# Логические основы теории сложности доказательств

Александр Смаль

Лекция №3

24 апреля 2009 г.

# Принцип минимума

## Определение

Аксиомы **минимизации** (**принципа минимального числа**) для множества формул $\Phi$ обозначаются $\Phi$**−MIN** и состоят из формул

$$\exists z \varphi(z) \supset \exists y \big(\varphi(y) \wedge \neg \exists x (x < y \wedge \varphi(x))\big),$$

где $\varphi$ — формула из $\Phi$.

# Принцип минимума

## Определение

Аксиомы **минимизации** (**принципа минимального числа**) для множества формул $\Phi$ обозначаются $\Phi$–**MIN** и состоят из формул

$$\exists z \varphi(z) \supset \exists y \big(\varphi(y) \wedge \neg \exists x (x < y \wedge \varphi(x))\big),$$

где $\varphi$ — формула из $\Phi$.

## Теорема

$$\mathbf{I}\Delta_0 \vdash \Delta_0\text{–}\mathbf{MIN}.$$

# Принцип минимума

## Определение

Аксиомы **минимизации** (**принципа минимального числа**) для множества формул $\Phi$ обозначаются $\Phi-\mathbf{MIN}$ и состоят из формул

$$\exists z \varphi(z) \supset \exists y \big(\varphi(y) \wedge \neg \exists x (x < y \wedge \varphi(x))\big),$$

где $\varphi$ — формула из $\Phi$.

## Теорема

$$\mathbf{I}\Delta_0 \vdash \Delta_0-\mathbf{MIN}.$$

## Доказательство

Аксиома минимизации для формулы $\varphi(z)$ следует из аксиомы индукции для ограниченной формулы $\psi(z) \equiv \forall y_{\leq z}(\neg\varphi(y))$. $\square$

# Ограниченная представимость

## Теорема (Ограниченная представимость)

*Пусть $\mathcal{T}$ — полиномиально-ограниченная теория. Функция $f(\vec{x})$ (не из $\mathcal{T}$) $\Sigma_1$-представима в $\mathcal{T}$ iff существует определяющая аксиома*

$$y = f(\vec{x}) \leftrightarrow \varphi(\vec{x}, y),$$

*где $\varphi$ — ограниченная формула со свободными переменными $\vec{x}$ и $y$, а также $\mathcal{L}_A$-терм $t = t(\vec{x})$ такой, что из*

$$\mathcal{T} \vdash \forall \vec{x} \exists! y_{\leq t} \varphi(\vec{x}, y)$$

# Ограниченная представимость

## Теорема (Ограниченная представимость)

*Пусть* $\mathcal{T}$ *— полиномиально-ограниченная теория. Функция* $f(\vec{x})$ *(не из* $\mathcal{T}$*)* $\Sigma_1$*-представима в* $\mathcal{T}$ *iff существует определяющая аксиома*

$$y = f(\vec{x}) \leftrightarrow \varphi(\vec{x}, y),$$

*где* $\varphi$ *— ограниченная формула со свободными переменными* $\vec{x}$ *и* $y$*, а также* $\mathcal{L}_A$*-терм* $t = t(\vec{x})$ *такой, что из*

$$\mathcal{T} \vdash \forall \vec{x} \exists! y_{\leq t} \varphi(\vec{x}, y)$$

## Доказательство

$\Leftarrow$ из определения представимости.

$\Rightarrow$ из теоремы Париха.

# Ограниченная представимость

## Теорема (Ограниченная представимость)

*Пусть $\mathcal{T}$ — полиномиально-ограниченная теория. Функция $f(\vec{x})$ (не из $\mathcal{T}$) $\Sigma_1$-представима в $\mathcal{T}$ iff существует определяющая аксиома*

$$y = f(\vec{x}) \leftrightarrow \varphi(\vec{x}, y),$$

*где $\varphi$ — ограниченная формула со свободными переменными $\vec{x}$ и $y$, а также $\mathcal{L}_A$-терм $t = t(\vec{x})$ такой, что из*

$$\mathcal{T} \vdash \forall \vec{x} \exists! y_{\leq t} \varphi(\vec{x}, y)$$

## Доказательство

$\Leftarrow$ из определения представимости.

$\Rightarrow$ из теоремы Париха.

