

# Математическая логика

mk.cs.msu.ru → Лекционные курсы → Математическая логика (318, 319/2, 241, 242)

## Блок 42

Арифметика Пресбургера

Лектор:

**Подымов Владислав Васильевич**

E-mail:

**valdus@yandex.ru**

ВМК МГУ, 2025, февраль–май

# Арифметика Пресбургера

$Ar[\mathbb{N}_0; 0; +, \cdot, \mathbf{s}; =]$  — эта интерпретация оказалась непростой:

- ▶ её теория обязательно или неполна, или неперечислима
- ▶ не существует алгоритма, проверяющего справедливость арифметических теорем в этой сигнатуре

Попробуем посмотреть, насколько упростится интерпретация, если *слегка* сузить сигнатуру

**Напоминание:** арифметика Пресбургера (АП) — это полная теория интерпретации  $Ar[\mathbb{N}_0; 0; +, \mathbf{s}; =]$

В определении формальной арифметики, в отличие от арифметики Пресбургера, не было требования **полноты** — это намёк на то, что существуют «полезные» полные теории арифметической интерпретации без умножения

**Теорема.** Арифметика Пресбургера разрешима

# Разрешимость АП (доказательство)

$Ar$  — так будем обозначать в доказательстве интерпретацию  $Ar[\mathbb{N}_0; 0; +, s; =]$

Рассмотрим произвольную АП  $\mathcal{T}$

Так как теория  $\mathcal{T}$  полна и  $Ar \models \mathcal{T}$ , для любой формулы  $\varphi(\tilde{x}^n)$  верно

$$\models_{\mathcal{T}} \varphi \iff Ar \models \varphi \iff Ar \models \forall \tilde{x}^n \varphi$$

Значит, чтобы показать разрешимость  $\mathcal{T}$ , достаточно предоставить алгоритм проверки **истинности** произвольного **предложения**  $\varphi$  в  $Ar$

## Разрешимость АП (доказательство)

Заметим (вспомнив и теорему о подстановке определения), что в  $Ar$  выразимы следующие понятия:

- ▶ Заданное число  $\alpha$ ,  $\alpha \in \mathbb{N}_0$ :

$$y = \underbrace{s(s(\dots s(0)\dots))}_{\alpha \text{ раз}}$$

- ▶ Операция  $\beta \cdot \_$  умножения на заданное число  $\beta$ ,  $\beta \in \mathbb{N}_0$ :

$$y = \underbrace{x_1 + x_1 + \dots + x_1}_{\beta \text{ раз}}$$

- ▶ Отношение  $\_ > \_$ :

$$\exists z (x_1 = x_2 + z \ \& \ \neg(z = 0))$$

- ▶ Отношение  $\_ \equiv_\gamma \_$  равенства чисел по заданному модулю  $\gamma$ ,  $\gamma \in \mathbb{N}$ :

$$\exists z (x_1 + \gamma \cdot z = x_2 \ \vee \ x_2 + \gamma \cdot z = x_1)$$

- ▶ Отношения  $\geq$ ,  $<$ ,  $\leq$ ,  $\neq$ ,  $\neq_\gamma$ :

$$x_1 > x_2 \ \vee \ x_1 = x_2 \quad x_2 > x_1 \quad x_2 \geq x_1 \quad \neg(x_1 = x_2) \quad \neg(x_1 \equiv_\gamma x_2)$$

По теореме о подстановке определения, достаточно предоставить алгоритм проверки истинности произвольного предложения  $\varphi$  в интерпретации  $\widetilde{Ar}$ , полученной из  $Ar$  добавлением этих понятий

# Разрешимость АП (доказательство)

$$\widetilde{Ar} \models \varphi ?$$

*Самый простой случай:*  $\varphi$  — атомарное предложение

Тогда проверка соотношения  $\widetilde{Ar} \models \varphi$  — это проверка того, входят ли числа, являющиеся значениями выражений над  $\mathbb{N}_0$ ,  $+$ ,  $\mathbf{s}$  и  $\beta \cdot \_$ , в заданное отношение:  $>$ ,  $\geq$ ,  $<$ ,  $\leq$ ,  $=$ ,  $\neq$ ,  $\equiv_\alpha$  или  $\not\equiv_\alpha$

