Математическая логика: лекция 13

Станислав Олегович Сперанский

Санкт-Петербургский государственный университет

Санкт-Петербург 2020

Сложение на целых числах

Возьмём $\langle =^2, <^2; +^2, -^1; 0, 1\rangle$ в качестве σ.

Обозначим через $\mathfrak{Z}$ стандартную σ-структуру с носителем $\mathbb{Z}$.

Известно, что $\mathrm{Th}\,(\mathfrak{Z})$ не допускает элиминации кванторов, поскольку

$$\{2n \mid n \in \mathbb{Z}\}$$

нельзя определить в $\mathfrak{Z}$ посредством бескванторной формулы; однако элиминацию можно провести в слегка расширенной сигнатуре

$$\sigma^{\equiv} \;:=\; \sigma \cup \{\equiv_2, \equiv_3, \dots\},$$

где $\equiv_2$, $\equiv_3$, ... суть двухместные предикатные символы, интуитивно обозначающие сравнимость по модулям 2, 3, ...

Обозначим через $\mathfrak{Z}^{\equiv}$ стандартную $\sigma^{\equiv}$-структуру с носителем $\mathbb{Z}$.

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

$$nt \;:=\; \underbrace{t + \ldots + t}_{n \text{ штук } t},$$

как это делалось при обсуждении абелевых групп; отождествим $0t$ с 0. Кроме того, для каждого $n \in \mathbb{N}$ обозначим

$$\underline{n} \;:=\; n1.$$

Наконец, вместо $t_1 + (-t_2)$ мы будем нередко писать $t_1 - t_2$.

Замечание

Для каждого $m \in \mathbb{N} \setminus \{0, 1\}$ формула

$$\Phi_m(x, y) \;:=\; \exists z\,(x = y + mz)$$

определяет в $\mathfrak{Z}$ двухместное отношение сравнимости по модулю m, а значит, при переходе от $\mathfrak{Z}$ к $\mathfrak{Z}^{\equiv}$ совокупность всех определимых множеств не меняется.

Замечание

Очевидно, $\mathrm{Th}(\mathfrak{Z})$ сводится к $\mathrm{Th}(\mathfrak{Z}^{\equiv})$. Поскольку $\mathfrak{Z}^{\equiv}$ является «дефинициальным расширением» $\mathfrak{Z}$, верно и обратное. Чтобы убедиться в этом, для всех $t_1, t_2 \in \mathrm{Term}_\sigma$ и $m \in \mathbb{N} \setminus \{0, 1\}$ положим

$$P_m(t_1, t_2) \;:=\; \exists z\,(t_1 = t_2 + mz),$$

где z — первая переменная, не входящая ни в t_1, ни в t_2. Далее, рассмотрим $\eta : \mathrm{Form}_{\sigma\equiv} \to \mathrm{Form}_\sigma$, действующую по правилу

$$\eta(\Phi) \;:=\; \text{результат замены в } \Phi \text{ всех атом. подформул вида } t_1 \equiv_m t_2 \text{ на } P_m(t_1, t_2).$$

Как легко понять, для любой $\Phi \in \mathrm{Sent}_{\sigma\equiv}$,

$$\mathfrak{Z}^{\equiv} \Vdash \Phi \quad\Longleftrightarrow\quad \mathfrak{Z} \Vdash \eta(\Phi).$$

Стало быть, $\mathrm{Th}(\mathfrak{Z}^{\equiv})$ сводится к $\mathrm{Th}(\mathfrak{Z})$. В итоге $\mathrm{Th}(\mathfrak{Z}^{\equiv})$ и $\mathrm{Th}(\mathfrak{Z})$ оказываются эквивалентны с вычислительной точки зрения.

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 $\equiv_K$ при $K = 1$ отождествляется с $=$. 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 $\mathrm{Term}^{-x}_{\sigma^{\equiv}}$. 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. □

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 Φ. 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. $\square$

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 $\mathrm{Th}\,(\mathfrak{Z}^{=})$ была доказана в магистерской диссертации Моисея Пресбургера; поэтому $\mathrm{Th}\,(\mathfrak{Z})$ обычно называют арифметикой Пресбургера.

Явная аксиоматика для $\mathrm{Th}(\mathfrak{Z}^{\equiv})$

Извлечение аксиом из элиминации кванторов — нетривиальная, но сравнительно несложная задача. Обозначим через $\mathrm{ZA}^{\equiv}$ множество, состоящее из *универсальных замыканий* следующих $\sigma^{\equiv}$-формул.