## Следствие

*$f$ — $\Sigma_1$-представима в $\mathcal{T}$ iff $f$ — $\Delta_0$-представима в $\mathcal{T}$.*

# Полиномиальная иерархия по времени

В контексте ограниченной арифметики будем считать, что элементами сложностных классов вроде **P** являются не *языки*, а *подмножества* $\mathbb{N}$.

# Полиномиальная иерархия по времени

В контексте ограниченной арифметики будем считать, что элементами сложностных классов вроде **P** являются не *языки*, а *подмножества* $\mathbb{N}$. Подмножества задаются *отношениями*, и в этом случае считается, что числа задаются в двоичной записи.

# Полиномиальная иерархия по времени

В контексте ограниченной арифметики будем считать, что элементами сложностных классов вроде **P** являются не *языки*, а *подмножества* $\mathbb{N}$. Подмножества задаются *отношениями*, и в этом случае считается, что числа задаются в двоичной записи.

## Определение

Класс $\Sigma_0^p = \mathbf{P}$ — это класс всех отношений $R(x_1, \ldots, x_k)$ на $\mathbb{N}$ таких, что $R$ может быть проверено на некоторой детерминированной МТ $M_R$ за полиномиальное от $|x_1| + \cdots + |x_k|$ время.

# Полиномиальная иерархия по времени

В контексте ограниченной арифметики будем считать, что элементами сложностных классов вроде **P** являются не *языки*, а *подмножества* $\mathbb{N}$. Подмножества задаются *отношениями*, и в этом случае считается, что числа задаются в двоичной записи.

## Определение

Класс $\Sigma_0^p = \mathbf{P}$ — это класс всех отношений $R(x_1, \ldots, x_k)$ на $\mathbb{N}$ таких, что $R$ может быть проверено на некоторой детерминированной МТ $M_R$ за полиномиальное от $|x_1| + \cdots + |x_k|$ время.

## Определение

Класс $\Sigma_{i+1}^p$ для $i \geq 0$, представляющий **$(i+1)$-й уровень полиномиальной иерархии**, определяется индуктивно

$$\Sigma_{i+1}^p = \mathbf{NP}^{\Sigma_i^p},$$

где $\mathbf{NP}^{\Sigma_i^p}$ — это множество отношений, проверяемых за полиномиальное время на НМТ с оракулом из $\Sigma_i^p$.

# Полиномиальная иерархия по времени (продолжение)

## Замечание 1

Классы $\Sigma_i^p$ могут быть также определены, как множества отношений, принимаемых за полиномиальное время некоторой *чередующейся (alternating) MT*, которой позволено не более $i$ чередований, начиная с экзистенциального состояния.

# Полиномиальная иерархия по времени (продолжение)

## Замечание 1

Классы $\Sigma_i^p$ могут быть также определены, как множества отношений, принимаемых за полиномиальное время некоторой *чередующейся (alternating) MT*, которой позволено не более $i$ чередований, начиная с экзистенциального состояния.

## Замечание 2

Для $i = 1$ имеем

$$\Sigma_1^p = \mathbf{NP}.$$

# Полиномиальная иерархия по времени (продолжение)

## Замечание 1

Классы $\Sigma_i^p$ могут быть также определены, как множества отношений, принимаемых за полиномиальное время некоторой *чередующейся (alternating) MT*, которой позволено не более $i$ чередований, начиная с экзистенциального состояния.

## Замечание 2

Для $i = 1$ имеем

$$\Sigma_1^p = \mathbf{NP}.$$

## Определение

**Полиномиальная иерархия по времени**

$$\mathbf{PH} = \bigcup_{i=0}^{\infty} \Sigma_i^p.$$

# Линейная иерархия по времени

## Определение

**NLinTime** — это класс отношений, принимаемых за время $O(n)$ на недетерминированной многоленточной МТ. Тогда

$$\Sigma_1^{lin} = \textbf{NLinTime}$$

# Линейная иерархия по времени

## Определение

**NLinTime** — это класс отношений, принимаемых за время $O(n)$ на недетерминированной многоленточной МТ. Тогда

$$\Sigma_1^{lin} = \textbf{NLinTime}$$

## Определение

Для $i \geq 1$ индуктивно определим $\Sigma_{i+1}^{lin} = \textbf{NLinTime}^{\Sigma_i^{lin}}$.

