Конспект лекций по теоремам Гёделя о неполноте

Автор-составитель: С. Л. Кузнецов

Это запись лекций №№ 2–7 специального курса «Математическая логика», часть 2, прочитанного весной 2020 г. на механико-математическом факультете МГУ. Чтение обновлённой версии курса в 2020 г. поддержано грантом фонда «БАЗИС».

Содержание

1 Арифметика Пеано и бета-функция Гёделя

1.1 Аксиоматика PA и её простейшие следствия

Сформулируем арифметику Пеано PA как теорию первого порядка. Зафиксируем *арифметическую сигнатуру* Ω_{Ar}: в неё входит константа 0, одноместный функциональный символ S (переход к следующему натуральному числу), два двуместных функциональных символа $+$ и $\cdot$ (сложение и умножение) и двуместный предикатный символ $=$ (равенство, про него в базовое исчисление предикатов добавлены соответствующие аксиомы).

Вместо $\neg(u = v)$ будем писать $u \neq v$.

Аксиомы PA суть следующие 6 формул:

1. $0 \neq Sx$
2. $Sx = Sy \to x = y$
3. $x + 0 = x$
4. $x + Sy = S(x + y)$
5. $x \cdot 0 = 0$
6. $x \cdot Sy = (x \cdot y) + x$

и бесконечная серия *аксиом индукции:*

$$\big(\varphi(0,\vec{z}) \wedge \forall y\, (\varphi(y,\vec{z}) \to \varphi(Sy,\vec{z}))\big) \to \varphi(x,\vec{z}).$$

(Приписка ..., $\vec{z}$ показывает, что у формулы φ могут быть *параметры* — дополнительные свободные переменные $z_1, \ldots, z_k$.)

Стандартной моделью арифметики Пеано служит множество натуральных чисел, на которых операции S, $+$ и $\cdot$ определены обычным образом. Легко видеть, что PA истинна в стандартной модели: $\mathbb{N} \vDash \mathsf{PA}$. Интересно отметить, что каждый элемент стандартной модели (т.е. каждое натуральное число) имеет «имя» в рамках Ω_{Ar}, т.е. задаётся замкнутым термом:

$$\underline{n} = \underbrace{S(S\ldots(S}_{n \text{ раз}}0)\ldots).$$

Этот терм называется *нумералом* числа n.

Задача. Докажите в PA простейшие утверждения о натуральных числах.

1. $x = 0 \vee \exists y\, x = Sy$
2. $x + y = y + x$
3. $x + (y + z) = (x + y) + z$
4. $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$
5. $x \cdot (y \cdot z) = (x \cdot y) \cdot z$
6. $x \cdot y = y \cdot x$

Задача. Докажите, что если $n = m+k$, то $\mathsf{PA} \vdash \underline{n} = \underline{m}+\underline{k}$, а если $n = m\cdot k$, то $\mathsf{PA} \vdash \underline{n} = \underline{m}\cdot\underline{k}$. Нужна ли для этого аксиома индукции?

В сигнатуре Ω_{Ar} нет символа для неравенства. Тем не менее, неравенство определимо следующим образом:

$$(x < y) \;=\; \exists z\, (x + Sz = y)$$

$$(x \leqslant y) \;=\; \exists z\, (x + z = y)$$

Задача. Докажите в PA:

1. $x \leqslant y \leftrightarrow (x < y \vee x = y)$
2. $\neg(x < x)$
3. $(x < y \wedge y < z) \to x < z$
4. $x < y \to x + z < y + z$
5. $x \leqslant y \to x \cdot z \leqslant y \cdot z$
6. $(0 < z \wedge x < y) \to x \cdot z < y \cdot z$
7. $\underline{n} < \underline{m}$ при условии $n < m$
8. $x < \underline{n} \leftrightarrow (x = 0 \vee x = \underline{1} \vee \ldots \vee x = \underline{n-1})$

Задача. Докажите в PA принципы *полной индукции* и *наименьшего числа*:

$$\forall x\, \big(\forall y\, (y < x \to \varphi(y)) \to \varphi(x)\big) \to \varphi(z)$$

$$\varphi(x) \to \exists x'\, \big(\varphi(x') \wedge \forall y (y < x' \to \neg\varphi(y))\big)$$

1.2 Доказуемо тотальные функции и псевдотермы

Зададимся следующим вопросом — с какими *функциями* на натуральных числах может эффективно работать арифметика Пеано? Поверхностный ответ таков: те функции, которые определимы термами в языке PA. Однако этот класс функций крайне беден — в него входят только многочлены с натуральными коэффициентами.

Даже небольшое отклонение делает функцию невыразимой термом. Например, $x^2 - 2x + 1$ — это многочлен с отрицательным коэффициентом, при этом все его значения неотрицательны. Значит, он задаёт функцию $f\colon \mathbb{N} \to \mathbb{N}$. Однако эта функция не может быть выражена термом в PA.

Более мощное средство для работы с функциями — определять их, а точнее их *графики,* с помощью арифметических *формул.* Итак, для функции n аргументов $f\colon \mathbb{N}^k \to \mathbb{N}$ нужна формула $F(x_1, \ldots, x_k, y)$ с $k+1$ свободной переменной, выражающая утверждение "$f(x_1, \ldots, x_k) = y$". Сокращённо пишем $F(\vec{x}, y)$ и $f(\vec{x}) = y$. Однако остаётся нетривиальный вопрос, *в каком именно смысле* формула F задаёт график функции f. В стандартной модели ответ на этот вопрос простой:

$$f(\vec{n}) = m \iff \mathbb{N} \vDash F(\underline{\vec{n}}, \underline{m}).$$

Можно попробовать перенести это определение на PA:

$$f(\vec{n}) = m \iff \mathsf{PA} \vdash F(\underline{\vec{n}}, \underline{m}).$$

Однако может оказаться, что если $f(\vec{n}) \neq m$, то формула $F(\underline{\vec{n}}, \underline{m})$ не доказуема и при этом не опровержима в PA. Добавим «негативное» условие:

$$f(\vec{n}) \neq m \Rightarrow \mathsf{PA} \vdash \neg F(\underline{\vec{n}}, \underline{m}).$$

Но и этого недостаточно! Допустим, мы хотим доказать в PA существование какого-то объекта, построив его применением функции f. Если f задана термом (см. выше), то существование получается по аксиоме $\varphi(u) \to \exists z\, \varphi(x)$, где u — терм. Однако если f определена формулой F так, как описано выше, мы не можем доказать, что для любого $\vec{x}$ существует $y = f(\vec{x})$ — функция f может оказаться не всюду определённой (не *тотальной*).

Нужное нам понятие даёт следующее определение *доказуемо тотальной функции.*

Определение. Функция $f\colon \mathbb{N}^k \to \mathbb{N}$ доказуемо тотальна в PA, если существует такая формула $F(\vec{x}, y)$, что:

1. $f(\vec{n}) = m \iff \mathsf{PA} \vdash F(\underline{\vec{n}}, \underline{m})$;
2. $\mathsf{PA} \vdash \forall \vec{x}\, \exists! y\, F(\vec{x}, y)$.

(«Негативное» условие следует из доказуемости $\forall \vec{x}\, \exists! y\, F(\vec{x}, y)$.)

Силу доказуемой тотальности демонстрирует следующая теорема, которая практически уравнивает в правах доказуемо тотальные функции с функциями, задаваемыми термами. Сформулируем теорему для теории в произвольной сигнатуре (не обязательно арифметической).

Теорема 1 (о консервативности)**.** *Пусть T — теория 1-го порядка в сигнатуре Ω; f — новый функциональный символ валентности k; $F(\vec{x}, y)$ — формула сигнатуры Ω. Обозначим через $\Omega + f$ сигнатуру Ω, расширенную функциональными символом f; пусть T_f — теория в сигнатуре $\Omega + f$, содержащая теорию T и формулу $\forall \vec{x}, y\, \big(y = f(\vec{x}) \leftrightarrow F(\vec{x}, y)\big)$. Тогда если $T \vdash \forall \vec{x}\, \exists! y\, F(\vec{x}, y)$, то T_f является консервативным расширением T, т.е. для любой формулы φ в сигнатуре Ω имеем $T_f \vdash \varphi \iff T \vdash \varphi$.*

Доказательство. Всегда $T \vdash \varphi \Rightarrow T_f \vdash \varphi$. Интересна другая импликация. Докажем её семантически.

Пусть $T \nvdash \varphi$. Тогда по теореме Гёделя о полноте существует контрмодель $\mathcal{M}$, в которой φ ложна. (Предполагаем, что φ замкнута, иначе добавим кванторы всеобщности по свободным переменным.) Полученная $\mathcal{M}$ — структура в сигнатуре Ω, $\mathcal{M} \vDash T$, $\mathcal{M} \nvDash \varphi$. Расширим $\mathcal{M}$ до структуры $\mathcal{M}_f$ сигнатуры $\Omega + f$. Для этого нужно определить интерпретацию нового функционального символа f.

Поскольку $\mathcal{M} \vDash T$, имеем $\mathcal{M} \vDash \forall \vec{x}\, \exists! y\, F(\vec{x}, y)$. Это значит, что для любых элементов $a_1, \ldots, a_k$ носителя $\mathcal{M}$ существует и единствен элемент b, для которого $\mathcal{M} \vDash F(a_1, \ldots, a_k, b)$. Определим в $\mathcal{M}_f$ интерпретацию символа f так: $\hat{f}(a_1, \ldots, a_k) = b$, где b — тот самый единственный элемент, для которого $\mathcal{M} \vDash F(a_1, \ldots, a_k, b)$.

Ясно, что $\mathcal{M}_f \vDash T$ и $\mathcal{M}_f \nvDash \varphi$ (интерпретацию сигнатуры Ω мы не меняли). Покажем, что $\mathcal{M}_f \vDash \forall \vec{x}, y\, \big(y = f(\vec{x}) \leftrightarrow F(\vec{x}, y)\big)$. Пусть $x_1, \ldots, x_k$ проинтерпретировались элементами $a_1, \ldots, a_k$, а y — элементом c. Тогда если $c = b$, то $c = f(\vec{a})$ и $F(\vec{a}, c)$ одновременно истинны, а если $c \neq b$ — то одновременно ложны.

Итак, $\mathcal{M}_f \vDash T_f$ и $\mathcal{M}_f \nvDash \varphi$, откуда $T_f \nvdash \varphi$ по теореме о корректности. □

Таким образом, в консервативном расширении T_f можно пользоваться f как функциональным символом. Консервативность при этом гарантирует, что если таким образом доказать какое-то утверждение, не содержащее символа f, то это утверждение доказуемо и в исходной теории T. Всё это имеет место, однако, только в условиях доказуемой тотальности (иначе переход от T к T_f дополнительно постулировал бы эту самую тотальность).

Более того, от функционального символа f можно избавляться следующим образом:

$$T_f \vdash \varphi(f(\vec{x})) \leftrightarrow \exists y \big(F(\vec{x}, y) \wedge \varphi(y)\big),$$

«заплатив» за это одним дополнительным квантором существования. Ввиду сказанного выше, формулы $F(\vec{x}, y)$ с доказуемым условием тотальности называют *псевдотермами.* В упрощённой записи можно использовать соответствующие им новые функциональные символы (точный смысл им придают консервативные расширения T_f), а если нужно перейти в исходную сигнатуру, то избавляться от этих символов, как показано выше.

Приведём простой и важный пример псевдотерма (доказуемо тотальной функции) в PA — взятие остатка при делении. Мы будем обозначать его ост(x, y). Формула $F(x, y, z)$, задающая "ост$(x, y) = z$" ("z — остаток при делении x на y") записывается следующим образом:

$$F(x, y, z) = \big((y = 0 \wedge z = x) \vee (z < y \wedge \exists q\, (x = q \cdot y + z))\big).$$

Заметим, что в этом определении мы считаем, что остаток при делении на ноль всегда равен делимому (это нужно, чтобы наша функция была всюду определённой).

Задача. $\mathsf{PA} \vdash \forall x, y\, \exists! z\, F(x, y, z)$.

Определим также два вспомогательных псевдотерма — наибольшее общее кратное (НОК) и максимум первых k значений некоторого заранее построенного псевдотерма f. Обозначения: НОК$[f(i), i < k]$ и $\max[f(i), i < k]$. Единственный аргумент обоих псевдотермов — k. Формулы, задающие их, таковы:

$$\text{НОК}(k, y) = (\forall i < k\, f(i) \mid y) \wedge (\forall y'\, (\forall i < k\, f(i) \mid y') \to y \mid y')$$

(где $x \mid y$ значит $\exists q\; y = q \cdot x$) и

$$\text{Max}(k, y) = (\exists i < k\; f(i) = y) \wedge (\forall j < k\; f(j) \leqslant y).$$

Задача. Проверьте доказуемую тотальность для НОК и max.

1.3 Китайская теорема об остатках

Сначала докажем леммы:

Лемма 2 (линейное представление)**.** $\mathsf{PA} \vdash \big(a, b > 1 \land a \text{ и } b \text{ взаимно просты}\big) \to \exists x, y\, (ax + 1 = by)$.

Доказательство. Рассуждаем в PA. Рассмотрим i_0 — наименьшее $i > 0$, для которого $\exists x, y\, (ax+i = by)$. Такие i существуют — например, годится $i = a$; далее применяем принцип наименьшего числа.

Любое другое такое i делится на i_0 — иначе $i = qi_0+r$, $0 < r < i_0$, и при этом $ax+i = by$, $ax_0 + i_0 = by_0$, и если взять

$$\begin{aligned} x' &= x + qby_0 + (b-1)qx_0, \\ y' &= y + qax_0 + (a-1)qy_0, \end{aligned}$$

то будет $ax' + r = by'$ (проверьте). Это противоречит минимальности i_0.

Такой трюк понадобился, потому что мы не можем использовать отрицательные числа.

Поскольку a и b также подходят в качестве i (действительно, $a \cdot (b-1) + a = b \cdot a$ и $a \cdot b + b = b \cdot (a+1)$), получаем $i_0 \mid a$ и $i_0 \mid b$. Т.к. a и b взаимно просты, $i_0 = 1$. Значит, $ax + 1 = by$ для некоторых x, y. □

Лемма 3. $\mathsf{PA} \vdash (p \text{ простое} \land p \mid ab) \to (p \mid a \lor p \mid b)$.

