Семинар по сложности доказательств
Ограниченная арифметика: основные определения

Золотов Б.

1.

Язык ограниченной арифметики — $=,\ \leq;\quad 0,\ S,\ +,\ \cdot,\ \lfloor \frac{x}{2} \rfloor,\ |x|,\ \#,\ \leq.\ \ x\#y = 2^{|x|\cdot|y|}$.

Ограниченный квантор — вида $(Qx \leq t)$. Остро ограниченный — вида $(Qx \leq |t|)$. Ограниченная формула — логическая формула только с такими кванторами.

Иерархия ограниченных формул Σ^b_k, Π^b_k — определяется чередованием ограниченных кванторов, на строго ограниченные забиваем. Предикат лежит в классе Σ^p_k полиномиальной иерархии, если и только если определяется Σ^b_k–формулой.

2.

T^i_2 — первопорядковая теория в языке ограниченной арифметики, задающаяся аксиомами: (а) BASIC, описывающими свойства арифметических операций (б) аксиомой индукции для каждой формулы из Σ^b_i с одной свободной переменной.

S^i_2 — то же самое, но вместо аксиомы индукции для каждой формулы A включаем аксиому PIND, где переход от $\lfloor \frac{x}{2} \rfloor$ к x. $S^1_2 \subseteq T^1_2 \subseteq S^2_2 \subseteq T^2_2 \subseteq \ldots$.

$f\colon\ \mathbb{N} \longrightarrow \mathbb{N}$ — Σ^b_i–определяется теорией R, если существует формула $A(\vec{x}, y) \in \Sigma^b_i$ такая, что

(1) Всегда верно $A(\vec{n}, f(\vec{n}))$;

(2) Из R можно вывести, что для любого $\vec{n}$ существует *ровно один* y, такой что $A(\vec{n}, y)$.

Предикат $P \subseteq \mathbb{N}$ — Δ^b_i–определяется теорией R, если существуют Σ^b_i–формула A и Π^b_i формула B такие, что они обе задают P, и в R можно доказать их эквивалентность.

3.

Теорема: Пусть $A \in \Sigma^b_i$ — тогда существуют $B \in \Sigma^b_i, f \in \square^p_i$ и терм t такие, что:

(1) $S^i_2 \vdash B$ верна только если верна A;

(2) Для всякого $\vec{x}$ существует единственный y, т. ч. $B(\vec{x}, y)$,

(3) И этот y не превосходит t;

(4) Для всякого $\vec{n}$ верно $\mathbb{N} \models B(\vec{n}, f(\vec{n}))$, то есть, формула B задаёт функцию f.

Теорема: Если $f \in \square^p_i$, то существует задающая её формула B, такая что (2)–(4).

Теорема: Функции, Σ^b_i–определяющиеся теорией S^i_2, — в точности $\square^p_i$.

Теорема: Предикаты, Δ^b_i–определяющиеся теорией S^i_2, — в точности Δ^p_i из полиномиальной иерархии.

4.

Cut:

$$\frac{\Gamma \longrightarrow \Delta, A \qquad A, \Pi \longrightarrow X}{\Gamma,\ \Pi \quad \longrightarrow \quad \Delta, X}$$

Обычно стараемся от них избавиться (хотя бы от некоторых), чтобы было *subformula property*.

5.

Definition Fix $i \geq 1$. Let $B(\vec{a})$ be a Σ^b_i-formula with all free variables indicated. Then $Witness^{i,\vec{a}}_B(w,\vec{a})$ is a formula defined inductively by:

(1) If $B \in \Sigma^b_{i-1} \cup \Pi^b_{i-1}$ then $Witness^{i,\vec{a}}_B(w,\vec{a}) \Leftrightarrow B(\vec{a})$.

(2) If $B = C \vee D$ then

$$Witness^{i,\vec{a}}_B(w,\vec{a}) \Leftrightarrow Witness^{i,\vec{a}}_C(\beta(1,w),\vec{a}) \vee Witness^{i,\vec{a}}_D(\beta(2,w),\vec{a}).$$

(3) If $B = C \wedge D$ then

$$Witness^{i,\vec{a}}_B(w,\vec{a}) \Leftrightarrow Witness^{i,\vec{a}}_C(\beta(1,w),\vec{a}) \wedge Witness^{i,\vec{a}}_D(\beta(2,w),\vec{a}).$$

(4) If $B = (\exists x \leq t) C(\vec{a},x)$ then

$$Witness^{i,\vec{a}}_B(w,\vec{a}) \Leftrightarrow \beta(1,w) \leq t \wedge Witness^{i,\vec{a},b}_{C(\vec{a},b)}(\beta(2,w),\vec{a},\beta(1,w)).$$

(5) If $B = (\forall x \leq |t|) C(\vec{a},x)$ then

$$Witness^{i,\vec{a}}_B(w,\vec{a}) \Leftrightarrow (\forall x \leq |t|)\, Witness^{i,\vec{a},b}_{C(\vec{a},b)}(\beta(x+1,w),\vec{a},x).$$

(6) If $B = \neg C$ use prenex operations to push the negation sign inside.

6.

1. По доказательству в теории S^1_2 можно построить extended Frege–доказательство полиномиального размера.
2. По доказательству в теории $S_2 = \bigcup S^i_2 = T_2$ можно построить Frege–доказательство полиномиального размера и фиксированной глубины.