*Алгоритмы вычисления значений таких выражений и проверки таких соотношений вам должны быть уже знакомы*

# Разрешимость АП (доказательство)

$$\widetilde{A}r \models \varphi ?$$

Будем называть формулу **бескванторной**, если она не содержит ни одного квантора

*Простой случай:*  $\varphi$  — бескванторное предложение

Тогда проверку соотношения  $\widetilde{A}r \models \varphi$  можно устроить так (рекурсивно):

▶  $\varphi = \psi_1 \ \& \ \psi_2$ :

$$\widetilde{A}r \models \varphi \quad \Leftrightarrow \quad \widetilde{A}r \models \psi_1 \text{ и } \widetilde{A}r \models \psi_2$$

▶  $\varphi = \psi_1 \ \vee \ \psi_2$ :

$$\widetilde{A}r \models \varphi \quad \Leftrightarrow \quad \widetilde{A}r \models \psi_1 \text{ или } \widetilde{A}r \models \psi_2$$

▶  $\varphi = \psi_1 \rightarrow \psi_2$ :

$$\widetilde{A}r \models \varphi \quad \Leftrightarrow \quad \widetilde{A}r \not\models \psi_1 \text{ или } \widetilde{A}r \models \psi_2$$

▶  $\varphi = \neg\psi_1$ :

$$\widetilde{A}r \models \varphi \quad \Leftrightarrow \quad \widetilde{A}r \not\models \psi_1$$

▶  $\varphi$  — атом: это **самый простой случай**

# Разрешимость АП (доказательство)

$$\widetilde{A}r \models \varphi ?$$

*Общий случай:*  $\varphi$  — произвольное предложение

Покажем, как можно свести общий случай к простому:  
преобразовать  $\varphi$  в бескванторное предложение  $\psi$ , такое что

$$\widetilde{A}r \models \varphi \Leftrightarrow \widetilde{A}r \models \psi$$

**Лемма (об элиминации квантора  $\exists$ ).** Для любой формулы вида  $\exists x \varphi(x, \widetilde{x}^n)$ , где  $\varphi$  — бескванторная формула, существует бескванторная формула  $\psi(\widetilde{x}^n)$ , реализующая в  $\widetilde{A}r$  то же отношение

## Лемма об элиминации квантора $\exists$ (доказательство)

$$\exists x \varphi(x, \tilde{x}^n) \rightsquigarrow \psi(\tilde{x}^n)$$

Используя **основные равносильности**, можно:

- ▶ преобразовать  $\varphi$  в равносильную

**дизъюнктивную нормальную форму (ДНФ):**

$$\varphi \sim \exists x (L_1 \& \dots \& L_p \vee L'_1 \& \dots \& L'_q \vee \dots)$$

- ▶ вынести за квантор слагаемые ДНФ, не содержащие  $x$ :

$$\exists x (\chi_2(x, \tilde{x}^n) \vee \chi_1(\tilde{x}^n)) \sim \exists x (\chi_1(\tilde{x}^n) \vee \chi_2(x, \tilde{x}^n)) \sim \chi_1(\tilde{x}^n) \vee \exists x \chi_2(x, \tilde{x}^n)$$

- ▶ распространить квантор по слагаемым, оставшимся в ДНФ:

$$\exists x (K_1 \vee \dots \vee K_m) \sim \exists x K_1 \vee \dots \vee \exists x K_m$$

Осталось показать, как преобразовать каждую формулу  $\exists x K_i(x, \tilde{x}^n)$  в бескванторную формулу  $\psi_i(\tilde{x}^n)$ , реализующую то же отношение в  $\bar{A}r$

## Лемма об элиминации квантора $\exists$ (доказательство)

$$\exists x K_i(x, \tilde{x}^n) \rightsquigarrow \psi_i(\tilde{x}^n)$$

$K_i$  — это слагаемое ДНФ, то есть конъюнкция атомов и их отрицаний

Заменим каждое отрицание атома в  $K_i$

на атом с противоположным отношением:

$$\neg(t_1 < t_2) \text{ — на } t_1 \geq t_2,$$

$$\neg(t_1 = t_2) \text{ — на } t_1 \neq t_2,$$

...