Доказательство. Пусть p не делит a. Тогда p и a взаимно просты, откуда $ax + 1 = py$. Следовательно, $abx + b = pby$. Поскольку $p \mid ab$, имеем $p \mid abx$, откуда $p \mid b$. □

Лемма 4. $\mathsf{PA} \vdash (p \text{ простое} \land p \mid \text{НОК}[m(i), i < k]) \to \exists j < k\, (p \mid m(j))$.

Доказательство. Индукция по k. База очевидна (НОК пустого множества равен 1). Шаг доказывается следующим образом: $\text{НОК}[m(i), i \leqslant k] \mid \text{НОК}[m(i), i < k] \cdot m(k)$. Далее или $p \mid m(k)$, или $p \mid \text{НОК}[m(i), i < k]$, и мы применяем предположение индукции. □

Теорема 5 (китайская теорема об остатках)**.** *Пусть m и h — псевдотермы. Тогда*

$$\begin{aligned} \mathsf{PA} \vdash \big(&\forall i < k\ (m(i) > 1 \land m(i) > h(i)) \land \\ &\land \forall i, j\ (i < j < k \to m(i) \text{ и } m(j) \text{ взаимно просты})\big) \to \\ &\to \exists a < \text{НОК}[m(i), i < k]\ \forall i < k\ \big(\text{ост}(a, m(i)) = h(i)\big). \end{aligned}$$

Будем для удобства вместо $m(i)$, $h(j)$ писать m_i, h_j. Итак, у нас есть набор «делителей» $m_0, \ldots, m_{k-1}$ (каждый больше 1) и набор «желаемых остатков» $h_0, \ldots, h_{k-1}$. Каждый остаток, как и положено, меньше соответствующего делителя. Кроме того, делители «независимы» — взаимно просты. Тогда утверждается, что можно подобрать такое число a, что оно при делении на m_i будет давать нужный остаток h_i. Более того, имеется верхняя оценка на a, задаваемая псевдотермом $\text{НОК}[m_i, i < k]$.

Доказательство теоремы 5 в сущности повторяет стандартное доказательство китайской теоремы об остатках, известное из учебников алгебры и теории чисел. Некоторое отличие состоит в том, что в PA мы не можем рассуждать об отрицательных числах (даже внутри доказательства).

Доказательство. Рассуждаем в PA. Пусть для данного k выполнены условия (левая часть импликации):

$$\forall i < k\ (m_i > 1 \wedge m_i > h_i)$$
$$\forall i, j\ (i < j < k \to m_i \text{ и } m_j \text{ взаимно просты})$$

Будем доказывать индукцией по k' следующее утверждение:

$$k' \leqslant k \to \exists a\ \forall i < k' \big(\text{ост}(a, m_i) = h_i\big).$$

(Верхнюю оценку на a сделаем потом.)

База индукции тривиальна: при $k' = 0$ условие $i < k'$ не может выполняться, и годится любое a.

Докажем индуктивный переход. По предположению индукции найдётся некоторое a, для которого $\forall i < k' \big(\text{ост}(a, m_i) = h_i\big)$. Обозначим $\ell = \text{НОК}[m_i, i < k']$ и $m = m_{k'}$. Числа m и ℓ взаимно просты: действительно, если $p \mid \ell$, то $p \mid m_j$ для некоторого $j < k'$ (лемма 4). Значит, p не делит m, поскольку m_j и m взаимно просты.

По лемме 2 существуют x и y, для которых $\ell x + 1 = my$. Умножим это равенство на $a + (\ell - 1)h_{k'}$ (ясно, что $\ell > 1$). Получим:

$$(\ell x + 1)(a + (\ell - 1)h_{k'}) = \ell x' + a + (\ell - 1)h_{k'}$$
$$my(a + (\ell - 1)h_{k'}) = my'$$

для некоторых новых x' и y'. Итак,

$$\ell x' + a + (\ell - 1)h_{k'} = my'.$$

Положим $\tilde{a} = a + \ell(x' + h_{k'})$. Тогда $\tilde{a} = my' + h_{k'}$, т.е. $\text{ост}(\tilde{a}, m_{k'}) = \text{ост}(\tilde{a}, m) = h_{k'}$. Кроме того, поскольку при $i < k'$ имеем $m_i \mid \ell$, то $\text{ост}(\tilde{a}, m_i) = \text{ост}(a, m_i) = h_i$. Таким образом, $\tilde{a}$ даёт искомые остатки при делении на $m_0, m_1, \ldots, m_{k'-1}, m_{k'}$.

По индукции получим некое значение a, которое даёт остатки $h_0, \ldots, h_{k-1}$ при делении на $m_0, \ldots, m_{k-1}$ соответственно. Осталось добиться выполнения неравенства $a < \text{НОК}[m_i, i < k]$. Разделим a на $\text{НОК}[m_i, i < k]$ с остатком. Получим $a = b + a'$, где b делится на $\text{НОК}[m_i, i < k]$, а $a' < \text{НОК}[m_i, i < k]$. Поскольку $\text{НОК}[m_i, i < k]$ делится на все m_i, получаем $\text{ост}(a', m_i) = \text{ост}(a, m_i) = h_i$. Новое a' даёт те же остатки, и при этом удовлетворяет верхней оценке. □

1.4 Бета-функция Гёделя и лемма о продолжении

Теперь перейдём к кодированию конечных последовательностей натуральных чисел с помощью *бета-функции Гёделя.* Особенность этого кодирования в том, что операции над последовательностями будут заведомо доказуемо тотальны в PA. Основная идея — используя китайскую теорему об остатках, для данной последовательности $h_0, \ldots, h_{k-1}$ найти такие числа a и $m_0, \ldots, m_{k-1}$, чтобы $h_i = \text{ост}(a, m_i)$. При этом m_i будут задаваться термом с некоторым параметром b. Таким образом, вся последовательность будет кодироваться тремя числами: a, b, k.

Реализуется эта идея следующим образом. Положим

$$\beta(a, b, i) = \text{ост}(a, 1 + (i + 1)b).$$

Это и есть бета-функция Гёделя. Как мы уже видели, функция взятия остатка доказуемо тотальна в PA. Значит, β можно рассматривать как псевдотерм. (Если мы захотим от него избавиться, то перейдём к формуле $B(a, b, i, z)$ — “$\beta(a, b, i) = z$”.)

Лемма 6 (лемма Гёделя о бета-функции). *Пусть h — псевдотерм от одной переменной. Тогда* $\mathsf{PA} \vdash \forall k\ \exists a, b\ \beta(a,b,i) = h(i)$. *Более того, если положить* $s = \max\{k, \max[h(i), i < k]\}$, *то можно ещё потребовать* $a \leqslant \text{НОК}[1 + (i+1)b, i < k]$ *и* $b \leqslant \text{НОК}[i+1, i \leqslant s]$.

Доказательство. Рассуждаем в PA. Положим $b = \text{НОК}[i+1, i \leqslant s]$ и обозначим $m_i = 1 + (i+1)b$. Докажем, что при $i < j < k$ числа m_i и m_j взаимно просты. Пусть p — общий простой делитель m_i и m_j. Тогда p делит $m_j - m_i = (j-i)p$, а значит $p \mid (j-i)$ или $p \mid b$. Однако, поскольку $1 \leqslant j - i < k \leqslant s$, число b делится на $(j-i)$. Значит, в любом случае p делит b. Но тогда $p \mid (i+1)b$, откуда p не делит $1 + (i+1)b = m_i$. Противоречие.

Кроме того, для каждого i имеем $h(i) \leqslant s < b < 1 + (i+1)b = m_i$. Применяем китайскую теорему об остатках и получаем искомое a. □

С помощью леммы Гёделя о бета-функции можно кодировать числами a и b конечные фрагменты (от 0 до $k-1$) последовательностей значений псевдотермов. Нас будет интересовать особый случай этой теоремы, рекурсивно использующий *саму бета-функцию.*

Лемма 7 (лемма о расширении). $\mathsf{PA} \vdash \forall c, d, k, h\ \exists a, b\ \big((\forall i < k\ \beta(a,b,i) = \beta(c,d,i)) \wedge \beta(a,b,k) = h\big)$.

Здесь числа c и d кодируют последовательность длины k: $\beta(c,d,i)$ при $i < k$. Новые числа a и b кодируют уже последовательность длины $k+1$, первые k элементов которой совпадают с соответствующими элементами исходной, а последний равен данному числу h.

Доказательство. Определим новый псевдотерм

$$H(i,y) = \big((i < k \wedge y = \beta(c,d,i)) \vee (i \geqslant k \wedge y = h)\big).$$

Легко проверить доказуемую тотальность: $\forall i\ \exists! y\ H(i,y)$. Значит, мы можем использовать функцию

$$h(i) = \begin{cases} \beta(c,d,i), & i < k \\ h, & i \geqslant k \end{cases}$$

Применяем лемму 6. □

Наконец, сформулируем следующую тривиальную лемму об одноэлементной последовательности:

Лемма 8. $\mathsf{PA} \vdash \forall n\ \exists a, b\ \beta(a,b,0) = n.$

Доказательство. Положим $a = b = n$. Тогда $a < b + 1 = 1 + (0+1)b$, откуда $\beta(a,b,0) = \text{ост}(a, 1 + (0+1)b) = a = n$. □

1.5 Σ_1-формулы и Σ_1-полнота

Определим специальный подкласс арифметических формул, для которых (при отсутствии свободных переменных) истинность в стандартной модели будет равносильна доказуемости в PA — то есть, будет иметь место *полнота.* При этом глобальной нашей целью будет доказательство *неполноты* для произвольных формул.

Определение. Формула δ (возможно, со свободными переменными) принадлежит классу Δ_0, если она построена из атомарных и константы $\bot$ с помощью логических операций (в нашем языке таковая одна — импликация) и *ограниченного квантора* $\forall z \leqslant u(\vec{x})$. Формула δ' называется Δ_0-формулой в широком смысле, если $\mathsf{PA} \vdash \delta' \leftrightarrow \delta$ для некоторой δ из класса Δ_0.

Ограниченный квантор выразим через обычный: $\forall z \leqslant u(\vec{x})\ \psi(\vec{x}, z)$ равносильно (в PA) $\forall z\,(z \leqslant u(\vec{x}) \to \psi(\vec{x}, z))$. При этом неравенство выражается через равенство с помощью квантора существования: $z \leqslant u(\vec{x})$ равносильно $\exists y\,(z+y = u(\vec{x}))$. Ограниченный квантор существования выражается через ограниченный квантор всеобщности: $\bigl(\exists z \leqslant u(\vec{x})\ \psi(\vec{x}, z)\bigr) \equiv \bigl(\neg\forall z \leqslant u(\vec{x})\ \neg\psi(\vec{x}, z)\bigr)$. (Напомним, что $\neg\xi \equiv (\xi \to \perp)$.)

Определение. Формула σ принадлежит классу Σ_1 (в узком смысле), если $\sigma = \bigl(\exists x\, \delta(x)\bigr)$, где δ принадлежит классу Δ_0. Формула σ' называется Σ_1-формулой в широком смысле, если $\mathsf{PA} \vdash \sigma' \leftrightarrow \sigma$ для некоторой σ, принадлежащей Σ_1 в узком смысле.

Ясно, что класс Δ_0 замкнут относительно всех булевых операций и ограниченных кванторов. Интересно, что класс Σ_1 (в широком смысле) также обладает некоторыми из этих свойств:

Теорема 9. *Класс Σ_1-формул в широком смысле замкнут относительно конъюнкции, дизъюнкции, квантора существования и ограниченного квантора всеобщности.*

Важно, что класс Σ_1 **не** замкнут относительно отрицания (и, следовательно, импликации). Отрицания Σ_1-формул образуют двойственный класс Π_1-формул, и окажется, что с точки зрения доказуемости в PA они ведут себя существенно иначе. А именно, 2-я теорема Гёделя о неполноте утверждает, что в PA недоказуемо (будучи истинным) утверждение о непротиворечивости PA. Это утверждение лежит в классе Π_1.

Для начала введём *кодирование пар* натуральных чисел следующим образом:

$$\langle x, y\rangle = 2((x+y)^2 + x + 1).$$

Заметим, что $\langle x, y\rangle$ — это многочлен (т.е. терм в арифметической сигнатуре) от x и y. Код пары всегда чётен — это сделано специально для целей гёделевой нумерации (см. § 2.2). Кроме того, функция взятия пары монотонна по обоим аргументам, а также $\langle x, y\rangle > x$ и $\langle x, y\rangle > y$. Последнее существенно для Δ_0- и Σ_1-кодирования.

Доказательство теоремы 9. Замкнутость класса Σ_1 относительно $\vee$ и $\wedge$ устанавливается следующими равносильностями (выводимы в исчислении предикатов):

$$(\exists x\, \delta_1(x)) \vee (\exists x\, \delta_2(x)) \quad \leftrightarrow \quad \exists x\, (\delta_1(x) \vee \delta_2(x))$$

$$(\forall x\, \delta_1(x)) \wedge (\forall x\, \delta_2(x)) \quad \leftrightarrow \quad \forall y\, \forall z\, (\delta_1(y) \wedge \delta_2(z))$$

Замкнутость относительно квантора существования доказывается с помощью операции взятия пары:

$$\exists y\, \bigl(\exists x\, \delta(x, y)\bigr) \quad \leftrightarrow \quad \exists z\, \exists x \leqslant z\, \exists y \leqslant z\, (\delta(x, y) \wedge z = \langle x, y\rangle)$$

(На самом деле, можно даже и не требовать $z = \langle x, y\rangle$: тогда импликация $\to$ устанавливается взятием $z = \max\{x, y\}$; обратная импликация доказуема в исчислении предикатов.)

Наконец, замкнутость относительно ограниченного квантора всеобщности использует кодирование последовательностей. Формула $\forall y \leqslant u(\vec{z})\, \exists x\, \delta(x, y, \vec{z})$ ($\vec{z}$ — параметры) может быть неформально переписана, с перестановкой кванторов, так: $\exists x_0, \ldots, x_{u(\vec{z})}\ \forall y \leqslant u(\vec{z})\ \delta(x_y, y, \vec{z})$. Внутренний квантор существования по числу x (при данном y) заменился на внешний квантор существования *конечной последовательности* значений x, для каждого y. Последовательность же кодируем при помощи β-функции:

$$\exists a, b\, \forall y \leqslant u(\vec{z})\ \bigl(\delta(\beta(a, b, y), y, \vec{z})\bigr)$$

Эквивалентность этой формулы и исходной доказывается индукцией по значению $u(\vec{z})$ при помощи леммы 7.

