Математическая логика: лекция 12

Станислав Олегович Сперанский

Санкт-Петербургский государственный университет

Санкт-Петербург 2020

О разрешимых и перечислимых множествах

Напоминаю, что $f :\subseteq \mathbb{N}^\ell \to \mathbb{N}$ называется вычислимой, если существует алгоритм, который по каждому $\vec{n} \in \operatorname{dom} f$ находит $f(\vec{n})$, причём на элементах $\mathbb{N}^\ell \setminus \operatorname{dom} f$ этот алгоритм «зависает».

Замечание

Здесь под алгоритмами мы понимаем, например, машины Тьюринга, которые по умолчанию подразумеваются *детерминированными*.

Пусть $A \subseteq \mathbb{N}$. Говорят, что:

- A разрешимо, или вычислимо, если его характеристическая функция, обозначаемая χ_A, вычислима.
- A перечислимо, если либо $A = \varnothing$, либо $A = \operatorname{range} f$ для нек. вычислимой $f : \mathbb{N} \to \mathbb{N}$.

В рассуждениях мы будем свободно использовать:

Тезис Чёрча–Тьюринга

$f :\subseteq \mathbb{N}^\ell \to \mathbb{N}$ интуитивно вычислима тогда и только тогда, когда она вычислима посредством некоторой машины Тьюринга.

Этот тезис невозможно ни доказать, ни опровергнуть математически ввиду того, что здесь участвуют одновременно:

- неформ. (немат.) понятие интуитивно вычислимой функции;
- форм. (мат.) понятие вычислимой по Тьюрингу функции.

Статус тезиса Чёрча–Тьюринга отражает наши представления о том, как математическая модель алгоритма связана с «реальностью».

Грубо говоря, если подходить к вопросу эмпирически:

- никто не смог придумать алгоритма в традиционном, интуитивном его понимании, который невозможно смоделировать посредством подходящей машины Тьюринга.

Если же подходить к вопросу чисто математически:

- все известные формализации концепции алгоритма/понятия вычислимости равносильны: по алгоритмам одного рода мы можем эффективно строить алгоритмы другого рода, вычисляющие те же частичные функции из $\mathbb{N}^\ell$ в $\mathbb{N}$.

Наконец, тезис Чёрча–Тьюринга приобретает особую актуальность, когда речь заходит об алгоритмической *неразрешимости*.

Замечание

Определим $\mathrm{pair} : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ по правилу

$$\mathrm{pair}\,(n, m) \;:=\; 2^n \cdot (2m+1) - 1.$$

Ясно, что pair — вычислимая биекция из $\mathbb{N} \times \mathbb{N}$ на $\mathbb{N}$, причём по ней легко строятся вычислимые $\mathrm{left}, \mathrm{right} : \mathbb{N} \to \mathbb{N}$ такие, что

$$\mathrm{left}\,(\mathrm{pair}\,(n, m)) \;=\; n \quad \text{и} \quad \mathrm{right}\,(\mathrm{pair}\,(n, m)) \;=\; m.$$

Далее, с помощью pair для всякого $\ell \geqslant 2$ можно построить вычислимую биекцию ℓ-tuple из $\mathbb{N}^\ell$ на $\mathbb{N}$:

$$\begin{aligned} 3\text{-tuple}\,(n_1, n_2, n_3) \;&:=\; \mathrm{pair}\,(\mathrm{pair}\,(n_1, n_2), n_3) \\ 4\text{-tuple}\,(n_1, n_2, n_3, n_4) \;&:=\; \mathrm{pair}\,(\mathrm{pair}\,(\mathrm{pair}\,(n_1, n_2), n_3), n_4) \\ &\;\;\vdots \end{aligned}$$

Разумеется, посредством этих биекций можно переходить от подмножеств $\mathbb{N}$ к подмножествам $\mathbb{N}^\ell$, и наоборот.

Предложение

Пусть $A, B \subseteq \mathbb{N}$ *разрешимы. Тогда* $A \cap B$, $A \cup B$ *и* $\mathbb{N} \setminus A$ *разрешимы.*

Доказательство.

Пусть χ_A и χ_B вычислимы. Заметим, что для любого $n \in \mathbb{N}$:

$$\begin{aligned}
\chi_{A \cap B}(n) &= \min\{\chi_A(n), \chi_B(n)\}; \\
\chi_{A \cup B}(n) &= \max\{\chi_A(n), \chi_B(n)\}; \\
\chi_{\mathbb{N} \setminus A}(n) &= 1 - \chi_A(n).
\end{aligned}$$

Поэтому $\chi_{A \cap B}$, $\chi_{A \cup B}$ и $\chi_{\mathbb{N} \setminus A}$ вычислимы. $\square$

Для произвольного $A \subseteq \mathbb{N}$ зададим $\chi^*_A :\subseteq \mathbb{N} \to \mathbb{N}$ по правилу

$$\chi^*_A(n) \; := \begin{cases} 1 & \text{если } \; n \in A \\ \uparrow & \text{иначе,} \end{cases}$$

где $\uparrow$ означает, что функция «зависает»; χ^*_A иногда называют полу-характеристической функцией A.

Предложение

Для любого $A \subseteq \mathbb{N}$,

$$A \;\; \textit{перечислимо} \quad \Longleftrightarrow \quad \chi^*_A \;\; \textit{вычислима}.$$

Доказательство.

