

Уточнение исчисления предикатов

- ▶ Пусть требуется доказывать утверждения про равенство. Введём $E(p, q)$ — предикат «равенство».
- ▶ Однако $\not\models E(p, q) \rightarrow E(q, p)$: если $D = \{0, 1\}$ и $E(p, q) ::= (p > q)$, то $\not\models E(p, q) \rightarrow E(q, p)$.
- ▶ Конечно, можем указывать $\forall p. \forall q. E(p, q) \rightarrow E(q, p) \vdash \varphi$.
- ▶ Но лучше добавим аксиому $\forall p. \forall q. E(p, q) \rightarrow E(q, p)$.
- ▶ Добавив необходимые аксиомы, получим *теорию первого порядка*.

Теория первого порядка

Определение

Теорией первого порядка назовём исчисление предикатов с дополнительными («нелогическими» или «математическими»):

- ▶ *предикатными и функциональными символами;*
- ▶ *аксиомами.*

Сущности, взятые из исходного исчисления предикатов, назовём логическими

Порядок логики/теории

Порядок	Кванторы	Формализует суждения...	Пример
нулевой	запрещены	об отдельных значениях	И.В.
первый	по предметным переменным	о множествах	И.П.
	$\{2, 3, 5, 7, \dots\} = \{t \mid \forall p. \forall q. (p \neq 1 \ \& \ q \neq 1) \rightarrow (t \neq p \cdot q)\}$		
второй	по предикатным переменным	о множествах множеств	Типы
	$S = \{\{t \mid P(t)\} \mid \varphi[p := P]\}$		
	...		

Пример (логики 2 порядка)

$\alpha \rightarrow \beta \rightarrow \alpha$ (сх. акс. 1)

$\forall a. \forall b. a \rightarrow b \rightarrow a$

```
let rec map f l = match l with  
| [] -> []
```

$map : \forall a. \forall b. (a \rightarrow b) \rightarrow a \text{ list} \rightarrow b \text{ list}$

```
| l1::ls -> f l1 :: map f ls
```

```
map ((+) 1) [1;2;3] = [2;3;4]
```

Формальная арифметика

Определение

Формальная арифметика — теория первого порядка, со следующими добавленными нелогическими . . .

- ▶ двухместными функциональными символами $(+)$, (\cdot) ; одноместным функциональным символом $(')$, нульместным функциональным символом 0 ;
- ▶ двухместным предикатным символом $(=)$;
- ▶ восемью нелогическими аксиомами:
 - (A1) $a = b \rightarrow a = c \rightarrow b = c$ (A5) $a + 0 = a$
 - (A2) $a = b \rightarrow a' = b'$ (A6) $a + b' = (a + b)'$
 - (A3) $a' = b' \rightarrow a = b$ (A7) $a \cdot 0 = 0$
 - (A4) $\neg a' = 0$ (A8) $a \cdot b' = a \cdot b + a$
- ▶ нелогической схемой аксиом индукции $\psi[x := 0] \ \& \ (\forall x. \psi \rightarrow \psi[x := x']) \rightarrow \psi$ с метапеременными x и ψ .

Докажем, что $a = a$

Пусть $\top ::= 0 = 0 \rightarrow 0 = 0 \rightarrow 0 = 0$, тогда:

- | | | |
|------|---|--------------------|
| (1) | $a = b \rightarrow a = c \rightarrow b = c$ | (Акс. A1) |
| (2) | $(a = b \rightarrow a = c \rightarrow b = c) \rightarrow \top \rightarrow (a = b \rightarrow a = c \rightarrow b = c)$ | (Сх. акс. 1) |
| (3) | $\top \rightarrow (a = b \rightarrow a = c \rightarrow b = c)$ | (М.Р. 1, 2) |
| (4) | $\top \rightarrow (\forall c. a = b \rightarrow a = c \rightarrow b = c)$ | (Введ. \forall) |
| (5) | $\top \rightarrow (\forall b. \forall c. a = b \rightarrow a = c \rightarrow b = c)$ | (Введ. \forall) |
| (6) | $\top \rightarrow (\forall a. \forall b. \forall c. a = b \rightarrow a = c \rightarrow b = c)$ | (Введ. \forall) |
| (7) | \top | (Сх. акс 1) |
| (8) | $(\forall a. \forall b. \forall c. a = b \rightarrow a = c \rightarrow b = c)$ | (М.Р. 7, 6) |
| (9) | $(\forall a. \forall b. \forall c. a = b \rightarrow a = c \rightarrow b = c) \rightarrow$
$\rightarrow (\forall b. \forall c. a + 0 = b \rightarrow a + 0 = c \rightarrow b = c)$ | (Сх. акс. 11) |
| (10) | $\forall b. \forall c. a + 0 = b \rightarrow a + 0 = c \rightarrow b = c$ | (М.Р. 8, 9) |
| (12) | $\forall c. a + 0 = a \rightarrow a + 0 = c \rightarrow a = c$ | (М.Р. 10, 11) |
| (14) | $a + 0 = a \rightarrow a + 0 = a \rightarrow a = a$ | (М.Р. 12, 13) |
| (15) | $a + 0 = a$ | (Акс. A5) |
| (16) | $a + 0 = a \rightarrow a = a$ | (М.Р. 15, 14) |
| (17) | $a = a$ | (М.Р. 15, 16) |

Арифметизация логики

Общие замечания

- ▶ Рассматриваем функции $\mathbb{N}_0^n \rightarrow \mathbb{N}_0$.
- ▶ Обозначим вектор $\langle x_1, x_2, \dots, x_n \rangle$ как \vec{x} .

Примитивно-рекурсивные функции

Определение (Примитивы Z , N , U , S)

1. Примитив «Ноль» (Z)

$$Z : \mathbb{N}_0 \rightarrow \mathbb{N}_0, \quad Z(x_1) = 0$$

2. Примитив «Инкремент» (N)

$$N : \mathbb{N}_0 \rightarrow \mathbb{N}_0, \quad N(x_1) = x_1 + 1$$

3. Примитив «Проекция» (U) — семейство функций; пусть $k, n \in \mathbb{N}_0, k \leq n$

$$U_n^k : \mathbb{N}_0^n \rightarrow \mathbb{N}_0, \quad U_n^k(\vec{x}) = x_k$$

4. Примитив «Подстановка» (S) — семейство функций; пусть

$$g : \mathbb{N}_0^k \rightarrow \mathbb{N}_0, \quad f_1, \dots, f_k : \mathbb{N}_0^n \rightarrow \mathbb{N}_0$$

$$S\langle g, f_1, f_2, \dots, f_k \rangle(\vec{x}) = g(f_1(\vec{x}), \dots, f_k(\vec{x}))$$

Примитивная рекурсия

Определение (примитив «примитивная рекурсия», R)

Пусть $f : \mathbb{N}_0^n \rightarrow \mathbb{N}_0$ и $g : \mathbb{N}_0^{n+2} \rightarrow \mathbb{N}_0$. Тогда $R\langle f, g \rangle : \mathbb{N}_0^{n+1} \rightarrow \mathbb{N}_0$, причём

$$R\langle f, g \rangle(\vec{x}, y) = \begin{cases} f(\vec{x}), & y = 0 \\ g(\vec{x}, y-1, R\langle f, g \rangle(\vec{x}, y-1)), & y > 0 \end{cases}$$

Пояснение

```
res := f(x1...xn);  
for yi = 0 to y-1 do  
    res := g(x1...xn, yi, res);
```

Пример

$$\begin{aligned} R\langle f, g \rangle(\vec{x}, 3) &= g(\vec{x}, 2, R\langle f, g \rangle(\vec{x}, 2)) \\ &= g(\vec{x}, 2, g(\vec{x}, 1, R\langle f, g \rangle(\vec{x}, 1))) \\ &= g(\vec{x}, 2, g(\vec{x}, 1, g(\vec{x}, 0, R\langle f, g \rangle(\vec{x}, 0)))) \\ &= g(\vec{x}, 2, g(\vec{x}, 1, g(\vec{x}, 0, f(\vec{x})))) \end{aligned}$$

Примитивно-рекурсивные функции

Определение

Функция f — примитивно-рекурсивна, если может быть выражена как композиция примитивов Z , N , U , S и R .