# Линейная иерархия по времени

## Определение

**NLinTime** — это класс отношений, принимаемых за время $O(n)$ на недетерминированной многоленточной МТ. Тогда

$$\Sigma_1^{lin} = \textbf{NLinTime}$$

## Определение

Для $i \geq 1$ индуктивно определим $\Sigma_{i+1}^{lin} = \textbf{NLinTime}^{\Sigma_i^{lin}}$.

## Определение

**Линейная иерархия по времени**

$$\textbf{LTH} = \bigcup_{i=1}^{\infty} \Sigma_i^{lin}.$$

# Линейная иерархия по времени (продолжение)

## Замечание 1

Класс **LinTime** **плох** тем, что зависит от количества лент. Детерминированная МТ с $k+1$ лентой может распознавать такие множества, которые не может распознавать ни одна ДМТ с $k$ лентами. Соответственно, машина с произвольным доступом может распознавать за линейное время множества не из **LinTime**

# Линейная иерархия по времени (продолжение)

## Замечание 1

Класс **LinTime** **плох** тем, что зависит от количества лент. Детерминированная МТ с $k+1$ лентой может распознавать такие множества, которые не может распознавать ни одна ДМТ с $k$ лентами. Соответственно, машина с произвольным доступом может распознавать за линейное время множества не из **LinTime**

## Замечание 2

Класс **NLinTime** **хорош** тем, что **не** зависит от количества лент. Каждое множество из этого класса может быть распознано за линейное время на двухленточной НМТ.

# Представление **LTH** отношений

## Определение

$\Delta_0^{\mathbb{N}}$ — класс всех $\Delta_0$-представимых отношений.

## Теорема (**LTH** теорема)

$$\mathbf{LTH} = \Delta_0^{\mathbb{N}}.$$

## Определение

Класс $\mathbf{NTimeSpace}(f(n), g(n))$ состоит из всех отношений, которые принимаются недетерминированной многоленточной МТ за время $O(f(n))$, использующей $O(g(n))$ места.

## Теорема (Непомнящий)

*Пусть $\epsilon$ — рациональное число $0 < \epsilon < 1$, и $a$ — положительное целое. Тогда*

$$\mathbf{NTimeSpace}(n^a, n^\epsilon) \subseteq \mathbf{LTH}.$$

# Доказательство теоремы Непомнящего

## Доказательство

# Доказательство теоремы Непомнящего

## Доказательство

1. Предположим, что мы хотим доказать **NTimeSpace**$(n^2, n^{0.6}) \subseteq$ **LTH**.

# Доказательство теоремы Непомнящего

## Доказательство

1. Предположим, что мы хотим доказать **NTimeSpace**$(n^2, n^{0.6}) \subseteq$ **LTH**.
2. Пусть $M$ — НМТ работающая время $n^2$ и использующая $n^{0.6}$ места.

# Доказательство теоремы Непомнящего

## Доказательство

1. Предположим, что мы хотим доказать **NTimeSpace**$(n^2, n^{0.6}) \subseteq$ **LTH**.
2. Пусть $M$ — НМТ работающая время $n^2$ и использующая $n^{0.6}$ места.
3. $M$ принимает $x$, если $\exists \vec{y}(\vec{y}$ принимающее вычисления для $x)$, где $\vec{y} = y_1, \ldots, y_{n^2}$ и каждая $y_i$ —строка длины $n^{0.6}$.

# Доказательство теоремы Непомнящего

## Доказательство

1. Предположим, что мы хотим доказать **NTimeSpace**$(n^2, n^{0.6}) \subseteq$ **LTH**.
2. Пусть $M$ — НМТ работающая время $n^2$ и использующая $n^{0.6}$ места.
3. $M$ принимает $x$, если $\exists \vec{y}(\vec{y}$ принимающее вычисления для $x)$, где $\vec{y} = y_1, \ldots, y_{n^2}$ и каждая $y_i$ —строка длины $n^{0.6}$.
4. Т. е. $|\vec{y}| = n^{2.6}$, что слишком длинно для линейной ЧМТ.

# Доказательство теоремы Непомнящего

## Доказательство

1. Предположим, что мы хотим доказать **NTimeSpace**$(n^2, n^{0.6}) \subseteq$ **LTH**.
2. Пусть $M$ — НМТ работающая время $n^2$ и использующая $n^{0.6}$ места.
3. $M$ принимает $x$, если $\exists \vec{y}(\vec{y}$ принимающее вычисления для $x)$, где $\vec{y} = y_1, \ldots, y_{n^2}$ и каждая $y_i$ —строка длины $n^{0.6}$.
4. Т. е. $|\vec{y}| = n^{2.6}$, что слишком длинно для линейной ЧМТ.
5. Предположим, что $\vec{z} = z_1, \ldots, z_n$ выражает каждую $n$-тую строку из $\vec{y}$.