В результате получится конъюнкция атомов  $K'_i$ , реализующая то же отношение, что и  $K_i$

Арифметический смысл такой конъюнкции атомов — это **система линейных (не)равенств**  $\Sigma$  над переменными  $x, \tilde{x}^n$

Осталось показать, как можно **спроектировать**  $\Sigma$  по переменной  $x$ : преобразовать  $\Sigma$  в совокупность  $\Delta$  систем над  $\tilde{x}^n$  так, чтобы набор  $(a_1, \dots, a_n)$  был решением  $\Delta$  тогда и только тогда, когда существует число  $a$ , такое что  $(a, a_1, \dots, a_n)$  — решение системы  $\Sigma$

## Лемма об элиминации квантора $\exists$ (доказательство)

$$\Sigma(x, \tilde{x}^n) \stackrel{\exists x}{\rightsquigarrow} \Delta(\tilde{x}^n)$$

Равенства и неравенства из  $\Sigma$  имеют вид

$$\begin{array}{cccc} t_1 = t_2 & t_1 < t_2 & t_1 \leq t_2 & t_1 \equiv_{\gamma} t_2 \\ t_1 \neq t_2 & t_1 > t_2 & t_1 \geq t_2 & t_1 \not\equiv_{\gamma} t_2, \end{array}$$

где  $t_1$  и  $t_2$  — выражения, состоящие из чисел  $\mathbb{N}_0$  и операций  $\mathbf{s}$ ,  $+$ , и  $\beta \cdot \_$

С использованием несложных известных

**арифметических равносильностей** можно привести эти элементы к виду:

$$\begin{array}{cccc} \alpha x + t_1 = t_2 & \alpha x + t_1 < t_2 & \alpha x + t_1 \leq t_2 & \alpha x + t_1 \equiv_{\gamma} t_2 \\ \alpha x + t_1 \neq t_2 & \alpha x + t_1 > t_2 & \alpha x + t_1 \geq t_2 & \alpha x + t_1 \not\equiv_{\gamma} t_2, \end{array}$$

где  $t_1$  и  $t_2$  — выражения того же вида, не содержащие  $x$

## Лемма об элиминации квантора $\exists$ (доказательство)

$$\Sigma(x, \tilde{x}^n) \stackrel{\exists x}{\rightsquigarrow} \Delta(\tilde{x}^n)$$

Перейдя от системы к совокупности систем, можно устранить атомы четырёх видов:

$$A \not\equiv_{\gamma} B \Leftrightarrow \begin{cases} A \equiv_{\gamma} B + 1 \\ A \equiv_{\gamma} B + 2 \\ \dots \\ A \equiv_{\gamma} B + (\gamma - 1) \end{cases} \quad A \geq B \Leftrightarrow \begin{cases} A = B \\ A > B \end{cases}$$

$$A \neq B \Leftrightarrow \begin{cases} A > B \\ A < B \end{cases} \quad A \leq B \Leftrightarrow \begin{cases} A = B \\ A < B \end{cases}$$

Осталось показать, как можно спроектировать по  $x$  систему  $\Sigma$  уравнений и неравенств вида

$\alpha x + t_1 = t_2$      $\alpha x + t_1 < t_2$      $\alpha x + t_1 > t_2$      $\alpha x + t_1 \equiv_{\gamma} t_2$ ,  
 где  $t_1$  и  $t_2$  — выражения, состоящие из чисел  $\mathbb{N}_0$  и операций  $s$ ,  $+$ , и  $\beta$ .