Наконец, нужно избавиться от нового функционального символа β. В общем случае это бы добавило квантор существования по её значению, который оказался бы под $\forall y \leqslant u(\vec{z})$ (что сделало бы всю нашу деятельность бессмысленной). Однако для бета-функции верно (и доказуемо в PA), что её значение всегда не больше её первого аргумента (остаток не больше делимого). Значит, этот квантор можно сделать ограниченным:

$$\exists a, b\, \forall y \leqslant u(\vec{z})\, \exists x \leqslant a\, \big(\delta(x, y, \vec{z}) \wedge B(a, b, y, x)\big).$$

Формулу $B(a, b, y, x)$ можно записать в классе Δ_0: квантор по q в определении деления с остатком ограничивается делимым. $\square$

Наконец, докажем полноту арифметики Пеано на формулах из класса Σ_1:

Теорема 10 (Σ_1-полнота PA)**.** *Если σ — замкнутая Σ_1-формула и $\mathbb{N} \vDash \sigma$, то $\mathsf{PA} \vdash \sigma$.*

Доказательство. Достаточно ограничиться Σ_1-формулами в узком смысле (остальные приводятся к ним эквивалентными преобразованиями в PA, а тем более в $\mathbb{N}$).

Для начала докажем Δ_0-полноту. Для замкнутой (нам таких достаточно) Δ_0-формулы δ докажем совместной индукцией два утверждения:

$$\begin{aligned} \mathbb{N} \vDash \delta \quad &\Rightarrow \quad \mathsf{PA} \vdash \delta; \\ \mathbb{N} \nvDash \delta \quad &\Rightarrow \quad \mathsf{PA} \vdash \neg\delta. \end{aligned}$$

Пусть δ — атомарная формула вида $u = v$, где u и v — замкнутые (без переменных) арифметические термы. Термы u и v имеют конкретные числовые значения, и нам в первом случае дано, что они совпадают. Пусть это число n. Тогда (см. задачи из § 1.1) $\mathsf{PA} \vdash u = \underline{n}$ и $\mathsf{PA} \vdash v = \underline{n}$, откуда получаем требуемое. Во втором случае $\mathsf{PA} \vdash u = \underline{n}$, $\mathsf{PA} \vdash v = \underline{m}$, где m и n разные. Считаем без ограничения общности, что $n < m$. Тогда (опять же, была такая задача в § 1.1) $\mathsf{PA} \vdash \underline{n} < \underline{m}$, откуда $\mathsf{PA} \vdash u \neq v$.

Считаем, что в нашем логическом языке из булевых операций есть только константа $\bot$ (ложь) и импликация. Остальные связки выразимы. Для $\delta = \bot$ всё тривиально: имеем $\mathbb{N} \nvDash \bot$ и $\mathsf{PA} \vdash \neg\bot$. Пусть теперь $\delta = \delta_1 \to \delta_2$. Тогда если $\mathbb{N} \vDash \delta$, то или $\mathbb{N} \nvDash \delta_1$, или $\mathbb{N} \vDash \delta_2$. В первом случае по предположению индукции $\mathsf{PA} \vdash \neg\delta_1$, во втором — $\mathsf{PA} \vdash \delta_2$. В обоих случаях получаем $\mathsf{PA} \vdash \delta_1 \to \delta_2$. Если же $\mathbb{N} \nvDash \delta$, то одновременно $\mathbb{N} \vDash \delta_1$ и $\mathbb{N} \nvDash \delta_2$, откуда $\mathsf{PA} \vdash \delta_1$, $\mathsf{PA} \vdash \neg\delta_2$, следовательно $\mathsf{PA} \vdash \neg(\delta_1 \to \delta_2)$.

Наконец, разберём случай ограниченного квантора. Пусть $\delta = \forall y \leqslant u\, \delta'(y)$. Терм u замкнутый, значит, его можно заменить на нумерал его числового значения: $\delta = \forall y \leqslant \underline{n}\, \delta'(y)$. Далее, поскольку $y \leqslant \underline{n} \leftrightarrow \big(y = 0 \vee y = \underline{1} \vee \ldots \vee y = \underline{n}\big)$ (см. § 1.1), формула δ равносильна формуле $\delta'(0) \wedge \delta'(\underline{1}) \wedge \ldots \wedge \delta'(\underline{n})$. Если $\mathbb{N} \vDash \delta$, то все формулы в этой конъюнкции истинны в $\mathbb{N}$, и по предположению индукции доказуемы в PA. Значит, доказуема конъюнкция. Если конъюнкция ложна, то для какого-то $m < n$ имеем $\mathbb{N} \nvDash \delta'(\underline{m})$, откуда $\mathsf{PA} \vdash \neg\delta'(\underline{m})$, значит, $\mathsf{PA} \vdash \neg\delta$.

Теперь пусть $\sigma = \exists x\, \delta(x)$ и $\mathbb{N} \vDash \sigma$. В этом случае существует *конкретное* натуральное число n, для которого $\mathbb{N} \vDash \delta(\underline{n})$. По доказанному ранее, отсюда следует $\mathsf{PA} \vdash \delta(\underline{n})$, откуда $\mathsf{PA} \vdash \exists x\, \delta(x)$. $\square$

1.6 Представление примитивно-рекурсивных функций

Теперь мы готовы доказать один из важнейших результатов на пути к теоремам Гёделя о неполноте — доказуемую тотальность в PA примитивно-рекурсивных функций.

Напомним, что примитивно-рекурсивные функции строятся следующим образом:

1. Базовые функции: $Z(x) = 0$, $S(x) = x + 1$, $I^k_n(x_1, \ldots, x_n) = x_k$.
2. Композиция: $f(x_1, \ldots, x_n) = h(g_1(\vec{x}), \ldots, g_m(\vec{x}))$
3. Примитивная рекурсия:

$$\begin{cases} f(0, \vec{y}) = g(\vec{y}) \\ f(x + 1, \vec{y}) = h(f(x, \vec{y}), x, \vec{y}) \end{cases}$$

(Когда мы строим f, мы предполагаем, что g и h уже построены.)

Теорема 11. *Всякая примитивно-рекурсивная функция доказуемо тотальна в* PA*; более того, формула $F(\vec{x}, y)$, представляющая примитивно-рекурсивную функцию f, принадлежит классу Σ_1, и в* PA *(точнее, в её консервативном расширении) доказуемы рекурсивные условия: $\forall x, \vec{y}\, (f(Sx, \vec{y}) = h(f(x, \vec{y}), x, \vec{y}))$ и т.д.*

Последнее утверждение нужно слегка уточнить: одну и ту же функцию можно по-разному представить как примитивно-рекурсивную (запрограммировать разными *примитивно-рекурсивными программами*). Каждой программе соответствует своя формула, представляющая функцию в PA и, соответственно, доказуемость своих рекурсивных условий.

Доказательство. Базовые функции представляются естественным образом: $Z(x, y) = \big(y = 0\big)$, $S(x, y) = \big(y = S\big)$, $I^k_n(x_1, \ldots, x_n, y) = \big(y = x_k\big)$. Доказуемая тотальность очевидна (каждая такая функция представляется явным термом). Для композиции рассмотрим простой случай $f(x) = h(g(x))$. Функция f в консервативном расширении (с функциональными символами g и h) определяется термом $h(g(x))$. Для терма выполняется условие доказуемой тотальности; кроме того, доказуемо условие композиции $\forall x\, f(x) = h(g(x))$.

Важное замечание: при переходе от расширенного языка к обычному арифметическому добавляются неограниченные кванторы существования. Например, в арифметическом языке композиция выражается так: $F(x, y) = \big(\exists z\, (G(x, z) \wedge H(z, y))\big)$. В силу теоремы 9, мы не выходим за рамки класса Σ_1 (в широком смысле).

Интересен случай примитивной рекурсии. Здесь мы будем использовать бета-функцию Гёделя. Общая схема такая: $f(x, \vec{y}) = z$, если существует последовательность $z_0, z_1, \ldots, z_x$, что $z_0 = g(\vec{y})$, $z_x = z$ и $z_{i+1} = h(z_i, i, \vec{y})$ для каждого $i < x$. Эту последовательность мы закодируем двумя числами a и b с помощью бета-функции:

$$F(x, \vec{y}, z) \quad = \quad \exists a, b \big(\beta(a, b, 0) = g(\vec{y}) \wedge \forall i < x\, (\beta(a, b, Si) = h(\beta(a, b, i), i, \vec{y})) \wedge \beta(a, b, x) = z\big).$$

Опять же, мы не вышли за пределы класса Σ_1: снаружи стоят кванторы существования, а внутри — если перейти к арифметическому языку — комбинация Σ_1-формул для функций g и h с помощью конъюнкции и ограниченного квантора. (Как отмечалось выше, сама бета-функция реализуется Δ_0-формулой.)

Наши определения были так подобраны, что $\mathbb{N} \vDash F(\underline{\vec{n}}, \underline{m})$ тогда и только тогда, когда $f(\vec{n}) = m$. Поскольку формула $F(\underline{\vec{n}}, \underline{m})$ замкнута и принадлежит Σ_1, истинность в $\mathbb{N}$ можно заменить на выводимость в PA по теореме 10 (Σ_1-полнота). Таким образом, получаем первое условие в определении доказуемой тотальности.

Второе условие, $\mathsf{PA} \vdash \forall \vec{x}\, \exists! y\, F(\vec{x}, y)$, интереснее. Мы уже проверили его для базовых функций и композиции, рассмотрим случай примитивной рекурсии: $\forall x, \vec{y}\, \exists! z\, F(x, \vec{y}, z)$. Рассуждаем в PA индукцией по x.

База индукции, $x = 0$, устанавливается по лемме 8: $\exists a, b\; \beta(a, b, 0) = g(\vec{y})$. Для доказательства существования z возьмём $z = \beta(a, b, 0)$ — этим достигается выполнение третьего условия в формуле F. Второе условие в формуле F, $\forall i < 0 \ldots$, тривиально. Для доказательства единственности заметим, что из $F(0, \vec{y}, z)$ следует $z = g(\vec{y})$. Наконец, отметим, что мы параллельно доказали и выполнение рекурсивного условия для базового случая: $F(0, \vec{y}, z) \to z = g(\vec{y})$, откуда в консервативном расширении $f(0, \vec{y}) = g(\vec{y})$.

Перейдём к шагу индукции. Дано: $\exists! z\, F(x, \vec{y}, z)$, надо: $\exists! z'\, F(Sx, \vec{y}, z')$. Сначала докажем существование. Переименуем переменные в $F(x, \vec{y}, z)$:

$$F(x, \vec{y}, z) \quad = \quad \exists c, d \big(\beta(c, d, 0) = g(\vec{y}) \wedge \forall i < x\, (\beta(c, d, Si) = h(\beta(c, d, i), i, \vec{y})) \wedge \beta(c, d, x) = z\big).$$

и применим лемму 7 с $k = Sx$ и $h = h(z, x, \vec{y})$. Получим значения a и b и объявим $z' = h = h(z, x, \vec{y})$. Проверим, что для них выполняется нужные условия:

$$\beta(a, b, 0) = g(\vec{y}) \wedge \forall i < Sx\, (\beta(a, b, Si) = h(\beta(a, b, i), i, \vec{y})) \wedge \beta(a, b, Sx) = z'.$$

Первое следует из $\beta(a, b, 0) = \beta(c, d, 0)$ (поскольку $0 < Sx = k$). Для второго разберём два случая. Если $i < x$, то, опять же, $\beta(a, b, Si) = \beta(c, d, Si)$ (т.к. $Si < Sx = k$) и $\beta(a, b, i) = \beta(c, d, i)$, и мы применяем $F(x, \vec{y}, z)$. Для $i = x$ имеем $\beta(a, b, x) = \beta(c, d, x)$ и $\beta(a, b, Sx) = \beta(a, b, k) = h = h(z, x, \vec{y})$. Поскольку $\beta(c, d, x) = z$, получаем требуемое $\beta(a, b, Sx) = h(\beta(a, b, x), x, \vec{y})$. Наконец, третье условие выполнено в силу выбора z'.

Доказательство единственности следующее: из $F(Sx, \vec{y}, z')$ следует, что существует z (а именно, $z = \beta(a, b, x)$), для которого выполнена $F(x, \vec{y}, z)$ и при этом $z = h(z', x, \vec{y})$. По предположению индукции такой z единствен. Значит, единствен и z'.

Тут же мы доказали и рекурсивное условие: $(F(Sx, \vec{y}, z') \wedge F(x, \vec{y}, z)) \to z = h(z', x, \vec{y})$. Действительно, из единственности z получаем, что $z = \beta(a, b, x)$ (где a и b даны первой формулой F, для z'). Теперь первая формула F даёт $z' = \beta(a, b, Sx) = h(\beta(a, b, x), x, \vec{y}) = h(z, x, \vec{y})$. В консервативном расширении с функциональным символом f формула запишется красивее: $f(Sx, \vec{y}) = h(f(x, \vec{y}), x, \vec{y})$. Можно, наоборот, перейти в чисто арифметический язык: $(F(Sx, \vec{y}, z') \wedge F(x, \vec{y}, z)) \to H(z, x, \vec{y}, z')$. $\square$

2 Предикат и условия доказуемости

2.1 Операции на последовательностях

После доказательства теоремы 11 можно перейти к более простому кодированию последовательностей. А именно, последовательность $[a_0, a_1, \ldots, a_{\ell-1}]$ будем кодировать числом $p_0^{a_0+1} p_1^{a_1+1} \ldots p_{\ell-1}^{a_{\ell-1}+1}$, где p_i — i-е простое число ($p_0 = 2$, $p_1 = 3$, $p_2 = 5$, ...). Пустая последовательность кодируется числом 1. Функции $i \mapsto p_i$ и $x, y \mapsto x^y$ примитивно-рекурсивны — значит, теперь мы можем ими пользоваться как псевдотермами.

Удобство такого кодирования последовательностей, в сравнении с бета-функцией, в его однозначности: у каждой последовательности есть ровно один код. При этом, однако, не каждое число есть код последовательности (например, таковыми не являются 0 и $63 = 3^2 \cdot 7$). Однако свойство «быть последовательностью» кодируется следующей Δ_0-формулой:

$$\mathrm{Seq}(x) \quad = \quad (x \neq 0) \wedge \forall p \leqslant x\, \forall q < p\, \big((p,\, q \text{ простые} \wedge p \mid x) \to q \mid x\big).$$

На последовательностях можно определить следующие основные функции — все они будут примитивно-рекурсивными.