Аксиомы линейно упорядоченных абелевых групп:

- $(x + y) + z = x + (y + z)$,
- $x + y = y + x$,
- $x + 0 = x$,
- $x + (-x) = 0$,
- $x \not< x$,
- $x < y \wedge y < z \to x < z$,
- $x \neq y \to x < y \vee y < x$ и
- $x < y \to x + z < y + z$.

Аксиомы для (нуля и) единицы:

- $0 < 1$ и
- $x \leqslant 0 \vee 1 \leqslant x$.

Аксиомы для сравнений по модулю:

- $x \equiv_m y \leftrightarrow \exists z\, x = y + mz$ и
- $\bigvee_{k=0}^{m-1}(x \equiv_m \underline{k})$ для $m \in \{2, 3, \dots\}$.

Очевидно, $\mathfrak{Z}^{\equiv}$ является моделью $\mathrm{ZA}^{\equiv}$, а потому

$$[\mathrm{ZA}^{\equiv}] \subseteq \mathrm{Th}(\mathfrak{Z}^{\equiv}).$$

Наша ближайшая цель — доказать, что $\mathrm{ZA}^{\equiv}$ выводит все истинные в $\mathfrak{Z}^{\equiv}$ / опровергает все ложные в $\mathfrak{Z}^{\equiv}$ бескв. $\sigma^{\equiv}$-предложения.

Напоминаю, что вместо $-\underline{n}$, где $n \in \mathbb{N}$, мы иногда пишем $\underline{-n}$.

Замечание

Разумеется, как и в теории абелевых групп, в $\mathrm{ZA}^{=}$ выводимы

$$-(x+y) \;=\; (-x)+(-y) \quad \text{и} \quad -(-x) = x.$$

Поэтому, в частности, для каждого $n \in \mathbb{N}$ в $\mathrm{ZA}^{=}$ можно вывести

$$\underline{-n} \;=\; n(-1) \quad \text{и} \quad -(\underline{-n}) \;=\; \underline{n}.$$

Предложение

Пусть $a, b \in \mathbb{Z}$. Тогда $\mathrm{ZA}^{=} \vdash \underline{a} + \underline{b} = \underline{a+b}$.

Доказательство.

Это можно легко получить из аксиом абелевых групп. □

Лемма

Пусть $t \in \mathrm{Term}^{\circ}_{\sigma^{\equiv}}$. *Тогда* $\mathrm{ZA}^{\equiv} \vdash t = \underline{t^{\mathfrak{Z}^{\equiv}}}$.

Доказательство.

Преобразуем t следующим образом.

i. Проносим $-$ внутрь t, чтобы $-$ стояло только перед 0 и 1.

ii. С помощью предложения выше получаем замнутый $\sigma^{\equiv}$-терм вида $\underline{a}$, где $a \in \mathbb{Z}$. В итоге $\mathrm{ZA}^{\equiv} \Vdash t = \underline{a}$; при этом a совпадёт со значением t в $\mathfrak{Z}^{\equiv}$, разумеется.

□

Пример

Рассмотрим замкнутый $\sigma^{\equiv}$-терм

$$t \;:=\; (\underline{1} - (\underline{2} - \underline{5})) + (\underline{3} - \underline{2}).$$

Тогда в $\mathrm{ZA}^{\equiv}$ мы получаем следующую цепочку равенств:

$$\begin{aligned}
(\underline{1} - (\underline{2} - \underline{5})) + (\underline{3} - \underline{2}) &= \\
(\underline{1} + (-(\underline{2} + (-\underline{5})))) + (\underline{3} + (-\underline{2})) &= \\
(\underline{1} + ((-\underline{2}) + (-(-\underline{5})))) + (\underline{3} + (-\underline{2})) &= \\
(\underline{1} + ((-\underline{2}) + \underline{5})) + (\underline{3} + (-\underline{2})) &= \\
(\underline{1} + \underline{3}) + (\underline{3} + (-\underline{2})) &= \\
\underline{4} + (\underline{3} + (-\underline{2})) &= \\
\underline{4} + \underline{1} &= \\
\underline{5}\ .&
\end{aligned}$$

Значит, $\mathrm{ZA}^{\equiv} \Vdash t = \underline{5}$.