## Лемма об элиминации квантора $\exists$ (доказательство)

$$\Sigma(x, \tilde{x}^n) \stackrel{\exists x}{\rightsquigarrow} \Delta(\tilde{x}^n)$$

Если  $\Sigma$  содержит хотя бы одно равенство  $=$ , то исключить  $x$  можно так:

$$\begin{cases} \alpha x + t_1 = t_2 \\ \beta x + t_3 > t_4 \\ \dots \end{cases} \Leftrightarrow \begin{cases} \alpha x + t_1 = t_2 \\ \alpha\beta x + \alpha t_3 > \alpha t_4 \\ \dots \end{cases} \Leftrightarrow \begin{cases} \alpha x + t_1 = t_2 \\ \alpha t_3 + \beta t_2 > \alpha t_4 + \beta t_1 \\ \dots \end{cases}$$

$$\begin{cases} \alpha x + t_1 = t_2 \\ \beta x + t_3 < t_4 \\ \dots \end{cases} \Leftrightarrow \begin{cases} \alpha x + t_1 = t_2 \\ \alpha\beta x + \alpha t_3 < \alpha t_4 \\ \dots \end{cases} \Leftrightarrow \begin{cases} \alpha x + t_1 = t_2 \\ \alpha t_3 + \beta t_2 < \alpha t_4 + \beta t_1 \\ \dots \end{cases}$$

$$\begin{cases} \alpha x + t_1 = t_2 \\ \beta x + t_3 \equiv_{\gamma} t_4 \\ \dots \end{cases} \Leftrightarrow \begin{cases} \alpha x + t_1 = t_2 \\ \alpha\beta x + \alpha t_3 \equiv_{\alpha\gamma} \alpha t_4 \\ \dots \end{cases} \Leftrightarrow \begin{cases} \alpha x + t_1 = t_2 \\ \alpha t_3 + \beta t_2 \equiv_{\alpha\gamma} \alpha t_4 + \beta t_1 \\ \dots \end{cases}$$

$$\begin{cases} \alpha x + t_1 = t_2 \\ \Sigma'(\tilde{x}^n) \end{cases} \Leftrightarrow_{(\tilde{x}^n)} \begin{cases} t_1 \equiv_{\alpha} t_2 \\ t_2 \geq t_1 \\ \Sigma'(\tilde{x}^n) \end{cases}$$

Пусть теперь система  $\Sigma$  не содержит равенств  $=$

## Лемма об элиминации квантора $\exists$ (доказательство)

$$\Sigma(x, \tilde{x}^n) \stackrel{\exists x}{\rightsquigarrow} \Delta(\tilde{x}^n)$$

Во всех строгих неравенствах системы  
можно получить одинаковые левые части:

$$\left\{ \begin{array}{l} \alpha x + t_1 \geq t_2 \\ \beta x + t_3 \geq t_4 \\ \dots \end{array} \right. \Leftrightarrow \left\{ \begin{array}{l} \alpha\beta x + \beta t_1 \geq \beta t_2 \\ \alpha\beta x + \alpha t_3 \geq \alpha t_4 \\ \dots \end{array} \right. \Leftrightarrow \left\{ \begin{array}{l} \alpha\beta x + \beta t_1 + \alpha t_3 \geq \beta t_2 + \alpha t_3 \\ \alpha\beta x + \beta t_1 + \alpha t_3 \geq \alpha t_4 + \beta t_1 \\ \dots \end{array} \right.$$

Если система содержит много строгих неравенств *в одну сторону*  
с одинаковыми левыми частями, то можно исключить  $x$   
из всех неравенств, кроме одного:

$$\left\{ \begin{array}{l} \alpha x + t > t_1 \\ \alpha x + t > t_2 \\ \dots \end{array} \right. \Leftrightarrow \left\{ \begin{array}{l} \left[ \begin{array}{l} \left\{ \begin{array}{l} \alpha x + t > t_1 \\ t_1 \geq t_2 \\ \alpha x + t > t_2 \\ t_2 \geq t_1 \end{array} \right. \\ \dots \end{array} \right. \end{array} \right. \quad \left\{ \begin{array}{l} \alpha x + t < t_1 \\ \alpha x + t < t_2 \\ \dots \end{array} \right. \Leftrightarrow \left\{ \begin{array}{l} \left[ \begin{array}{l} \left\{ \begin{array}{l} \alpha x + t < t_1 \\ t_1 \leq t_2 \\ \alpha x + t < t_2 \\ t_2 \leq t_1 \end{array} \right. \\ \dots \end{array} \right. \end{array} \right.$$