$\mathrm{len}(s)$	длина последовательности s
$(s)_i$	взятие i-го элемента последовательности s
$s_1 * s_2$	конкатенация последовательностей s_1 и s_2
$[a]$	последовательность из одного элемента a

Из рекурсивных соотношений для этих примитивно-рекурсивных функций можно вывести следующее:

Лемма 12. *В* PA *доказуемо:*

1. $\mathrm{Seq}(x) \wedge \mathrm{Seq}(y) \to \mathrm{Seq}(x * y)$
2. $\mathrm{Seq}([a])$
3. $([a])_0 = a$
4. $\mathrm{Seq}(x) \wedge \mathrm{Seq}(y) \to \forall i < \mathrm{len}(x)\ ((x)_i = (x * y)_i)$
5. $\mathrm{Seq}(x) \wedge \mathrm{Seq}(y) \to \forall j < \mathrm{len}(y)\ ((y)_j = (x * y)_{j+\mathrm{len}(x)})$

Задача. Докажите лемму 12. *Подсказка:* для упрощения рассуждений может оказаться проще не определять наши функции как примитивно-рекурсивные, а непосредственно реализовать их формулами в PA с условием доказуемой тотальности.

С помощью кодирования последовательностей можно реализовать *возвратную рекурсию.* Для функции f через $f_\sharp$ обозначим следующую функцию:

$$f_\sharp(x, \vec{y}) = [f(0, \vec{y}), \ldots, f(x-1, \vec{y})]$$

В частности, $f_\sharp(0, \vec{y}) = [] = 1$. Возвратной рекурсией называется рекурсия, при которой при определении $f(x, \vec{y})$ используется значение $f_\sharp(x, \vec{y})$:

$$f(x, \vec{y}) = h(f_\sharp(x, \vec{y}), x, \vec{y}).$$

Возвратная рекурсия для f сводится к примитивной для $f_\sharp$:

$$\begin{cases} f_\sharp(0, \vec{y}) = 1 \\ f_\sharp(x+1, \vec{y}) = f_\sharp(x, \vec{y}) * [h(f_\sharp(x, \vec{y}), x, \vec{y})]. \end{cases}$$

При этом $f(x, \vec{y}) = \big(f_\sharp(x+1, \vec{y})\big)_x$.

2.2 Гёделева нумерация термов и формул

Напомним, что мы используем простое кодирование последовательностей: последовательность $[a_0, a_1, \ldots, a_{\ell-1}]$ кодируется числом $p_0^{a_0+1} p_1^{a_1+1} \ldots p_{\ell-1}^{a_{\ell-1}+1}$ и следующее кодирование пар: $\langle x, y\rangle = 2((x+y)^2 + x + 1)$. Код пары всегда чётен.

Определим *гёделеву нумерацию* — кодирование термов и формул арифметической сигнатуры натуральными числами. Мы предъявим конкретную нумерацию. На самом деле, выбор её относительно произволен, но нужно, чтобы выполнялись следующие условия: (1) синтаксические операции над кодами должны быть примитивно-рекурсивными; (2) код формулы (терма) должен быть больше кодов её подформул (подтермов). Последнее условие позволяет использовать возвратную рекурсию там, где нужна рекурсия по структуре формул и термов. В частности, таким образом определяется операция подстановки.

Начнём с нумерации букв арифметического языка:

$$\ulcorner \bot \urcorner = 1, \quad \ulcorner \to \urcorner = 3, \quad \ulcorner \forall \urcorner = 5, \quad \ulcorner = \urcorner = 7, \quad \ulcorner 0 \urcorner = 9, \quad \ulcorner S \urcorner = 11, \quad \ulcorner + \urcorner = 13, \quad \ulcorner \cdot \urcorner = 15;$$

для i-й переменной x_i полагаем $\ulcorner x_i \urcorner = 2i + 17$. Отметим, что все эти коды нечётны. Коды более сложных объектов будут чётными.

Далее, термы и формулы кодируются парами или тройками соответствующих гёделевых номеров: $\ulcorner Su \urcorner = \langle \ulcorner S \urcorner, \ulcorner u \urcorner \rangle$, $\ulcorner \varphi \to \psi \urcorner = \langle \ulcorner \to \urcorner, \langle \ulcorner \varphi \urcorner, \ulcorner \psi \urcorner \rangle\rangle$, и т.д. Например, $\ulcorner 2 + 2 \urcorner = \langle \ulcorner + \urcorner, \langle \ulcorner 2 \urcorner, \ulcorner 2 \urcorner \rangle\rangle$, при этом $\ulcorner 2 \urcorner = \ulcorner S(S0) \urcorner = \langle \ulcorner S \urcorner, \langle \ulcorner S \urcorner, \ulcorner 0 \urcorner \rangle\rangle$.

В таком кодировании очень удобно — просто термами — определяется построение более сложных объектов из более простых. Например, если $x = \ulcorner\varphi\urcorner$, $y = \ulcorner\psi\urcorner$, то $\langle\ulcorner{\to}\urcorner, \langle x, y\rangle\rangle = \ulcorner\varphi \to \psi\urcorner$. Напомним, что функция взятия пары задаётся многочленом (термом). Свойство «быть термом», «быть формулой» определяются как примитивно-рекурсивные, возвратной рекурсией. Так, характеристическая функция множества кодов термов, χ_{Tm}, можно определить так: $\chi_{\mathrm{Tm}}(x) = 1$, если выполняется одно из условий (разбор случаев примитивно-рекурсивен). Здесь π_1 и π_2 — функции проекций пары (взятия первого и второго элементов).

1. $x = \ulcorner 0\urcorner$;
2. $x = \ulcorner x_i\urcorner$ (т.е. $2i + 17$ для некоторого i);
3. x чётно, $\pi_1(x) = \ulcorner S\urcorner$, $\chi_{\mathrm{Tm}}(\pi_2(x)) = 1$;
4. x чётно, $\pi_1(x) = \ulcorner +\urcorner$ или $\ulcorner\cdot\urcorner$, $\pi_2(x)$ чётно, $\chi_{\mathrm{Tm}}(\pi_1(\pi_2(x))) = \chi_{\mathrm{Tm}}(\pi_2(\pi_2(x))) = 1$.

Заметим, что всегда $\pi_{1,2}(x) < x$, поэтому здесь корректно применена возвратная рекурсия.

Определим $\mathrm{Tm}(x) = \bigl(\chi_{\mathrm{Tm}}(x) = 1\bigr)$ (в консервативном расширении). Из доказуемости рекурсивных соотношений получаем:

1. $\mathsf{PA} \vdash \mathrm{Tm}(x) \to \mathrm{Tm}(\langle\ulcorner S\urcorner, x\rangle)$
2. $\mathsf{PA} \vdash (\mathrm{Tm}(x) \wedge \mathrm{Tm}(y)) \to \mathrm{Tm}(\langle\ulcorner +\urcorner, \langle x, y\rangle\rangle)$
3. $\mathsf{PA} \vdash (\mathrm{Tm}(x) \wedge \mathrm{Tm}(y)) \to \mathrm{Tm}(\langle\ulcorner\cdot\urcorner, \langle x, y\rangle\rangle)$

Проверим первое. Рекурсивное условие формулируется следующим образом: $\chi_{\mathrm{Tm}}(x) = \bigl(\chi_{\mathrm{Tm}\sharp}(x+1)\bigr)_x = h(\chi_{\mathrm{Tm}\sharp}(x), x)$. Последнее равенство доказуемо по лемме 12. Функция h реализует разбор случаев в определении χ_{Tm}. В данном случае используем п. 3: имеем $\bigl(\chi_{\mathrm{Tm}\#}(x)\bigr)_{\pi_2(x)} = 1$, откуда значение h равно 1. Всё это рассуждение происходит внутри PA.

Аналогично определяется функция χ_{Fm} и предикат Fm „являться гёделевым номером формулы“.

Примитивной рекурсией можно определить гёделев номер нумерала данного числа: $\mathrm{num}(0) = \ulcorner 0\urcorner$, $\mathrm{num}(x+1) = \langle\ulcorner S\urcorner, \mathrm{num}(x)\rangle$. Индукцией доказывается, что нумерал — всегда терм ($\forall x\, \mathrm{Tm}(\mathrm{num}(x))$).

Наконец, опять же возвратной рекурсией определяются примитивно-рекурсивные функции подстановки. Нас будет интересовать одна из них — подстановка данного терма вместо переменной x:

$$\mathrm{sub}_x(\ulcorner\varphi(x)\urcorner, \ulcorner u\urcorner) = \ulcorner\varphi(u)\urcorner.$$

2.3 Формулы Prf и Pr. Условия Гильберта – Бернайса – Лёба

Свойство „быть аксиомой PA“ также примитивно-рекурсивно (интересный случай здесь — схемы аксиом исчисления предикатов и аксиома индукции, где нам потребуется подстановка). Значит, можно задать это свойство арифметической формулой $\mathrm{Ax}(x)$.

Теперь мы готовы записать формулу „быть доказательством“, где доказательство понимается как последовательность формул, каждая из которых либо аксиома, либо получается из предыдущих по правилам modus ponens или усиления. Следующая формула $\mathrm{Prf}(y, x)$ означает „y кодирует доказательство формулы с гёделевым номером x“:

$$\begin{aligned}
&\mathrm{Prf}(y, x) = \\
&\qquad = \mathrm{Seq}(y) \wedge \mathrm{Fm}(x) \wedge (y)_{\mathrm{len}(y)-1} = x \wedge \forall i < \mathrm{len}(y)\bigl(\mathrm{Ax}((y)_i) \vee \\
&\qquad\qquad \vee \exists j, k < i\, ((y)_k = \langle\ulcorner{\to}\urcorner, \langle (y)_j, (y)_i\rangle\rangle) \vee \\
&\qquad\qquad\qquad \vee \exists j < i\, \exists v\, (\exists k\, (v = 2k + 17) \wedge (y)_i = \langle\ulcorner\forall\urcorner, \langle v, (y)_j\rangle\rangle)\bigr).
\end{aligned}$$

Формула Prf принадлежит классу Σ_1. В стандартной модели она выражает нужное свойство: если n — код доказательства формулы φ, то $\mathbb{N} \vDash \mathrm{Prf}(n, \ulcorner\varphi\urcorner)$. Из Σ_1-полноты получаем $\mathsf{PA} \vdash \mathrm{Prf}(\underline{n}, \ulcorner\varphi\urcorner)$.

Далее, определим предикат (формулу) *доказуемости* следующим естественным способом:

$$\mathrm{Pr}(x) \quad = \quad \exists y\, \mathrm{Prf}(y, x).$$

В стандартной модели $\mathrm{Pr}(\ulcorner\varphi\urcorner)$ выражает доказуемость формулы φ. Нас будут интересовать свойства этого предиката, доказуемые в PA. Эти свойства называются *условиями доказуемости,* или *условиями Гильберта – Бернайса – Лёба:*

GL-1: если $\mathsf{PA} \vdash \varphi$, то $\mathsf{PA} \vdash \mathrm{Pr}(\ulcorner\varphi\urcorner)$
GL-2: $\mathsf{PA} \vdash (\mathrm{Pr}(\ulcorner\varphi \to \psi\urcorner) \wedge \mathrm{Pr}(\ulcorner\varphi\urcorner)) \to \mathrm{Pr}(\ulcorner\psi\urcorner)$
GL-3: $\mathsf{PA} \vdash \mathrm{Pr}(\ulcorner\varphi\urcorner) \to \mathrm{Pr}(\ulcorner\mathrm{Pr}(\ulcorner\varphi\urcorner)\urcorner)$

Здесь φ и ψ — конкретные замкнутые арифметические формулы. Отметим, что для формулировки GL-3 нужно переписать Pr в арифметическом языке (без дополнительных функциональных символов) — иначе не определён гёделев номер $\ulcorner\mathrm{Pr}(\ulcorner\varphi\urcorner)\urcorner$.

Условие GL-1 сразу следует из Σ_1-полноты: если $\mathsf{PA} \vdash \varphi$, то $\mathbb{N} \vdash \mathrm{Pr}(\ulcorner\varphi\urcorner)$, откуда $\mathsf{PA} \vdash \mathrm{Pr}(\ulcorner\varphi\urcorner)$, поскольку $\mathrm{Pr}(\ulcorner\varphi\urcorner)$ — замкнутая Σ_1-формула. Условие GL-3 мы докажем позже (§ 2.5).

Теорема 13 (условие GL-2). $\mathsf{PA} \vdash (\mathrm{Pr}(\ulcorner\varphi \to \psi\urcorner) \wedge \mathrm{Pr}(\ulcorner\varphi\urcorner)) \to \mathrm{Pr}(\ulcorner\psi\urcorner)$.

Доказательство. Требуемое утверждение сразу следует из «явного» свойства, для формулы Prf:

$$(\mathrm{Prf}(y, \ulcorner\varphi \to \psi\urcorner) \wedge \mathrm{Prf}(z, \ulcorner\varphi \to \phi\urcorner)) \to \mathrm{Prf}(y * z * [\ulcorner\varphi\urcorner], \ulcorner\psi\urcorner).$$

Доказательство последнего использует доказуемые свойства кодирования последовательностей (лемма 12). Действительно, $y * z * [\ulcorner\varphi\urcorner]$ — это последовательность, составленная из гёделевых номеров формул, причём каждый из них лежит либо в y, либо в z, либо есть $\ulcorner\varphi\urcorner$. (Для двух последних частей происходит соответствующий сдвиг нумерации.) Свойство каждой формулы либо быть аксиомой, либо получаться из предыдущих по правилу вывода для y и z дано в условии (для z сдвигаем нумерацию). Для последнего элемента последовательности берём $k = \mathrm{len}(y) - 1$ и $j = \mathrm{len}(y) + \mathrm{len}(z) - 1$. Этот последний элемент как раз равен $\ulcorner\psi\urcorner$. □

2.4 Параметрическая доказуемость («переменные с точками»)

Если формула φ замкнута (не содержит свободных переменных), то $\mathrm{Pr}(\ulcorner\varphi\urcorner)$ кодирует доказуемость этой формулы в PA. Поговорим теперь о роли свободных переменных под знаком $\mathrm{Pr}(\ulcorner\ldots\urcorner)$. Для простоты записей пусть $\psi(x)$ — арифметическая формула с одной свободной переменной x. Если написать просто $\mathrm{Pr}(\ulcorner\psi(x)\urcorner)$, то получится формула, означающая доказуемость в PA формулы $\psi(x)$ со *свободной* переменной x. В силу правила обобщения, в одну сторону, и аксиомы $(\forall x\, \psi(x)) \to \psi(u)$ (для произвольного терма u) и условия GL-2 в другую, $\mathrm{Pr}(\ulcorner\psi(x)\urcorner)$ равносильно $\mathrm{Pr}(\ulcorner\forall x\, \psi(x)\urcorner)$. (Эта равносильность доказуема в PA.) Отметим, что формула $\mathrm{Pr}(\ulcorner\psi(x)\urcorner)$ *замкнута,* x не является её параметром (свободной переменной).