Предложение

Пусть $m \in \mathbb{N} \setminus \{0, 1\}$ *и* $k \in \{1, \ldots, m-1\}$. *Тогда* $\mathrm{ZA}^{\equiv} \vdash \neg \underline{k} \equiv_m 0$.

Доказательство.

Будем рассуждать *внутри* $\mathrm{ZA}^{\equiv}$.

Пусть $\underline{k} \equiv_m 0$. Значит, $\underline{k} = mz$ для некоторого z.

- Если $z > 0$, то $z \geqslant 1$, а потому

$$\underline{k} \;=\; mz \;\geqslant\; m1 \;>\; k1 + (m-k)0 \;=\; \underline{k}$$

  — противоречие.

- Если $z \leqslant 0$, то мы получаем

$$0 \;=\; m0 \;\geqslant\; mz \;=\; \underline{k} \;>\; k0 \;=\; 0$$

  — противоречие.

□

Лемма

Для любого атомарного $\sigma^{\equiv}$-предложения Ω:

i. *если* $\mathfrak{Z}^{\equiv} \Vdash \Omega$, *то* $\mathsf{ZA}^{\equiv} \vdash \Omega$;

ii. *если* $\mathfrak{Z}^{\equiv} \nVdash \Omega$, *то* $\mathsf{ZA}^{\equiv} \vdash \neg\Omega$.

Доказательство.

i. Пусть $\mathfrak{Z}^{\equiv} \Vdash \Omega$. Разумеется, Ω имеет вид $t_1 \circ t_2$, где $t_1, t_2 \in \mathrm{Term}^{\circ}_{\sigma^{\equiv}}$ и $\circ \in \{=, <, \equiv_2, \equiv_3, \dots\}$. Для удобства обозначим

$$a_1 := t_1^{\mathfrak{Z}^{\equiv}} \quad \text{и} \quad a_2 := t_2^{\mathfrak{Z}^{\equiv}}.$$

В силу леммы выше, в $\mathsf{ZA}^{\equiv}$ выводимы $t_1 = \underline{a_1}$ и $t_2 = \underline{a_2}$.

...

Доказательство (продолжение).

- Пусть Ω имеет вид $t_1 = t_2$. Тогда a_1 равно a_2. Поэтому в $\mathrm{ZA}^{=}$ выводимо

$$t_1 \;=\; \underline{a_1} \;=\; \underline{a_2} \;=\; t_2.$$

- Пусть Ω имеет вид $t_1 < t_2$. Тогда a_1 (строго) меньше a_2. Поэтому в $\mathrm{ZA}^{=}$ выводимо

$$\begin{aligned} t_2 \;=\; \underline{a_2} \;=\; \underline{a_1} + \underline{a_2 - a_1} \;&=\; \underline{a_1} + (a_2 - a_1)\,1 \\ &>\; \underline{a_1} + (a_2 - a_1)\,0 \;=\; \underline{a_1} \;=\; t_1. \end{aligned}$$

. . .

Доказательство (продолжение).

- Пусть Ω имеет вид $t_1 \equiv_m t_2$. Тогда a_1 равно $a_2 + mb$ для нек. $b \in \mathbb{Z}$. Поэтому в $\mathrm{ZA}^{\equiv}$ выводимо

$$t_1 \;=\; \underline{a_1} \;=\; \underline{a_2 + mb} \;=\; \underline{a_2} + m\underline{b} \;=\; t_2 + m\underline{b}.$$

Стало быть, $\mathrm{ZA}^{\equiv} \vdash \exists z\, t_1 = t_2 + mz$. Значит, $\mathrm{ZA}^{\equiv} \vdash t_1 \equiv_m t_2$.

ii. Нетрудно убедиться, что в $\mathrm{ZA}^{\equiv}$ выводимы

$$\neg x = y \leftrightarrow (x < y \vee y < x),$$
$$\neg x < y \leftrightarrow (x = y \vee y < x) \quad \text{и}$$
$$\neg x \equiv_m y \leftrightarrow (x \equiv_m y + \underline{1} \vee \cdots \vee x \equiv_m y + \underline{m-1}),$$

где $m \in \mathbb{N} \setminus \{0, 1\}$. Поэтому (ii) можно получить из (i). □

Предложение

Для любого бескванторного $\sigma^{\equiv}$-предложения Φ:

i. *если* $\mathfrak{Z}^{\equiv} \Vdash \Phi$, *то* $\mathrm{ZA}^{\equiv} \vdash \Phi$;

ii. *если* $\mathfrak{Z}^{\equiv} \nVdash \Phi$, *то* $\mathrm{ZA}^{\equiv} \vdash \neg\Phi$.