Теорема

$f(x) = x + 2$ примитивно-рекурсивна

Доказательство.

$$f = S\langle N, N \rangle$$

$$N(x) = x + 1$$

$$S\langle g, f \rangle(x) = g(f(x))$$

$$f, g = N$$

$$S\langle N, N \rangle(x) = N(N(x)) = (x + 1) + 1$$



Примитивно-рекурсивные функции: $x + y$

Лемма

$f(a, b) = a + b$ примитивно-рекурсивна

Доказательство.

$f = R\langle U_1^1, S\langle N, U_3^3 \rangle \rangle$:

$$R\langle f, g \rangle(x, y) = \begin{cases} f(x), & y = 0 \\ g(x, y - 1, R\langle f, g \rangle(x, y - 1)), & y > 0 \end{cases}$$

- База. $R\langle U_1^1, S\langle N, U_3^3 \rangle \rangle(x, 0) = U_1^1(x) = x$
- Переход. $R\langle U_1^1, S\langle N, U_3^3 \rangle \rangle(x, y + 1) =$
... $= S\langle N, U_3^3 \rangle(x, y, R\langle U_1^1, S\langle N, U_3^3 \rangle \rangle(x, y)) =$
... $= S\langle N, U_3^3 \rangle(x, y, x + y) =$
... $= N(x + y) = x + y + 1$



Какие функции примитивно-рекурсивные?

1. Сложение, вычитание
2. Умножение, деление
3. Вычисление простых чисел
4. Неформально: все функции, вычисляемые конечным числом вложенных циклов for:

```
for (int i1 = 0; i1 < g1(x1...xn); i1++) {  
    for (int i2 = 0; i2 < g2(x1...xn,i1); i2++) {  
        ...  
        for (int ik = 0; ik < gk(x1...xn,i1,i2...); ik++) {  
            // выражение без циклов  
        }  
        ...  
    }  
}
```

Общерекурсивные функции

Определение

Функция — общерекурсивная, если может быть построена при помощи примитивов Z , N , U , S , R и примитива минимизации:

$$M\langle f \rangle(x_1, x_2, \dots, x_n) = \min\{y : f(x_1, x_2, \dots, x_n, y) = 0\}$$

Если $f(x_1, x_2, \dots, x_n, y) > 0$ при любом y , результат не определён.

Пример:

Пусть $f(x, y) = x - y^2$, тогда $\lceil \sqrt{x} \rceil = M\langle f \rangle(x)$

```
int sqrt(int x) {  
    int y = 0;  
    while (x-y*y > 0) y++;  
    return y;  
}
```

Выразительная сила

Определение

Функция Аккермана:

$$A(m, n) = \begin{cases} n + 1, & m = 0 \\ A(m - 1, 1), & m > 0, n = 0 \\ A(m - 1, A(m, n - 1)), & m > 0, n > 0 \end{cases}$$

Пример

n	0	1	2	3	4	...
0	1	2	3	5	13	
1	2	3	5	13	65533	
2	3	4	7	29	$2^{65536} - 3$	
n	$n + 1$	$n + 2$	$2n + 3$	$2^{n+3} - 3$	$\underbrace{2^{2^{\dots^2}}}_{n+3} - 3$	

Лемма о росте функции Аккермана

Определение

$$A^{(p)}(k, x) = \underbrace{A(k, A(k, A(k, \dots, A(k, x))))}_{p \text{ раз}}$$

$$A(m, n) = \begin{cases} n + 1, & m = 0 \\ A(m - 1, 1), & m > 0, n = 0 \\ A(m - 1, A(m, n - 1)), & m > 0, n > 0 \end{cases}$$

Лемма

1. $A(p, q) = A^{(q+1)}(p - 1, 1)$
2. $A^{(x+2)}(k, x) < A(k + 2, x)$

$$\begin{aligned} A(0, n) &= n + 1 \\ A(2, n) &= 2n + 3 \end{aligned}$$

Доказательство.