# Доказательство теоремы Непомнящего

## Доказательство

1. Предположим, что мы хотим доказать $\mathbf{NTimeSpace}(n^2, n^{0.6}) \subseteq \mathbf{LTH}$.
2. Пусть $M$ — НМТ работающая время $n^2$ и использующая $n^{0.6}$ места.
3. $M$ принимает $x$, если $\exists \vec{y}(\vec{y}$ принимающее вычисления для $x)$, где $\vec{y} = y_1, \ldots, y_{n^2}$ и каждая $y_i$ —строка длины $n^{0.6}$.
4. Т. е. $|\vec{y}| = n^{2.6}$, что слишком длинно для линейной ЧМТ.
5. Предположим, что $\vec{z} = z_1, \ldots, z_n$ выражает каждую $n$-тую строку из $\vec{y}$.
6. Тогда $M$ принимает $x$, если

$$\exists \vec{z} \forall i_{<n} \exists \vec{u}(\vec{u} \text{ показывает, что } z_{i+1} \text{ следует из } z_i \text{ за } n \text{ шагов, и } z_n \text{ — принимающее}).$$

# Доказательство теоремы Непомнящего

## Доказательство

1. Предположим, что мы хотим доказать **NTimeSpace**$(n^2, n^{0.6}) \subseteq$ **LTH**.
2. Пусть $M$ — НМТ работающая время $n^2$ и использующая $n^{0.6}$ места.
3. $M$ принимает $x$, если $\exists \vec{y}(\vec{y}$ принимающее вычисления для $x)$, где $\vec{y} = y_1, \ldots, y_{n^2}$ и каждая $y_i$ —строка длины $n^{0.6}$.
4. Т. е. $|\vec{y}| = n^{2.6}$, что слишком длинно для линейной ЧМТ.
5. Предположим, что $\vec{z} = z_1, \ldots, z_n$ выражает каждую $n$-тую строку из $\vec{y}$.
6. Тогда $M$ принимает $x$, если

$$\exists \vec{z} \forall i_{<n} \exists \vec{u}(\vec{u} \text{ показывает, что } z_{i+1} \text{ следует из } z_i \text{ за } n \text{ шагов, и } z_n \text{ — принимающее}).$$

7. Теперь $|\vec{z}| = |\vec{u}| = n^{1.6}$.

# Доказательство теоремы Непомнящего

## Доказательство

1. Предположим, что мы хотим доказать **NTimeSpace**$(n^2, n^{0.6}) \subseteq$ **LTH**.
2. Пусть $M$ — НМТ работающая время $n^2$ и использующая $n^{0.6}$ места.
3. $M$ принимает $x$, если $\exists \vec{y}(\vec{y}$ принимающее вычисления для $x)$, где $\vec{y} = y_1, \ldots, y_{n^2}$ и каждая $y_i$ —строка длины $n^{0.6}$.
4. Т. е. $|\vec{y}| = n^{2.6}$, что слишком длинно для линейной ЧМТ.
5. Предположим, что $\vec{z} = z_1, \ldots, z_n$ выражает каждую $n$-тую строку из $\vec{y}$.
6. Тогда $M$ принимает $x$, если

$$\exists \vec{z} \forall i_{<n} \exists \vec{u}(\vec{u} \text{ показывает, что } z_{i+1} \text{ следует из } z_i \text{ за } n \text{ шагов, и } z_n \text{ — принимающее}).$$

7. Теперь $|\vec{z}| = |\vec{u}| = n^{1.6}$.
8. Еще два применения этого трюка (для $\vec{z}$ и для $\vec{u}$) и длины всех строк под кванторами станут меньше $n$. □

# Следствие

## Следствие

$$\textbf{NLogSpace} \subseteq \textbf{LTH}$$

## Доказательство

Воспользуемся фактом, что $\textbf{NLogSpace} \subseteq \textbf{NTimeSpace}(n^{O(1)}, \log n)$. □

## Замечание

Мы знаем

$$\textbf{LogSpace} \subseteq \textbf{LTH} \subseteq \textbf{PH} \subseteq \textbf{PSPACE}.$$

