, y)\} \ .$$

Это, действительно, более сильная аксиома чем $I(f)$, если мы располагаем A_0 и вдобавок аксиомой, заявляющей, что каждое ненулевое число является последователем : действительно, если фиксированное $\bar{x}$ удовлетворяет посылку $I(f)$, то оно удовлетворяет также посылку $I'(f)$, так как A_0 обязывает $y < y + 1$. Но в действительности, так как мы уже увидели по поводу простых чисел, эти две разновидности индукции эквивалентны, так как $I'(f(\bar{x}, y))$ является следствием $I((\forall z \leq y)f(\bar{x}, z))$.

Есть еще другой способ введения индукции, который выражает то, что каждое непустое множество натуральных чисел имеет наименьший элемент, или еще :

$$I''(f) \qquad (\forall \bar{x})\{(\exists y)f(\bar{x}, y) \to (\exists y)[f(\bar{x}, y)) \wedge (\forall z < y)\neg f(\bar{x}, y)]\} \ .$$

Без труда видно, что $I'(f)$ и $I"(\neg f)$ эквивалентны.

В тесном родстве с аксиомами индукции находятся аксиомы *коллекции*, выражающие, что числа, удовлетворяющие формуле $f(t)$ и меньшие некоторого числа z , образуют конечное множество в смысле модели :

$$C(f) \qquad (\forall \bar{x})(\forall z)(\exists y)(\forall t)(t \in y \leftrightarrow t \leq z \wedge f(\bar{x}, t)) \ .$$

Когда изучают модель M для A_0 , пытаются повторить на ней то, что известно про стандартные натуральные числа. Например, пытаются определить показательную функцию, беря ту же формулу, которую мы использовали для определения графика показательной функции на настоящих натуральных числах. Проблема в том, что априори нет оснований, что в M эта формула определит график функции; и при положительном ответе, можно ещё сомневаться в том, что если n – стандартное число, то значение 2^n в M то же самое, что в стандартной модели; и даже если и это истинно, то нет еще оснований, чтобы обычные свойства показательной функции были истинны в M .

Рассмотрим фрагмент T арифметики, содержащей A_0 , или даже просто непротиворечивую теорию содержащую A_0 (т.е. T может содержать ложные аксиомы для настоящих натуральных чисел); пусть f – функция из ω в ω , график которой определяется арифметической формулой $\varphi(x, y)$. Мы говорим что f – *доказуемая в* T общая функция если из T следует, что φ является графиком функции : $(\forall x)(\exists! y)\varphi(x, y)$; и в этом случае мы говорим, что f *хороша для* T , если кроме того для каждого стандартного n верно $T \vdash \varphi(n, f(n))$; очевидно, это определение может ввести в заблуждение : речь идет о свойствах формулы φ , а не функции f , которую она определяет, так как не имеется оснований, по которому два определения f , эквивалентные для настоящих натуральных чисел, остаются таковыми во всех моделях T .

Аналогично, рассмотрим подмножество A в ω , определенное формулой $\varphi(x)$; мы говорим, что A *хорошо для* T если для каждого стандартного n справедливо $T \vdash \varphi(n)$, если $n \in A$, и $T \vdash \neg\varphi(n)$ если $n \notin A$. Если A определяется Σ_n-формулой φ и Π_n-формулой ψ, то говорим что оно Δ_n-*доказуемо в* T, если T обеспечивает эквивалентность φ и ψ, т.е. $T \vdash (\forall x)(\varphi(x) \leftrightarrow \psi(x))$.

Когда мы работаем в ослабленной арифметике, надо подстраховать нашу интуицию, которая нас побуждает распространять без проверки некоторые очевидные свойства настоящих натуральных чисел на все модели рассматриваемой теории. Если мы хотим перевести без изменения результаты, полученные в предыдущих разделах, нам надо убедиться в том, что все множества и функции, участвующие в манипуляциях кодов формул хорошие; если наша теория слишком слаба для этого, то надо это осознавать и быть особенно бдительным. Например, мы отметили, что квантификация, ограниченная рекурсивной функцией, не выводит за классы Σ_1 или Π_1. Если, скажем, φ и $y = f(x)$ суть Π_1-формулы, то $(\forall y \leq f(x))\varphi(x, y)$ эквивалентна Π_1-формуле: чтобы это осталось истинным в T , надо доказать, что в T $y = f(x)$ определяет общую функцию, это необходимо, чтобы в T мы могли заменить $y \neq f(x)$ Π_1-формулой.

Ясно что множества Δ_0 хороши для минимальной арифметики A_0 : в проверке факта $n \in A$ участвуют только числа меньше n ; впрочем, то же самое

верно и для каждого множества определенного формулой, где квантификации ограничены многочленами от n . Теперь заметим, что для каждой теории T, содержащей A_0 , *каждое* Δ_1*-доказуемое множество хорошее.* Действительно, множество A определяется в модели настоящих натуральных чисел Σ_1-формулой $\varphi(x)$ и также Π_1-формулой $\psi(x)$, и $T \vdash (\forall x)(\varphi(x) \leftrightarrow \psi(x))$. Пусть M – модель T, если n – стандартное число, и если $n \in A$, то $\omega \vdash \varphi(n)$, таким образом, $M \vdash \varphi(n)$ так как $\varphi \in \Sigma_1$ и ω – начальный сегмент M. Точно так же, если $n \notin A$, то $M \vdash \neg\psi(n)$, и так как $T \vdash (\forall x)(\varphi(x) \leftrightarrow \psi(x))$, то $M \vdash \neg\varphi(n)$. Например, *доказуємо рекурсивная функция* (т.е. Σ_1-формула, про которую можно доказать в T , что она – график общей функции) хороша.

Какой фрагмент арифметики нам обеспечивает, что обычные функции, или существенные отношения, которые появляются в кодировании комбинаторики или языка хороши ? Один приемлемый фрагмент – это Σ_1-индукция; она позволяет действительно доказать аксиому, выражающую, что если A – множество, кодированное функцией β , то для любого a множество $A \cup \{a\}$ также кодируется этой функцией β ; это упражнение требует трудолюбия, основанного на китайской лемме, которое мы оставляем читателю: в любом случае, если бы она не была доказуема по Σ_1-индукции, то надо было бы срочно её добавить.

Это свойство позволяет обеспечить, что построения простой рекурсией хороши: если мы взглянем на определение показательной функции в 7.d, то видим, что Σ_1-индукцией (по y) можно доказать, что для всех x и y существует единственный z такой, что $z = x^y$; сущность заключается в доказательстве существования кода для последовательности $x, x^2, \ldots, x^y, x^{y+1}$ при условии, что известен только код $x, x^2, \ldots, x^y$; кроме того, мы можем также доказать элементарные свойства показательной функции такие, как $x^{u+v} = x^u \cdot x^v$, выявив соответствующие рекурсии на Σ_1-формулах.

Вообще, те же рассуждения показывают, что *примитивно рекурсивные функции – доказуемо общие в* Σ_1*-индукции*, и они, таким образом, доказуемо рекурсивны и хороши для неё. Так как мы предусмотрительно проверили в лемме 7.21, что функция γ примитивно рекурсивна, то теперь видно, что комбинаторика и наше отношение $\in$ хороши для Σ_1-индукции : в одной из её моделей M найдутся "ложные" конечные множества (т.е. конечные множества нестандартной мощности), но настоящие конечные множества настоящих чисел (т.е. множества стандартной мощности, у которых все элементы стандартны) гарантированно получают тот же код в M, что и в ω . Итак, если Вы убеждены что "обычные" функции примитивно рекурсивны, а множества, присутствующие "естественно" в математическом контексте, имеют примитивно рекурсивную характеристическую функцию, то Вы теперь можете быть спокойны за надежность Σ_1-индукции.

Мы можем теперь сравнить различные виды аксиом индукции, которые мы ввели:

Теорема 7.23 *При наличии* Σ_1*-индукции,* Σ_n*-коллекция и* Π_n*-коллекция эквивалентны, а* Σ_n*-коллекция влечет* Σ_n*- и* Π_n*-индукцию, в то время как* Σ_{n+1}*- или* Π_{n+1}*-индукция влечет* Σ_n*-коллекцию.*

Доказательство. Аксиома коллекции $C(f)$ эквивалентна аксиоме $C(\neg f)$;

действительно, если a кодирует множество y таких, что $y \leq z \wedge f(z)$, то

$$\{y \mid y \leq z \wedge \neg f(y)\} = \{y \mid y \leq z \wedge y \notin a\} \ ,$$

существование кода этого последнего множества доказывается Σ_1-индукцией по z. Тогда Σ_n-коллекция позволяет доказать Σ_n и Π_n-индукцию, применением принципа, по которому каждое конечное подмножество натуральных чисел имеет наименьший элемент, что доказуемо Σ_1-индукцией.