1. $A(p, q) = A(p - 1, A(p, q - 1)) = \dots = A(p - 1, A(p - 1, \dots, A(p, 0))) = A^{(q)}(p - 1, A(p, 0)) = A^{(q+1)}(p - 1, 1)$
2. $A(k + 2, x) = A(k + 1, A(k + 2, x - 1)) = A^{(A(k+2, x-1)+1)}(k, 1) \geq A^{(A(2, x-1)+1)}(k, 1) = A^{(2(x-1)+3+1)}(k, 1) = A^{(2x+2)}(k, 1) = A^{(x+2)}(k, A^{(x)}(k, 1)) \geq A^{(x+2)}(k, A^{(x)}(0, 1)) = A^{(x+2)}(k, x + 1) > A^{(x+2)}(k, x)$



Функция Аккермана не примитивно-рекурсивна

Теорема

Пусть $f(\vec{x})$ — примитивно-рекурсивная. Тогда найдётся k , что $f(\vec{x}) < A(k, \max(\vec{x}))$

Доказательство.

Индукция по структуре f .

1. $f = Z$, тогда $k = 0$, т.к. $A(0, x) = x + 1 > Z(x) = 0$;
2. $f = N$, тогда $k = 1$, т.к. $A(1, x) = x + 2 > N(x) = x + 1$;
3. $f = U_s^n$, тогда $k = 0$, т.к. $f(\vec{x}) \leq \max(\vec{x}) < A(0, \max(\vec{x}))$;
4. $f = S\langle g, h_1, \dots, h_n \rangle$, тогда $k = k_g + \max(k_{h_1}, \dots, k_{h_n}) + 2$;
5. $f = R\langle g, h \rangle$, тогда $k = \max(k_g, k_h) + 2$.



Доказательство оценки для R

Лемма

Пусть $f = R\langle g, h \rangle$. Тогда при $k = \max(k_g, k_h) + 2$ выполнено $f(\vec{x}, y) \leq A^{(y+1)}(k - 2, \max(\vec{x}, y))$.

Доказательство.

Индукция по y .

- База: $y = 0$. Тогда:

$$f(\vec{x}, 0) = g(\vec{x}) \leq A(k_g, \max(\vec{x})) \leq A^{(1)}(k - 2, \max(\vec{x}, 0)).$$

- Переход: пусть $f(\vec{x}, y) \leq A^{(y+1)}(k - 2, \max(\vec{x}, y))$. Тогда

$$\begin{aligned} f(\vec{x}, y + 1) &= h(\vec{x}, y, f(\vec{x}, y)) \leq A(k_h, \max(\vec{x}, y, f(\vec{x}, y))) \leq \\ &A(k_h, \max(\vec{x}, y, A^{(y+1)}(k - 2, \max(\vec{x}, y)))) = A(k_h, A^{(y+1)}(k - 2, \max(\vec{x}, y))) \leq \\ &A^{(y+2)}(k - 2, \max(\vec{x}, y + 1)) \end{aligned}$$



Заметим, что $A^{(y+1)}(k - 2, \max(\vec{x}, y)) \leq A^{(\max(\vec{x}, y)+1)}(k - 2, \max(\vec{x}, y)) \leq A^{(\max(\vec{x}, y)+2)}(k - 2, \max(\vec{x}, y)) < A(k, \max(\vec{x}, y))$

Тезис Чёрча

Определение

Тезис Чёрча для общерекурсивных функций: любая эффективно-вычислимая функция $\mathbb{N}_0^k \rightarrow \mathbb{N}_0$ является общерекурсивной.

Новые обозначения

Определение

Запись вида $\psi(\theta_1, \dots, \theta_n)$ означает $\psi[x_1 := \theta_1, \dots, x_n := \theta_n]$

Определение (Литерал числа)

$$\bar{a} = \begin{cases} 0, & \text{если } a = 0 \\ (\bar{b})', & \text{если } a = b + 1 \end{cases}$$

Пример: пусть $\psi := x_1 = 0$. Тогда $\psi(\bar{3})$ соответствует формуле $0''' = 0$

Выразимость отношений в Ф.А.

Определение

Будем говорить, что отношение $R \subseteq \mathbb{N}_0^n$ выразимо в ФА, если существует формула ρ , что:

1. если $\langle a_1, \dots, a_n \rangle \in R$, то $\vdash \rho(\overline{a_1}, \dots, \overline{a_n})$
2. если $\langle a_1, \dots, a_n \rangle \notin R$, то $\vdash \neg \rho(\overline{a_1}, \dots, \overline{a_n})$

Теорема

отношение «равно» выразимо в Ф.А.: $R = \{ \langle x, x \rangle \mid x \in \mathbb{N}_0 \}$

Доказательство.