## Лемма об элиминации квантора $\exists$ (доказательство)

$$\Sigma(x, \tilde{x}^n) \stackrel{\exists x}{\rightsquigarrow} \Delta(\tilde{x}^n)$$

Равенства по модулю разных чисел можно привести к равенствам по модулю одного числа:

$$\begin{cases} \alpha x + t_1 \equiv_{\gamma} t_2 \\ \beta x + t_3 \equiv_{\delta} t_4 \\ \dots \end{cases} \Leftrightarrow \begin{cases} \alpha\delta x + \delta t_1 \equiv_{\gamma\delta} \delta t_2 \\ \beta\gamma x + \gamma t_3 \equiv_{\gamma\delta} \gamma t_4 \\ \dots \end{cases}$$

Осталось показать, как исключить  $x$  из системы, содержащей

- ▶ не более одного неравенства  $\alpha x + t > t_1$ ,
- ▶ не более одного неравенства  $\alpha x + t < t_2$  с той же левой частью и
- ▶ произвольное число равенств  $\beta_i x + t_3^i \equiv_{\gamma} t_4^i$   
по одинаковому модулю  $\gamma$

## Лемма об элиминации квантора $\exists$ (доказательство)

$$\left\{ \begin{array}{l} [\alpha x + t > t_1] \\ [\alpha x + t < t_2] \\ \beta x + t_3 \equiv_{\gamma} t_4 \\ \dots \end{array} \right. \stackrel{\exists x}{\rightsquigarrow} \Delta(\tilde{x}^n)$$

Для каждого решения  $(\delta, \tilde{\delta}^n)$  системы, такого что  $t[\tilde{\delta}^n] \leq t_1[\tilde{\delta}^n]$ , найдётся такое решение  $(\delta', \tilde{\delta}^n)$ , отличающееся только значением  $x$ :

$$(\alpha x + t)[\delta', \tilde{\delta}^n] \in \{t_1 + 1, t_1 + 2, \dots, t_1 + \alpha\gamma\}$$

Значит, неравенство  $\alpha x + t > t_1$  можно заменить на совокупность

$$\left[ \begin{array}{l} t > t_1 \\ \alpha x + t = t_1 + 1 \\ \alpha x + t = t_1 + 2 \\ \dots \\ \alpha x + t = t_1 + \alpha\gamma \end{array} \right.$$

Устранение  $x$  из систем с = обсуждалось ранее

Так можно устранить  $>$  из рассматриваемой системы

## Лемма об элиминации квантора $\exists$ (доказательство)

$$\left\{ \begin{array}{l} [\alpha x + t < t_1] \\ \beta x + t_2 \equiv_{\gamma} t_3 \\ \dots \end{array} \right. \stackrel{\exists x}{\rightsquigarrow} \Delta(\tilde{x}^n)$$

$$\left\{ \begin{array}{l} [\alpha x + t < t_1] \\ \beta x + t_2 \equiv_{\gamma} t_3 \\ \dots \end{array} \right. \Leftrightarrow \left[ \begin{array}{l} \left\{ \begin{array}{l} [t < t_1] \\ t_2 \equiv_{\gamma} t_3 \\ \dots \end{array} \right. \\ \left\{ \begin{array}{l} [\alpha + t < t_1] \\ \beta + t_2 \equiv_{\gamma} t_3 \\ \dots \end{array} \right. \\ \dots \\ \left\{ \begin{array}{l} [\alpha(\gamma - 1) + t < t_1] \\ \beta(\gamma - 1) + t_2 \equiv_{\gamma} t_3 \\ \dots \end{array} \right. \end{array} \right.$$