Наконец, если заметим, что 2^{z+1} – максимальный код подмножеств сегмента $[0, z]$, то видим, что аксиома коллекции для f доказывается индукцией по формуле:

$$(\exists t \leq 2^{z+1})(\forall y \leq z)(y \in t \leftrightarrow f(y)) \ ,$$

являющейся по выбору Σ_{n+1} или Π_{n+1}, если f есть Σ_n или Π_n .

□

Таким образом, в модели Σ_1-индукции мы имеем хорошее множество формул со стандартным кодом; они – настоящие формулы, коды которых вычисляются тем же способом, что в стандартной модели. Стандартные Σ_n-формулы в M являются таковыми и в самом ω ; и когда в M мы осуществляем операцию замены переменной стандартной константой, мы делаем точно ту же операцию, что и в ω : все это происходит из-за того, что используемые комбинаторные манипуляции хороши, что подтверждается доказательством примитивно рекурсивного характера функций, участвующих в них.

Следовательно, теорема Тарского может обобщаться следующим образом:

Теорема 7.24 (Тарский) *Пусть M – модель Σ_1-индукции; не существует формулы $V(x)$, такой, что для каждого стандартного n $M \vdash V(n)$ тогда и только тогда, когда n является кодом истинного предложения в M .*

Доказательство. Повторите доказательство теоремы 7.9, используя то, что функции замены хороши.

□

Естественно, теорема Тарского остается верной для структуры, скажем, в конечном языке (если язык счетен, то надо дать его "эффективное" перечисление), в котором можно определять модель Σ_1-индукции. Σ_1-индукция также не является абсолютно необходимой для теоремы Тарского; она может быть доказана для еще более слабых фрагментов арифметики. Но если мы работаем в очень слабой теории, то надо предвидеть возможный бред кодирований и комбинаторики.

Нестандартные формулы удовлетворяют формальным законам, определяющим истинные формулы, но невозможно им придать смысл: именно об этом говорит теорема Тарского. Напротив, мы располагаем Σ_n-предикатом $V\Sigma_n$, чтобы выразить истинность Σ_n-формул. Легко доказать Σ_1-индукцией, снова из-за того, что функции замены переменной константой хороша, что для каждого стандартного m $M \vdash V\Sigma_n(m)$ если и только если m является кодом Σ_n-предложения, истинного в M (Это не означает, что $V\Sigma_n$ хорошее: Σ_n-предложения, истинные в ω, и те, что истинны в M, не обязательно одни и те

же!). Таким образом, используя этот Σ_n-предикат истинности, можно определить понятие выполнимости для нестандартных Σ_n-формул, где n – стандартный и фиксированный, даже если они имеют нестандартное число свободных переменных. Но для формул Σ_x с нестандартным x это безнадежно. Это доказывается практически тем же методом, что модели Σ_1-индукции удовлетворяют усилению теоремы Тарского (теорема 7.22), запрещающим существование Σ_n-формулы, такой, что стандартные числа, которые ей удовлетворяют, были кодами Σ_n-предложений, ложных в модели.

7.h Нестандартные модели в арифметическом определении

Одной из нестандартных моделей теории порядка является $\omega + Z$; легко упорядочить натуральные числа изоморфно $\omega + Z$ бинарным Δ_1-отношением: достаточно представить элемент n из ω через $3n$, элемент $-n$, $n \neq 0$, из Z через $3n-1$, и элемент n из Z через $3n+1$. Мы видим так же, что модель суммы, описанная в конце параграфа 7.c , изоморфна Δ_1-определенной структуре на настоящих натуральных числах. Если мы верим, что Δ_1-множества – "эффективно описанные" множества, то мы "эффективно" построили нестандартные модели теории порядка и теории суммы.

По теореме Левенгейма-Сколема, существуют счетные нестандартные модели арифметики, модели, для которых носителем может быть ω. В начале раздела 7.d я сказал, что я не буду её пытаться строить "эффективно"; теперь мы увидим, что сумма и произведение в такой модели не могут быть одновременно определимыми в арифметике, и тем более не существует Δ_1-определения; мы можем даже уточнить на каком уровне нестандартная модель A_0 , определимая в арифметике, обязательно лжет, то есть удовлетворяет Σ_n- или Π_n-предложению, ложному для настоящих натуральных чисел (теорема 7.25). Следовательно, даже если отождествление Δ_1 с понятием "эффективный" кажется вам сомнительным, Вы должны признать, что не существует нестандартной модели арифметики, имеющей такое же простое определение, что эти две вышеописанные структуры.

Итак, рассмотрим модель M Σ_1-индукции, определенную на базе ω натуральных чисел, в которой сумма $x +_M y$ и произведение $x \cdot_M y$ имеют графики, определенные формулами из Σ_n , значит, также из Π_n , так как речь идет об общих функциях. Другие обычные отношения и функции, сопровождающие M, будут иметь также арифметические определения, возможно, чуть более сложными чем Δ_n . Например, порядок $\leq_M$ в M, определенный Σ_n-формулой $(\exists z)(x +_M z = y)$ может быть вне Δ_n . Действительно, квантор в его определении не может быть ограниченным (в смысле $\leq$, а не $\leq_M$) : если y – нестандартное, то $\{z : z \leq_M y\}$ – бесконечное и, значит, неограниченное подмножество в ω ! Мы видим, что в определении функции γ из леммы 7.8 функция $r_M(u, v)$ остается в Σ_n , но квантор $(\forall j)$ также не может быть ограниченным, так что можно только доказать что функция $\gamma \in \Sigma_{n+1}$, а $x \in_M y$ есть Δ_{n+1}-отношение. В сле-

дующей теореме мы требуем, чтобы эта принадлежность была Σ_n-отношением; если в нашей модели сумма и её произведение только Δ_n-определимы, то надо заменить n на $n+1$.

Теорема 7.25 *Пусть M – нестандартная модель Σ_1-индукции и Π_n-коллекции с носителем ω, у которой сумма, произведение и принадлежность Σ_n-определимы; тогда существует Σ_n- или Π_n-предложение, истинное в арифметике (т.е. в стандартной модели) и ложное в M .*

Доказательство. Предположим, что каждое истинное в арифметике предложение из Σ_n или из Π_n , истинно также в M. Если m – стандартное число, то m-ый последователь 0_M в M обозначим через m_M . Так как $V\Pi_n(x)$ является Π_n-формулой, то $M \vdash V\Pi_n(m_M) \Leftrightarrow \omega \vdash V\Pi_n(m) \Leftrightarrow m$ является кодом предложения Π_n , истинного в обеих структурах !

Если мы обозначим через $V\Pi_n^M(x)$ формулу, полученную заменой в $V\Pi_n(x)$ символа $+$ на $+_M$ и $\cdot$ на $\cdot_M$, то $M \vdash V\Pi_n M(m_M) \Leftrightarrow \omega \vdash V\Pi_n^M(m_M)$. Отметим маленькую двусмысленность в обозначениях: сказать, что M удовлетворяет предложению $V\Pi_n(m)$, это значит, что формула $V\Pi_n(x)$ удовлетворена элементом m_M ; это вызвано тем, что мы склонны смешивать константу с символом, который его представляет в языке.

Пусть a – нестандартный элемент в M; по Π_n-коллекции существует b, который в M кодирует $\{x \mid x \leq a \wedge V\Pi_n(x)\}$; значит,

$$\omega \vdash x \in_M b \leftrightarrow x \leq_M a \wedge V\Pi_n^M(x).$$

Следовательно, если мы вернемся в ω , то для того, чтобы видеть что x – код истинной Π_n-формулы, надо понять, что $x_M \in_M b$. Однако функция $x \mapsto x_M$ определяется Σ_n-формулой "существует конечная последовательность $a_0, \ldots, a_x$, такая что $a_0 = 0_M$ и $a_{i+1} = a_i +_M 1_M$ для каждого $i < x$, и $x_M = a_x$". Это представляет Σ_n-определение множества кодов Π_n-предложений, истинных в арифметике, что противоречит теореме 7.22.

□

При большей тщательности, можно распространить этот результат на модели Σ_1-индукции : если N – модель Σ_1-индукции, и если M – модель Σ_1-индукции и Π_n-коллекции, чьи сумма, произведение и принадлежность Σ_n-определимы в N, и если M и N удовлетворяют одним тем же Π_n-предложениям, тогда отображение $x \mapsto x_M$ из N в M является изоморфизмом.