Доказательство.

Индукция по построению Φ, причём сразу для обоих пунктов.

- Пусть $\Phi \in \mathrm{At}_{\sigma}$. Тогда всё следует из леммы выше.
- Пусть $\Phi = \neg\Psi$. Если $\mathfrak{Z}^{\equiv} \Vdash \Phi$, то $\mathfrak{Z}^{\equiv} \nVdash \Psi$, а потому $\mathrm{ZA}^{\equiv} \vdash \neg\Psi$, в силу инд. гипотезы. Если $\mathfrak{Z}^{\equiv} \nVdash \Phi$, то $\mathfrak{Z}^{\equiv} \Vdash \Psi$, откуда, ввиду инд. гипотезы, $\mathrm{ZA}^{\equiv} \vdash \Psi$, а потому $\mathrm{ZA}^{\equiv} \vdash \neg\neg\Psi$.

. . .

Доказательство (продолжение).

- Пусть $\Phi = \Psi \wedge \Theta$. Если $\mathfrak{Z}^{\equiv} \Vdash \Phi$, то

$$\mathfrak{Z}^{\equiv} \Vdash \Psi \quad \text{и} \quad \mathfrak{Z}^{\equiv} \Vdash \Theta,$$

откуда, в силу инд. гипотезы, $\mathrm{ZA}^{\equiv} \vdash \Psi$ и $\mathrm{ZA}^{\equiv} \vdash \Theta$, а потому $\mathrm{ZA}^{\equiv} \vdash \Psi \wedge \Theta$. Если $\mathfrak{Z}^{\equiv} \nVdash \Phi$, то

$$\mathfrak{Z}^{\equiv} \nVdash \Psi \quad \text{или} \quad \mathfrak{Z}^{\equiv} \nVdash \Theta,$$

откуда, в силу инд. гипотезы, $\mathrm{ZA}^{\equiv} \vdash \neg\Psi$ или $\mathrm{ZA}^{\equiv} \vdash \neg\Theta$, что влечёт $\mathrm{ZA}^{\equiv} \vdash \neg\,(\Psi \wedge \Theta)$.

- Аналогично для $\Phi = \Psi \vee \Theta$ и $\Phi = \Psi \to \Theta$.

Вариация на доказательство.

Пусть Φ — бесквантворное $\sigma^{\equiv}$-предложение. Ясно, что Φ представляет собой булеву комбинацию атомарных $\sigma^{\equiv}$-предложений. Ввиду леммы выше, Φ либо истинно во всех моделях $\mathrm{ZA}^{\equiv}$, либо ложно во всех моделях $\mathrm{ZA}^{\equiv}$, т.е.

$$\text{либо } \mathrm{ZA}^{\equiv} \models \Phi, \quad \text{либо } \mathrm{ZA}^{\equiv} \models \neg\Phi.$$

В первом случае мы получаем $\mathrm{ZA}^{\equiv} \vdash \Phi$, а во втором — $\mathrm{ZA}^{\equiv} \vdash \neg\Phi$.

Значит, для любого бесквантворного $\sigma^{\equiv}$-предложения Φ,

$$\mathfrak{Z}^{\equiv} \Vdash \Phi \quad \Longleftrightarrow \quad \mathrm{ZA}^{\equiv} \vdash \Phi;$$

при этом, как легко понять, $\mathfrak{Z}^{\equiv} \Vdash \Phi$ равносильно $\mathrm{Th}\,(\mathfrak{Z}^{\equiv}) \vdash \Phi$.

Теорема (следствие элиминации кванторов)

$\mathrm{Th}\,(\mathfrak{Z}^{=}) = [\mathrm{ZA}^{=}]$.

Доказательство.