Пусть $\rho := x_1 = x_2$. Тогда:

- ▶ $\vdash p = p$ при $p := \overline{k}$ при всех $k \in \mathbb{N}_0$: $\vdash 0 = 0$, $\vdash 0' = 0'$, $\vdash 0'' = 0''$, ...
- ▶ $\vdash \neg p = q$ при $p := \overline{k}$, $q := \overline{s}$ при всех $k, s \in \mathbb{N}_0$ и $k \neq s$.
 $\vdash \neg 0 = 0'$, $\vdash \neg 0 = 0''$, $\vdash \neg 0''' = 0'$, ...



Представимость функций в Ф.А.

Определение

Будем говорить, что функция $f : \mathbb{N}_0^n \rightarrow \mathbb{N}_0$ представима в ФА, если существует формула φ , что:

1. если $f(a_1, \dots, a_n) = u$, то $\vdash \varphi(\overline{a_1}, \dots, \overline{a_n}, \overline{u})$
2. если $f(a_1, \dots, a_n) \neq u$, то $\vdash \neg \varphi(\overline{a_1}, \dots, \overline{a_n}, \overline{u})$
3. для всех $a_i \in \mathbb{N}_0$ выполнено
 $\vdash (\exists x. \varphi(\overline{a_1}, \dots, \overline{a_n}, x)) \ \& \ (\forall p. \forall q. \varphi(\overline{a_1}, \dots, \overline{a_n}, p) \ \& \ \varphi(\overline{a_1}, \dots, \overline{a_n}, q) \rightarrow p = q)$

Соответствие рекурсивных и представимых функций

Теорема

Любая рекурсивная функция представима в Ф.А.

Теорема

Любая представимая в Ф.А. функция рекурсивна.

Примитивы Z , N , U представимы в $\Phi.A.$

Теорема

Примитивы Z , N и U_n^k представимы в $\Phi.A.$

Доказательство.

- ▶ $\zeta(x_1, x_2) := x_2 = 0$, формальнее: $\zeta(x_1, x_2) := x_1 = x_1 \ \& \ x_2 = 0$
- ▶ $\nu(x_1, x_2) := x_2 = x'_1$
- ▶ $v(x_1, \dots, x_n, x_{n+1}) := x_k = x_{n+1}$
формальнее: $v(x_1, \dots, x_n, x_{n+1}) := \left(\bigwedge_{i \neq k, n+1} x_i = x_i \right) \ \& \ x_k = x_{n+1}$



Примитив S представим в Ф.А.

$$S\langle f, g_1, \dots, g_k \rangle(x_1, \dots, x_n) = f(g_1(x_1, \dots, x_n), \dots, g_k(x_1, \dots, x_n))$$

Теорема

Пусть функции f, g_1, \dots, g_k представимы в Ф.А. Тогда $S\langle f, g_1, \dots, g_k \rangle$ представима в Ф.А.

Доказательство.

Пусть f, g_1, \dots, g_k представляются формулами $\varphi, \gamma_1, \dots, \gamma_k$.

Тогда $S\langle f, g_1, \dots, g_k \rangle$ будет представлена формулой

$$\exists g_1 \dots \exists g_k. \varphi(g_1, \dots, g_k, x_{n+1}) \ \& \ \gamma_1(x_1, \dots, x_n, g_1) \ \& \ \dots \ \& \ \gamma_k(x_1, \dots, x_n, g_k)$$



β -функция Гёделя

Задача: закодировать последовательность натуральных чисел произвольной длины.

Определение

β -функция Гёделя: $\beta(b, c, i) := b \% (1 + (i + 1) \cdot c)$

Здесь $(\%)$ — остаток от деления.

Теорема

β -функция Гёделя представима в $\Phi.A.$ формулой

$$\hat{\beta}(b, c, i, d) := \exists q. (b = q \cdot (1 + c \cdot (i + 1)) + d) \& (d < 1 + c \cdot (i + 1))$$

Деление b на x с остатком: найдутся частное (q) и остаток (d) , что $b = q \cdot x + d$ и $0 \leq d < x$.