7.i Арифметический перевод метода Генкина

В предыдущем параграфе, мы поняли то, что достаточно сложный список аксиом (аксиомы Пеано плюс множество истинных формул из Σ_n или из Π_n) не может иметь слишком простую нестандартную модель. Здесь, мы рассмотрим обратную проблему: для данного списка аксиом, найти метод, выявляющий

непротиворечив ли он или нет, и при положительном ответе построить также его самую простую модель, которая возможна. Для этого мы собираемся выразить в арифметике метод Генкина.

Итак, мы рассмотрим множество A аксиом, на конечном или счетном (ясно, что несчетный язык невозможно закодировать в арифметике !) языке L. Чтобы применить метод Генкина, мы сведем проблему сначала к случаю, когда язык включает только символы отношений, то что делается автоматически. Таким образом, мы имеем в языке L список $r_1, \ldots, r_n, \ldots$ символов отношений, и мы предположим, что функция, которая n сопоставляет местность r_n , рекурсивна (это действительно минимальное требование; если язык L конечен, то проблем с представлением языка нет). Сопоставляя каждому символу языка условный номер, можно кодировать его формулы так, чтобы различные "естественные" манипуляции с формулами выражались рекурсивными функциями, как это мы сделали для языка арифметики.

Язык L порождает язык L^H перечисления Генкина, состоящий из списка символов констант a_{ij} и символов отношения f^Hдля каждой формулы f, служащих для элиминации кванторов; L^H кодируется тем же способом. Теперь рассмотрим список $T(H)$ структурных предложений языка L^H, данный в 4.c; так как все погружается в эффективность самого низкого уровня, функция, которая сопоставляет формуле её свидетеля, рекурсивна, и это $T(H)$ есть Δ_1-множество.

Константы a_{ij} пронумерованы $\omega \times \omega$; но так как мы располагаем рекурсивной биекцией между $\omega \times \omega$ и ω , мы можем их пронумеровать ω : можно говорить " k первых a_{ij} "; также могут быть пронумерованы ω все символы f^H с помощью "функции перечисления" множества (см. лемму 7.18).

Мы назовем "деревом Генкина" следующий частичный порядок $\mathcal{H}$: элементом $\mathcal{H}$ для фиксированного натурального k , называющегося его высотой, является задание ограничений k первых отношений $f_0^H, \ldots, f_{k-1}^H$ на k первых элементов a_{ij} (это, таким образом, конечное множество условий вида $\bar{a} \in f_i^H$ или $\bar{a} \notin f_i^H$, содержащего для каждого условия его само или его отрицание, но не оба, где $\bar{a}$ пробегает множество кортежей соответствующей длины, берущихся среди k первых a_{ij}), и всех структурных предложений, в которых участвуют только k первых f_i^H и k первых a_{ij} (не забываем, что речь идет о предложениях без кванторов!). Мы упорядочиваем это множество включением : $p \subset q$, если каждое условие из q присутствует в p и, значит, высота q не меньше высоты p .

Ясно, что $\mathcal{H}$ так же, как его отношение порядка, есть Δ_1-множество. Отметим также, что существует функция $h(x)$, рекурсивная и легко вычислимая (как говорят теоретики чисел), которая ограничивает коды элементов $\mathcal{H}$ высоты не больше x. Кроме того, функция, которая формуле f в L сопоставляет его перевод без квантора f^H , рекурсивна (она определяется простой рекурсией); следовательно, если A есть Σ_n-, Π_n- или Δ_n-множество, то таков же и его образ A^H от этой функции; напомним, что если e – предложение, то e^H есть не что иное, как символ нульместного отношения.

Мы называем *деревом Генкина, присоединенным к* A, подмножество $\mathcal{H}(A)$ в $\mathcal{H}$, образованное элементами удовлетворяющими, если они достаточной высоты, предложения A^H ; элемент высоты k принадлежит $\mathcal{H}(A)$, если он удо-

влетворяет всем e^H , имеющим номер меньше k ; принадлежность к $\mathcal{H}(A)$ выражается формулой " $p \in \mathcal{H}$ и для каждого символа f с номером не большим высоты p, $f^H \notin A^H$ или f^H присутствует в p "; мы видим таким образом, что $\mathcal{H}(A)$ есть Π_n-множество, если A $\in \Sigma_n$, и Σ_n-множество, если A $\in \Pi_n$, и Δ_n-множество, если A $\in \Delta_n$. Что может произойти в этом дереве ? Возможны два случая:

- $\mathcal{H}(A)$ не имеет элемента высоты k для некоторого k ; это означает, как мы увидим, что $\mathcal{H}(A)$ конечно; построение дерева Генкина останавливается, то есть, следуя всевозможным ветвям, мы находим в конце концов противоречие. Это означает, как мы отметили в разделе 4.c, что множество A противоречиво (или, более точно, чем оно не имеет непустую модель; мы оставляем читателю удовольствие решения вопроса: имеет ли множество предложений пустую модель!).

- иначе, построение продолжается всегда; мы увидим, что тогда дерево $p(A)$ имеет бесконечную ветвь; ветвь есть не что иное, как последовательное задание ограничений структуры на k первые константы, затем на $k+1$ первых констант, и т.д., удовлетворяющие предложениям Генкина. В конце ветви, получают перечисление Генкина некоторой модели A .

Эти замечания нам позволят выражать в арифметике совместность Σ_n-множества предложений, и даже в случае совместности дадут определимую модель в арифметике. Но чтобы их оправдать, надо сначала доказать лемму о деревьях: мы называем здесь *деревом* частично упорядоченное множество, с наименьшим элементом, который называется его *корнем*, и такое, что миноранты каждого элемента x образуют конечную цепь, число элементов которой называется *высотой* x ; *ветвь* дерева – это его максимальная подцепь. Дерево называется *конечно ветвящимся* если каждый элемент высоты k имеет только конечное число (возможно нуль) мажорант высоты $k+1$. Дерево Генкина имеет очевидно все эти свойства (его корень – пустая последовательность).

Теорема 7.26 (Денеш Кёниг) *Каждое бесконечное дерево с конечным ветвлением имеет бесконечную ветвь; более точно, если это Π_n-дерево, высота элементов дается Σ_{n+1}-функцией, и если коды элементов высоты k ограничены Σ_{n+1}-функцией от k , тогда оно имеет бесконечную Δ_{n+1}-ветвь.*

Доказательство. Пусть $\mathcal{A}$ – наше дерево, и пусть $\mathcal{A}^*$ – дерево, образованное элементами $\mathcal{A}$, имеющими бесконечное число мажорант; $\mathcal{A}^*$ содержит корень $\mathcal{A}$, и так как $\mathcal{A}$ конечного ветвления, каждый элемент высоты k в $\mathcal{A}^*$ (высота в $\mathcal{A}^*$ та же самая, что и в $\mathcal{A}$!) имеет в $\mathcal{A}^*$ мажоранту высоты $k+1$; любая ветвь $\mathcal{A}^*$ является бесконечной ветвью $\mathcal{A}$. Дерево $\mathcal{A}^*$ определяется следующей формулой : $p \in \mathcal{A}$, и для каждого k, превышающего высоту p , существует элемент q в $\mathcal{A}$ высоты k , мажорирующий p . Мы определяем ветвь $\mathcal{A}^*$, полученную выбором на каждом шаге элемента с наименьшим кодом, следующим образом: $p \in \mathcal{A}^*$ и существует последовательность $p_0, p_1, \ldots, p_k$, чья длина k есть высота p , такая, что p_0 – корень $\mathcal{A}^*$ и p_{i+1} – мажоранта высоты $i+1$ (это ограничивает квантификацию) элемента p_i, имеющий минимальный код в $\mathcal{A}^*$, для каждого $i \leq k$, и наконец, $p_k = p$.

При посылках второй части теоремы, квантифицировать по элементам высоты меньшей, чем высота p, значит делать квантификацию ограниченную Σ_{n+1}-функцией, так что $\mathcal{A}^*$ так же, как его ветвь, имеет Δ_{n+1}-определение.

□

Теорема 7.27 *Утверждение, что Σ_n-множество предложений несовместно выражается Σ_n-предложением; каждое совместное Σ_n-множество предложений имеет Δ_{n+1}-модель.*

Замечание. Не путайте "Σ_n-множество предложений", что означает множество кодов предложений, среди которых каждый может быть произвольно большой сложности, и не обязательно на языке арифметики, с "Σ_n-предложением" или "множеством Σ_n-предложений".

