Математическая логика: 5

Станислав Олегович Сперанский

Санкт-Петербургский государственный университет

Санкт-Петербург 2020

Теорема

$\mathrm{Th}\,(\mathfrak{Z}^{\equiv})$ *допускает эффективную элиминацию кванторов.*

Доказательство.

Начнём с частного, но принципиального случая. Пусть $\Omega_0, \ldots, \Omega_n$ — атомарные $\sigma^{\equiv}$-формулы, а x — переменная. Возьмём

$$\Theta \;:=\; \Omega_0 \wedge \cdots \wedge \Omega_n.$$

Давайте эффективно построим $\Theta_{\exists x} \in \mathrm{Form}^{\circ}_{\sigma^{\equiv}}$ такую, что

$$\mathrm{Th}\,(\mathfrak{Z}^{\equiv}) \vdash \exists x\,\Theta \leftrightarrow \Theta_{\exists x} \quad \text{и} \quad \mathrm{FV}\,(\Theta_{\exists x}) \;\subseteq\; \mathrm{FV}\,(\exists x\,\Theta).$$

Обозн. за $\mathrm{Term}^{-x}_{\sigma^{\equiv}}$ множество всех $\sigma^{\equiv}$-термов, в которые не входит x.

. . .

Доказательство (продолжение).

Заметим, что для любого $i \in \{0, \ldots, n\}$:

- если Ω_i — равенство или неравенство, то

$$\mathrm{Th}\left(\mathfrak{Z}^{\equiv}\right) \vdash \Omega_i \leftrightarrow k_i x = t_i \quad \text{или} \quad \mathrm{Th}\left(\mathfrak{Z}^{\equiv}\right) \vdash \Omega_i \leftrightarrow k_i x \leqslant t_i$$

  для подходящих $k_i \in \mathbb{N}$ и $t_i \in \mathrm{Term}_{\sigma\equiv}^{-x}$;

- если Ω_i — сравнение по модулю, то

$$\mathrm{Th}\left(\mathfrak{Z}^{\equiv}\right) \vdash \Omega_i \leftrightarrow k_i x \equiv_{m_i} t_i$$

  для подходящих $k_i \in \mathbb{N}$, $t_i \in \mathrm{Term}_{\sigma\equiv}^{-x}$ и $m_i \in \mathbb{N} \setminus \{0, 1\}$.

Не ограничивая общности, мы будем считать, что $\Omega_0, \ldots, \Omega_n$ имеют соответствующий вид.

...

Доказательство (продолжение).

Далее, мы можем считать, что x входит в каждую из $\Omega_0, \ldots, \Omega_n$, т.е. $k_i > 0$ для всех $i \in \{0, \ldots, n\}$. Возьмём

$$K \;:=\; \text{наименьшее общее кратное } k_0, \ldots, k_n.$$

Унифицируем коэффициенты при x следующим образом.

- Если Ω_i — равенство или неравенство, то «домножим» обе его части на K/k_i.
- Если Ω_i — сравнение по модулю, то «домножим» обе его части и модуль сравнения на K/k_i.

...

Доказательство (продолжение).

Поскольку для всех $k \in \mathbb{N} \setminus \{0\}$ и каждого $m \in \mathbb{N} \setminus \{0, 1\}$,

$$\mathrm{Th}\,(\mathfrak{Z}^{\equiv}) \vdash x = y \leftrightarrow kx = ky,$$
$$\mathrm{Th}\,(\mathfrak{Z}^{\equiv}) \vdash x < y \leftrightarrow kx < ky,$$
$$\mathrm{Th}\,(\mathfrak{Z}^{\equiv}) \vdash x \equiv_m y \leftrightarrow kx \equiv_{km} ky,$$

в результате получатся эквивалентные атомарные $\sigma^{\equiv}$-формулы:

$$\Omega'_0, \quad \ldots, \quad \Omega'_n,$$

в которых коэффициенты при x совпадают с K. Разумеется,

$$\mathrm{Th}\,(\mathfrak{Z}^{\equiv}) \vdash \Theta \leftrightarrow (\Omega'_0 \wedge \cdots \wedge \Omega'_n).$$

. . .

Доказательство (продолжение).