Пусть $A = \varnothing$. Тогда χ_A^* — «пустая функция». Значит, A перечислимо и χ_A^* вычислима. Отныне мы будем считать, что $A \neq \varnothing$.

$\boxed{\Longrightarrow}$ Пусть $A = \operatorname{range} f$ для некот. вычислимой $f : \mathbb{N} \to \mathbb{N}$. Тогда χ_A^* можно вычислить посредством следующего алгоритма.

0: Положим $k := 0$.

1: Вычислим $f(k)$. Если $f(k) = n$, то выдадим 1. Иначе положим $k := k + 1$ и `GoTo 1`.

Здесь n — это значение аргумента на входе.

...

Доказательство (продолжение).

$\boxed{\Longleftarrow}$ Пусть χ_A^* вычислима посредством нек. алгоритма $\mathtt{P}$. Как легко убедиться, существуют вычислимые $h_1, h_2 : \mathbb{N} \to \mathbb{N}$ такие, что

$$\{(h_1(n), h_2(n)) \mid n \in \mathbb{N}\} \;=\; \mathbb{N} \times \mathbb{N}.$$

Далее, зафиксируем какой-нибудь $a_0 \in A$. Рассмотрим $f : \mathbb{N} \to \mathbb{N}$, вычисляемую посредством следующего алгоритма.

0: Вычислим $h_1(n)$ и $h_2(n)$. Если алг. $\mathtt{P}$ останавливается за $h_1(n)$ шагов на входе $h_2(n)$, то выдадим $h_2(n)$. Иначе выдадим a_0.

Ясно, что $\operatorname{range} f = A$. $\square$

Замечание

Перечислимость иногда называют полуразрешимостью.

Следствие

$A \subseteq \mathbb{N}$ перечислимо тогда и только тогда, когда $A = \operatorname{dom} f$ для некот. вычислимой $f : \subseteq \mathbb{N} \to \mathbb{N}$.

Доказательство.

$\boxed{\Longrightarrow}$ Пусть χ_A^* вычислима. Тогда, поскольку $A = \operatorname{dom} \chi_A^*$, мы можем взять χ_A^* в качестве искомой f.

$\boxed{\Longleftarrow}$ Пусть $A = \operatorname{dom} f$ для некоторой вычислимой $f : \subseteq \mathbb{N} \to \mathbb{N}$. Для удобства обозначим $\chi_{\mathbb{N}}$ через $\mathbf{1}$, т.е. $\mathbf{1} = \lambda n.[1]$. Тогда

$$\chi_A^* = f \circ \mathbf{1}.$$

Стало быть, χ_A^* вычислима. $\square$

Следствие

$A \subseteq \mathbb{N}$ перечислимо тогда и только тогда, когда $A = \operatorname{range} f$ для нек. вычислимой $f :\subseteq \mathbb{N} \to \mathbb{N}$.

Доказательство.

$\boxed{\Longrightarrow}$ Тривиально.

$\boxed{\Longleftarrow}$ Пусть $A = \operatorname{range} f$ для некоторой вычислимой $f :\subseteq \mathbb{N} \to \mathbb{N}$. По предыдущему следствию $\operatorname{dom} f$ перечислимо.

- Если $\operatorname{dom} f = \varnothing$, то $\operatorname{range} f = \varnothing$, а потому A перечислимо.
- Если $\operatorname{dom} f \neq \varnothing$, то $\operatorname{dom} f = \operatorname{range} g$ для некоторой вычислимой $g : \mathbb{N} \to \mathbb{N}$, откуда

$$\operatorname{range} f = \operatorname{range} (g \circ f),$$

  а потому A перечислимо.

$\square$

Предложение

Пусть $A, B \subseteq \mathbb{N}$ *перечислимы. Тогда* $A \cap B$ *и* $A \cup B$ *перечислимы.*

Доказательство.

Как мы знаем, сущ. вычислимые $f, f', g, g' : \subseteq \mathbb{N} \to \mathbb{N}$ такие, что

$$A = \operatorname{dom} f = \operatorname{range} f' \quad \text{и} \quad B = \operatorname{dom} g = \operatorname{range} g'.$$

Зададим вычислимую $h : \subseteq \mathbb{N} \to \mathbb{N}$ по правилу

$$h(n) := f(n) \cdot g(n)$$

а вычислимую $h' : \subseteq \mathbb{N} \to \mathbb{N}$ — по правилу

$$h'(n) := \begin{cases} f'(n/2) & \text{если } n \text{ чётно} \\ g'((n-1)/2) & \text{если } n \text{ нечётно.} \end{cases}$$

Тогда $\operatorname{dom} h = \operatorname{dom} f \cap \operatorname{dom} g$ и $\operatorname{range} h' = \operatorname{range} f' \cup \operatorname{range} g'$; поэтому $A \cap B$ и $A \cup B$ перечислимы. $\square$

Предложение

Пусть $A \subseteq \mathbb{N}$ разрешимо. Тогда A перечислимо.

Доказательство.

Заметим, что из вычислимости χ_A следует вычислимость χ_A^*. $\square$

Замечание

Обратное опровергается. В частности, множество Halt, которое кодирует проблему остановки для машин Тьюринга, перечислимо, однако разрешимым оно не является.

Предложение (теорема Поста)

$A \subseteq \mathbb{N}$ разрешимо, если и только если A и $\mathbb{N} \setminus A$ перечислимы.