Доказательство. Пусть A – наше множество предложений. Так как $\mathcal{H}(A)$ – поддерево рекурсивного $\mathcal{H}$, высота в $\mathcal{H}(A)$ является рекурсивной функцией и квантификации по элементам высоты меньше k ограничены рекурсивной функцией. Чтобы выразить несовместность A, надо сказать, что $\mathcal{H}(A)$ конечно, или ещё оно не содержит элемента высоты k для некоторого k: "существует k, такое, что $p \notin \mathcal{H}(A)$ для каждого элемента p из $\mathcal{H}$ высоты k". Если $A \in \Sigma_n$, то $\mathcal{H}(A) \in \Pi_n$ и его дополнение, как и последнее предложение, принадлежит Σ_n.

В случае, когда A – непротиворечивое Σ_n-множество, дерево $\mathcal{H}(A) \in \Pi_n$ и его высота удовлетворяет гипотезе теоремы 7.26. Таким образом, оно имеет бесконечную Δ_{n+1}-ветвь. Эта ветвь порождает модель для A на множестве констант a_{ij} : чтобы понять, что атомная формула выполнима, достаточно установить, что она появляется на ветви когда надо; это вполне определяет Δ_{n+1}-структуру, за исключением того, что равенство не интерпретируется истинным равенством, а Δ_{n+1}-отношением эквивалентности $\sim$. Чтобы получить модель с настоящим равенством, ограничимся элементами с наименьшими кодами в своих $\sim$-классах, определяющимися Δ_{n+1}-формулой $(\forall y < x) y \not\sim x$.

Если мы получим конечную модель из m элементов, то можно их перевести на m первых натуральных чисел ; иначе получаем бесконечную модель с Δ_{n+1}-носителем и Δ_{n+1}-отношениями, определенными на нем; переведя сюръективно это бесконечное Δ_{n+1}-множество на ω посредством своей функции перечисления (см. лемму 7.18), получаем Δ_{n+1}-модель с носителем ω.

□

Несколько комментариев об этой последней теореме; во-первых, естественно искать Δ-модели ; действительно, если A является системой аксиом на языке L , расширим язык, добавляя символ r' для каждого реляционного отношения языка L вместе с аксиомой $\neg r \leftrightarrow r'$, и получим множество A$'$ аксиом, которое имеет ту же сложность по Σ , Π или Δ, что и A; и Σ- или Π-модель для A$'$ является тем же, что Δ-модель для A !

Можно напротив интересоваться почему теорема 7.27 дает Δ_{n+1}-модель для Σ_n- или Δ_n-теории, и дает только Δ_{n+2}-модель для Π_n-теории. Ключ к этой асимметрии между Σ_n и Π_n дается следующей теоремой, которая будет принята на ура преподавателями и унтер-офицерами так же, как и всеми лицами, у которых главная задача – повторять без устали одни и те же вещи.

Теорема 7.28 (плеоназма) *Для каждого Σ_{n+1}-множества предложений существует Π_n-множество (Δ_1-множество, если $n = 0$) предложений, имеющее те же следствия.*

Доказательство. Пусть A – наше множество предложений, определенное формулой $(\exists y)f(x, y)$, где f – формула из Δ_0 или Π_n в зависимости от случая; идея заключается в том , чтобы заменить пару, образованную формулой x и числом y , формулой, полученной $2y$ отрицаниями x. Получаем таким образом множество B, имеющее, как нетрудно видеть, те же следствия, что и A ; так как для одного x из A могут существовать несколько y , формула x появится много раз под эквивалентной формой в B , откуда имя "теоремы плеоназма".

Включение $z \in B$ определяется формулой : "существует подформула x в z и целое y меньшей сложности чем x , такие, что (x, y) удовлетворяет f и что z получается $2y$ отрицанием x"; так как кванторы ограничены рекурсивными функциями, B действительно имеет указанную сложность.

□

Мы видим также, что метод Генкина не мог дать теорему, лучшую чем 7.27, так как мы можем надеяться только на то, что Π_n-дерево имеет Δ_n-ветвь (представьте, например, что оно состоит из единственной ветви!); тем не менее, контрпримеры, которые мы дали в 7.25, не доказывают, что оценка из 7.27 – наилучшая из возможных, так как они говорили о Π_n-теориях, не имеющих Δ_n-моделей, а именно:

- язык состоит из символов $0, 1, \leq, +, \cdot, \in, a$;
- включаются аксиомы Пеано (Δ_1-список) и аксиома определяющая $\in$ через сумму и произведение ;
- включается также Δ_1-список аксиом $a \geq n$, выражающих, что элемент a не стандартный ;
- добавляется Δ_n-список аксиом, полученный плеоназмом, эквивалентный списку истинных Σ_n-предложений ;
- наконец, включается Π_n-список истинных Π_n-предложений.

Чтобы получить непротиворечивый Σ_n-список предложений, не имеющий Δ_n-модели, нужны чуть более тонкие методы, которые мы оставим в стороне.

7.j Понятие доказательства, разрешимые теории

Если x и y – предложения (т.е. коды предложений), то $x \vdash y$ значит, что множество $\{x, \neg y\}$ несовместно. Как мы увидели в предыдущем параграфе, множество пар (x, y) предложений, таких, что y является следствием x определяется Σ_1-формулой $Pr(x, y)$ ("y доказуемо из x"). Кстати, что мы понимаем под доказательством? Мы тестируем непротиворечивость $\{x, \neg y\}$ методом

Генкина, и получаем доказательство того, что y является следствием x, тогда, когда мы достигнем высоты k, где ветви дерева обрываются, т.е. приводят к противоречию. Вот это натуральное k и есть та неограниченная переменная в предикате доказательства.

Я утверждаю, что это Σ_1-отношение $Pr(x,y)$ не принадлежит Π_1 ; действительно, минимальная арифметика является конечным множеством аксиом A_0 , которое можно заменить одним единственным предложением – их конъюнкцией; если бы доказуемость была Π_1- предикатом, то предложения, доказуемые из A_0 так же, как и Σ_1-предложения, доказуемые из A_0 , образовали бы Π_1-множества. Однако каждое Σ_1-предложение, истинное в арифметике – следствие A_0 , и кроме того, так как A_0 истинно для настоящих натуральных чисел, то оно не может доказать ничего ложного. Следовательно, Σ_1-предложения, являющиеся следствиями A_0 , в точности те, что истинны в арифметике, и они образуют Σ_1-множество, не являющееся Π_1-множеством.

Этот последний результат просит не волноваться о будущем нашей профессии: так как доказуемость не Δ_1-предикат, невозможно запрограммировать компьютер так, чтобы для любой конечной системы аксиом x и любого предложения y он выяснил за конечное время: является ли y следствием x. Такая программа делала бы бесполезной работу математика или, по крайней мере тех среди них, кто верит в добродетели аксиоматического метода!

Если A является Σ_n-множеством предложений, то его следствия образуют Σ_n-множество: выразим, что $A \cup \{\neg y\}$ несовместно методом Генкина, или еще, что x доказуем из конъюнкции конечного числа элементов A. Если $A \in \Pi_n$, то его следствия образуют Σ_{n+1}-множество; мы не можем делать лучше из-за теоремы плеоназма 7.28.

Мы знаем уже давно (теорема Тарского), что не можем определить в арифметике множество ее истинных предложений. Если у нас была надежда на арифметическую аксиоматизацию, то мы теперь понимаем, что эта надежда напрасна: если теория имеет Σ_n-аксиоматизацию, то она должна быть Σ_n-множеством! Когда мы провозглашали аксиоматизации для порядка или суммы натуральных чисел, мы приводили Δ_1-списки аксиом, то есть нам удавались очень простые аксиоматики. Арифметика не может иметь аксиоматизацию такого вида, и самое простое определение арифметики, что мы можем дать, следующее: "это предложения, истинные для суммы и произведения настоящих натуральных чисел"!

Установив, что арифметика Пеано более чем достаточна для арифметических потребностей нормального математика, и обманутые скрытым метафизическим вдохновением (спасли, как могли, аксиому индукции второго порядка, переводя её в язык первого порядка), мы могли поверить в какой-то момент, что она достаточна для того, чтобы аксиоматизировать арифметику. Теперь мы понимаем, что были очень далеки от истины, так как это – Δ_1-аксиоматика (" быть аксиомой индукции " есть Δ_1-свойство); только оттого, что она Σ_1-определима, она не может доказывать все истинные Π_1-предложения, и модель арифметики Пеано может лгать на самом низком уровне, возможном для модели A_0 , то есть Π_1 . Мы видим, что огромное расстояние отделяет то, что истинно для настоящих натуральных чисел, и то, что доказуемо по Пеано, или

в любой аксиоматической системе, определимой в арифметике.