Более того, коэффициент при x можно сделать равным 1 с помощью следующего трюка. Для всякого $i \in \{0, \ldots, n\}$ положим

$$\Omega_i^* \;:=\; \text{результат замены } Kx \text{ в } \Omega_i' \text{ на } x.$$

Тогда, как легко убедиться,

$$\mathrm{Th}\,(\mathfrak{Z}^{\equiv}) \vdash \exists x\, \Theta \leftrightarrow \exists x\, (\Omega_0^* \wedge \cdots \wedge \Omega_n^* \wedge x \equiv_K 0).$$

где $x \equiv_K 0$ при $K = 1$ отождествляется с $\top$. Для удобства обозначим

$$\widehat{\Theta} \;:=\; \Omega_0^* \wedge \cdots \wedge \Omega_n^* \wedge x \equiv_K 0.$$

. . .

Доказательство (продолжение).

Теперь нужно избавиться от квантора в $\exists x\,\widehat{\Theta}$. Если один из конъюнктов $\widehat{\Theta}$ имеет вид $x = t$, то

$$\vdash \exists x\,\widehat{\Theta} \leftrightarrow \widehat{\Theta}\,(x/t).$$

Будем считать, что среди конъюнктов $\widehat{\Theta}$ нет равенств. Положим

$$T_- \;:=\; \text{множество всех «нижних граней» для } x \text{ в } \widehat{\Theta},$$
$$T_+ \;:=\; \text{множество всех «верхних граней» для } x \text{ в } \widehat{\Theta}.$$

Очевидно, T_- и T_+ суть конечные подмножества $\mathrm{Term}_{\sigma\equiv}^{-x}$. Возьмём

$$M \;:=\; \begin{array}{c}\text{наименьшее общее кратное всех модулей,}\\ \text{по которым ведутся сравнения в } \widehat{\Theta}.\end{array}$$

. . .

Доказательство (продолжение).

Теперь рассмотрим

$$\begin{aligned} T_\star \;:=\; & \{t + \underline{m} \mid t \in T_- \text{ и } 1 \leqslant m \leqslant M\} \cup \\ & \{t - \underline{m} \mid t \in T_+ \text{ и } 1 \leqslant m \leqslant M\} \cup \\ & \{\underline{m} \mid 1 \leqslant m \leqslant M\}. \end{aligned}$$

Очевидно, $T_\star$ — конечное подмножество $\mathrm{Term}_{\sigma^{\equiv}}^{-x}$. Утверждается, что

$$\mathrm{Th}\,(\mathfrak{Z}^{\equiv}) \vdash \exists x\, \widehat{\Theta} \leftrightarrow \bigvee_{t \in T_\star} \widehat{\Theta}\,(x/t).$$

т.е. можно определить $\Theta_{\exists x}$ как $\bigvee_{t \in T_\star} \widehat{\Theta}\,(x/t)$.

. . .

Доказательство (продолжение).

$\boxed{\leftarrow}$ Очевидно.

$\boxed{\rightarrow}$ Мы будем рассуждать *внутри* $\mathrm{Th}\,(\mathfrak{Z}^{\equiv})$. С учётом BR2 достаточно получить

$$\widehat{\Theta}\,(x/x) \to \bigvee_{t \in T_\star} \widehat{\Theta}\,(x/t).$$

Пусть $\widehat{\Theta}\,(x/x)$. Покажем, что $\widehat{\Theta}\,(x/t)$ для некоторого $t \in T_\star$.

i. Пусть $T_- = T_+ = \varnothing$, т.е. $\widehat{\Theta}$ — конъюнк. сравнений по модулю. Разумеется, найдётся $t \in \{\underline{1}, \ldots, \underline{M}\}$, которое сравнимо с x по всем встречающимся в $\widehat{\Theta}$ модулям. Тогда $\widehat{\Theta}\,(x/t)$.

...

Доказательство (продолжение).

ii. Пусть T_- непусто. Для удобства обозначим

$$t_{\max} \;:=\; \text{наибольший элемент } T_-.$$

Очевидно, $t_{\max} < x$. Если $x \leqslant t_{\max} + \underline{M}$, то

$$x \;=\; t_{\max} + \underline{m} \quad \text{для некоторого } m \in \{1, \ldots, M\},$$

откуда $\widehat{\Theta}\,(x / t_{\max} + \underline{m})$. Если $t_{\max} + \underline{M} < x$, то

$$t_{\max} + \underline{1}, \quad \ldots, \quad t_{\max} + \underline{M}$$

будут удовлетворять всем неравенствам в $\widehat{\Theta}$, причём один из них будет сравним с x по всем встречающимся в $\widehat{\Theta}$ модулям, а значит, удовлетворять всей $\widehat{\Theta}$.

iii. Пусть T_+ непусто. Тогда можно рассуждать по аналогии с (ii).