## Разрешимость АП (доказательство)

**Лемма (об элиминации квантора  $\forall$ ).** Для любой формулы вида  $\forall x \varphi(x, \tilde{x}^n)$ , где  $\varphi$  — бескванторная формула, существует бескванторная формула  $\psi(\tilde{x}^n)$ , реализующая в  $\tilde{Ar}$  то же отношение

**Доказательство.**

Согласно **основным равносильностям**,  $\forall x \varphi(x, \tilde{x}^n) \sim \neg \exists x \neg \varphi(x, \tilde{x}^n)$

По **предыдущей лемме**, существует бескванторная формула  $\psi'(\tilde{x}^n)$ , реализующая в  $\tilde{Ar}$  то же отношение, что и  $\exists x \neg \varphi(x, \tilde{x}^n)$

Тогда  $\psi = \neg \psi'$  — требуемая формула **▼ (леммы)**

**Возвращаемся к общему случаю:**  $\varphi$  — произвольная  $\rightsquigarrow \psi$  — бескванторная

Для преобразования произвольного предложения в бескванторное, достаточно конечное число раз применить

**леммы об элиминации кванторов  $\exists$  и  $\forall$ ,**

устраняя кванторы по одному от внутренних к внешним **▼**

## Выразительность АП (теорема)

Отношение  $R$  выразимо в  $Ar[\mathbb{N}_0; 0; +, s; =]$  тогда и только тогда, когда оно является множеством решений какой-либо совокупности систем линейных (не)равенств  $=, \neq, >, <, \geq, \leq, \equiv_\alpha, \not\equiv_\alpha$  над  $\mathbb{N}_0$

Доказательство.

( $\Rightarrow$ ) Рассмотрим формулу  $\varphi(\tilde{x}^n)$ , реализующую отношение  $R$ . Согласно **общему случаю** в доказательстве теоремы о разрешимости АП, существует **бескванторная** формула  $\psi(\tilde{x}^n)$ , реализующая отношение  $R$ .

Применяя **законы булевой алгебры**,

можно преобразовать  $\psi$  в равносильную ДНФ  $\chi$ .

Арифметическая трактовка  $\chi$  — это совокупность систем линейных (не)равенств: отношение, реализуемое  $\chi$ , совпадает с множеством решений совокупности систем, записанной в форме ДНФ.

( $\Leftarrow$ ) Совокупность систем  $\Sigma$  указанного вида может быть представлена в виде соответствующей ДНФ  $\varphi$ , и тогда формулой  $\varphi$  реализуется множество решений  $\Sigma$  ▼

# Аксиомы АП

Один из известных наборов аксиом арифметики Пресбургера устроен так ( $\mathcal{T}$ ):

- ▶  $\forall x (x + 0 = x)$
- ▶  $\forall x \forall y (x + \mathbf{s}(y) = \mathbf{s}(x + y))$
- ▶  $\forall x (x = x)$
- ▶  $\forall x \forall y ((x = y) \rightarrow (y = x))$
- ▶  $\forall x \forall y \forall z ((x = y) \& (y = z) \rightarrow (x = z))$
- ▶  $\forall x \forall y ((x = y) \rightarrow (\mathbf{s}(x) = \mathbf{s}(y)))$
- ▶  $\forall x \forall y ((\mathbf{s}(x) = \mathbf{s}(y)) \rightarrow (x = y))$
- ▶  $\forall x \neg(0 = \mathbf{s}(x))$
- ▶  $\varphi\{x/0\} \& \forall x (\varphi \rightarrow \varphi\{x/\mathbf{s}(x)\}) \rightarrow \forall x \varphi,$   
где  $\varphi$  — произвольная формула с одной свободной переменной  $x$

Можно легко убедиться, что  $Ar[\mathbb{N}_0; 0; +, \mathbf{s}; =] \models \mathcal{T}$

А доказать полноту этой теории можете попробовать самостоятельно