Предикат доказуемости, который был введен в этом разделе, полностью удовлетворяет нужды теоретика моделей. Но в ветви логики, называемой "теорией доказательств" и посвященной понятию доказательства, принято его анализировать более подробно: как это было объяснено в начале раздела 4.c, дается конечное число правил, позволяющих "выводить" формулу из конечного множества других формул; из этих правил очевидно, что если x вывели из A, то он является следствием A. И говорят, что x доказуемо из множества A, если его получают из конечного подмножества A последовательным применением правил вывода. Ясно, что такая доказуемость есть Σ_1-предикат. Ещё надо показать, и это делается в основном методом близким к методу Генкина, что если x является следствием A, то он доказуем из A.

Этот результат, выражающий адекватность синтаксического понятия (доказуемости) семантическому понятию (следствия) называется "теоремой полноты Геделя". Что любопытно, что он был доказан Геделем и другими до ясного осознания явления компактности; впрочем, компактность выводили из этой самой теоремы, учитывая, что в доказательстве противоречивости A участвуют только конечное число элементов A. Это было в духе того времени, семантические понятия, такие, как "x является следствием A", то есть "каждая модель A удовлетворяет x", были под подозрением, что логики искали абсолютную истинность в мире математических рассуждений, а не в какой-то модели, и они были в основном увлечены эффективным характером понятий, которые они вводили.

По инерции, или из-за уважения к истории, учебники тиражируют это представление, весьма чуждое духу теории моделей, которая основывается на семантических понятиях. Это представление – скучное, если его рассматривать во всех деталях, и непонятное, если их опустить : в обеих случаях, оно окончательно разочаровывает кандидатов в логики. И это методическая ошибка, так как компактность является более фундаментальным свойством чем Σ_1-характер вывода: все доказательства адекватности выводимости понятию следствия используют, часто скрытно, сходимость последовательностей в компактных пространствах.

Некоторые говорят, что теория T (т.е. совместное множество предложений, и замкнутое относительно вывода) аксиоматизируема, если $T \in \Sigma_1$; так как по теореме плеоназма Σ_1-теория является тем же, что теория, имеющая Δ_1-аксиоматизацию, они этим хотят сказать, что эта теория обладает эффективной аксиоматизацией (эффективный $= \Delta_1$). Поскольку каждая теория имеет, эффективную или нет, аксиоматизацию, то в этом случае лучше сказать *рекурсивно аксиоматизируемая.* Наконец, T называется *разрешимой*, если она является Δ_1-теорией (теория сама, а не одна из её аксиоматизаций!): это означает, что мы располагаем механическим методом, выясняющим верно ли, что предложение принадлежит T или нет. Естественно, все это предполагает, что мы закодировали соответствующим способом язык T в арифметике, от уточнения которого обычно воздерживаемся, особенно если этот язык конечен. Следующий простой результат полезен :

Лемма 7.29 *Полная Σ_n-теория является Δ_n-теорией.*

Доказательство. Если T полна, то $x \notin T$ тогда и только тогда, когда $\neg x \in T$ и это дает Σ_n-определение дополнения T.

□

Следовательно, следующие полные Σ_1-теории разрешимы, для которых мы раньше дали эффективные аксиоматизации: плотный порядок без концевых точек, отношение эквивалентности с бесконечным числом бесконечных классов, теория следования, порядка или суммы натуральных чисел, алгебраически замкнутые поля данной характеристики, дифференциально замкнутые поля нулевой характеристики, и т.д.

Лемма 7.30 *Теория алгебраически замкнутых полей разрешима.*

Доказательство. Пусть T – эта теория, $T \in \Sigma_1$; предложение x не принадлежит T если и только если $\neg x$ является следствием

$$T \cup \{2 \neq 0, 3 \neq 0, \ldots, p \neq 0, \ldots\}$$

или если существует p, такое, что $\neg x$ – следствие $T \cup \{p = 0\}$; это дает Σ_1-определение дополнения T. (Действительно, по компактности, если x не в T , то существует p, такое, что $\neg x$ – следствие $T \cup \{p = 0\}$).

□

Пример теорий, рекурсивно аксиоматизируемых и неразрешимых: A_0 , и по той же причине (множество её Σ_1-следствий не разрешимо) каждая Σ_1-теория, содержащая A_0. Напомним, что A_0 конечно аксиоматизируема.

Доброжелатели не забывают предупреждать о "неэффективном" характере доказательств элиминации кванторов главы 6, использующих не формализуемые в арифметике аргументы компактности. Они сами предпочитают трудоемкие, и главное, не очень надежные методы, состоящие в том, чтобы показывать шаг за шагом, что формулу f можно заменить формулой без кванторов, что они делают теоретически эффективно в зависимости от f . Следующий результат им доказывает, что бесполезно себя мучить с построением объекта (по случаю алгоритма элиминации), когда можно понять очень просто, что он существует: действительно, *каждая Σ_1-теория, элиминирующая кванторы, элиминирует их эффективно.*

Лемма 7.31 *Если T – Σ_n-теория, элиминирующая кванторы, то существует Σ_n-функция, сопоставляющая каждой формуле эквивалентную ей по модулю T формулу без квантора.*

Доказательство. Применяем принцип Σ_n-выбора (лемма 7.17) к бинарному Σ_n-отношению, образованному из пар $(f(\bar{x}), g(\bar{x}))$ формул, таких, что g не имеет кванторов и $(\forall \bar{x})(f(\bar{x}) \leftrightarrow g(\bar{x}))$ доказуема в T.

□

Могут естественно возразить против алгоритмов, предложенных вышеупомянутыми результатами, из-за их ужасно непрактичного характера. Если мы имеем полную рекурсивно аксиоматизируемую теорию, алгоритм решения, который мы предлагаем, вопроса о том, что лежит ли f в T или нет, состоит в

перечислении всех следствий T до тех пор, пока не встретим f или $\neg f$, основывающимся на систематическом исследовании противоречивых деревьев Генкина! Точно так же в алгоритме элиминации кванторов ждут до тех пор, пока не появится формула без кванторов, эквивалентная $f(x)$. Такого рода алгоритмы, где ждут, когда произойдет некоторое явление, без оценки возможного времени ожидания, абсолютно нереалистичны; выполнение такой программы занимает такое фантастическое количество времени, что от них волосы на голове программиста встают дыбом! И эти алгоритмы могут потребовать не только значительное количество времени, а также большой объем памяти для проведения этих расчетов.

В случае алгебраически замкнутых полей, мы располагаем более эффективным алгоритмом, но который становится также быстро непрактичным, последовательного исключения неизвестных в полиномиальных уравнениях и неравенствах, следуя методу, известному с самых античных времен.

Для теоретика моделей эффективная конструкция хорошего алгоритма элиминации представляла бы интерес только, если бы он имел действительно намерение им воспользоваться, чего не бывает никогда. Именно поэтому достаточно напрасное упражнение – пытаться точно оценить количество времени и объема памяти (вычисленных как функции от длины проверяемой формулы f), необходимое для проверки принадлежности к разрешимой теории T. Однако, если мы ищем точные верхние оценки этого времени и этого пространства, то снова метод конечного челнока Фраиссе дает лучшие результаты, так как он позволяет свести выполнимость предложения f в структуре S к выполнимости предложения f в конечной подструктуре S .

Пусть действительно необходимо тестировать выполнимость предложения f, в структуре S чисто реляционного языка, и ранг квантификации f равен k ; пусть C_k – конечное множество представителей классов $(k-1)$-эквивалентности элементов S ; пусть C_{k-1} – конечное множество, такое, что для каждого a из C_k , каждый класс $(k-2)$-эквивалентности (a,x) имеет представителя (a,b), с b в C_{k-1} , и так далее: определяем таким образом конечные множества $C_k \subset C_{k-1} \subset \cdots \subset C_1$.

Мы говорим, что квантор в f ранга i, если i – ранг квантификации формулы, которая находится под областью его действия; из определения i-эквивалентности ясно следует, что f истинно в S если и только, если там истинно предложение f, полученное релятивизацией по C_i каждого квантора ранга i (заменой $(\exists x$ на $(\exists x \in C_i)$ и $(\forall x)$ на $(\forall x \in C_i)$). Следовательно, если мы располагаем очень простым описанием классов k-эквивалентности, как в случае дискретного порядка раздела 1.b, сведем выполнимость предложения к выполнимости предложений в конечных структурах небольших мощностей, что в благоприятных случаях дает хороший алгоритм решения.