...

Доказательство (продолжение).

Общий случай сводится к частному так же, как и ранее; при этом от $\neg$ перед атомарными подформулами можно избавиться, используя

$$\mathrm{Th}\,(\mathfrak{Z}^{\equiv}) \vdash \neg x = y \leftrightarrow (x < y \vee y < x),$$
$$\mathrm{Th}\,(\mathfrak{Z}^{\equiv}) \vdash \neg x < y \leftrightarrow (x = y \vee y < x),$$
$$\mathrm{Th}\,(\mathfrak{Z}^{\equiv}) \vdash \neg x \equiv_m y \leftrightarrow (x \equiv_m y + \underline{1} \vee \cdots \vee x \equiv_m y + \underline{m-1}),$$

где $m \in \mathbb{N} \setminus \{0, 1\}$. В итоге мы получим желаемую τ. $\square$

Следствие

$\mathrm{Th}\,(\mathfrak{Z}^{\equiv})$ *и* $\mathrm{Th}\,(\mathfrak{Z})$ *разрешимы.*

Доказательство.

Достаточно показать разрешимость $\mathrm{Th}\,(\mathfrak{Z}^{\equiv}) \cap \mathrm{Form}^{\circ}_{\sigma^{\equiv}}$. Заметим, что любое ат. $\sigma^{\equiv}$-предложение можно эффективным образом привести к одному из видов

$$\underline{n} = 0, \quad \underline{n} < 0, \quad 0 < \underline{n} \quad \text{или} \quad \underline{n} \equiv_m 0,$$

где $n \in \mathbb{N}$ и $m \in \{2, 3, 4, \dots\}$; поэтому проблема истинности в $\mathfrak{Z}^{\equiv}$ для ат. $\sigma^{\equiv}$-предложений разрешима. Стало быть, проблема истинности в $\mathfrak{Z}^{\equiv}$ для бесквантворных $\sigma^{\equiv}$-предложений также разрешима. □

Замечание

Очевидно, $\mathrm{Th}\left(\mathfrak{Z}^{\equiv}\right)$ непротиворечиво и полно. Поэтому разрешимость $\mathrm{Th}\left(\mathfrak{Z}^{\equiv}\right)$ можно было бы попробовать доказать посредством нахождения перечислимого $\Gamma \subseteq \mathrm{Sent}_{\sigma^{\equiv}}$ такого, что $[\Gamma] = \mathrm{Th}\left(\mathfrak{Z}^{\equiv}\right)$, т.е.

$$\mathfrak{Z}^{\equiv} \Vdash \Gamma \quad \text{и} \quad [\Gamma] \text{ полно.}$$

Здесь возникают следующие трудности.

- Если в качестве Γ взять какое-н. естественное перечислимое множество $\sigma^{\equiv}$-предложений, истинных в $\mathfrak{Z}^{\equiv}$, то не ясно, как показать его полноту.
- Если в качестве Γ взять саму $\mathrm{Th}\left(\mathfrak{Z}^{\equiv}\right)$, то, напротив, не ясно, как показать его перечислимость.

На самом деле, нужное (и довольно естественное) $\Gamma \subseteq \mathrm{Sent}_{\sigma^{\equiv}}$ можно извлечь из эф. элиминации кванторов в $\mathrm{Th}\left(\mathfrak{Z}^{\equiv}\right)$. Кроме того, с помощью этого Γ легко получить $\Delta \subseteq \mathrm{Sent}_{\sigma}$ такое, что $[\Delta] = \mathrm{Th}\left(\mathfrak{Z}\right)$.