Сравнительно нетрудно проверить, что в доказательстве элиминации кванторов в $\mathrm{Th}\,(\mathfrak{Z}^{=})$, приведённом ранее,

$$\text{«}\mathrm{Th}\,(\mathfrak{Z}^{=}) \vdash \text{»}\ \text{всюду можно заменить на «}\mathrm{ZA}^{=} \vdash \text{»}.$$

Поэтому τ, которая реализует элиминацию кванторов в $\mathrm{Th}\,(\mathfrak{Z}^{=})$, реализует её и в $\mathrm{ZA}^{=}$. В частности, для всякого $\Phi \in \mathrm{Sent}_{\sigma^{=}}$:

$$\begin{aligned} \mathrm{ZA}^{=} \vdash \Phi \quad &\Longleftrightarrow \quad \mathrm{ZA}^{=} \vdash \tau\,(\Phi); \\ \mathrm{Th}\,(\mathfrak{Z}^{=}) \vdash \Phi \quad &\Longleftrightarrow \quad \mathrm{Th}\,(\mathfrak{Z}^{=}) \vdash \tau\,(\Phi), \end{aligned}$$

причём $\mathrm{Th}\,(\mathfrak{Z}^{=}) \vdash \tau\,(\Phi)$, как мы знаем, равносильно $\mathrm{ZA}^{=} \vdash \tau\,(\Phi)$. $\square$

Замечание

На самом деле, то, что элиминацию кванторов для $\mathrm{ZA}^{\equiv}$ реализует та же самая функция, несущественно. Важно следующее:

a. $\mathfrak{Z}^{\equiv}$ является моделью $\mathrm{ZA}^{\equiv}$;

b. $\mathrm{ZA}^{\equiv}$ допускает элиминацию кванторов;

c. $\mathrm{ZA}^{\equiv}$ знает всё про бескванторные $\sigma^{\equiv}$-предложения.

Действительно, пусть функция τ' реализует элиминацию кванторов в $\mathrm{ZA}^{\equiv}$. Рассмотрим произвольное $\Phi \in \mathrm{Sent}_{\sigma^{\equiv}}$.

- Пусть $\mathfrak{Z}^{\equiv} \Vdash \Phi$. Тогда $\mathfrak{Z}^{\equiv} \Vdash \tau'(\Phi)$, поскольку $\mathrm{ZA}^{\equiv} \vdash \Phi \leftrightarrow \tau'(\Phi)$ и $\mathfrak{Z}^{\equiv} \Vdash \mathrm{ZA}^{\equiv}$. Значит, $\mathrm{ZA}^{\equiv} \vdash \tau'(\Phi)$, откуда $\mathrm{ZA}^{\equiv} \vdash \Phi$.
- Пусть $\mathrm{ZA}^{\equiv} \vdash \Phi$. Тогда $\mathfrak{Z}^{\equiv} \Vdash \Phi$ ввиду $\mathfrak{Z}^{\equiv} \Vdash \mathrm{ZA}^{\equiv}$.

Отметим, что от τ' не требуется вычислимости.

Явная аксиоматика для $\mathrm{Th}(\mathfrak{Z})$

Обозначим через ZA множество, состоящее из *универс. замыканий* следующих σ-формул.

- Аксиомы линейно упорядоченных абелевых групп.
- Аксиомы для нуля и единицы: $0 < 1$ и $x \leqslant 0 \vee 1 \leqslant x$.
- Новые аксиомы для сравнений по модулю:

$$\bigvee_{k=0}^{m-1} P_m(x, \underline{k}) \quad \text{для } m \in \{2, 3, \dots\};$$

тут $P_m(x, \underline{k})$ обозначает $\exists z\,(x = \underline{k} + mz)$, где z отлична от x.

Теорема

$\mathrm{Th}(\mathfrak{Z}) = [\mathrm{ZA}]$.

Доказательство.

Очевидно, $\mathrm{Th}(\mathfrak{Z}) = \mathrm{Th}(\mathfrak{Z}^{\equiv}) \cap \mathrm{Sent}_\sigma$. С другой стороны:

- каждую модель ZA можно (ед. об.) обогатить до модели $\mathrm{ZA}^{\equiv}$;
- каждую модель $\mathrm{ZA}^{\equiv}$ можно обеднить до модели ZA.