Все включения нестрогие. Хотя $\textbf{LogSpace} \subset \textbf{PH}$.
Мы также знаем, что

$$\textbf{LTH} \subseteq \textbf{LinSpace} \subset \textbf{PSPACE}.$$

# От отношений к функциям

**LTH** — класс *отношений*. Соответствующий класс функций определяется в терминах **графиков функций**.

## Определение

**График функции** $f(\vec{x})$ — это отношение $G_f(\vec{x}, y)$:

$$G_f(\vec{x}, y) \leftrightarrow (y = f(\vec{x})).$$

## Определение

Функция $f : \mathbb{N}^k \to \mathbb{N}$ принадлежит классу **FLTH**, если её график $G_f(\vec{x}, y)$ лежит в **LTH** и длина $f$ растёт не более чем линейно, т. е.

$$f(\vec{x}) = (x_1 + \cdots + x_k)^{O(1)}.$$

# Связь **LTH** и $\mathbf{I}\Delta_0$

В общем случае для того, чтобы связать теорию со сложностным классом, нам нужно показать, что функции в классе совпадают с $\Sigma_1$-представимыми функциями теории.

# Связь **LTH** и $\mathbf{I}\Delta_0$

В общем случае для того, чтобы связать теорию со сложностным классом, нам нужно показать, что функции в классе совпадают с $\Sigma_1$-представимыми функциями теории.

## Теорема ($\mathbf{I}\Delta_0$-представимость)

*Функция $\Sigma_1$-представим в $\mathbf{I}\Delta_0$ iff она из* **FLTH**.

## Доказательство

$\Rightarrow$ следует из теоремы о представимости, определения **FLTH** и **LTH** теоремы. Для $\Leftarrow$ предположим, что $f(\vec{x})$ из **FLTH**.

# Связь **LTH** и $\mathbf{I}\Delta_0$

В общем случае для того, чтобы связать теорию со сложностным классом, нам нужно показать, что функции в классе совпадают с $\Sigma_1$-представимыми функциями теории.

## Теорема ($\mathbf{I}\Delta_0$-представимость)

*Функция $\Sigma_1$-представим в $\mathbf{I}\Delta_0$ iff она из* **FLTH**.

## Доказательство

$\Rightarrow$ следует из теоремы о представимости, определения **FLTH** и **LTH** теоремы. Для $\Leftarrow$ предположим, что $f(\vec{x})$ из **FLTH**.

- По определению отношение $(y = f(\vec{x}))$ лежит в **LTH**.

# Связь **LTH** и $\mathbf{I}\Delta_0$

В общем случае для того, чтобы связать теорию со сложностным классом, нам нужно показать, что функции в классе совпадают с $\Sigma_1$-представимыми функциями теории.

## Теорема ($\mathbf{I}\Delta_0$-представимость)

*Функция $\Sigma_1$-представим в $\mathbf{I}\Delta_0$ iff она из* **FLTH**.

## Доказательство

$\Rightarrow$ следует из теоремы о представимости, определения **FLTH** и **LTH** теоремы. Для $\Leftarrow$ предположим, что $f(\vec{x})$ из **FLTH**.

- По определению отношение $(y = f(\vec{x}))$ лежит в **LTH**.
- По **LTH** теореме есть $\Delta_0$ формула $\varphi(\vec{x}, y)$: $y = f(\vec{x}) \leftrightarrow \varphi(\vec{x}, y)$.

# Связь **LTH** и $\mathbf{I}\Delta_0$

В общем случае для того, чтобы связать теорию со сложностным классом, нам нужно показать, что функции в классе совпадают с $\Sigma_1$-представимыми функциями теории.

## Теорема ($\mathbf{I}\Delta_0$-представимость)

*Функция $\Sigma_1$-представим в $\mathbf{I}\Delta_0$ iff она из* **FLTH**.

## Доказательство

$\Rightarrow$ следует из теоремы о представимости, определения **FLTH** и **LTH** теоремы. Для $\Leftarrow$ предположим, что $f(\vec{x})$ из **FLTH**.

- По определению отношение $(y = f(\vec{x}))$ лежит в **LTH**.
- По **LTH** теореме есть $\Delta_0$ формула $\varphi(\vec{x}, y)$: $y = f(\vec{x}) \leftrightarrow \varphi(\vec{x}, y)$.
- Т.к. $|f(\vec{x})|$ линейно ограничена, то есть $\mathcal{L}_A$-терм, такой что $f(\vec{x}) \leq t(\vec{x})$.