Мы же запишем доказуемость со свободной переменной x в другом смысле: x будет *параметром* нашей новой формулы доказуемости, которая будет означать доказуемость $\psi(x)$ при данном конкретном x.

Давайте временно обозначать «внутренние» переменные, под знаком гёделева номера, другим шрифтом: вместо $\mathrm{Pr}(\ulcorner\psi(x)\urcorner)$ пишем $\mathrm{Pr}(\ulcorner\psi(\mathfrak{x})\urcorner)$. Цель, к которой мы движемся,

— записать формулу, которая, получая на вход значение свободной переменной x, создаёт гёделев номер соответствующего нумерала, подставляет его в $\psi(\mathfrak{x})$ вместо внутренней переменной $\mathfrak{x}$ и выдаёт значение Pr на гёделевом номере полученной замкнутой формулы.

Технически эта идея реализуется с помощью примитивно-рекурсивных функций. Сначала реализуем функцию num, выдающую по своему аргументу гёделев номер соответствующего нумерала:

$$\begin{aligned}&\mathrm{num}(0) = \ulcorner 0 \urcorner;\\&\mathrm{num}(n+1) = \langle \ulcorner S \urcorner, \mathrm{num}(n) \rangle.\end{aligned}$$

Для функции num вводится соответствующий псевдотерм (функциональный символ в расширенном языке). Рекурсивные условия на функцию num позволяют доказать, что каждый нумерал является термом: $\mathsf{PA} \vdash \forall z\ \mathrm{Tm}(\mathrm{num}(z))$.

Далее, у нас есть функция подстановки, действующая следующим образом: для терма u и формулы $\psi(\mathfrak{x})$,

$$\mathrm{sub}_{\mathfrak{x}}(\ulcorner \psi(\mathfrak{x}) \urcorner, \ulcorner u \urcorner) = \ulcorner \psi(u) \urcorner.$$

(Индекс у sub выделяет переменную, вместо которой мы подставляем u; можно передавать номер этой переменной как третий аргумент функции sub.) Функция sub определяется примитивной (точнее, возвратной) рекурсией по первому аргументу, что соответствует рекурсии по структуре формулы ψ. При *фиксированной* ψ, однако, можно считать sub, как функцию от второго аргумента, просто многочленом. Действительно, пусть, например,

$$\psi(\mathfrak{x}) = \bigl(\neg \exists \mathfrak{z}\ S\mathfrak{z} + \mathfrak{x} = \mathfrak{x}\bigr).$$

Тогда подстановка воспроизводит *конечное* число шагов построения формулы ψ вложенным применением функции пары:

$$\mathrm{sub}_{\mathfrak{x}}(\ulcorner \psi(\mathfrak{x}) \urcorner, k) = \langle \ulcorner \neg \urcorner, \langle \ulcorner \exists \urcorner, \langle \ulcorner \mathfrak{z} \urcorner, \langle \ulcorner = \urcorner, \langle \langle \ulcorner + \urcorner, \langle \langle \ulcorner S \urcorner, \ulcorner \mathfrak{z} \urcorner \rangle, k \rangle \rangle, k \rangle \rangle \rangle \rangle \rangle.$$

(Напомним, что $\langle x, y \rangle = 2((x+y)^2 + x + 1)$, так что справа написан многочлен от переменной k.) В наших построениях формулы будут как правило фиксированы, поэтому нам будет достаточно такой упрощённой функции подстановки, не требующей примитивной рекурсии по структуре формулы. Однако будет место, где важна примитивная рекурсивность $\mathrm{sub}_{\mathfrak{x}}$ по первому аргументу!

Наконец, определим параметрическую формулу доказуемости следующим образом:

$$\mathrm{Pr}(\ulcorner \psi(\dot{x}) \urcorner) = \mathrm{Pr}(\mathrm{sub}_{\mathfrak{x}}(\ulcorner \psi(\mathfrak{x}) \urcorner, \mathrm{num}(x))).$$

«Выведение» x как внешнего параметра из формулы доказуемости по традиции обозначается точкой над вхождениями x в ψ.

Аналогично можно определить параметрическую доказуемость для нескольких параметров, записывая соответствующую sub как многочлен нескольких переменных:

$$\mathrm{Pr}(\ulcorner \psi(\dot{x}_1, \ldots, \dot{x}_n) \urcorner) = \mathrm{Pr}(\mathrm{sub}_{\mathfrak{x}_1, \ldots, \mathfrak{x}_n}(\ulcorner \psi(\mathfrak{x}_1, \ldots, \mathfrak{x}_n) \urcorner, \mathrm{num}(x_1), \ldots, \mathrm{num}(x_n))).$$

Для краткости пишут $\mathrm{Pr}(\ulcorner \psi(\dot{\vec{x}}) \urcorner)$. Наша параметрическая формула записана в расширенном языке (с псевдотермом num); её можно перевести в арифметический язык, не выходя за пределы класса Σ_1:

$$\begin{aligned}\mathrm{Pr}(\ulcorner \psi(\dot{x}_1, \ldots, \dot{x}_n) \urcorner) \equiv \exists z_1\ \ldots\ \exists z_n\ \bigl(&\mathrm{Pr}(\mathrm{sub}_{\mathfrak{x}_1, \ldots, \mathfrak{x}_n}(\psi(\mathfrak{x}_1, \ldots, \mathfrak{x}_n), z_1, \ldots, z_n)) \wedge \\ &\wedge \mathrm{Num}(x_1, z_1) \wedge \ldots \wedge \mathrm{Num}(x_n, z_n)\bigr).\end{aligned}$$

Заметим, что $\mathrm{sub}_{\mathfrak{x}_1,\ldots,\mathfrak{x}_n}(\psi(\mathfrak{x}_1,\ldots,\mathfrak{x}_n), z_1,\ldots,z_n)$ — это настоящий арифметический терм (многочлен) от z_1, $\ldots$, z_n; Num — Σ_1-формула, представляющая примитивно-рекурсивную функцию num в смысле теоремы 11.

Условие GL-2 (теорема 13) можно сделать параметрическим: доказательство остаётся то же, со свободными переменными $x_1,\ldots,x_n$.

Теорема 14. $\mathsf{PA} \vdash (\mathrm{Pr}(\ulcorner\varphi(\dot{\vec{x}}) \to \psi(\dot{\vec{x}})\urcorner) \wedge \mathrm{Pr}(\ulcorner\varphi(\dot{\vec{x}})\urcorner)) \to \mathrm{Pr}(\ulcorner\psi(\dot{\vec{x}})\urcorner))$

Лемма 15. *Параметрический* Pr *слабее непараметрического:* $\mathsf{PA} \vdash \mathrm{Pr}(\ulcorner\psi(\mathfrak{x}_1,\ldots,\mathfrak{x}_n)\urcorner) \to \mathrm{Pr}(\ulcorner\psi(\dot{x}_1,\ldots,\dot{x}_n)\urcorner)$.

Доказательство. Для простоты пусть параметр один. По правилу обобщения получаем $\mathrm{Pr}(\ulcorner\forall x\,\psi(x)\urcorner)$. Далее рассмотрим аксиому $(\forall x\,\psi(x)) \to \psi(u)$, где u — произвольный терм. Наша формула Ax (возникшая из примитивно-рекурсивного кодирования множества аксиом) обладает доказуемым свойством $\mathrm{Tm}(z) \to \mathrm{Ax}(\mathrm{sub}_{\mathfrak{z}}(\ulcorner(\forall x\,\psi(x)) \to \psi(\mathfrak{z})\urcorner, z))$. Поскольку формула ψ конкретная, можно считать (используя рекурсивные условия), что функция подстановки реализована просто как многочлен от z.

Отсюда получаем $\mathrm{Ax}(\ulcorner(\forall x\,\psi(x)) \to \psi(\dot{x})\urcorner)$, а значит $\mathrm{Pr}(\ulcorner(\forall x\,\psi(x)) \to \psi(\dot{x})\urcorner)$. Остаётся применить параметрическую версию GL-2 (теорема 14). □

2.5 Доказуемая Σ_1-полнота и условие GL-3

Так же, как условие GL-1 следует из Σ_1-полноты PA (см. § 1.5), более сильное условие GL-3 следует из *доказуемой* Σ_1-полноты PA:

$$\mathsf{PA} \vdash \sigma \to \mathrm{Pr}(\ulcorner\sigma\urcorner) \qquad \text{для произвольной замкнутой } \Sigma_1\text{-формулы } \sigma.$$

Далее, как и обычная, доказуемая Σ_1-полнота выводится из (доказуемой же) Δ_0-полноты. При этом если в утверждении о Σ_1-полноте рассматривались только замкнутые формулы, для Δ_0-полноты понадобится рассматривать формулы со свободными переменными. Таким образом, нам будет нужно *параметрическое* (в смысле предыдущего параграфа) утверждение.

Лемма 16 (параметрическая доказуемая Δ_0-полнота)**.** *Пусть* $\delta(\vec{x})$ — Δ_0*-формула со свободными переменными* $\vec{x} = (x_1,\ldots,x_n)$*. Тогда*

$$\mathsf{PA} \vdash \delta(\vec{x}) \to \mathrm{Pr}(\ulcorner\delta(\dot{\vec{x}})\urcorner).$$

Заметим, что в формуле $\delta(\vec{x}) \to \mathrm{Pr}(\ulcorner\delta(\dot{\vec{x}})\urcorner)$ переменные $\vec{x}$ свободные — таким образом, можно навесить квантор: $\forall\vec{x}\,\bigl(\delta(\vec{x}) \to \mathrm{Pr}(\ulcorner\delta(\dot{\vec{x}})\urcorner)\bigr)$. Читается это утверждение следующим образом: если для данных значений $\vec{x}$ верна формула $\delta(\vec{x})$, то она доказуема при подстановке в неё соответствующих нумералов.

Доказательство. Рассуждаем внешней (за пределами PA) индукцией по построению формулы δ, параллельно доказывая два утверждения:

$$\mathsf{PA} \vdash \delta(\vec{x}) \to \mathrm{Pr}(\ulcorner\delta(\dot{\vec{x}})\urcorner)$$

$$\mathsf{PA} \vdash \neg\delta(\vec{x}) \to \mathrm{Pr}(\ulcorner\neg\delta(\dot{\vec{x}})\urcorner)$$

Наиболее интересен, как ни странно, случай атомарной формулы δ. Сначала разберёмся с его простейшей реализацией: $\delta(\vec{x}, y) = \bigl(y = u(\vec{x})\bigr)$ для некоторого терма u с переменными из набора $\vec{x}$. Действуем индукцией (опять же внешней) по структуре терма u. Будем пока что доказывать только первое утверждение (без отрицания).

- Если u — переменная, то имеем $\delta(x, y) = \big(y = x\big)$, и $\mathsf{PA} \vdash y = x \to \ulcorner \dot{y} = \dot{x} \urcorner = \ulcorner \dot{x} = \dot{x} \urcorner$. (Напомним, что $\ulcorner \dot{y} = \dot{x} \urcorner$ — псевдотерм, соответствующий примитивно-рекурсивной функции, осуществляющей подстановку соответствующих нумералов; если $y = x$, то первый её аргумент, y, можно заменить на x.)

  Далее, в аксиоматизации PA есть аксиомы $\forall z\,(z = z)$ и $(\forall z\,\psi(z)) \to \psi(t)$ для произвольного терма t. Последняя кодируется через функцию подстановки формулы ψ и терма t — в частности, $\mathsf{PA} \vdash \mathrm{Ax}(\ulcorner(\forall z\,(z = z)) \to (\dot{x} = \dot{x})\urcorner)$, со свободной x.

  Отсюда, применяя параметрическое условие GL-2 (теорема 14), получаем $\mathsf{PA} \vdash \Pr(\ulcorner \dot{x} = \dot{x} \urcorner)$, а следовательно $\mathsf{PA} \vdash y = x \to \Pr(\ulcorner \dot{y} = \dot{x} \urcorner)$.

- Если u — константа 0, то $\mathsf{PA} \vdash y = 0 \to \ulcorner \dot{y} \urcorner = \ulcorner 0 \urcorner$, поскольку таково значение примитивно-рекурсивной функции num при нулевом аргументе (это одно из рекурсивных условий!): $\mathsf{PA} \vdash \mathrm{num}(0) = \ulcorner 0 \urcorner$. Отсюда $\mathsf{PA} \vdash \ulcorner \dot{y} = 0 \urcorner = \ulcorner 0 = 0 \urcorner$. Поскольку $\mathsf{PA} \vdash \Pr(\ulcorner 0 = 0 \urcorner)$ (по GL-1), получаем $\mathsf{PA} \vdash y = 0 \to \Pr(\ulcorner \dot{y} = 0 \urcorner)$.

- Теперь пусть $u = Su'$.

  Докажем **вспомогательное утверждение:**

$$\mathsf{PA} \vdash (z = Sw) \to \Pr(\ulcorner \dot{z} = S\dot{w} \urcorner).$$

  Его можно переписать ещё и так: $\mathsf{PA} \vdash \Pr(\ulcorner \overset{\cdot}{\widehat{Sw}} = S\dot{w} \urcorner)$. Это довольно тонкий момент: здесь сказано, что не важно, когда прибавлять единицу — до взятия нумерала или после, приписыванием S. Утверждение следует из такого: $\mathsf{PA} \vdash \mathrm{num}(Sw) = \langle S, \mathrm{num}(w) \rangle$, а это — в точности рекурсивное условие функции num.

  Разберём (в PA) два случая для y. Случай $y = 0$ тривиален: в этом случае опровергается посылка $y = Su'(\vec{x})$. Пусть теперь $y = Sy'$. В этом случае из $Sy' = Su'(\vec{x})$ получаем $y' = u'(\vec{x})$, и по предположению внешней индукции (u' проще u) имеем $\Pr(\ulcorner \dot{y}' = u'(\dot{\vec{x}}) \urcorner)$.