Стало быть, для любого $\Phi \in \mathrm{Sent}_\sigma$,

$$\mathrm{ZA} \models \Phi \quad \Longleftrightarrow \quad \mathrm{ZA}^{\equiv} \models \Phi.$$

Так как $\models$ совпадает с $\vdash$, это означает, что $[\mathrm{ZA}] = [\mathrm{ZA}^{\equiv}] \cap \mathrm{Sent}_\sigma$. Следовательно, $[\mathrm{ZA}] = \mathrm{Th}(\mathfrak{Z})$ ввиду $[\mathrm{ZA}^{\equiv}] = \mathrm{Th}(\mathfrak{Z}^{\equiv})$. □

Замечание

То, что $[\mathrm{ZA}]$ совпадает с $[\mathrm{ZA}^{\equiv}] \cap \mathrm{Sent}_\sigma$, нетрудно доказать и из чисто дедуктивных соображений, не прибегая к помощи моделей.

Вместо аксиом для сравнений можно рассмотреть σ-формулы вида

$$\Phi(x/0) \wedge \forall x\,(0 \leqslant x \wedge \Phi \to \Phi(x/(x+1))) \to \forall x\,(0 \leqslant x \to \Phi).$$

Мы будем называть их аксиомами индукции. Обозначим соответствующее множество σ-предложений через ZA'.

Предложение

$[\mathrm{ZA}'] = [\mathrm{ZA}]$.

Доказательство.

$\boxed{\subseteq}$ Ясно, что $\mathfrak{Z} \Vdash \mathrm{ZA}'$, а потому $[\mathrm{ZA}'] \subseteq \mathrm{Th}(\mathfrak{Z}) = [\mathrm{ZA}]$.

. . .

Доказательство (продолжение).

$\supseteq$ Достаточно показать, что универсальные замыкания аксиом для сравнений выводимы в ZA'. Пусть $m \in \mathbb{N} \setminus \{0, 1\}$. Обозначим

$$\Psi_m(x) \;:=\; \bigvee_{k=0}^{m-1} P_m(x, \underline{k}).$$

Далее будем рассуждать внутри ZA'.

Сначала по индукции докажем, что $\forall x\,(0 \leqslant x \to \Psi_m(x))$.

База: Очевидно, $0 = \underline{0} + m0$, а потому $P_m(0, \underline{0})$, откуда $\Psi_m(x/0)$.

...

Доказательство (продолжение).

Шаг индукции: Пусть $\Psi_m(x)$, т.е. найдётся $k \in \{0, \ldots, m-1\}$ такое, что $P_m(x, \underline{k})$. Значит, $x = \underline{k} + mz$ для некоторого z. Отсюда

$$x+1 \;=\; \underline{k} + mz + 1 \;=\; \underline{k+1} + mz.$$

При этом $k+1 \leqslant m$, поскольку $k < m$.

- Если $k+1 < m$, то $\Psi_m(x/(x+1))$ ввиду $P_m(x+1, \underline{k+1})$.
- Если $k+1 = m$, то $x+1 = \underline{m} + mz = m(z+1)$, а потому $P_m(x+1, \underline{0})$, откуда вновь $\Psi_m(x/(x+1))$.

...

Доказательство (продолжение).

Теперь докажем, что $\forall x\,(x < 0 \to \Psi_m\,(x))$.

Пусть $x < 0$. Тогда $0 < -x$. Поэтому найдутся $k \in \{0, \ldots, m-1\}$ и z такие, что $-x = \underline{k} + mz$.

- Пусть $k = 0$. Тогда $x = -mz$, а потому $P_m\,(x, \underline{0})$, откуда $\Psi_m\,(x)$.
- Пусть $k \neq 0$. Тогда $x = \underline{-k} - mz$, что можно переписать как

$$x \;=\; \underline{m} - \underline{k} - mz - \underline{m} \;=\; \underline{m-k} - m\,(z+1),$$

  а потому $P_m\,(x, \underline{m-k})$, откуда $\Psi_m\,(x)$.

Наконец, объединяя вместе случаи $0 \leqslant x$ и $x < 0$, мы получаем

$$\forall x\,((0 \leqslant x \vee x < 0) \to \Psi_m\,(x)),$$

что равносильно $\forall x\,\Psi_m\,(x)$. □

Вариация на тему

Зададим σ_+ как $\langle =^2, <^2; \mathsf{s}^1, +^2; 0\rangle$.

Обозначим стандартную σ_+-структуру с носителем $\mathbb{N}$ через $\mathfrak{N}_+$.