# Связь **LTH** и $\mathbf{I}\Delta_0$

В общем случае для того, чтобы связать теорию со сложностным классом, нам нужно показать, что функции в классе совпадают с $\Sigma_1$-представимыми функциями теории.

## Теорема ($\mathbf{I}\Delta_0$-представимость)

*Функция $\Sigma_1$-представим в $\mathbf{I}\Delta_0$ iff она из* **FLTH**.

## Доказательство

$\Rightarrow$ следует из теоремы о представимости, определения **FLTH** и **LTH** теоремы. Для $\Leftarrow$ предположим, что $f(\vec{x})$ из **FLTH**.

- По определению отношение $(y = f(\vec{x}))$ лежит в **LTH**.
- По **LTH** теореме есть $\Delta_0$ формула $\varphi(\vec{x}, y)$: $y = f(\vec{x}) \leftrightarrow \varphi(\vec{x}, y)$.
- Т.к. $|f(\vec{x})|$ линейно ограничена, то есть $\mathcal{L}_A$-терм, такой что $f(\vec{x}) \leq t(\vec{x})$.
- Высказывание $\forall \vec{x} \exists! y \varphi(\vec{x}, y)$ верно, но непонятно почему оно доказуемо в $\mathbf{I}\Delta_0$.

# Связь **LTH** и $\mathbf{I}\Delta_0$ (продолжение)

## Доказательство (продолжение)

# Связь **LTH** и $\mathsf{I}\Delta_0$ (продолжение)

## Доказательство (продолжение)

- Разберёмся с уникальностью $y$. Для формулы $A(y)$ определим $\mathrm{Min}_y[A(y)](y)$ как минимальное число, удовлетворяющее $A(y)$.

# Связь **LTH** и $\mathsf{I}\Delta_0$ (продолжение)

## Доказательство (продолжение)

- Разберёмся с уникальностью $y$. Для формулы $A(y)$ определим $\mathrm{Min}_y[A(y)](y)$ как минимальное число, удовлетворяющее $A(y)$.
- $\mathrm{Min}_y[A(y)](y) \equiv_{def} A(y) \wedge \forall z_{<y}(\neg A(z))$.

# Связь **LTH** и $\mathbf{I}\Delta_0$ (продолжение)

## Доказательство (продолжение)

- Разберёмся с уникальностью $y$. Для формулы $A(y)$ определим $\mathrm{Min}_y[A(y)](y)$ как минимальное число, удовлетворяющее $A(y)$.
- $\mathrm{Min}_y[A(y)](y) \equiv_{def} A(y) \wedge \forall z_{<y}(\neg A(z))$.
- Т. о., если $A(y)$ ограниченно, то мы можем применить принцип наименьшего к $A(y)$, чтобы получить

$$\mathbf{I}\Delta_0 \vdash \exists y A(y) \supset \exists! y \mathrm{Min}_y[A(y)](y).$$

# Связь **LTH** и $\mathbf{I}\Delta_0$ (продолжение)

## Доказательство (продолжение)

- Разберёмся с уникальностью $y$. Для формулы $A(y)$ определим $\mathrm{Min}_y[A(y)](y)$ как минимальное число, удовлетворяющее $A(y)$.
- $\mathrm{Min}_y[A(y)](y) \equiv_{def} A(y) \wedge \forall z_{<y}(\neg A(z))$.
- Т. о., если $A(y)$ ограниченно, то мы можем применить принцип наименьшего к $A(y)$, чтобы получить
$$\mathbf{I}\Delta_0 \vdash \exists y A(y) \supset \exists! y \mathrm{Min}_y[A(y)](y).$$
- Теперь надо доказать существование. Определим
$$\psi(\vec{x}, y) \equiv_{def} (\varphi(\vec{x}, y) \vee y = t(\vec{x}) + 1).$$