Возможность осуществления этого алгоритма нас мало интересует: неразрешимость или разрешимость теории не связан со структурными свойствами его моделей, являющихся предметом теории моделей. И он не привносит ничего в изучение рекурсивности или сложности алгоритмов, которые вмешиваются в эти темы только рутинной техникой. Если мы слишком часто встречаем теоретиков моделей которые, некоторой отягощающей верностью логи-

ческим происхождением теории моделей, считают себя обязанными отмечать, что такая-та теория группы, кольца, и т.д. разрешима, это по большому счету потому, что теория моделей не сумела выковать специфический язык, чтобы формулировать свои результаты: они хотят сказать что рассматриваемая теория *проста*, что они умеют описывать её типы и, может быть, классифицировать её модели. Эта структурная простота не имеет в принципе ничего общего с рекурсивностью, которая измеряет в некотором смысле сложность системы аксиом, а не классов структур. Эта сложность более чувствительна ко всевозможным лингвистическим манипуляциям, без структурных воздействий. Однако на практике констатируют часто, что легко аксиоматизируемая теория структурно проста, и наоборот, хотя нетрудно привести – это детская игра – контрпримеры.

Отметим также, что понятие доказуемости, к которому мы привязались, не воспроизводит реальное функционирование мысли математика: чтобы доказать что-то, он не делает никогда систематическое исследование на противоречие по дереву Генкина! Чтобы доказать этим способом теорему 7.5, где показана эквивалентность двух систем, аксиоматизирующих сумму натуральных чисел (опираясь на аргументы, рассматриваемые как приемлемые для любого математика, чтобы убедить читателя, что каждая модель одной системы является моделью другой), надо было бы исписать целый том.

В заключение отметим, что алгоритм элиминации не является обязательно разрешающим алгоритмом: предложение f заменяется предложением g без квантора, ему эквивалентным по модулю T , но решение вопроса принадлежности g теории T – это другая проблема.

7.k Теорема Геделя

По теореме Тарского, мы знаем, что если A есть Σ_n-фрагмент арифметики, то существует Π_n-предложение арифметики, не являющееся следствием A : действительно, Π_n-следствия из A образуют Σ_n-множество, которое не может быть множеством всех истинных Π_n-предложений.

Теорема Геделя дает пример такого предложения. Мы знаем, что существует Σ_n-формула, обозначенная $Pr_A(x,y)$, которая выполняется тогда и только тогда, когда x является кодом формулы с одной свободной переменной, и предложение, полученное заменой этой переменной на y является следствием A; мы обозначим Π_n-формулу $\neg Pr_A(x,x)$ через $G_A(x)$.

Теорема 7.32 (Первая теорема Геделя) *Если A является Σ_n-фрагментом арифметики, и если a есть код формулы $G_A(x)$, то Π_n-предложение $G_A(a)$ истинно в стандартной модели и не является следствием A.*

Доказательство. Предположим, что $A \vdash G_A(a)$. Следовательно, в настоящем мире $G_A(a)$ доказуемо из A и для настоящих натуральных чисел $Pr(a,a)$ истинно так же, как и $\neg G_A(a)$, а $G_A(a)$ ложно; так как настоящие натуральные числа удовлетворяют A, все что доказуемо из A, истинно в стандартной

модели : получаем противоречие. Следовательно, $A \nvdash G_A(a)$ и для настоящих натуральных чисел $P_A(a,a)$ ложно, а $G_A(a)$ истинно.

□

В случае Σ_1-фрагментов арифметики, Гедель замечательным образом нашел гораздо более волнующую форму своей теоремы. Мы знаем, что непротиворечивость Σ_n-фрагмента A арифметики выражается Π_n-предложением, которое мы обозначим $Cons(A)$: на самом деле достаточно выразить, что $0 \neq 0$ не является следствием A, или выразить, что дерево Генкина, соответствующее A , бесконечно.

Теорема 7.33 (Вторая теорема Геделя) *Если A является Σ_1-фрагментом арифметики, содержащим Σ_1-индукцию (или нечто разумно близкое к Σ_1-индукции), то $Cons(A)$ истинно в стандартной модели и не является следствием A.*

Доказательство. Формула $Cons(A)$ истинно для настоящих натуральных чисел, так как A имеет модель (настоящих натуральных чисел!) и, следовательно, действительно непротиворечив. Мы хотим показать что $G_A(a)$ является следствием $A \cup \{Cons(A)\}$, и тогда по первой теореме Геделя $Cons(A)$ не может быть следствием A .

Предположим, что это не так и что мы имеем модель N для $A \cup \{Cons(A)\}$, удовлетворяющую $\neg G_A(a)$. Так как N удовлетворяет $Cons(A)$, она позволяет строить методом Генкина Δ_2-структуру M, являющуюся моделью A, или точнее структурных предложений Генкина (которые без кванторов!) соответствующих A. Так как N удовлетворяет $\neg G_A(a)$ и $Pr_A(a,a)$, то докажем, снова методом Генкина, что $G_A(a)$ является следствием A и, в частности, что модель M удовлетворяет $G_A(a)$.

Но M является моделью A_0, и мы можем определить в N отображение, которое x сопоставляет элемент x_M , являющимся x-ым последователем нуля в M (не забываем, что модель N верит, что настоящие натуральные числа – это она; это мы, которые видим её извне, не разделяем эту точку зрения). Образ N' множества N при этом отображении является начальным сегментом M, это то, что N считает "стандартной частью" M. Но M удовлетворяет Π_1-предложение $G_A(a)$, как и его начальный сегмент N', и, значит, также N, что противоречит гипотезе.

Где применяется в этом доказательстве гипотеза о том, что A содержала Σ_1-индукцию ? Сначала чтобы доказать существование модели M , то есть существование бесконечной ветви в бесконечном дереве с конечным ветвлением; затем для адекватности некоторых утверждений в модели N реальности: например, когда N утверждает, что (стандартное) предложение $G_A(a)$ удовлетворяется M, надо чтобы это было действительно так, чтобы замены переменных константами осуществлялись правильно; надо также, чтобы предложения Генкина, соответствующие $G_A(a)$ в N, вели себя корректно, и влекли действительно $G_A(a)$ для M.

□

Мы констатируем, что эта теорема Геделя, даже если она не применяет в игре очень сложный технический аппарат, достаточна тонка: первая теорема

доказана в реальном мире, то есть в настоящих натуральных числах, в то время как вторая воспроизводит доказательство первой в модели N. Со временем начинающий логик оценит её красоту, с каждым днем все больше и больше; это один из редких математических результатов, что испытываешь каждый раз новое удовольствие восстанавливая его доказательство (если удается !), после того как его забыл.

Таким образом, существует модель арифметики Пеано, которая содержит доказательство противоречивости арифметики Пеано! Естественно, это "доказательство" – нестандартное, и не соответствует ничему в реальности: уровень, где все ветви дерева Генкина оканчиваются противоречием, является нестандартным числом, которое конечно только при рассмотрении внутри обсуждаемой модели. Логика спасена, но это тем не менее впечатляет!

Чтобы иметь версию второй теоремы для Σ_n-фрагмента A арифметики, надо к ней добавить что-то, нарушающее ее эстетику: назовем Σ_n-истинностью Σ_n-множество Σ_n-предложений, истинных в арифметике, множество определенное Σ_n-формулой $V\Sigma_n$. Тогда доказывается, что предложение Π_n , утверждающее совместность $A + \Sigma_n$-истинность не доказуема в A ; естественно, модель N не удовлетворяет тем же предложениям Σ_n , что стандартная модель: $Cons(A + \Sigma_n$-истинность$)$ означает, что N позволяет строить методом Генкина модель M для A , удовлетворяющую тем же предложениям Σ_n , что и она! Если в случае Σ_1 не было нужды в этой предосторожности, то это потому, что мы смогли перевести в N то, что A влечет Σ_n-истинность. И надо предположить что A содержит что-нибудь вроде Σ_n-индукции, чтобы иметь нашу ветвь в дереве, а также чтобы выполнимость Σ_n-предложений, стандартных в N, соответствовали чему-нибудь разумному.

Теорема Геделя естественно распространяется на теории, например ω-непротиворечивые, позволяющие интерпретировать модель арифметики, или по крайней мере не слишком безумную модель A_0. Говорят, что T ω-непротиворечива если как только $T \vdash f(n)$ для любого стандартного n, то $(\forall x)f(x)$ совместна с T; или что T ω-противоречива, если существует формула $f(x)$ такая, что $T \vdash (\exists x)f(x)$ и $T \vdash \neg f(n)$ для любого стандартного n.