Доказательство.

$\boxed{\Longrightarrow}$ Пусть A разрешимо. Тогда и $\mathbb{N} \setminus A$ разрешимо. Следовательно, они оба перечислимы.

$\boxed{\Longleftarrow}$ Пусть A и $\mathbb{N} \setminus A$ перечислимы. Если одно из них пусто, то они оба вычислимы. Будем считать, что A и $\mathbb{N} \setminus A$ непусты. Значит, сущ. вычислимые $f, g : \mathbb{N} \to \mathbb{N}$ такие, что

$$A = \operatorname{range} f \quad \text{и} \quad \mathbb{N} \setminus A = \operatorname{range} g.$$

...

Доказательство (продолжение).

Тогда χ_A можно вычислить посредством следующего алгоритма.

0: Положим $k := 0$.

1: Вычислим $f(k)$ и $g(k)$. Если $f(k) = n$, то выдадим 1, а если $g(k) = n$ — выдадим 0. Иначе положим $k := k + 1$ и `GoTo 1`.

Так как $\operatorname{range} f \cup \operatorname{range} g = \mathbb{N}$ и $\operatorname{range} f \cap \operatorname{range} g = \varnothing$, алгоритм всегда завершает работу корректным образом. □

Замечание

В частности, дополнение Halt неперечислимо.

Пусть $A, B \subseteq \mathbb{N}$. Говорят, что A сводится к B, и пишут $A \leqslant B$, если существует вычислимая $f : \mathbb{N} \to \mathbb{N}$ такая, что для любого $n \in \mathbb{N}$,

$$n \in A \iff f(n) \in B,$$

т.е. $f^{-1}[B]$ совпадает с A. Пишут $A \equiv B$, называя A и B эквивалентными, если $A \leqslant B$ и $A \leqslant A$; традиционно классы эквивалентности по $\equiv$ именуют степенями.

Замечание

Классическая терминология: m-сводимость и так далее. Если дополнительно потребовать от сводящих функций (f) инъективности, мы получим 1-сводимость и т.д.; это очень важные понятия, но они нам в ближайшее время не понадобятся.

Замечание (без доказательства)

Если от сводящих функций потребовать вычислимости за *полиномиальное время*, мы получим полиномиальную сводимость. Она играет ключевую роль в теории вычислительной сложности.

Опуская ряд технических деталей, обозначим

NP := класс всех множеств, характеристические функции которых вычислимы за пол. время посредством *недетерминированных* машин Тьюринга.

Среди элементов NP есть наиболее сложный, точнее тот, к которому полиномиально сводятся все элементы NP, причём он единственен с точностью до пол. эквивалентности. Им окажется

$$\mathrm{Prop\text{-}Sat} := \{n \in \mathbb{N} \mid \text{проп. формула с кодом } n \text{ выполнима}\},$$

в силу упоминавшейся ранее теоремы Кука–Левина.

Предложение

Отношение сводимости является предпорядком на $\mathcal{P}(\mathbb{N})$.

Доказательство.

Пусть $A, B, C \subseteq \mathbb{N}$. Очевидно, id_A сводит A к A. Далее, если f сводит A к B, а g — B к C, то для любого $n \in \mathbb{N}$,

$$n \in A \iff f(n) \in B \iff g(f(n)) \in C,$$

а значит, $f \circ g$ сводит A к C. Стало быть, отношение сводимости как бинарное отношение на $\mathcal{P}(\mathbb{N})$ рефлексивно и транзитивно. $\square$

Поэтому отношение сводимости индуцирует (частичный) порядок на совокупности всех степеней.

Предложение

Пусть $A, B \subseteq \mathbb{N}$ и $A \leqslant B$. Тогда:

i. *если B разрешимо, то A разрешимо;*

ii. *если B перечислимо, то A перечислимо.*

Доказательство.

Зафиксируем вычислимую $f : \mathbb{N} \to \mathbb{N}$, сводящую A к B. Ясно, что

$$\chi_A = f \circ \chi_B \quad \text{и} \quad \chi_A^* = f \circ \chi_B^*.$$

Стало быть, из вычислимости χ_B следует вычислимость χ_A, а из вычислимости χ_B^* — вычислимость χ_A^*. $\square$

Замечание (без доказательства)

Среди перечислимых множеств есть наиболее сложное, а именно, то, к которому сводятся все перечислимые множества, причём оно единственно с точностью до эквивалентности. Им окажется Halt.

Самая базовая интуиция такова:

- чтобы доказать разрешимость A, мы сводим A к подходящему разрешимому множеству;
- чтобы доказать неразрешимость A, мы, напротив, сводим подходящее неразрешимое множество к A.

В некотором смысле «простейшим» среди естественно возникающих неразрешимых множеств является Halt.

Общие комментарии

- Теория вычислимости, также известная как теория рекурсии / теория алгоритмов, — интересный и глубокий предмет. В частности, про одни только перечислимые множества и их степени можно написать увесистую книгу.
- Выше приведено лишь несколько простейших фактов, нужных для понимания дальнейшего материала.
- Результаты и методы теории вычислимости во многом вдохновили то, что происходит в теории вычислит. сложности.

- Учебники по базовой теории вычислимости:

[1] Rogers, H., (1967). *Theory of Recursive Functions and Effective Computability*. McGraw-Hill Book Company. xxii+482 p.