Для проведения элиминации опять нужно расширить σ_+:

$$\sigma_+^{\equiv} \;:=\; \sigma_+ \cup \{\equiv_2, \equiv_3, \dots\}.$$

Обозначим за $\mathfrak{N}_+^{\equiv}$ стандартную $\sigma_+^{\equiv}$-структуру с носителем $\mathbb{N}$.

С незначительными изменениями все результаты, замечания и комментарии, касающиеся $\mathfrak{Z}$ и $\mathfrak{Z}^{\equiv}$, переносятся на $\mathfrak{N}_+$ и $\mathfrak{N}_+^{\equiv}$.

Под арифметикой Пресбургера понимают как $\mathrm{Th}(\mathfrak{Z})$, так и $\mathrm{Th}(\mathfrak{N}_+)$.

- Поскольку $\mathfrak{N}_+$ в некотором смысле является частью $\mathfrak{Z}$, может показаться, что $\mathfrak{N}_+$ проще $\mathfrak{Z}$. Однако, как известно, элементы $\mathbb{Z}$ можно моделировать с помощью элементов $\mathbb{N} \times \mathbb{N}$; поэтому $\mathfrak{N}_+$ и $\mathfrak{Z}$ оказываются «взаимно интерпретируемы».

- У $\mathrm{Th}\,(\mathfrak{N}_+)$ имеется аксиоматика, аналогичная ZA. Но тут есть свои нюансы, связанные с тем, что порой «поз. утверждения» выводятся в ZA с помощью $-$. Так, в ZA выводимо

$$x + z \;<\; y + z \quad \longrightarrow \quad x \;<\; y$$

поскольку к обеим частям исходного неравенства можно добавить $-z$. Разумеется, это должно быть выводидимо из аксиом для $\mathrm{Th}\,(\mathfrak{N}_+)$, хотя $-z$ при этом использовать нельзя.

Одна из явных аксиоматик для $\mathrm{Th}(\mathfrak{N}_+)$

Для разнообразия рассмотрим аксиоматику для $\mathrm{Th}(\mathfrak{N}_+)$, которая внешне непохожа на ZA. Обозначим через PrA множество, состоящее из *универсальных* замыканий σ_+-формул

- $\mathsf{s}(x) \neq 0$,
- $\mathsf{s}(x) = \mathsf{s}(y) \to x = y$,
- $x + 0 = x$,
- $x + \mathsf{s}(y) = \mathsf{s}(x + y)$,
- $x \not< 0$ и
- $x < \mathsf{s}(y) \leftrightarrow (x < y \vee x = y)$,

а также универсальных замыканий всех σ_+-формул вида

$$\Phi(x/0) \wedge \forall x\,(\Phi(x/x) \to \Phi(x/\mathsf{s}(x))) \to \forall x\,\Phi,$$

которые в совокупности называются схемой аксиом индукции в σ_+.

Упражнение

Следующие σ_+-формулы (их универс. замыкания) выводимы в PrA*:*

a. $(x + y) + z = x + (y + z)$;

b. $x + y = y + x$;

c. $x \nless x$;

d. $x < y \wedge y < z \to x < z$;

e. $x \neq y \to x < y \vee y < x$;

f. $x < y \leftrightarrow x + z < y + z$;

g. $x < \mathsf{s}(x)$;

h. $y \leqslant x \vee \mathsf{s}(x) \leqslant y$;

i. $x \leqslant y \to \exists! z\, x + z = y$.

В результате PrA начинает походить на ZA$'$.

Замечание

Далее, по аналогии с тем, как мы доказывали $[\mathrm{ZA}'] = \mathrm{Th}(\mathfrak{Z})$, можно показать, что [PrA] совпадает с $\mathrm{Th}(\mathfrak{N}_+)$. Таким образом, $\mathrm{Th}(\mathfrak{N}_+)$ — это разрешимая теория, которая задается весьма естественным множеством аксиом. Вместе с тем известно, что при добавлении в язык умножения разрешимость теряется бесповоротно. В дальнейшем это утверждение будет уточнено и аккуратно сформулировано.

Больше примеров разрешимых теорий

- Теория вещественно замкнутых (упорядоченных) полей, которая совпадает с теорией упор. поля вещественных чисел.
- Теория линейных порядков.
- Теория булевых алгебр.
- Теория линейно упорядоченных абелевых групп.
- Теория класса всех *конечных* полей.