  По вспомогательному утверждению, $\Pr(\ulcorner \dot{y} = S\dot{y}' \urcorner)$. Кроме того, из аксиомы $z = w \to Sz = Sw$ подстановкой (как мы уже делали раньше) получаем $\Pr(\ulcorner S\dot{y}' = Su'(\dot{\vec{x}}) \urcorner)$ и, наконец, из аксиомы транзитивности равенства, через параметрическое GL-2, $\Pr(\ulcorner \dot{y} = Su'(\dot{\vec{x}}) \urcorner)$.

- Пусть $u = u_1 + u_2$. Тогда, рассуждая в PA в предположении $y = u(\vec{x})$, можно ввести две новые переменные y_1 и y_2 с условиями $y_1 = u_1(\vec{x})$, $y_2 = u_2(\vec{x})$ и $y = y_1 + y_2$. Докажем в PA, что $y = y_1 + y_2 \to \Pr(\ulcorner \dot{y} = \dot{y}_1 + \dot{y}_2 \urcorner)$. Действуем индукцией (на этот раз внутренней) в PA по y_2.

  База индукции: $y_2 = 0$, откуда (не забываем, что всё это происходит внутри PA) $y = y_1$. Значит, $\ulcorner \dot{y} = \dot{y}_1 + \dot{y}_2 \urcorner = \ulcorner \dot{y} = \dot{y} + 0 \urcorner$, а это — подстановочный пример формулы $\forall z(z = z + 0)$, которая выводится из аксиомы $\forall z(z + 0 = z)$ (всё это совершается под знаком Pr за счёт GL-2).

  Далее, пусть $y_2 = Sy_2'$. Тогда $y = Sy'$ и $y' = y_1 + y_2'$. По предположению индукции $\Pr(\ulcorner \dot{y}' = \dot{y}_1 + \dot{y}_2' \urcorner)$, откуда $\Pr(\ulcorner S\dot{y}' = S(\dot{y}_1 + \dot{y}_2' \urcorner)$ и, применяя аксиому $\forall z, w\,(z + Sw = S(z + w))$, получаем $\Pr(\ulcorner S\dot{y}' = \dot{y}_1 + S\dot{y}_2' \urcorner)$. Наконец, по сформулированному выше вспомогательному утверждению $\Pr(\ulcorner S\dot{y}' = \dot{y} \urcorner)$ и $\Pr(\ulcorner S\dot{y}_2' = \dot{y}_2' \urcorner)$, откуда получаем требуемое $\Pr(\ulcorner \dot{y} = \dot{y}_1 + \dot{y}_2 \urcorner)$.

  Кроме того, по внешнему предположению индукции имеем $\Pr(\ulcorner \dot{y}_1 = u_1(\dot{\vec{x}}) \urcorner)$ и $\Pr(\ulcorner \dot{y}_2 = u_2(\dot{\vec{x}}) \urcorner)$, откуда получаем требуемое $\Pr(\ulcorner \dot{y} = u(\dot{\vec{x}}) \urcorner)$.

- Случай $u = u_1 \cdot u_2$ разбирается аналогично, достаточно установить $\mathsf{PA} \vdash y = y_1 \cdot y_2 \to \mathrm{Pr}(\ulcorner \dot{y} = \dot{y}_1 \cdot \dot{y}_2 \urcorner)$. Действуем индукцией по y_2. В базовом случае под знаком Pr оказывается $\ulcorner 0 = \dot{y}_1 \cdot 0 \urcorner$, доказуемо по аксиоме. На шаге индукции $y_2 = Sy_2'$, $y = y' + y_1$ и $y' = y_1 \cdot y_2'$. Всё это погружается под знак доказуемости: $\mathrm{Pr}(\ulcorner \dot{y}_2 = S\dot{y}_2' \urcorner)$ по вспомогательному утверждению, $\mathrm{Pr}(\ulcorner \dot{y} = \dot{y}' + \dot{y}_1 \urcorner)$ из предыдущего пункта и $\mathrm{Pr}(\ulcorner \dot{y}' = \dot{y}_1 \cdot \dot{y}_2' \urcorner)$ из предположения индукции по y_2. Кроме того, рекурсивная аксиома для умножения даёт $\mathrm{Pr}(\ulcorner \dot{y}_1 \cdot \dot{y}_2' + \dot{y}_1 = \dot{y}_1 \cdot S\dot{y}_2' \urcorner)$. Собирая всё вместе, получаем искомое.

Теперь вернёмся к произвольной Δ_0-формуле вида $\delta(\vec{x}) = \big(u(\vec{x}) = v(\vec{x})\big)$, где u и v — термы. Рассуждаем в PA в предположении $\delta(\vec{x})$ и вводим дополнительную переменную y: $y = u(\vec{x})$ и $y = v(\vec{x})$. (Формально в исчислении предикатов мы доказываем равносильность $u(\vec{x}) = v(\vec{x})$ и $\exists y \big(y = u(\vec{x}) \wedge y = v(\vec{x})\big)$, после чего выносим квантор $\exists y$ из посылки: $\forall y \, \big(y = u(\vec{x}) \wedge y = v(\vec{x}) \to \mathrm{Pr}(\ulcorner \delta(\vec{x}) \urcorner)\big)$. Так появляется новая переменная.)

Мы уже доказали, что $\mathsf{PA} \vdash y = u(\vec{x}) \to \mathrm{Pr}(\ulcorner \dot{y} = u(\dot{\vec{x}}) \urcorner)$ и $\mathsf{PA} \vdash y = v(\vec{x}) \to \mathrm{Pr}(\ulcorner \dot{y} = v(\dot{\vec{x}}) \urcorner)$. Значит, получаем $\mathrm{Pr}(\ulcorner u(\dot{\vec{x}}) = v(\dot{\vec{x}}) \urcorner)$, применяя под знаком Pr транзитивность равенства (опять же по параметрическому GL-2).

Нужно также разобрать случай отрицания, т.е. установить $\mathsf{PA} \vdash \neg\delta(\vec{x}) \to \mathrm{Pr}(\ulcorner \neg\delta(\dot{\vec{x}}) \urcorner)$. Введём две переменные: $y = u(\vec{x})$, $z = v(\vec{x})$, $y \neq z$. Мы уже получили $\mathrm{Pr}(\ulcorner \dot{y} = u(\dot{\vec{x}}) \urcorner)$ и $\mathrm{Pr}(\ulcorner \dot{z} = v(\dot{\vec{z}}) \urcorner)$. Остаётся $\mathsf{PA} \vdash y \neq z \to \mathrm{Pr}(\ulcorner \neg(\dot{y} = \dot{z}) \urcorner)$. В PA, если $y \neq z$, то либо $y < z$, либо $z < y$. Разберём первый случай (второй симметричен). В этом случае для некоторого w имеем $z = y + Sw$. Отсюда, по доказанному ранее, $\mathrm{Pr}(\ulcorner \dot{z} = \dot{y} + S\dot{w} \urcorner)$. С другой стороны, $\mathsf{PA} \vdash \forall z, y, w \, \big(z = y + Sw \to y \neq z\big)$. Применяя аксиомы исчисления предикатов и параметрическое GL-2, получаем искомое $\mathrm{Pr}(\ulcorner \neg\dot{y} = \dot{z} \urcorner)$.

Теперь разберём неатомарные случаи для δ.

- Если $\delta = \bot$, то $\mathsf{PA} \vdash \bot \to \mathrm{Pr}(\ulcorner \bot \urcorner)$ *ex falso* и $\mathsf{PA} \vdash \neg\bot \to \mathrm{Pr}(\ulcorner \neg\bot \urcorner)$, поскольку заключение выводимо по GL-1.

- Если $\delta(\vec{x}) = \delta_1(\vec{x}) \to \delta_2(\vec{x})$, рассуждаем следующим образом. По предположению индукции имеем $\mathsf{PA} \vdash \delta_i(\vec{x}) \to \mathrm{Pr}(\ulcorner \delta_i(\dot{\vec{x}}) \urcorner)$ и $\mathsf{PA} \vdash \neg\delta_i(\vec{x}) \to \mathrm{Pr}(\ulcorner \neg\delta_i(\dot{\vec{x}}) \urcorner)$, где $i = 1, 2$.

  Поскольку $\delta(\vec{x})$ равносильно (в PA) $\neg\delta_1(\vec{x}) \vee \delta_2(\vec{x})$, получаем $\mathrm{Pr}(\ulcorner \neg\delta_1(\dot{\vec{x}}) \urcorner) \vee \mathrm{Pr}(\ulcorner \delta_2(\dot{\vec{x}}) \urcorner)$. При этом, поскольку $\neg\delta_1 \to (\delta_1 \to \delta_2)$ и $\delta_2 \to (\delta_1 \to \delta_2)$ выводимы в исчислении высказываний, к ним можно применить (параметрический) предикат доказуемости. По параметрическому GL-2 получаем (из каждого из дизъюнктов) $\mathrm{Pr}(\ulcorner \delta_1(\dot{\vec{x}}) \to \delta_2(\dot{\vec{x}}) \urcorner)$.

  Отрицание: $\neg\delta(\vec{x})$ равносильно $\delta_1(\vec{x}) \wedge \neg\delta_2(\vec{x})$. Значит, $\mathrm{Pr}(\ulcorner \delta_1(\dot{\vec{x}}) \urcorner)$ и $\mathrm{Pr}(\ulcorner \neg\delta_2(\dot{\vec{x}}) \urcorner)$. Применяя параметрическое GL-2 с $\delta_1 \to (\neg\delta_2 \to \neg(\delta_1 \to \delta_2))$ (теорема исчисления высказываний), получаем искомое.

- $\delta(\vec{x}) = \forall z \leqslant u(\vec{x}) \;\; \delta'(\vec{x}, z)$. Для рассуждения в «положительном» случае заведём новую переменную w: $w = u(\vec{x})$ и $\forall z \leqslant w \;\; \delta'(\vec{x}, z)$. Доказываем $\mathrm{Pr}(\ulcorner \forall z \leqslant \dot{w} \;\; \delta'(\dot{\vec{x}}, z) \urcorner)$ индукцией по w.

  При $w = 0$ имеем $\mathrm{Pr}(\ulcorner \delta'(\dot{\vec{x}}, 0) \urcorner)$ и $\mathrm{Pr}(\ulcorner \delta'(\dot{\vec{x}}, 0) \to \forall z \leqslant 0 \;\; \delta'(\dot{\vec{x}}, z) \urcorner)$. (Последнее доказуемо в PA с кванторами по $\vec{x}$, а значит и в любой подстановке.) По параметрическому GL-2 получаем $\mathrm{Pr}(\ulcorner \forall z \leqslant 0 \;\; \delta'(\dot{\vec{x}}, z) \urcorner)$.

  При $w = Sw'$ получаем $\mathrm{Pr}(\ulcorner \forall z \leqslant \dot{w}' \;\; \delta'(\dot{\vec{x}}, z) \urcorner)$ и $\mathrm{Pr}(\ulcorner \delta'(\dot{\vec{x}}, S\dot{w}) \urcorner)$ (здесь использовано вспомогательное утверждение). Поскольку $\mathrm{Pr}(\ulcorner \big(\forall z \leqslant \dot{w}' \;\; \delta'(\dot{\vec{x}}, z)\big) \to \big(\delta'(\dot{\vec{x}}, S\dot{w}) \to \forall z \leqslant S\dot{w}' \;\; \delta'(\dot{\vec{x}}, z)\big) \urcorner)$ (доказуемо даже с кванторами всеобщности по $\vec{x}$ и w), получаем искомое по параметрическому GL-2: $\mathrm{Pr}(\ulcorner \forall z \leqslant S\dot{w}' \;\; \delta'(\dot{\vec{x}}, z) \urcorner)$. (Заменяем $S\dot{w}'$ на $\dot{w}$ по вспомогательному утверждению.)

Наконец, $\dot{w}$ можно заменить на $u(\dot{\vec{x}})$ по $\mathrm{Pr}(\ulcorner \dot{w} = u(\dot{\vec{x}})\urcorner)$ (случай атомарного равенства).

Рассуждение в «отрицательном» случае ещё проще. Если $\exists z \leqslant u(\vec{x})\ \neg\delta'(\vec{x}, z)$, то существует z_0, для которого выполнено $\delta'(\vec{x}, z_0)$ и $z_0 \leqslant u(\vec{x})$. Первое даёт $\mathrm{Pr}(\ulcorner \neg\delta'(\dot{\vec{x}}, \dot{z}_0)\urcorner)$, второе — $\mathrm{Pr}(\ulcorner \dot{z}_0 \leqslant u(\dot{\vec{x}})\urcorner)$ (для этого нужно ввести дополнительную переменную w: $z_0 + w = u(\vec{x})$ и воспользоваться атомарным случаем). Пользуясь $\mathrm{Pr}(\ulcorner \neg\delta'(\dot{\vec{x}}, \dot{z}_0) \to (\dot{z}_0 \leqslant u(\dot{\vec{x}}) \to \exists z \leqslant u(\dot{\vec{x}})\ \neg\delta'(\dot{\vec{x}}, z))\urcorner)$, получаем искомое.

$\square$

Теорема 17 (доказуемая Σ_1-полнота)**.** *Пусть σ — замкнутая Σ_1-формула. Тогда* $\mathsf{PA} \vdash \sigma \to \mathrm{Pr}(\ulcorner \sigma \urcorner)$.

Доказательство. Имеем $\sigma = \exists x\ \delta(x)$, где δ — Δ_0-формула. Докажем, что $\mathsf{PA} \vdash (\exists x\ \delta(x)) \to \mathrm{Pr}(\ulcorner \exists x\ \delta(x)\urcorner)$ или, что то же, $\mathsf{PA} \vdash \forall x\ \big(\delta(x) \to \mathrm{Pr}(\ulcorner \exists x\ \delta(x)\urcorner)\big)$.