[2] Soare, R. I. (2016). *Turing Computability*. Springer. xxxvi+263 p.

- К этому добавляются многочисленные исследования в теории вычислимых моделей, «вычислимом анализе», алгоритмической теории случайности и других современных областях.

О кодировании термов и формул

Чтобы отождествлять алгоритмические проблемы над дискретным типом данных с вычислением функций над $\mathbb{N}$, прибегают к кодированию, или нумерации, входов.

Нас интересует нумерация для логики первого порядка над σ. Для наглядности возьмём в качестве σ сигнатуру арифметики.

Замечание

В контексте изучения алгоритмических вопросов мы ограничиваемся конечными и счётными сигнатурами, причём счётность должна быть в некотором смысле «эффективной».

Определим $\# : \mathrm{Term}_\sigma \cup \mathrm{Form}_\sigma \to \mathbb{N}$ следующим образом:

$$
\begin{aligned}
\#(v_n) &:= \mathrm{pair}(1, n);\\
\#(0) &:= \mathrm{pair}(2, 0);\\
\#(\mathrm{s}(t)) &:= \mathrm{pair}(3, \#(t));\\
\#(t_1 + t_2) &:= \mathrm{pair}(4, \mathrm{pair}(\#(t_1), \#(t_2)));\\
\#(t_1 \cdot t_2) &:= \mathrm{pair}(5, \mathrm{pair}(\#(t_1), \#(t_2)));\\
\#(t_1 = t_2) &:= \mathrm{pair}(6, \mathrm{pair}(\#(t_1), \#(t_2)));\\
\#(\neg\Psi) &:= \mathrm{pair}(7, \#(\Psi));\\
\#(\Psi \vee \Theta) &:= \mathrm{pair}(8, \mathrm{pair}(\#(\Psi), \#(\Theta)));\\
\#(\Psi \vee \Theta) &:= \mathrm{pair}(9, \mathrm{pair}(\#(\Psi), \#(\Theta)));\\
\#(\Psi \to \Theta) &:= \mathrm{pair}(10, \mathrm{pair}(\#(\Psi), \#(\Theta)));\\
\#(\forall v_n\, \Psi) &:= \mathrm{pair}(11, \mathrm{pair}(n, \#(\Psi)));\\
\#(\exists v_n\, \Psi) &:= \mathrm{pair}(12, \mathrm{pair}(n, \#(\Psi))).
\end{aligned}
$$

Предложение

$\#$ *инъективна.*

Доказательство.

Очевидно, $\#[\mathrm{Term}_\sigma] \cap \#[\mathrm{Form}_\sigma] = \varnothing$, а потому достаточно показать инъективность

$$\#_{\mathrm{T}} \;:=\; \# \restriction_{\mathrm{Term}_\sigma} \quad \text{и} \quad \#_{\mathrm{F}} \;:=\; \# \restriction_{\mathrm{Form}_\sigma}.$$

Докажем, что для любых $t, t' \in \mathrm{Term}_\sigma$,

$$\#(t) \;=\; \#(t') \quad \Longrightarrow \quad t \;=\; t'.$$

Сделаем это индукцией по построению t. Пусть $\#(t) = \#(t')$.

...

Доказательство (продолжение).

- Если $t = v_n$, где $n \in \mathbb{N}$, то, очевидно, $t' = v_n$.
- Если $t = 0$, то, очевидно, $t' = 0$.
- Предположим, что $t = \mathrm{s}\,(t_1)$. Тогда $\mathrm{left}\,(\#\,(t)) = 3 = \mathrm{left}\,(\#\,(t'))$, а потому $t' = \mathrm{s}\,(t_1')$ для некоторого t_1'. При этом

$$\#\,(t_1) \;=\; \mathrm{right}\,(\#\,(t)) \;=\; \mathrm{right}\,(\#\,(t')) \;=\; \#\,(t_1'),$$

  откуда $t_1 = t_1'$, в силу индукционной гипотезы.
- Случаи $t = t_1 + t_2$ или $t = t_1 \cdot t_2$ разбираются аналогично.

Значит, $\#_{\mathrm{T}}$ инъективна. Аналогично для $\#_{\mathrm{F}}$. $\square$

Стало быть, $\mathrm{Term}_\sigma \cup \mathrm{Form}_\sigma$ можно мысленно отождествить с $\mathrm{range}\,\#$.

Замечание

Ясно, что для любых $n, m \in \mathbb{N}$,

$$\begin{aligned} \mathrm{pair}\,(n, m) &= 2^n \cdot (2m+1) - 1 \\ &\geqslant \max\{2^n - 1, 2m\} \\ &\geqslant \max\{n, m\}, \end{aligned}$$

а в случае, когда $n \neq 0$, мы имеем

$$\mathrm{pair}\,(n, m) \;\geqslant\; 4m+1 \;>\; m.$$

В частности, легко показать, что для любых $o_1, o_2 \in \mathrm{Term}_\sigma \cup \mathrm{Form}_\sigma$,

$$o_1 \preccurlyeq o_2 \quad \text{и} \quad o_1 \neq o_2 \quad \Longrightarrow \quad \#(o_1) < \#(o_2).$$

Это позволяет пользоваться возвратной индукцией/рекурсией.