Теорема Геделя хотя имеет почти чем 70-летний возраст, всё еще сильно в моде в тех местах, где любят поболтать. По правде сказать, эпистомологи-любители не видят почти ничего кроме афоризма вида "никакая теория не может доказать сама свою собственную непротиворечивость", или "никто не может доказать свое собственное существование ", и только удивляются технической настойчивостью математика, показывающего так старательно то, что должно быть очевидно по здравому смыслу; чрезвычайно противоречивый здравый смысл, так как те же лица признают в общем картезианскую аксиому "я думаю, значит я существую"! Это недооценка этой теоремы ; сначала потому, что она говорит на самом деле ни о доказательствах, ни о формулах, а о кодах (что бы ни говорили, в шутку, логики); ещё потому, что обсуждаемая теория должна быть из Σ_1 (Должны ли мы верить в то, что существуют только "аксиоматизируемые" теории?), или на худой конец из Σ_n . Но фраза "непротиворечивость арифметики не доказуема в арифметике" не имеет никакого смысла, так как по теореме Тарского непротиворечивость арифметики

не соответствует никакому предложению языка арифметики. И каждая эпистомологическая интерпретация этой теоремы основывается на рискованном предположении её законности и законности синтаксиса и семантики теории моделей за узкими пределами математической логики. Но несомненно только одно: прежде чем философствовать по поводу этой теоремы, надлежит знать её точное утверждение и, если можно, доказательство ; например, бесполезно её рассказывать студентам, которые не справляются с разложением числа на простые делители.

Однако это точно, что теорема Геделя, так же и Тарского, основывались, с точностью до кодирования, на простой аргумент – парадокс лгуна, который, от Святого Павла и до Бертрана Рассела, служит основанием для бесчисленных более или менее удачных математических шуток; иногда себя спрашиваешь, эти теоремы Геделя, Тарского или Berloquin! В случае Тарского, ищут формулу которая говорит "я лгу"; в случае Геделя, который определенно более тонок, ищут аргумент, доказывающий свою собственную противоречивость.

Когда проводят математическое доказательство такого типа, то ученые говорят, что использовали "аргумент диагонализации". Именно такой аргумент использовал Кантор, чтобы доказать, что не существует биекции между множеством и множеством его подмножеств (см. главу 8). Эти аргументы участвовали существенным образом при изучении иерархии Σ_n и Π_n определимых множеств в арифметике.

Так как этот метод – очень общий, аргумент диагонализации Геделя может быть применен к любому языку (первого порядка или нет), *при условии, что можно определить отношение доказуемости*: наличие Σ_1-предиката доказуемости является, вместе с компактностью, основным свойством синтаксиса и семантики, изучаемых в теории моделей.

7.1 Немного математической фикции

Арифметика, в отличие от таких теорий, как теория алгебраически замкнутых полей, часто вводит нас в сомнения. Мы можем там закодировать наш язык и механизмы нашей мысли; нам тяжело выполнять роль наблюдателя, внешнего и беспристрастного, и мы испытываем сладкую дрожь при этой тонкой игре, состоящей в том, чтобы делать вид, что мы – только автомат, манипулирующий нашей моделью.

Определенно, что её изучение дало нам понять пределы наших возможностей, или более точно, возможностей аксиоматического метода: мы знаем, например, что не можем аксиоматизировать арифметику кодируемым в арифметике способом. Со времен Евклида, вместе с Лейбницем, а затем с Уайтхедом, Расселом и Гильбертом, математики мечтали разработать систему аксиом, которая удовлетворила бы окончательно их потребности: раз и навсегда утвердить список примитивных вещей, допущенных как истинные, так же, как список допущенных способов доказательств, и затем развивать математику не выходя из этой системы, из этого "рая". Дать априори все правила игры – это была, для большинства математиков в начале этого века, единственной

гарантией строгости. Это было бы впрочем чисто относительной строгостью, так как она опиралась бы на адекватность базовых понятий, которые основывают выбранную аксиоматическую систему: говорят о множествах маленьким детям, им дают примеры множеств, но кто им сказал, что это – множество? Этот подход заставляет только отодвинуть основополагающие проблемы в математике к этим базовым понятиям, что все же улучшает их изучение, при отсутствии их решений.

Теорема Геделя заставляет сомневаться в преимуществе такого метода, так как она ясно указывает, что какова бы ни была выбранная аксиоматика, надо будет из неё выйти. Очевидная слабость аксиоматического метода в том, что если T является теорией (рекурсивно перечислимой; но кто предложит другую систему аксиом?), содержащей как минимум арифметику, то невозможно доказать в T непротиворечивость T. Но она – еще более катастрофическая для своих сторонников: теорема Геделя позволяет строить теории, которые доказывают собственную противоречивость, и которые непротиворечивы! Действительно, Пеано $+ \neg Cons$(Пеано) является непротиворечивой теорией, и так как здесь доказывается, что Пеано несовместна, тем более доказывается что Пеано $+ \neg Cons$(Пеано) несовместна! Если таким образом Вы находитесь в данной аксиоматической системе, и что случайно Вы докажете в этой системе, что эта система несовместна, то это еще не значит, что Вы действительно доказали противоречивость вашей системы. Может быть, просто Вы признали как аксиому свойство, ложное для настоящих натуральных чисел.

Теорема Геделя была представлена с полным основанием своим автором в качестве доказательства окончательного провала того, что известна под именем "программа Гильберта", которая является надеждой, лелеянной в начале 20 века, о возможностях аксиоматического метода. В то время, некоторые математики брали под сомнение законность бесконечных методов, доказательств трансфинитной индукцией так же, как и существование "актуальной бесконечности", с которой как минимум должны были обращаться с предосторожностью. Гильберт думал, что за отсутствием исчерпывающего ответа на метафизический вопрос о настоящем существовании бесконечного, мы могли бы по крайней мере показать его совместность: если так, то все были бы довольны; даже если Вы не верите в актуальную бесконечность, Вы должны будете допустить что её присутствие в математических доказательствах не может привести к противоречию (он хотел также, чтобы успокоить своих оппонентов, показать что то, что мы можем доказать используя актуальную бесконечность, и что не касается её непосредственно, может быть также доказано и без неё); но, чтобы аргумент был полностью убедительным, эту непротиворечивость надо было доказать чисто финитистскими средствами. Таким образом, математики старались, если выразиться анахронически, показать чисто арифметическими методами непротиворечивость теории множеств; или более точно, доказать в аксиоматизируемой арифметике непротиворечивость аксиоматической теории множеств. Но теория множеств позволяет определить модель арифметики из множества натуральных чисел; и если Вы не служите предметом серьезной шизофрении, Вы должны выбрать такую теорию множеств, которая охватывает допущенную Вами арифметику. Таким образом, непротиворечивость вашей теории множеств доказывает непротиворечивость вашей арифметики и, следо-

вательно, не доказуема в вашей арифметике!

Почти не удивительно видеть авторов учебников, уступающих удобствам аксиоматики, предпосылая своим трудам главу 0 про "теорию множеств", устанавливая правила игры для последующего; это уступка возможности априорного, догматического и не критического изложения содержания какой-то науки и это успокаивает студентов, которые очень любят, чтобы им вдолбили надежные истины, даже если в них они ничего не понимают. Напротив, то что удивительно, это признанные математики, придерживающиеся такого очень формального взгляда и не сделавшие выводы из известной, и уже старой, теоремы Геделя. Наиболее характерным является Никола Бурбаки, который принялся писать трактат о математике, начиная с самых "начал". Это – старая энциклопедическая мечта, по мнению автора этого курса, который считает, что энциклопедия не является больше подходящей формой выражения научной мысли нашего времени. Некоторые удивляются Бурбаки, или по крайней мере некоторым из его последователей, ставящих так высоко основания математики и так низко логиков. Но это позиция, в целом, логичная, так как если аксиомы являются оракулами и если строгость является предметом культа, то кощунственно делать из неё позитивное исследование, и надлежит отстранить без жалости тех, кто имеет такую претензию.

Теоремы Геделя и Тарского – очень отрицательные результаты о возможностях аксиоматического подхода. Что хотят люди (математики)? От логиков не ждут особых прояснений об арифметике, но можно надеяться на то, что как только теоретик чисел докажет некоторый глубокий арифметический результат, логик немедленно сумеет ему сказать, является ли этот результат следствием некоторой аксиоматики типа Пеано. Вот это и есть работа логика! Работа безнадежная, так как модель Пеано может лгать на самом низком уровне, то есть Π_1 . Единственное, что может ответить логик: чтобы быть уверенным, что результат является следствием Пеано, надо провести доказательство в Пеано!