Следствие

Для любого $S \subseteq \mathbb{Z}$ следующие условия эквивалентны:

i. *S определимо в $\mathfrak{Z}$;*

ii. *S определимо в $\mathfrak{Z}^{\equiv}$;*

iii. *S определимо в $\mathfrak{Z}^{\equiv}$ посредством бескванторной формулы.* □

Замечание

Так как каждый элемент $\mathbb{Z}$ определим в $\mathfrak{Z}$, группы автоморфизмов $\mathfrak{Z}$ и $\mathfrak{Z}^{\equiv}$ тривиальны, т.е.

$$\mathrm{Aut}\,(\mathfrak{Z}) \;=\; \mathrm{Aut}\,(\mathfrak{Z}^{\equiv}) \;=\; \{\mathrm{id}_{\mathbb{Z}}\}.$$

Поэтому «метод автоморфизмов» бесполезен для анализа определимости в $\mathfrak{Z}$ и $\mathfrak{Z}^{\equiv}$.

Подробнее об определимости в $\mathfrak{Z}$

Для любых $a, b \in \mathbb{Z}$ положим

$$a + b\mathbb{N} \;:=\; \{a + bn \mid n \in \mathbb{N}\}.$$

Множества такого вида мы будем называть арифметическими прогрессиями. В частности, для каждого $a \in \mathbb{Z}$,

$$a + 0\mathbb{N} \;=\; \{a\},$$

так что $\{a\}$ — это арифметическая прогрессия. Далее, говорят, что $S \subseteq \mathbb{Z}$ полулинейно, если S представимо в виде

$$\bigcup \{A_1, \ldots, A_n\} \;=\; A_1 \cup \cdots \cup A_n,$$

где $n \in \mathbb{N}$ и $A_1, \ldots, A_n$ суть арифметические прогрессии; здесь при $n = 0$ получается $\bigcup \varnothing = \varnothing$, а потому $\varnothing$ полулилейно.

Предложение

Пусть $S, P \subseteq \mathbb{Z}$ полулинейны. Тогда $S \cup P$ и $S \cap P$ полулинейны.

Доказательство.

По условию сущ. арифметические прогрессии $A_1, \ldots, A_n$ и $B_1, \ldots, B_m$ такие, что

$$S = A_1 \cup \cdots \cup A_n \quad \text{и} \quad P = B_1 \cup \cdots \cup B_m.$$

Очевидно, $S \cup P$ полулинейно. Кроме того,

$$S \cap P = \bigcup_{i=1}^{n} \bigcup_{j=1}^{m} (A_i \cap B_j).$$

Стало быть, $S \cap P$ полулинейно, поскольку пересечение (двух) арифметических прогрессий снова явл. арифметической прогрессией. $\square$

Для любых $n \in \mathbb{N}_+$ и $t \in \mathrm{Term}_{\sigma\equiv}$ положим

$$\underline{-n} := -\underline{n} \quad \text{и} \quad (-n)\, t := -nt.$$

Эти обозначения позволят нам сократить запись в ряде случаев.

Лемма

Каждое полулинейное подмножество $\mathbb{Z}$ определимо в $\mathfrak{Z}$.

Доказательство.

Для любых $a, b \in \mathbb{Z}$ мы можем определить $a + b\mathbb{N}$ в $\mathfrak{Z}$ посредством σ-формулы

$$\Psi_{a,b}(x) := \exists u\,(0 \leqslant u \wedge x = \underline{a} + bu).$$

Значит, всякое полулинейное подмножество $\mathbb{Z}$ можно определить в $\mathfrak{Z}$ посредством дизъюнкции такого рода σ-формул. При этом под «пустой дизъюнкцией» понимается $\bot$, разумеется. $\square$

Лемма

Каждое подмножество $\mathbb{Z}$, определимое в $\mathfrak{Z}$, полулинейно.

Доказательство.

Пусть $S \subseteq \mathbb{Z}$ определимо в $\mathfrak{Z}$. Тогда, в силу элиминации кванторов в $\mathrm{Th}\,(\mathfrak{Z}^{\equiv})$, найдётся бескванторная $\sigma^{\equiv}$-формула $\Phi\,(x)$, которая определяет S в $\mathfrak{Z}^{\equiv}$, причём можно считать, что:

- $\neg$ не входит в Φ;
- каждая атомарная подформула Φ имеет один из видов

$$ax = \underline{b}, \quad ax < \underline{b} \quad \text{или} \quad ax \equiv_m \underline{b},$$

где $a, b \in \mathbb{Z}$ и $m \in \mathbb{N} \setminus \{0, 1\}$.