Предложение

$\#[\mathrm{Term}_\sigma]$ *и* $\#[\mathrm{Form}_\sigma]$ *разрешимы.*

Доказательство.

Хар. функцию $\#[\mathrm{Term}_\sigma]$ можно вычислить посредством следующего алгоритма.

0: Положим $S := \{n\}$.

1: Если $S = \varnothing$, то выдадим 1. Иначе положим $k := \max S$.

2: Если $\mathrm{left}(k) = 0$ или $\mathrm{left}(k) > 5$, то выдадим 0.

3: Если $\mathrm{left}(k) = 1$ или $k = \mathrm{pair}(2, 0)$, то положим $S := S \setminus \{k\}$ и `GoTo 1`.

...

Доказательство (продолжение).

4: Если $\mathrm{left}(k) = 3$, то положим

$$S \; := \; (S \setminus \{k\}) \cup \{\mathrm{right}(k)\}$$

и GoTo 1.

5: Если $\mathrm{left}(k) = 4$ или $\mathrm{left}(k) = 5$, то положим

$$S \; := \; (S \setminus \{k\}) \cup \{\mathrm{left}(\mathrm{right}(k)), \mathrm{right}(\mathrm{right}(k))\}$$

и GoTo 1.

Здесь n — это значение аргумента на входе.

Алгоритм всегда завершает работу, поскольку в случае добавления к S новых элементов (см. 4 и 5) уменьшается $\max S$.

Аналогично для $\#[\mathrm{Form}_\sigma]$. □

Далее, можно, например, построить алгоритмы $\mathtt{A}$, $\mathtt{B}$, $\mathtt{C}$, $\mathtt{D}$ такие, что:

- $\mathtt{A}$ по кодам x и t вычисляет, входит ли x в t;
- $\mathtt{B}$ по кодам x и Φ вычисляет, свободна ли x в Φ;
- $\mathtt{C}$ по кодам x, t и Φ вычисляет, свободен ли t для x в Φ;
- $\mathtt{D}$ по кодам x, t и Φ вычисляет код $\Phi(x/t)$.

Здесь x, t и Φ пробегают Var, Term_σ и Form_σ соответственно. В частности, мы получаем разрешимость $\#[\mathrm{Sent}_\sigma]$.

Грубо говоря, мы можем делать с кодами то же самое, что с термами и формулами, руководствуясь интуицией и здравым смыслом.

Замечание

Так как в pair используется экспонента, для целей теории сложности требуется другая, вычислимая за полиномиальное время биекция. В литературе популярна функция

$$\lambda n.\lambda m.\left[\frac{(n+m+1)(n+m)}{2}+m\right].$$

называемая канторовской нумерующей функцией. В качестве упражнения проверьте, что она является биекцией из $\mathbb{N}\times\mathbb{N}$ на $\mathbb{N}$.

Для простоты давайте считать σ конечной. В дальнейшем мы будем предполагать наличие фикс. процедуры эф. кодирования σ-термов и σ-формул и нередко отождествлять объекты с их кодами.

Для удобства для каждого $\Gamma \subseteq \mathrm{Sent}_\sigma$ обозначим

$$[\Gamma] \;:=\; \{\Phi \in \mathrm{Sent}_\sigma \mid \Gamma \vdash \Phi\},$$

т.е. $[\Gamma]$ — это дедуктивное замыкание Γ; ясно, что $[\Gamma] = \mathrm{Th}\,(\mathrm{Mod}\,(\Gamma))$.

Предложение

Пусть $\Gamma \subseteq \mathrm{Sent}_\sigma$ *перечислимо. Тогда* $[\Gamma]$ *перечислимо.*

Доказательство.

Не ограничивая общности, можно считать, что Γ непусто, поскольку $[\varnothing] = [\{\Phi\}]$, где Φ — какое-н. σ-предложение, выводимое из $\varnothing$.

Очевидно, Form_σ, будучи разрешимым, перечислимо. Так как Form_σ и Γ непусты, сущ. вычислимые $f, g : \mathbb{N} \to \mathrm{Form}_\sigma$ такие, что

$$\mathrm{range}\, f = \mathrm{Form}_\sigma \quad \text{и} \quad \mathrm{range}\, g = \Gamma.$$

Тогда $\chi^*_{[\Gamma]}$ можно вычислить посредством следующего алгоритма.

0: Положим $k := 1$.

1: Вычислим $f(0), \ldots, f(k), g(0), \ldots, g(k)$. Затем переберaем все последовательности элементов $\{f(0), \ldots, f(k)\}$ длины не более k: если среди них есть вывод Φ из $\{g(0), \ldots, g(k)\}$, то выдадим 1. Иначе положим $k := k + 1$ и `GoTo 1`.

Здесь $\Phi \in \mathrm{Sent}_\sigma$ — значение аргумента на входе. $\square$

Следствие

$[\varnothing]$ *перечислимо.* □

Следствие

Пусть $\Gamma \subseteq \mathrm{Sent}_\sigma$ *конечно. Тогда* $[\Gamma]$ *перечислимо.* □

Следствие

Пусть $\Gamma \subseteq \mathrm{Sent}_\sigma$ *разрешимо. Тогда* $[\Gamma]$ *перечислимо.* □

Пример

Теория абелевых групп перечислима, так как она задаётся конечным множеством предложений. Далее, теории групп без кручения и делимых групп будут перечислимы, так как каждую из них можно задать разрешимым множеством предложений.