Замечание

Вообще, если теория класса $\mathcal{K}$ разрешима, то теория класса $\mathcal{K}_{\text{fin}}$ всех конечных структур из $\mathcal{K}$ *обычно* также разрешима. Тот факт, что $\mathcal{K}_{\text{fin}}$ практически никогда не аксиоматизируем, на это не влияет.

Примеры неразрешимых теорий

- Теория стандартной модели арифметики.
- Теория кольца целых чисел.
- Теория поля рациональных чисел.
- Теория частичных порядков.
- Теория дистрибутивных решёток.
- Теория групп.
- Теория полей, а также теория полей характеристики 0.

При этом последние четыре теории оказываются эквивалентны Halt с выч. точки зрения, а первые три — «в $\aleph_0$ раз сложнее Halt».

Более специальные, но по-своему полезные неразрешимые теории:

- Теория симметричных иррефлексивных графов.
- Теория двух эквивалентностей.
- Теория двух линейных порядков.
- Теория эквивалентности и линейного порядка.

Все они будут эквивалентны Halt (с вычислительной точки зрения).

Замечание

Пусть $\Gamma \cup \{\Phi\} \subseteq \mathrm{Sent}_\sigma$. Тогда для любого $\Psi \in \mathrm{Sent}_\sigma$,

$$\Gamma \cup \{\Phi\} \vdash \Psi \quad \Longleftrightarrow \quad \Gamma \vdash \Phi \to \Psi.$$

Стало быть, $[\Gamma \cup \{\Phi\}] \leqslant [\Gamma]$. Поэтому, в частности:

- неразрешимость теории частичных порядков влечёт неразрешимость теории предпорядков, а из неразрешимости теории полей следует неразрешимость теории колец;
- из разрешимости теории линейных порядков получается разрешимость теории плотных линейных порядков.

Более тонкий метод — это «интерпретация одного класса в другом». Например, поскольку поле комплексных чисел можно смоделировать в рамках поля вещественных чисел, теорию первого можно свести к теории второго, а потому теория поля $\mathbb{C}$ разрешима.

Замечание

Теория класса $\mathcal{K}$ называется наследственно неразрешимой, если для всякого класса $\mathcal{K}'$,

$$\mathcal{K} \subseteq \mathcal{K}' \quad \Longrightarrow \quad \mathrm{Th}(\mathcal{K}') \text{ неразрешима.}$$

Часто, хотя и не всегда, неразрешимость теории можно получить из насл. неразр. теории подходящего класса конечных структур.

Например, известно, что класс всех конечных симметрических групп имеет наследственно неразрешимую теорию; поэтому теория любого его надкласса неразрешима.

Теории естественных классов конечных структур практически всегда имеют перечислимые дополнения. Те из них, что неразрешимы, обычно эквивалентны дополнению Halt.

Пример

Для удобства обозначим за $\mathfrak{Q}$ и $\mathfrak{R}$ стандартные поля над $\mathbb{Q}$ и $\mathbb{R}$ соответственно. Ясно, что $\mathfrak{Q}$ является подполем $\mathfrak{R}$. Вместе с тем:

- $\mathrm{Th}(\mathfrak{R})$ разрешимо;
- $\mathrm{Th}(\mathfrak{Q})$ неразрешимо (более того, далеко от перечислимости).

Поэтому $\mathbb{Q}$ не определимо в $\mathfrak{R}$, поскольку иначе мы могли бы смоделировать $\mathfrak{Q}$ в рамках $\mathfrak{R}$, что дало бы $\mathrm{Th}(\mathfrak{Q}) \leqslant \mathrm{Th}(\mathfrak{R})$.

С другой стороны, обогащение $\mathfrak{R}$ посредством добавления одноместного предиката «быть рациональным числом» имеет как мин. ту же — на самом деле, куда большую — сложность, что и $\mathfrak{Q}$.

Заключительные комментарии

- Разрешимые теории встречаются сравнительно редко, но обладают особой привлекательностью.
- Для доказательства разрешимости теорий таких классов как булевы алгебры, абелевы группы и *конечные* поля требуется глубокий анализ строения соответствующих структур.
- Большинство теорий неразрешимы. Сложность таких теорий можно измерять в терминах степеней.
- Чтобы глубже понять алгоритмические свойства теории, мы можем перейти к изучению её естественных фрагментов, которые состоят из формул специального вида.