По лемме 16, $\mathsf{PA} \vdash \delta(x) \to \mathrm{Pr}(\ulcorner \delta(\dot{x})\urcorner)$. Кроме того, $\mathsf{PA} \vdash \mathrm{Pr}(\ulcorner \delta(\dot{x}) \to \exists x\, \delta(x)\urcorner)$ (есть такая аксиома исчисления предикатов: $\psi(u) \to \exists x\, \psi(x)$). Отсюда получаем искомое $\mathsf{PA} \vdash \delta(x) \to \mathrm{Pr}(\ulcorner \exists x\ \delta(x)\urcorner)$ по параметрическому GL-2. Остаётся применить правило обобщения. $\square$

Следствие 18 (условие GL-3)**.** $\mathsf{PA} \vdash \mathrm{Pr}(\ulcorner \varphi \urcorner) \to \mathrm{Pr}(\ulcorner \mathrm{Pr}(\ulcorner \varphi \urcorner)\urcorner)$ *для любой формулы φ.*

3 Теорема о неподвижной точке

Последним нужным нам ингредиентом будет *теорема о неподвижной точке:*

Теорема 19 (теорема о неподвижной точке)**.** *Пусть $\varphi(x)$ — арифметическая формула с одной свободной переменной x. Тогда существует замкнутая арифметическая формула ψ, для которой*

$$\mathsf{PA} \vdash \psi \leftrightarrow \varphi(\ulcorner \psi \urcorner).$$

Формула ψ говорит „мой гёделев номер обладает свойством φ“. Доказательство теоремы о неподвижной точке довольно просто, и при этом немного парадоксально.

Доказательство. Рассмотрим следующую функцию

$$g\colon \ulcorner \zeta(\mathfrak{x})\urcorner \mapsto \ulcorner \zeta(\ulcorner \zeta(\mathfrak{x})\urcorner)\urcorner$$

(если на вход этой функции подать число, не являющееся гёделевым номером формулы с одной свободной переменной $\mathfrak{x}$, то мы допускаем любой результат).

Функция g примитивно-рекурсивна. Действительно, её можно реализовать следующим образом: $g(n) = \mathrm{sub}_{\mathfrak{x}}(n, \mathrm{num}(n))$. Первый аргумент — это гёделев номер $\zeta(\mathfrak{x})$, второй — соответствующий ему нумерал, который мы подставим в ζ вместо $\mathfrak{x}$.

Отметим, что здесь нам впервые понадобилась примитивная рекурсивность функции подстановки по первому аргументу.

Раз g примитивно-рекурсивна, она доказуемо тотальна в PA, и её график представляется Σ_1-формулой $G(x, y)$. Наш дальнейший план — построить формулу $\xi(x) = \varphi(g(x))$ и взять $\psi = \xi(\ulcorner \xi(\mathfrak{x})\urcorner)$. Тогда будет $\psi = \xi(\ulcorner \xi(\mathfrak{x})\urcorner) = \varphi(g(\ulcorner \xi(\mathfrak{x})\urcorner)) \leftrightarrow \varphi(\ulcorner \xi(\ulcorner \xi(\mathfrak{x})\urcorner)\urcorner) = \varphi(\ulcorner \psi \urcorner)$. К сожалению, мы не имеем право записывать ψ в языке, расширенном функциональным символом g, поскольку у нас нет гёделевых номеров для псевдотермов. Нужно «по-честному» записать ξ и ψ через формулу G:

$$\xi(x) = \big(\exists y\, (G(x, y) \wedge \varphi(y))\big) \qquad \text{и} \qquad \psi = \xi(\ulcorner \xi(\mathfrak{x})\urcorner).$$

Докажем, что $\psi \leftrightarrow \varphi(\ulcorner\psi\urcorner)$ или, что то же, $\xi(\ulcorner\xi(\mathfrak{x})\urcorner) \leftrightarrow \varphi(\ulcorner\xi(\ulcorner\xi(\mathfrak{x})\urcorner)\urcorner)$. Слева стоит формула $\exists y\,(G(\ulcorner\xi(\mathfrak{x})\urcorner, y) \wedge \varphi(y))$, в которой $G(\ulcorner\xi(\mathfrak{x})\urcorner, y)$ равносильна $y = \ulcorner\xi(\ulcorner\xi(\mathfrak{x})\urcorner)\urcorner$. Значит, вся формула равносильна $\varphi(\ulcorner\xi(\ulcorner\xi(\mathfrak{x})\urcorner)\urcorner)$ (квантор по y исчезает), что и требовалось. $\square$

4 Урожай

4.1 Гёделевы теории $T \supseteq \mathsf{PA}$. Теоремы Гёделя о неполноте

Помимо самой арифметики Пеано, будем рассматривать её «хорошие» расширения.

Определение. Будем называть *гёделевой теорией* теорию $T \supseteq \mathsf{PA}$, множество аксиом которой (включая аксиомы исчисления предикатов) задаётся Σ_1-формулой $\mathrm{Ax}_T(x)$ со следующими свойствами:

- если φ — аксиома теории T, то $\mathsf{PA} \vdash \mathrm{Ax}_T(\ulcorner\varphi\urcorner)$;
- если число n не является гёделевым номером аксиомы теории T (т.е. если n вообще не гёделев номер никакой формулы, либо $n = \ulcorner\psi\urcorner$, где ψ — не аксиома теории T), то $\mathsf{PA} \vdash \neg\mathrm{Ax}_T(\underline{n})$;
- $\mathsf{PA} \vdash \forall x\,(\mathrm{Ax}_{\mathsf{PA}}(x) \to \mathrm{Ax}_T(x))$, где $\mathrm{Ax}_{\mathsf{PA}}$ — стандартная формула, задающая множество аксиом PA.

(Правила вывода во всех рассматриваемых теориях стандартные — modus ponens и правило обобщения.)

Типичный случай гёделевой теории T — когда она задаётся примитивно-рекурсивным множеством дополнительных аксиом над PA. Сама PA также задана примитивно-рекурсивно; пусть её характеристическая функция представлена Σ_1-формулой $\alpha(x, y)$, а характеристическая функция множества дополнительных аксиом T — формулой $\alpha'(x, y)$. Тогда

$$\mathrm{Ax}_{\mathsf{PA}}(x) = \alpha(x, 1);$$
$$\mathrm{Ax}_T(x) = \alpha(x, 1) \vee \alpha'(x, 1).$$

Сразу ясно третье условие: $\mathrm{Ax}_{\mathsf{PA}}(x) \to \mathrm{Ax}_T(x)$ доказуемо в исчислении высказываний. Первое условие гарантируется Σ_1-полнотой арифметики Пеано. Что касается второго условия, оно опять же получается за счёт Σ_1-полноты, однако не напрямую. Формула $\neg\mathrm{Ax}_T(\underline{n})$ не принадлежит классу Σ_1, однако ему принадлежит более сильная (за счёт доказуемой тотальности) формула $\alpha(x, 0) \wedge \alpha'(x, 0)$.

Предикат доказательства Prf_T для теории T определяется так же, как и для PA, с заменой $\mathrm{Ax}_{\mathsf{PA}}$ на Ax_T. Аналогично определяется и предикат доказуемости:

$$\mathrm{Pr}_T(x) = \exists y\,\mathrm{Prf}_T(y, x).$$

Ясно, что Prf_T и Pr_T эквивалентны формулам из класса Σ_1.

Для краткости вместо $\mathrm{Pr}_T(\ulcorner\varphi\urcorner)$ будем писать $\Box_T\varphi$. Считаем, что приоритет знака $\Box_T$ выше, чем у логических связок.

Легко видеть, что условия Гильберта – Бернайса – Лёба сохраняются и для предиката доказуемости Pr_T. Обратите внимание, что в некоторых местах остаётся доказуемость в PA, как в метатеории, в рамках которой мы изучаем теорию T. Поскольку $\mathsf{PA} \subseteq T$, такие утверждения сильнее, чем аналогичные для самой T. В формулировках условий φ и ψ — произвольные замкнутые арифметические формулы.

- GL-1: если $T \vdash \varphi$, то $\mathsf{PA} \vdash \Box_T \varphi$;
- GL-2: $\mathsf{PA} \vdash (\Box_T(\varphi \to \psi) \land \Box_T \varphi) \to \Box_T \psi$;
- GL-3: $\mathsf{PA} \vdash \Box_T \varphi \to \Box_T \Box_T \varphi$.

Теперь вспомним теорему о неподвижной точке и применим её к формуле $\neg\mathrm{Pr}_T(x)$. Получим замкнутую арифметическую формулу γ со следующим свойством:

$$\mathsf{PA} \vdash \gamma \leftrightarrow \neg\mathrm{Pr}_T(\ulcorner\gamma\urcorner), \qquad (*)$$

т.е. $\mathsf{PA} \vdash \gamma \leftrightarrow \neg\Box_T\gamma$. Формула γ как бы говорит нам: „я не доказуема в теории T“.

Теорема 20 (1-я теорема Гёделя о неполноте)**.** *Пусть T — гёделева теория и $\mathbb{N} \models T$. Тогда теория T неполна, а именно $T \nvdash \gamma$ и $T \nvdash \neg\gamma$.*

Доказательство. Пусть $T \vdash \gamma$. Тогда в силу соотношения неподвижной точки $(*)$ получаем $T \vdash \neg\Box_T\gamma$, а в силу GL-1 — $T \vdash \Box_T\gamma$. Значит, T противоречива, что несовместимо с условием корректности $\mathbb{N} \models T$.

Пусть теперь $T \vdash \neg\gamma$. Тогда по $(*)$ имеем $T \vdash \Box_T\gamma$, значит $\mathbb{N} \models \Box_T\gamma$. Следовательно, γ действительно доказуема в T, поэтому T противоречива и $\mathbb{N} \not\models T$. □

Вопрос. Будет ли формула γ истинной или ложной в стандартной модели $\mathbb{N}$?

Лемма 21. $\mathsf{PA} \vdash \gamma \leftrightarrow \neg\Box_T\bot$.

Формула справа выражает непротиворечивость теории T и имеет специальное обозначение — $\mathrm{Con}(T)$ (от “consistent”).

Доказательство. Доказательство импликации “$\to$” проще. Для этого достаточно установить (по контрапозиции) $\Box_T\bot \to \Box_T\gamma$. Это выводится по GL-2: $(\Box_T(\bot \to \gamma) \land \Box_T\bot) \to \Box_T\gamma$. Здесь $\Box_T(\bot \to \gamma)$ — утверждение о доказуемости аксиомы ex falso.

Доказательство импликации “$\to$” таково (опять же, от противного):

$\neg\gamma$	(гипотеза)
$\neg\gamma \to \Box_T\gamma$	$(*)$
$\Box_T\gamma$	
$\Box_T\gamma \to \Box_T\Box_T\gamma$	GL-2
$\Box_T\Box_T\gamma$	
$\Box_T(\gamma \to \neg\Box_T\gamma)$	GL-1 из $(*)$
$\Box_T\neg\Box_T\gamma$	GL-1 из $\Box_T(\gamma \to \neg\Box_T\gamma)$ и $\Box_T\gamma$
$\Box_T\neg$	GL-1 из $\Box_T\neg\Box_T\gamma$ и $\Box_T\Box_T\gamma$, т.к. $\neg\,\xi = (\xi \to \bot)$

□

Теорема 22 (2-я теорема Гёделя о неполноте)**.** *Пусть T — непротиворечивая гёделева теория. Тогда $T \nvdash \mathrm{Con}(T)$ („непротиворечивая теория не может доказать своей непротиворечивости“).*

Доказательство. Заметим, что в доказательстве $T \nvdash \gamma$ (1-я теорема Гёделя) мы пользовались только непротиворечивостью T, а не её корректностью. Таким образом, $T \nvdash \gamma$. Значит, $T \nvdash \mathrm{Con}(T)$, поскольку $\mathrm{Con}(T)$ и γ эквивалентны (а значит, равновыводимы) в T по лемме 21. □

4.2 Теорема Гёделя – Россера

Заметим, что условия на теорию T в 1-й теореме Гёделя строже, чем во 2-й — хотя, казалось бы, 2-я теорема сильнее 1-й. Противоречия здесь нет: 2-я теорема Гёделя утверждает $T \nvdash \mathrm{Con}(T)$, но не $T \nvdash \neg\mathrm{Con}(T)$. Как ни странно, существуют непротиворечивые гёделевы теории, доказывающие свою собственную непротиворечивость!

Задача. Приведите пример непротиворечивой гёделевой теории T, для которой $T \vdash \neg\mathrm{Con}(T)$.

Тем не менее, 1-ю теорему Гёделя о неполноте можно обобщить на произвольные непротиворечивые теории, взяв другой пример формулы.

Теорема 23 (теорема Гёделя – Россера)**.** *Пусть T непротиворечивая гёделева теория. Тогда T неполна, т.е. существует замкнутая арифметическая формула ρ, такая что $T \nvdash \rho$ и $T \nvdash \neg\rho$.*

Доказательство. Определим альтернативный *россеровский* предикат доказуемости $\widetilde{\mathrm{Pr}}_T$:

$$\widetilde{\mathrm{Pr}}_T(x) = \exists y\,(\mathrm{Prf}_T(y,x) \wedge \forall z < y\ \neg\mathrm{Prf}_T(z, \hat{\neg}(x))).$$

Здесь $\hat{\neg}$ — символ для функции, которая по $\ulcorner\varphi\urcorner$ возвращает $\ulcorner\neg\varphi\urcorner$. При нашем кодировании $\hat{\neg}$ реализуется как настоящий терм: $\hat{\neg}(x) = \langle\ulcorner\to\urcorner, \langle x, \ulcorner\bot\urcorner\rangle\rangle$.

Неформально россеровский предикат доказуемости усиливает гёделевский, требуя, чтобы, во-первых, данная формула была доказуема, а, во-вторых, у неё не было опровержения с меньшим номером, чем её доказательство. Это называется *россеровским сравнением свидетельств.*

Для $\widetilde{\mathrm{Pr}}_T$ зададим «россеровскую» неподвижную точку ρ, для которой

$$\mathsf{PA} \vdash \rho \leftrightarrow \neg\widetilde{\mathrm{Pr}}_T(\ulcorner\rho\urcorner).$$

Докажем, что $T \nvdash \rho$ и $T \nvdash \neg\rho$.

Действительно, пусть $T \vdash \rho$ и пусть m — номер этого доказательства формулы ρ. Заметим, что — для данной формулы φ — предикат Prf_T обладает следующими свойствами:

если k — номер доказательства φ в T,	то $\mathsf{PA} \vdash \mathrm{Prf}_T(\underline{k}, \ulcorner\varphi\urcorner)$;
если k не является номером доказательства φ в T,	то $\mathsf{PA} \vdash \neg\mathrm{Prf}_T(\underline{k}, \ulcorner\varphi\urcorner)$.