По аналогии с проп. логикой $\Gamma \subseteq \mathrm{Sent}_\sigma$ называется полным, если для любого $\Phi \in \mathrm{Sent}_\sigma$ верно $\Phi \in \Gamma$ или $\neg\Phi \in \Gamma$.

Замечание

Разумеется, когда Γ непротиворечиво и полно,

$$\Gamma = \mathrm{Th}(\mathfrak{A}) \quad \text{для всех } \mathfrak{A} \in \mathrm{Mod}(\Gamma),$$

а потому Γ можно отождествить с $\mathrm{Th}(\mathfrak{A})$ для какой-нибудь особой $\mathfrak{A}$.

Предложение

Пусть $\Gamma \subseteq \mathrm{Sent}_\sigma$ *непротиворечиво. Если* $[\Gamma]$ *перечислимо и полно, то* $[\Gamma]$ *разрешимо.*

Доказательство.

Пусть $[\Gamma]$ перечислимо и полно. Очевидно, $[\Gamma]$ непусто, а значит, найдётся вычислимая $f : \mathbb{N} \to \mathrm{Form}_\sigma$ такая, что $\mathrm{range}\, f = [\Gamma]$. Тогда $\chi_{[\Gamma]}$ можно вычислить посредством следующего алгоритма.

```
0:
```
Положим $k := 0$.

```
1:
```
Вычислим $f(k)$. Если $f(k)$ равно Φ, то выдадим 1. Если $f(k)$ равно $\neg\Phi$, то выдадим 0. Иначе положим $k := k + 1$ и `GoTo 1`.

Здесь $\Phi \in \mathrm{Sent}_\sigma$ — значение аргумента на входе.

Поскольку $[\Gamma]$ полно, алгоритм всегда завершает работу, причём Φ и $\neg\Phi$ не могут оба принадлежать $[\Gamma]$, в силу непротиворечивости Γ. $\square$

Замечание

Пожалуй, основной недостаток этого подхода заключается в отсутствии явной оценки на количество шагов, нужное для решения вопроса о принадлежности σ-предложения к $[\Gamma]$.

Следствие

Для всякой σ-структуры $\mathfrak{A}$, если $\mathrm{Th}(\mathfrak{A})$ *перечислимо, то* $\mathrm{Th}(\mathfrak{A})$ *разр.*

Доказательство.

Достаточно заметить, что $\mathrm{Th}(\mathfrak{A})$ непротиворечиво и полно. $\square$

Замечание

Значит, чтобы доказать разрешимость $\mathrm{Th}(\mathfrak{A})$, достаточно построить перечислимое $\Gamma \subseteq \mathrm{Sent}_\sigma$ такое, что $[\Gamma] = \mathrm{Th}(\mathfrak{A})$.

Метод элиминации кванторов

Обозначим за $\mathrm{Form}^{\circ}_{\sigma}$ множество всех бескванторных σ-формул.

Пусть $\Gamma \subseteq \mathrm{Sent}_{\sigma}$. Говорят, что Γ допускает (эффективную) элиминацию кванторов, если существует (вычислимая) функция τ, которая по каждой $\Phi \in \mathrm{Form}_{\sigma}$ строит $\tau(\Phi) \in \mathrm{Form}^{\circ}_{\sigma}$ такую, что

$$\Gamma \vdash \Phi \leftrightarrow \tau(\Phi) \quad \text{и} \quad \mathrm{FV}(\tau(\Phi)) \subseteq \mathrm{FV}(\Phi).$$

Замечание

Для удобства мы будем считать, что в нашем языке имеются специальные логические константы

$$\top \quad \text{и} \quad \bot,$$

которые являются замкнутыми атомарными σ-формулами. Поэтому $\mathrm{Atom}_{\sigma} \cap \mathrm{Sent}_{\sigma}$ будет непусто даже в случае, когда $\mathrm{Const}_{\sigma} = \varnothing$.

Предложение

Пусть $\Gamma \subseteq \mathrm{Sent}_\sigma$ *допускает эф. элиминацию кванторов, и* $[\Gamma] \cap \mathrm{Form}^\circ_\sigma$ *разрешимо. Тогда* $[\Gamma]$ *разрешимо.*

Доказательство.

Пусть τ реализует эффективную элиминацию кванторов в Γ. Тогда, в частности, для любого $\Phi \in \mathrm{Sent}_\sigma$,

$$\Gamma \vdash \Phi \quad \Longleftrightarrow \quad \Gamma \vdash \tau(\Phi),$$

что можно переписать как

$$\Phi \ \in \ [\Gamma] \quad \Longleftrightarrow \quad \tau(\Phi) \ \in \ [\Gamma] \cap \mathrm{Form}^\circ_\sigma.$$

Стало быть, $[\Gamma] \leqslant [\Gamma] \cap \mathrm{Form}^\circ_\sigma$. Поэтому из разрешимости $[\Gamma] \cap \mathrm{Form}^\circ_\sigma$ следует разрешимость $[\Gamma]$. $\square$

Предложение

Пусть существует вычислимая функция ρ, которая по каждой σ-формуле Φ вида $\exists x\, \Psi$, где Ψ бескванторная, строит бескวант. σ-формулу $\rho(\Phi)$ такую, что

$$\Gamma \vdash \Phi \leftrightarrow \rho(\Phi) \quad \textit{и} \quad \mathrm{FV}(\rho(\Phi)) \subseteq \mathrm{FV}(\Phi).$$

Тогда Γ допускает эффективную элиминацию кванторов.