Тогда зачем так лелеять аксиоматику Пеано? Потому что мы чуть не поверили в первое время, что она составит полную аксиоматику арифметики? Мы теперь раскаиваемся в этой ошибке молодости. На чем основывается наше убеждение, что всякая обычная арифметическая теорема доказывается в Пеано, что каждая естественная функция ведет себя хорошо во всех моделях Пеано, убеждение, которое нарушается только если это сделано специально? Теорема Тарского нам говорит, что это чувство ни на чем не основано, если не на туманном принципе, который служит также обоснованием "обобщенного тезиса Чёрча", а именно, что наиболее часто встречающиеся объекты наименее вероятны. (Находите ли Вы в сборнике упражнений DEUG действительно разрывные функции ? или примитивные не вычислимые через элементарные функции?)

А что касается мысли о том, что хитрый Бог нас кажется поместил в нестандартную модель арифметики, не являющуюся может быть даже настоящей арифметикой, о чем естественно мы не могли бы отдать себе отчет, она может быть только продуктом затуманившегося разума. Это – потерять из виду, что язык, знакомый теоретику моделей, в основном был использован им

только по технической причине, потому что он дает доступную теорию моделей (компактность, определимость понятия доказательства, ...) и только из-за деформации разума в конце концов можно себе внушить, что это естественная рамка математической мысли : фактически, математик выходит из неё легко.

Как я уже однажды сказал, логики, или скорее теоретики моделей, являются простыми людьми; вводить элементарную эквивалентность локальными изоморфизмами – это избегать подхода к выполнимости, отравленного метафизическими остатками. Они верят, что натуральные числа, которыми они располагают являются настоящими числами, и что множество истинных в арифметике предложений существует, даже если оказывается, что оно не имеет такого же простого описания, как множество четных чисел; теорема Геделя, которую они излагают не пряча скрытые там кодирования, четко объясняется, для них, как свойство "ложных натуральных чисел", и никак не расшатывает в них веру в истинную арифметику. Одним словом, их счастье в немного наивной философии, которая заключается в одной фразе: "Математические объекты существуют, а их описание преходяще".

Чтобы завершить на приятной ноте, мы собираемся войти в фикцию. Одна из знаменитых теорем – это теорема Ферма; Может быть, она была доказана своим автором, но этот последний не оставил ничего проясняющего своим потомкам, и с тех пор теорема не поддается усилиям тысяч математиков. Она формулируется таким образом:

$$(\forall x)(\forall y)(\forall z)(\forall t)(x^t + y^t = z^t \to t \leq 2 \vee x \cdot y = 0) \ ;$$

Если заменить показательную функцию её определением через сумму и произведение, то видим, что это Π_1-предложение. Следовательно, если оно ложно, то его отрицание является следствием A_0 (имеем *настоящий* контрпример, и достаточно осуществить вычисления!), случай – неинтересный; мы выдвигаем таким образом гипотезу, что оно истинно, и мы можем представить, что если никто не смог его доказать до настоящего времени, может быть это именно потому, что оно не является следствием аксиом Пеано. Логик, у которого средства более ограничены чем у теоретика чисел, будет иметь более скромное намерение, чем он: вместо того, чтобы пытаться показывать, что теорема Ферма истинна, он попытается только доказать что она совместна.

В какой системе аксиом он собирается проводить свое доказательство? Естественно, в Пеано, являющейся нашей системой отсчета. Но, если модель N Пеано утверждает, что теорема Ферма совместна с A_0 , он построит модель M теоремы Ферма, с начальным сегментом N' , изоморфным N (см. доказательство второй теоремы Геделя), и только оттого, что теорема Ферма есть Π_1 , она также истинна в N' и в N : доказать в Пеано, что теорема Ферма совместна с Пеано , – это доказать в Пеано , что теорема Ферма истинна. Какова бы ни была система аксиом A , допущенных Маленьким Никола, он не может доказать, оставаясь в своей системе, что теорема Ферма совместна, не показывая что теорема Ферма истинна (т.е. следствие A). Все это говорит, что логика не продвигает ни на один шаг доказательство большой теоремы Ферма.

7.m Исторические и библиографические примечания

Теорема 7.1 о полноте категоричных теорий появилась в [ЛОСЬ, 1954] и [ВОТ, 1954]. Аксиоматика Пресбургера 7.5 описана в [ПРЕСБУРГЕР, 1930]; для теории произведения натуральных числа, консультируйтесь у [ЦЕГЕЛСКИЙ, 1981]. Хотя для нас это прямое следствие теоремы компактности, существование нестандартных моделей арифметики было немного озадачивающим явлением для наших отцов; одно из их первых появлений было в [СКОЛЕМ, 1934]. Кодирование комбинаторики и языка в арифметике восходят к [ГЁДЕЛЬ, 1931]; наше отношение $\in$ определялось в [АККЕРМАН, 1937]. Теорема Тарского в его знаменитой статье об истинности [ТАРСКИЙ, 1935].

Определение иерархии арифметических множеств, которая параллельна борелевским и аналитическим иерархиям, введенным поляками и другими славянами в дескриптивную теорию множеств, обязано [КЛИНИ, 1936]; примитивно рекурсивно функции определялись Геделем [ГЁДЕЛЬ, 1931], и общерекурсивные функции Клини [КЛИНИ, 1936]. Теорема Матиясевича опубликована в [МАТИЯСЕВИЧ, 1970]; она подводит конец длинной последовательности работ о проблеме, поставленной Гильбертом, который спрашивал, существует ли алгоритм, позволяющий определить, имеет ли многочлен с несколькими переменными, с целыми коэффициентами целый корень; ответ "нет", по теореме Матиясевича, которая превращает рекурсивным способом Σ_1-предложение в синонимичное диофантово предложение.

Тезис Чёрча формулировался в [ЧЁРЧ, 1936]; машины Тьюринга обязаны [ПОСТ, 1936] и [ТЬЮРИНГ, 1936]; степени рекурсивности и Σ_n-универсальных степеней появляются в [ПОСТ, 1948]. Как хороший вводный учебник по рекурсивности, я рекомендую [ШЕНФИЛД, 1971].

Термин "арифметика Пеано" воздает должное "Формуляру математики" Джузеппе Пеано [ПЕАНО , 1895–08]; эта книга, которая имела значительное влияние на современный математический символизм, состоит по большей части из систематического представления базовых математических понятий, а не из "аксиоматизации" в техническом смысле, как мы это понимаем сегодня; в то время, не имели никакого представления о значительном расстоянии, которая отделяет силы выражений языка второго порядка и языка первого порядка.

Конструкции моделей из разделов 7.h и 7.i являются частью фольклора логики 50-х годов ; можно например консультироваться у [ШЕНФИЛД, 1960]; не существование нестандартной рекурсивной модели арифметики Пеано обязано [ТЕННЕНБАУМ, 1959]; теорема Плеоназма должна иметь свое происхождение в [ФЕФЕРМАН, 1957]. Комбинаторная лемма Денеша Кёнига о деревьях очевидно гораздо старше: [КЁНИГ, 1927]. Как и для того, чтобы знакомиться с современной теорией моделей арифметики, так и для того, чтобы углубить свои знания о них, вы найдете материал в [БЕРЛИН-МАКАЛУН-РЕССЭР, 1982].

Адекватность понятия доказательства Σ_1 семантике логики первого порядка была показана [ЭРБРАН, 1928], [ГЁДЕЛЬ, 1930] и [ГЕНЦЕН, 1934], следуя заметно различным подходам; здесь неуместно рассматривать влияния которые

они оказали на современную теорию доказательств . Чтобы собрать материал об алгоритмической сложности некоторых логических теорий, очень решительный читатель может консультироваться у [ФЕРРАНТ-РАКОФФ, 1979].

Две теоремы Геделя из [ГЁДЕЛЬ, 1931] . Утверждение 7.33 содержит ингредиент, которого Гёдель тщательно избегал; в 7.33 речь идет о рекурсивных фрагментах настоящей арифметики; Гёдель никогда не говорил об истинности, ни о выполнимости в структуре, а о вещах доказуемых в (рекурсивной) теории, и он сформулировал свою теорему для ω-непротиворечивой теории, содержащей аксиомы Пеано (которая таким образом может содержать предложения, ложные для настоящих натуральных чисел); его результаты затем были обобщены Россером для непротиворечивых расширений аксиом Пеано, Однако, в учебнике логики, для которого главный сюжет не история идей, формулировка теоремы Гёделя в виде 7.33 – единственно важная.