Первое утверждение следует из Σ_1-полноты PA и того факта, что $\mathrm{Prf}_T \in \Sigma_1$. Второе было бы настолько же очевидным, если бы мы добились $\mathrm{Prf}_T \in \Delta_0$. Однако и в нашей Σ_1-формулировке предиката доказательства второе утверждение верно **(задача)**[1].

Итак, m — номер доказательства формулы ρ в теории T, откуда $\mathsf{PA} \vdash \mathrm{Prf}_T(\underline{m}, \ulcorner\rho\urcorner)$. Поскольку T непротиворечива, любое $k < m$ (и вообще любое k) не является номером доказательства $\neg\rho$. Отсюда $\mathsf{PA} \vdash \neg\mathrm{Prf}_T(\underline{k}, \hat{\neg}(\ulcorner\rho\urcorner))$ для всех $k < m$, и значит $\mathsf{PA} \vdash \forall z < \underline{m}\ \neg\mathrm{Prf}_T(z, \hat{\neg}(\ulcorner\rho\urcorner))$ (поскольку $\forall z < \underline{m}\ \psi(z) \leftrightarrow \psi(0) \vee \psi(1) \vee \ldots \vee \psi(\underline{m-1})$). Получили $\mathsf{PA} \vdash \widetilde{\mathrm{Pr}}_T(\ulcorner\rho\urcorner)$, следовательно, $T \vdash \widetilde{\mathrm{Pr}}_T(\ulcorner\rho\urcorner)$.

С другой стороны, по условию неподвижной точки из выводимости ρ следует выводимость $\neg\widetilde{\mathrm{Pr}}_T(\ulcorner\rho\urcorner)$ в T. Противоречие с непротиворечивостью T.

[1] *Подсказка.* Если множество аксиом теории T задаётся примитивно-рекурсивной характеристической функцией, то одновременно $\mathrm{Ax}_T(x) = \alpha(x,1) \in \Sigma_1$ и $\neg\mathrm{Ax}_T(x) \leftrightarrow \alpha(x,0) \in \Sigma_1$ (здесь α — формула, представляющая эту характеристическую функцию). Таким образом, как говорят, $\mathrm{Ax}_T \in \Delta_1$, и Σ_1-полноту можно применить как к самой формуле, так и к её отрицанию. Далее это свойство можно распространить на весь предикат доказательства Prf_T. Наше условие гёделевости T не требует примитивно-рекурсивной аксиоматизации, но фактически даёт то же свойство Δ_1.

Теперь пусть $T \vdash \neg\rho$. По условию неподвижной точки $T \vdash \widetilde{\Pr}_T(\ulcorner\rho\urcorner)$. Докажем, что одновременно $\mathsf{PA} \vdash \neg\widetilde{\Pr}_T(\ulcorner\rho\urcorner)$ (это даст искомое противоречие в T). Действительно, поскольку $T \vdash \neg\rho$, то для некоторого k имеем $\mathsf{PA} \vdash \mathrm{Prf}_T(\underline{k}, \hat{\neg}(\ulcorner\rho\urcorner))$. Далее

$$\neg\widetilde{\Pr}_T(\ulcorner\rho\urcorner) \leftrightarrow \forall y(\neg\mathrm{Prf}_T(y,\ulcorner\rho\urcorner) \vee \exists z < y\, \mathrm{Prf}_T(z, \hat{\neg}(\ulcorner\rho\urcorner))) \leftarrow \forall y \leqslant \underline{k}\, \neg\mathrm{Prf}_T(y,\ulcorner\rho\urcorner) \leftrightarrow$$
$$\leftrightarrow \neg\mathrm{Prf}_T(0,\ulcorner\rho\urcorner) \wedge \neg\mathrm{Prf}_T(1,\ulcorner\rho\urcorner) \wedge \ldots \wedge \neg\mathrm{Prf}_T(\underline{k},\ulcorner\rho\urcorner).$$

Поскольку T непротиворечива и $T \vdash \neg\rho$, никакое число (в частности, ни одно из 0, ..., k) не кодирует доказательство ρ в T. Значит, для любого $m \leqslant k$ имеем $\mathsf{PA} \vdash \neg\mathrm{Prf}_T(\underline{m},\ulcorner\rho\urcorner)$, откуда получаем искомое $\mathsf{PA} \vdash \neg\widetilde{\Pr}_T(\ulcorner\rho\urcorner)$.

Теорема Гёделя – Россера доказана. $\square$

Заметим, что россеровский предикат доказуемости существенно отличается от гёделевского. Почувствовать это даёт следующая задача.

Задача. Пусть $\widetilde{\mathrm{Con}}(T) = \neg\widetilde{\Pr}_T(\ulcorner\bot\urcorner)$ — россеровское утверждение о непротиворечивости. Покажите, что $T \vdash \widetilde{\mathrm{Con}}(T)$.

Задача. Выполняются ли для россеровского предиката доказуемости условия Гильберта – Бернайса – Лёба?

4.3 Теорема Лёба

Теорема 24 (теорема Лёба)**.** *Пусть T — непротиворечивая гёделева теория. Тогда если (для некоторой замкнутой формулы φ) $T \vdash \Box_T\varphi \to \varphi$, то $T \vdash \varphi$.*

Неформальный смысл теоремы Лёба такой. Если предположить, что теория T корректна ($\mathbb{N} \models T$), то утверждение $\Box_T\varphi \to \varphi$ (*рефлексия* для формулы φ) должно быть истинно для любой φ. Тем не менее, в силу теоремы Лёба, рефлексия может быть *доказана* в T только в тривиальном случае — когда доказуема сама формула T.

2-я теорема Гёделя о неполноте является частным случаем теоремы Лёба для $\varphi = \bot$: если $T \vdash \mathrm{Con}(T)$, то T противоречива.

Доказательство. Построим неподвижную точку λ:

$$\mathsf{PA} \vdash \lambda \leftrightarrow (\Pr_T(\ulcorner\lambda\urcorner) \to \varphi).$$

Далее при условии $T \vdash \Box_T\varphi \to \varphi$ проводим следующее рассуждение ($\Box$ значит $\Box_T$):

$\mathsf{PA} \vdash \lambda \to (\Box\lambda \to \varphi)$	
$\mathsf{PA} \vdash \Box\big(\lambda \to (\Box\lambda \to \varphi)\big)$	GL-1
$\mathsf{PA} \vdash \Box\lambda \to (\Box\Box\lambda \to \Box\varphi)$	GL-2
$\mathsf{PA} \vdash \Box\lambda \to \Box\Box\lambda$	GL-3
$\mathsf{PA} \vdash \Box\lambda \to \Box\varphi$	
$T \vdash \Box\varphi \to \varphi$	по условию
$T \vdash \Box\lambda \to \varphi$	
$\mathsf{PA} \vdash (\Box\lambda \to \varphi) \to \lambda$	
$\mathsf{PA} \vdash \Box\big((\Box\lambda \to \varphi) \to \lambda\big)$	GL-1
$\mathsf{PA} \vdash \Box(\Box\lambda \to \varphi) \to \Box\lambda$	GL-2
$\mathsf{PA} \vdash \Box(\Box\lambda \to \varphi)$	GL-1 из $T \vdash \Box\lambda \to \varphi$
$\mathsf{PA} \vdash \Box\lambda$	

Применяя modus ponens к $\Box\lambda \to \varphi$ и $\Box\lambda$, получаем $T \vdash \varphi$, что и требовалось. $\Box$

Доказательство теоремы Лёба можно полностью провернуть внутри арифметики Пеано:

Теорема 25 (формализованная теорема Лёба)**.** $\mathsf{PA} \vdash \Box_T(\Box_T\varphi \to \varphi) \to \Box_T\varphi$.

Доказательство. Как и в доказательстве обычной теоремы Лёба, берём неподвижную точку λ с условием $\lambda \leftrightarrow (\Box\lambda \to \varphi)$ и выводим в PA формулы $\Box\lambda \to \Box\varphi$ и $\Box(\Box\lambda \to \varphi) \to \Box\lambda$. Применяя к первой формуле GL-1, получаем $\mathsf{PA} \vdash \Box(\Box\lambda \to \Box\varphi)$. Далее доказываем $\Box(\Box\varphi \to \varphi) \to \Box\varphi$ в PA, используя теорему о дедукции (все формулы замкнутые, поэтому применение теоремы о дедукции допустимо):

$\Box(\Box\varphi \to \varphi)$	гипотеза
$\Box(\Box\lambda \to \Box\varphi)$	см. выше
$\Box\big((\Box\lambda \to \Box\varphi) \to ((\Box\varphi \to \varphi) \to (\Box\lambda \to \varphi))\big)$	GL-1, применённое к аксиоме
$\Box(\Box\lambda \to \varphi)$	GL-2 два раза
$\Box\lambda$	modus ponens с $\Box(\Box\lambda \to \varphi) \to \Box\lambda$
$\Box\varphi$	modus ponens с $\Box\lambda \to \Box\varphi$

Доказательство закончено. $\Box$

4.4 Теорема Тарского. Неразрешимость PA

Теорема 26 (Теорема Тарского)**.** *Истинность в $\mathbb{N}$ формулы с данным гёделевым номером неопределима арифметически, т.е. не существует такой формулы $\tau(x)$, что $\mathbb{N} \vDash \varphi$ тогда и только тогда, когда $\mathbb{N} \vDash \tau(\ulcorner\varphi\urcorner)$ (для любой замкнутой φ).*

Доказательство. По теореме о неподвижной точке построим формулу ξ, такую что $\mathsf{PA} \vdash \xi \leftrightarrow \neg\tau(\ulcorner\xi\urcorner)$. Тогда тем более $\mathbb{N} \vDash \xi \leftrightarrow \neg\tau(\ulcorner\xi\urcorner)$. Значит, если ξ истинна, то она ложна, и наоборот. Противоречие. $\Box$

Задача. Существует ли такая формула $\tau'(x)$, что $\mathbb{N} \vDash \varphi$ тогда и только тогда, когда $\mathsf{PA} \vdash \tau'(\ulcorner\varphi\urcorner)$?

Теперь докажем неразрешимость PA.

Теорема 27. *Проблема выводимости формул в PA алгоритмически неразрешима.*

Для начала напомним определение разрешимого множества — это множество, характеристическая функция которого вычислима. Вычислимость функции равносильна её *рекурсивности.* Класс рекурсивных функций определяется аналогично классу примитивно-рекурсивных функций, но с добавлением ещё одного конструктора — *неограниченного μ-оператора:*

$$g(\vec{a}) = \mu x.\big(f(x, \vec{a}) = 0\big).$$

Неформально, $\mu x.\big(f(x, \vec{a}) = 0\big) = \min\{x \mid f(x, \vec{a}) = 0\}$. Если, однако, при данных значениях $\vec{a}$ при всех x окажется $f(x, \vec{a}) \neq 0$, то $g(\vec{a})$ не определено. Так появляются частично определённые рекурсивные функции. Более того, сама функция f также могла быть частично определённой. Тогда если окажется, что x_0 — это наименьший x, для которого $f(x, \vec{a})$ не определено, а при всех меньших значениях x оказалось, что $f(x, \vec{a})$ определено и не равно нулю, то $g(\vec{a})$ также полагается неопределённым (хотя для какого-то $x > x_0$ может быть $f(x, \vec{a}) = 0$).

Такое определение соответствует вычислительной идее μ-оператора: при данных $\vec{a}$ вычислять $f(x, \vec{a})$ последовательно для $x = 0, 1, 2, \ldots$ При этом либо найдём ноль, либо доберёмся до x_0, при котором значение не определено («зависнем»), либо будем перебирать до бесконечности.

Для рекурсивных функций также имеет место теорема о представимости в арифметике, однако более слабая, чем для примитивно-рекурсивных.

Задача. Пусть f рекурсивна. Тогда существует Σ_1-формула $F(\vec{x}, y)$, такая что для любых $\vec{n} = n_1, \ldots, n_k$

$$f(\vec{n}) = m \iff \mathbb{N} \vDash F(\underline{\vec{n}}, \underline{m}).$$

Подсказка. Рассуждение проводится так же, как и для представимости примитивно-рекурсивных функций, однако добавляется случай μ-оператора.

Заметим, что в силу Σ_1-полноты формула $F(\underline{\vec{n}}, \underline{f(\vec{n})})$ (для конкретных $\vec{n}$) будет не только истинна в $\mathbb{N}$, но и доказуема в PA. Однако, даже если функция f оказалась всюду определённой, утверждение о её тотальности $\forall \vec{x}\, \exists!\, y\, F(\vec{x}, y)$, будучи истинным в $\mathbb{N}$, совершенно не обязательно окажется доказуемым в PA.

Задача. Докажите, что для любой перечислимой теории T найдётся всюду определённая рекурсивная функция f, для которой утверждение о её тотальности недоказуемо в T.

Теперь докажем теорему 27. Предположим, что проблема выводимости для арифметики Пеано разрешима. Это равносильно вычислимости следующей характеристической функции:

$$\chi_{\mathsf{PA}}(x) = \begin{cases} 1 & \text{если } x = \ulcorner\varphi\urcorner \text{ и } \mathsf{PA} \vdash \varphi; \\ 0 & \text{иначе (т.е. если } x \text{ — не гёделев номер или } x = \ulcorner\varphi\urcorner \text{ и } \mathsf{PA} \nvdash \varphi). \end{cases}$$

Для этой функции построим представляющую её арифметическую формулу $H(x, y)$ и возьмём её неподвижную точку $\mathsf{PA} \vdash \zeta \leftrightarrow H(\ulcorner\zeta\urcorner, 0)$.

Теперь если $\mathsf{PA} \vdash \zeta$, то $\mathbb{N} \vDash H(\ulcorner\zeta\urcorner, 0)$ (поскольку $\mathbb{N} \vDash \mathsf{PA}$), откуда $\mathsf{PA} \nvdash \zeta$. Если же $\mathsf{PA} \nvdash \zeta$, то $\mathbb{N} \vDash H(\ulcorner\zeta\urcorner, 0)$, а значит, $\mathsf{PA} \vdash H(\ulcorner\zeta\urcorner, 0)$, откуда по соотношению неподвижной точки $\mathsf{PA} \vdash \zeta$.

Список литературы

[1] G. Boolos. *The logic of provability.* Cambridge University Press, 1993.

[2] W. Rautenberg. *A concise introduction to mathematical logic.* Springer, 2010.