Доказательство.

Определим нужную τ по рекурсии следующим образом.

- Если Φ бескванторная, то $\tau(\Phi) := \Phi$.

...

Доказательство (продолжение).

- Если $\Phi = \Psi \circ \Theta$, где $\circ \in \{\wedge, \vee, \rightarrow\}$, то $\tau(\Phi) := \tau(\Psi) \circ \tau(\Theta)$.
- Если $\Phi = \neg\Psi$, то $\tau(\Phi) := \neg\tau(\Psi)$.
- Если $\Phi = \exists x\, \Psi$, то $\tau(\Phi) := \rho(\exists x\, \tau(\Psi))$.
- Если $\Phi = \forall x\, \Psi$, то $\tau(\Phi) := \neg\rho(\exists x\, \neg\tau(\Psi))$.

Легко проверить, что для всех $\Phi \in \mathrm{Form}_\sigma$,

$$\Gamma \vdash \Phi \leftrightarrow \tau(\Phi) \quad \text{и} \quad \mathrm{FV}(\tau(\Phi)) \subseteq \mathrm{FV}(\Phi),$$

т.е. τ реализует эффективную элиминацию кванторов в Γ. $\square$

Предложение

Пусть $\Gamma \subseteq \mathrm{Sent}_\sigma$ *допускает элиминацию кванторов,* $[\Gamma]$ *перечислимо. Тогда* Γ *допускает эффективную элиминацию кванторов.*

Доказательство.

Очевидно, $[\Gamma]$ непусто, а значит, найдётся вычислимая $f : \mathbb{N} \to \mathrm{Form}_\sigma$ такая, что $\mathrm{range}\, f = [\Gamma]$. Рассмотрим следующий алгоритм.

0: Положим $k := 0$.

1: Вычислим $f(k)$. Если $f(k)$ имеет вид $\Phi \leftrightarrow \Psi$, где $\Psi \in \mathrm{Form}^{\circ}_{\sigma}$, то выдадим Ψ. Иначе положим $k := k + 1$ и `GoTo 1`.

Здесь $\Phi \in \mathrm{Form}_\sigma$ — значение аргумента на входе.

Раз Γ допускает элиминацию кванторов, алгоритм всегда завершает работу. Вычисляемая им функция τ является искомой. $\square$

Замечание

Недостаток этого подхода заключается в отсутствии явной оценки на количество шагов, нужное для нахождения эквивалентной по модулю Γ бескванторной σ-формулы.

С другой стороны, в (неэффективной) элиминации кванторов можно применять более универсальные по своей природе теоретико-модельные методы, однако о них мы практически не говорили.

Возьмём $\langle =^2, <^2 \rangle$ в качестве σ.

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

Теорема

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

Доказательство.

Начнём с частного, но принципиального случая. Пусть $\Omega_0, \ldots, \Omega_n$ — атомарные σ-формулы, а x — переменная. Возьмём

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

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

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

...

Доказательство (продолжение).

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

- если Ω_i не содержит x, то

$$\vdash \exists x\, \Theta \leftrightarrow (\Omega_i \wedge \exists x\, (\Omega_0 \wedge \cdots \wedge \Omega_{i-1} \wedge \Omega_{i+1} \wedge \cdots \wedge \Omega_n));$$

- если Ω_i совпадает с $x < x$, то

$$\mathrm{Th}\,(\mathfrak{Q}) \vdash \exists x\, \Theta \leftrightarrow \bot.$$

- если Ω_i совпадает с $x = x$, причём $n > 0$, то

$$\vdash \exists x\, \Theta \leftrightarrow \exists x\, (\Omega_0 \wedge \cdots \wedge \Omega_{i-1} \wedge \Omega_{i+1} \wedge \cdots \wedge \Omega_n).$$

- если Ω_i совпадает с $x = x$, причём $n = 0$, т.е. Θ совп. с $x = x$, то

$$\vdash \exists x\, \Theta \leftrightarrow \top.$$

...

Доказательство (продолжение).

Поэтому, не ограничивая общности, мы можем считать, что:

a. x входит в каждую из $\Omega_0, \ldots, \Omega_n$;

b. ни $x = x$, ни $x < x$ не встречается среди $\Omega_0, \ldots, \Omega_n$.

Теперь избавиться от квантора в $\exists x\, \Theta$ можно следующим образом.

- Если одно из $\Omega_0, \ldots, \Omega_n$ имеет вид $x = y$, где $y \in \mathrm{Var} \setminus \{x\}$, то

$$\vdash \exists x\, \Theta \leftrightarrow \Theta\,(x/y).$$

- Если Θ имеет вид $\bigwedge_{i=0}^{n} u_i < x$, где $\{u_0, \ldots, u_n\} \subseteq \mathrm{Var} \setminus \{x\}$, то

$$\mathrm{Th}\,(\mathfrak{Q}) \vdash \exists x\, \Theta \leftrightarrow \top.$$

  Аналогично для $\bigwedge_{i=0}^{n} x < u_i$.

...

Доказательство (продолжение).