# Связь **LTH** и $\mathbf{I}\Delta_0$ (продолжение)

## Доказательство (продолжение)

- Разберёмся с уникальностью $y$. Для формулы $A(y)$ определим $\mathrm{Min}_y[A(y)](y)$ как минимальное число, удовлетворяющее $A(y)$.
- $\mathrm{Min}_y[A(y)](y) \equiv_{def} A(y) \wedge \forall z_{<y}(\neg A(z))$.
- Т. о., если $A(y)$ ограниченно, то мы можем применить принцип наименьшего к $A(y)$, чтобы получить
$$\mathbf{I}\Delta_0 \vdash \exists y A(y) \supset \exists! y \mathrm{Min}_y[A(y)](y).$$
- Теперь надо доказать существование. Определим
$$\psi(\vec{x}, y) \equiv_{def} (\varphi(\vec{x}, y) \vee y = t(\vec{x}) + 1).$$
- Подправим $\varphi$: $\varphi'(\vec{x}, y) \equiv_{def} \mathrm{Min}_y[\psi(\vec{x}, y)](\vec{x}, y)$.

# Связь **LTH** и $\mathbf{I}\Delta_0$ (продолжение)

## Доказательство (продолжение)

- Разберёмся с уникальностью $y$. Для формулы $A(y)$ определим $\mathrm{Min}_y[A(y)](y)$ как минимальное число, удовлетворяющее $A(y)$.
- $\mathrm{Min}_y[A(y)](y) \equiv_{def} A(y) \wedge \forall z_{<y}(\neg A(z))$.
- Т. о., если $A(y)$ ограниченно, то мы можем применить принцип наименьшего к $A(y)$, чтобы получить
$$\mathbf{I}\Delta_0 \vdash \exists y A(y) \supset \exists! y \mathrm{Min}_y[A(y)](y).$$
- Теперь надо доказать существование. Определим
$$\psi(\vec{x}, y) \equiv_{def} (\varphi(\vec{x}, y) \vee y = t(\vec{x}) + 1).$$
- Подправим $\varphi$: $\varphi'(\vec{x}, y) \equiv_{def} \mathrm{Min}_y[\psi(\vec{x}, y)](\vec{x}, y)$.
- $\varphi'(\vec{x}, y)$ тоже определяет отношение $(y = f(\vec{x}))$.

# Связь **LTH** и $\mathbf{I}\Delta_0$ (продолжение)

## Доказательство (продолжение)

- Разберёмся с уникальностью $y$. Для формулы $A(y)$ определим $\mathrm{Min}_y[A(y)](y)$ как минимальное число, удовлетворяющее $A(y)$.
- $\mathrm{Min}_y[A(y)](y) \equiv_{def} A(y) \wedge \forall z_{<y}(\neg A(z))$.
- Т. о., если $A(y)$ ограниченно, то мы можем применить принцип наименьшего к $A(y)$, чтобы получить
$$\mathbf{I}\Delta_0 \vdash \exists y A(y) \supset \exists! y \mathrm{Min}_y[A(y)](y).$$
- Теперь надо доказать существование. Определим
$$\psi(\vec{x}, y) \equiv_{def} (\varphi(\vec{x}, y) \vee y = t(\vec{x}) + 1).$$
- Подправим $\varphi$: $\varphi'(\vec{x}, y) \equiv_{def} \mathrm{Min}_y[\psi(\vec{x}, y)](\vec{x}, y)$.
- $\varphi'(\vec{x}, y)$ тоже определяет отношение $(y = f(\vec{x}))$.
- Т.к. $\mathbf{I}\Delta_0$ доказывает $\exists y \psi(\vec{x}, y)$, то $\mathbf{I}\Delta_0 \vdash \forall \vec{x} \exists! y \varphi'(\vec{x}, y)$. □

# Иерархия Buss-а

В своей диссертации на тему ограниченной арифметики Buss предлагает иерархию ограниченных теорий.

$$\mathbf{S}_2^1 \subseteq \mathbf{T}_2^1 \subseteq \mathbf{S}_2^2 \subseteq \mathbf{T}_2^2 \subseteq \cdots \subseteq \mathbf{S}_2^i \subseteq \mathbf{T}_2^i \subseteq \cdots$$

Также $\mathbf{S}_2 = \mathbf{T}_2 = \bigcup_{i=1}^{\infty} \mathbf{S}_2^i$.

# Иерархия Buss-a

В своей диссертации на тему ограниченной арифметики Buss предлагает иерархию ограниченных теорий.

$$\mathbf{S}_2^1 \subseteq \mathbf{T}_2^1 \subseteq \mathbf{S}_2^2 \subseteq \mathbf{T}_2^2 \subseteq \cdots \subseteq \mathbf{S}_2^i \subseteq \mathbf{T}_2^i \subseteq \cdots$$

Также $\mathbf{S}_2 = \mathbf{T}_2 = \bigcup_{i=1}^{\infty} \mathbf{S}_2^i$.