Теорема

Если $a_0, \dots, a_n \in \mathbb{N}_0$, то найдутся такие $b, c \in \mathbb{N}_0$, что $a_i = \beta(b, c, i)$

Доказательство свойства β -функции

Теорема

Китайская теорема об остатках (вариант формулировки): если u_0, \dots, u_n — попарно взаимно просты, и $0 \leq a_i < u_i$, то существует такой b , что $a_i = b \% u_i$.

Положим $c = \max(a_0, \dots, a_n, n)!$ и $u_i = 1 + c \cdot (i + 1)$.

► $\text{НОД}(u_i, u_j) = 1$, если $i \neq j$.

Пусть p — простое, $u_i \div p$ и $u_j \div p$ ($i < j$). Заметим, что $u_j - u_i = c \cdot (j - i)$. Значит, $c \div p$ или $(j - i) \div p$. Так как $j - i \leq n$, то $c \div (j - i)$, потому если и $(j - i) \div p$, всё равно $c \div p$. Но и $(1 + c \cdot (i + 1)) \div p$, отсюда $1 \div p$ — что невозможно.

► $0 \leq a_i < u_i$.

Условия китайской теоремы об остатках выполнены и найдётся b , что

$$a_i = b \% (1 + c \cdot (i + 1)) = \beta(b, c, i)$$



Примитив «примитивная рекурсия» представим в Ф.А.

Пусть $f : \mathbb{N}_0^n \rightarrow \mathbb{N}_0$ и $g : \mathbb{N}_0^{n+2} \rightarrow \mathbb{N}_0$ представлены формулами φ и γ .

Зафиксируем $x_1, \dots, x_n, y \in \mathbb{N}_0$.

Шаг вычисления

$$R\langle f, g \rangle(x_1, \dots, x_n, 0) = f(x_1, \dots, x_n)$$

$$R\langle f, g \rangle(x_1, \dots, x_n, 1) = g(x_1, \dots, x_n, 0, a_0)$$

...

$$R\langle f, g \rangle(x_1, \dots, x_n, y) = g(x_1, \dots, x_n, y-1, a_{y-1}) \quad a_y \quad \vdash \gamma(\overline{x_1}, \dots, \overline{x_n}, \overline{y-1}, \overline{a_y})$$

Об. Утверждение в Ф.А.

$$a_0 \quad \vdash \varphi(\overline{x_1}, \dots, \overline{x_n}, \overline{a_0})$$

$$a_1 \quad \vdash \gamma(\overline{x_1}, \dots, \overline{x_n}, 0, \overline{a_1})$$

По свойству β -функции, найдутся b и c , что $\beta(b, c, i) = a_i$ для $0 \leq i \leq y$.

Теорема

Примитив $R\langle f, g \rangle$ представим в Ф.А. формулой $\rho(x_1, \dots, x_n, y, a)$:

$$\exists b. \exists c. (\exists a_0. \hat{\beta}(b, c, 0, a_0) \& \varphi(x_1, \dots, x_n, a_0))$$

$$\& \quad \forall k. k < y \rightarrow \exists d. \exists e. \hat{\beta}(b, c, k, d) \& \hat{\beta}(b, c, k', e) \& \gamma(x_1, \dots, x_n, k, d, e)$$

$$\& \quad \hat{\beta}(b, c, y, a)$$

Представимость рекурсивных функций в Ф.А.

Теорема

Пусть функция $f : \mathbb{N}_0^{n+1} \rightarrow \mathbb{N}_0$ представима в Ф.А. формулой $\varphi(x_1, \dots, x_n, y, r)$. Тогда примитив $M\langle f \rangle$ представим в Ф.А. формулой

$$\mu(x_1, \dots, x_n, y) := \varphi(x_1, \dots, x_n, y, 0) \ \& \ \forall u. u < y \rightarrow \neg \varphi(x_1, \dots, x_n, u, 0)$$

Теорема

Если f — рекурсивная функция, то она представима в Ф.А.

Доказательство.

Индукция по структуре f .



Рекурсивность представимых функций в $\Phi.A.$

Фиксируем f и x_1, x_2, \dots, x_n . Обозначим $y = f(x_1, x_2, \dots, x_n)$. По представимости нам известна φ , что $\vdash \varphi(\overline{x_1}, \overline{x_2}, \dots, \overline{x_n}, \overline{y})$. Давайте просто переберём все результаты и доказательства!