Поскольку семейство всех полулин. подмножеств $\mathbb{Z}$ замкнуто относительно конечных объед. и пересеч., достаточно показать, что всякая атомарная подформула Φ определяет в $\mathfrak{Z}^{\equiv}$ полулин. множество.

. . .

Доказательство (продолжение).

Рассмотрим произв. атомарную подформулу Ω в Ф. Если коэфициент при x в Ω равен нулю, то Ω определяет $\varnothing$ или $\mathbb{Z}$ в $\mathfrak{Z}^{\equiv}$. При этом

$$\mathbb{Z} \;=\; (0 + 1\mathbb{N}) \cup (0 + (-1)\,\mathbb{N}).$$

Давайте считать, что коэффициент при x не равен нулю.

- Пусть Ω имеет вид $ax = \underline{b}$, где $a \neq 0$. Если $b/a \in \mathbb{Z}$, то Ω определяет $\{b/a\}$. Иначе Ω определяет $\varnothing$.

. . .

Доказательство (продолжение).

- Пусть Ω имеет вид $ax < \underline{b}$, где $a \neq 0$. Если $b/a \in \mathbb{Z}$ и $a < 0$, то Ω определяет

$$\left\{c \in \mathbb{Z} \mid c > \frac{b}{a}\right\} = \left\{c \in \mathbb{Z} \mid c \geqslant \frac{b}{a} + 1\right\}$$
$$= \left(\frac{b}{a} + 1\right) + 1\mathbb{N}.$$

Если $b/a \notin \mathbb{Z}$ и $a < 0$, то Ω определяет

$$\left\{c \in \mathbb{Z} \mid c > \frac{b}{a}\right\} = \left\{c \in \mathbb{Z} \mid c \geqslant \left\lceil\frac{b}{a}\right\rceil\right\}$$
$$= \left\lceil\frac{b}{a}\right\rceil + 1\mathbb{N}.$$

Аналогично для $a > 0$.

Доказательство (продолжение).

- Пусть Ω имеет вид $ax \equiv_m \underline{b}$, где $a \neq 0$. Если a делится на m, то Ω определяет $\varnothing$ или $\mathbb{Z}$. Поэтому мы будем считать, что a не делится на m. Возьмём

$$d \;:=\; \text{наибольший общий делитель } a \text{ и } m.$$

Если d не делит b, то Ω определяет $\varnothing$; если d делит b, то Ω определяет

$$\begin{aligned}\{c \in \mathbb{Z} \mid ac \equiv b \,(\mathrm{mod}\, m)\} &= \left\{c \in \mathbb{Z} \mid c \equiv c_0 \left(\mathrm{mod}\, \frac{m}{d}\right)\right\} \\ &= \left(c_0 + \frac{m}{d}\mathbb{N}\right) \cup \left(c_0 + \left(-\frac{m}{d}\right)\mathbb{N}\right),\end{aligned}$$

где c_0 — частное решение для $ax \equiv b \,(\mathrm{mod}\, m)$, которое строится эффективно по a, b и m.

Теорема

$S \subseteq \mathbb{Z}$ определимо в $\mathfrak{Z}$ тогда и только тогда, когда S полулинейно.

Доказательство.

Немедленно следует из двух лемм выше. □

Замечание

Очевидно, если $\mathfrak{A}$ — произвольная структура, то семейство всех множеств, определимых в $\mathfrak{A}$, замкнуто относительно дополнений. Стало быть, семество всех полулинейных подмножеств $\mathbb{Z}$ оказывается замкнуто относительно дополнений.

Общие комментарии

- Аналогичные результаты можно получить для подмножеств $\mathbb{Z}^\ell$.
- Полулинейные подмножества $(\mathbb{Z}^\ell)$ тесно связаны с такими разделами теоретической информатики как теория форм. языков и теория автоматов. К комбинаторике они тоже имеют прямое отношение. В общем, как объект изучения они интересны.
- Элиминация кванторов для $\mathrm{Th}\,(\mathfrak{Z}^{\equiv})$ была доказана в магистерской диссертации Моисея Пресбургера; поэтому $\mathrm{Th}\,(\mathfrak{Z})$ обычно называют арифметикой Пресбургера.