## Основная идея

Модифицируем теорию $\mathbf{I}\Delta_0$ так, чтобы представимыми были функции из полиномиальной иерархии, а не из линейной. Таким образом функции представимые в $\Sigma_1^p$ — это в точности полиномиально-вычислимые функции.

# Иерархия Buss-a

В своей диссертации на тему ограниченной арифметики Buss предлагает иерархию ограниченных теорий.

$$\mathbf{S}_2^1 \subseteq \mathbf{T}_2^1 \subseteq \mathbf{S}_2^2 \subseteq \mathbf{T}_2^2 \subseteq \cdots \subseteq \mathbf{S}_2^i \subseteq \mathbf{T}_2^i \subseteq \cdots$$

Также $\mathbf{S}_2 = \mathbf{T}_2 = \bigcup_{i=1}^{\infty} \mathbf{S}_2^i$.

## Основная идея

Модифицируем теорию $\mathbf{I}\Delta_0$ так, чтобы представимыми были функции из полиномиальной иерархии, а не из линейной. Таким образом функции представимые в $\Sigma_1^p$ — это в точности полиномиально-вычислимые функции.

## Как?

Добавим в язык функцию $\sharp$: $x \sharp y = 2^{|x| \cdot |y|}$. Таким образом функциям в $\mathbf{S}_2$ позволено расти полиномиально. Язык $\mathbf{S}_2^2$

$$\mathcal{L}_{\mathbf{S}_2^2} = [0, S, +, \cdot, \sharp, |x|, \left\lfloor \tfrac{1}{2} x \right\rfloor;\ =, \leq].$$

# Иерархия Buss-a (продолжение)

## Определение

**Жёстко ограниченные кванторы** — это кванторы вида $\forall x \leq |t|$ и $\forall y \leq |t|$, где $x$ не встречается в $t$.

## Определение

Класс $\Sigma_i^b$ состоит из формул, имеющих не более $i$ блоков ограниченных кванторов, начиная с $\exists$, с произвольным числом жёстко ограниченных кванторов обоих типов.

# Иерархия Buss-a (продолжение)

## Определение

**Жёстко ограниченные кванторы** — это кванторы вида $\forall x \leq |t|$ и $\forall y \leq |t|$, где $x$ не встречается в $t$.

## Определение

Класс $\Sigma_i^b$ состоит из формул, имеющих не более $i$ блоков ограниченных кванторов, начиная с $\exists$, с произвольным числом жёстко ограниченных кванторов обоих типов.

Соответственно, $\Sigma_1^b$ представляет **NP** отношения, а $\Sigma_i^b$ — отношения $\Sigma_i^p$ ($i$-го уровня полиномиальной иерархии). И следовательно, $\mathbf{S}_2$ в точности соответствует **PH**.

# Иерархия Buss-a (продолжение)

## Определение

**Жёстко ограниченные кванторы** — это кванторы вида $\forall x \leq |t|$ и $\forall y \leq |t|$, где $x$ не встречается в $t$.

## Определение

Класс $\Sigma_i^b$ состоит из формул, имеющих не более $i$ блоков ограниченных кванторов, начиная с $\exists$, с произвольным числом жёстко ограниченных кванторов обоих типов.

Соответственно, $\Sigma_1^b$ представляет **NP** отношения, а $\Sigma_i^b$ — отношения $\Sigma_i^p$ ($i$-го уровня полиномиальной иерархии). И следовательно, $\mathbf{S}_2$ в точности соответствует **PH**.

Аксиомы $\mathbf{T}_2^i$ состоят из 32 $\forall$-высказываний, которые определяют символы из $\mathcal{L}_{\mathbf{S}_2}$ совместно со схемой $\Sigma_i^b$–**IND**. Аксиомы $\mathbf{S}_2^i$ такие же, но вместо $\Sigma_i^b$–**IND** схема индукции $\Sigma_i^b$–**PIND**:

$$\left(\varphi(0) \wedge \forall x\left(\left\lfloor \tfrac{1}{2}x \right\rfloor\right) \supset \varphi(x)\right) \supset \forall x \varphi(x).$$