1. Закодируем доказательства натуральными числами.
2. Напишем рекурсивную функцию, проверяющую доказательства на корректность.
3. Параллельный перебор значений и доказательств: $s = 2^y \cdot 3^p$. Переберём все s , по s получим y и p . Проверим, что p — код доказательства $\vdash \varphi(\overline{x_1}, \overline{x_2}, \dots, \overline{x_n}, \overline{y})$.

Гёделева нумерация

1. Отдельный символ.

Номер	Символ	Номер	Символ	Имя	k, n	Гёделев номер
3	(17	&	0	0, 0	$27 + 6$
5)	19	\forall	(')	0, 1	$27 + 6 \cdot 3$
7	,	21	\exists	(+)	0, 2	$27 + 6 \cdot 9$
9	.	23	\vdash	(.)	1, 2	$27 + 6 \cdot 2 \cdot 9$
11	\neg	$25 + 6 \cdot k$	x_k	(=)	0, 2	$29 + 6 \cdot 9$
13	\rightarrow	$27 + 6 \cdot 2^k \cdot 3^n$	f_k^n			
15	\vee	$29 + 6 \cdot 2^k \cdot 3^n$	P_k^n			

2. Формула. $\phi \equiv s_0 s_1 \dots s_{n-1}$. Гёделев номер: $\ulcorner \phi \urcorner = 2^{\ulcorner s_0 \urcorner} \cdot 3^{\ulcorner s_1 \urcorner} \cdot \dots \cdot p_{n-1}^{\ulcorner s_{n-1} \urcorner}$.

3. Доказательство. $\Pi = \delta_0 \delta_1 \dots \delta_{k-1}$, его гёделев номер:

$$\ulcorner \Pi \urcorner = 2^{\ulcorner \delta_0 \urcorner} \cdot 3^{\ulcorner \delta_1 \urcorner} \cdot \dots \cdot p_{k-1}^{\ulcorner \delta_{k-1} \urcorner}$$

Проверка доказательства на корректность

Теорема

Следующая функция рекурсивна:

$$\text{proof}(f, x_1, x_2, \dots, x_n, y, p) = \begin{cases} 1, & \text{если } \vdash \phi(\overline{x_1}, \overline{x_2}, \dots, \overline{x_n}, \overline{y}), \\ & p \text{ — гёделев номер вывода, } f = \ulcorner \phi \urcorner \\ 0, & \text{иначе} \end{cases}$$

Идея доказательства.

1. Проверка доказательства вычислима.
2. Согласно тезису Чёрча, любая вычислимая функция вычислима с помощью рекурсивных функций.



Перебор доказательств

Лемма

Следующие функции рекурсивны:

1. Функции $plog_k(n) = \max\{p : n \leq k^p\}$, $fst(x) = plog_2(x)$ и $snd(x) = plog_3(x)$.
2. Числовые литералы: $\bar{k} : \mathbb{N}_0 \rightarrow \mathbb{N}_0$, $\bar{k}(x) = k$.

Теорема

Если $f : \mathbb{N}_0^n \rightarrow \mathbb{N}_0$, и f представима в Ф.А. формулой φ , то f — рекурсивна.

Доказательство.

Пусть заданы x_1, x_2, \dots, x_n . Ищем $\langle y, p \rangle$, что $\text{proof}(\ulcorner \varphi \urcorner, x_1, x_2, \dots, x_n, y, p) = 1$, напомним: $y = f(x_1, x_2, \dots, x_n)$, $p = \ulcorner \Pi \urcorner$, Π — доказательство $\varphi(\bar{x}_1, \bar{x}_2, \dots, \bar{x}_n, \bar{y})$.

$$f = S\langle \text{fst}, M\langle S\langle \text{proof}, \overline{\ulcorner \varphi \urcorner}, U_{n+1}^1, U_{n+1}^2, \dots, U_{n+1}^n, S\langle \text{fst}, U_{n+1}^{n+1} \rangle, S\langle \text{snd}, U_{n+1}^{n+1} \rangle \rangle \rangle \rangle$$