- Если Θ (с точностью до порядка конъюнктов) имеет вид

$$\left(\bigwedge\nolimits_{i=0}^{k} u_i < x\right) \wedge \left(\bigwedge\nolimits_{j=0}^{l} x < v_j\right),$$

где $\{u_0, \ldots, u_k, v_0, \ldots, v_l\} \subseteq \mathrm{Var} \setminus \{x\}$, то

$$\mathrm{Th}\,(\mathfrak{Q}) \vdash \exists x\, \Theta \leftrightarrow \left(\bigwedge\nolimits_{i=0}^{m} \bigwedge\nolimits_{j=0}^{l} u_i < v_j\right).$$

В конце мы получим искомую бескванторную формулу $\Theta_{\exists x}$, которая эквивалентна $\exists x\, \Theta$ по модулю $\mathrm{Th}\,(\mathfrak{Q})$.

. . .

Доказательство (продолжение).

Переходя к общему случаю, рассмотрим σ-формулу

$$\Phi \;=\; \exists x\, \Psi\,(x, \vec{y}),$$

где $\Psi \in \mathrm{Form}^{\circ}_{\sigma}$. Нужно построить $\rho\,(\Phi) \in \mathrm{Form}^{\circ}_{\sigma}$ такую, что

$$\mathrm{Th}\,(\mathfrak{Q}) \vdash \Phi \leftrightarrow \rho\,(\Phi) \quad \text{и} \quad \mathrm{FV}\,(\rho\,(\Phi)) \;\subseteq\; \mathrm{FV}\,(\Phi).$$

Мы действуем следующим образом.

i. С помощью законов де Моргана и снятия двойного отрицания проносим $\neg$ внутрь $\Psi\,(x, \vec{y})$, чтобы $\neg$ стояло только перед атомарными подформулами.

...

Доказательство (продолжение).

ii. Избавляемся от $\neg$ (перед атом. подформулами), используя

$$\mathrm{Th}\,(\mathfrak{Q}) \vdash \neg x < y \leftrightarrow (x = y \vee y < x),$$
$$\mathrm{Th}\,(\mathfrak{Q}) \vdash \neg x = y \leftrightarrow (x < y \vee y < x).$$

iii. Применяя законы дистрибутивности, получаем

$$\Theta_0 \vee \cdots \vee \Theta_n,$$

где $\Theta_0, \ldots, \Theta_n$ суть конъюнкции атомарных формул; при этом, как известно,

$$\vdash \exists x\,(\Theta_0 \vee \cdots \vee \Theta_n) \leftrightarrow \exists x\,\Theta_0 \vee \cdots \vee \exists x\,\Theta_n.$$

Описанный ранее алгоритм позволяет избавиться от кванторов в $\exists x\,\Theta_0, \ldots, \exists x\,\Theta_n$. В итоге получится $\rho\,(\Phi)$.

Наконец, из ρ можно сделать желаемую τ. $\square$

Обозначим через DLO конъюнкцию следующих σ-предложений:

- $\forall x\, x \not< x$;
- $\forall x\, \forall y\, \forall z\, (x < y \wedge y < z \to x < z)$;
- $\forall x\, \forall y\, (x \neq y \to x < y \vee y < x)$;
- $\forall x\, \forall y\, (x < y \to \exists u\, (x < u < y))$.
- $\forall x\, \exists y\, (y < x)$;
- $\forall x\, \exists y\, (x < y)$.

Очевидно, Mod (DLO) — это класс всех плотных (строгих) линейных порядков без концов, или п.л.п. без концов.

Следствие

$\mathrm{Th}\,(\mathfrak{Q}) = [\mathrm{DLO}]$.

Доказательство.

Нетрудно проверить, что в приведённом выше доказательстве

«$\mathrm{Th}\,(\mathfrak{Q}) \vdash$» всюду можно заменить на «$\mathrm{DLO} \vdash$».

Стало быть, функция τ реализует элиминацию кванторов и в $\mathrm{Th}\,(\mathfrak{Q})$, и в DLO. В частности, для всякого $\Phi \in \mathrm{Sent}_\sigma$:

$$\begin{aligned} \mathrm{DLO} \vdash \Phi \quad &\Longleftrightarrow \quad \mathrm{DLO} \vdash \tau\,(\Phi); \\ \mathrm{Th}\,(\mathfrak{Q}) \vdash \Phi \quad &\Longleftrightarrow \quad \mathrm{Th}\,(\mathfrak{Q}) \vdash \tau\,(\Phi). \end{aligned}$$

...

Доказательство (продолжение).

Поэтому достаточно показать, что для всех бескв. σ-предложений Ψ,

$$\mathsf{DLO} \vdash \Psi \quad \Longleftrightarrow \quad \mathsf{Th}(\mathfrak{Q}) \vdash \Psi,$$

т.е. $[\mathsf{DLO}] \cap \mathsf{Form}^{\circ}_{\sigma} = \mathsf{Th}(\mathfrak{Q}) \cap \mathsf{Form}^{\circ}_{\sigma}$.

Пусть Ψ — бескванторное σ-предложение. Ясно, что Ψ представляет собой булеву комбинацию $\perp$ и $\top$, так как $\mathsf{Const}_{\sigma} = \varnothing$. Поэтому либо $\vDash \Psi$, либо $\vDash \neg\Psi$.

- Если $\vDash \Psi$, то $\vdash \Psi$, а потому $\mathsf{DLO} \vdash \Psi$ и $\mathsf{Th}(\mathfrak{Q}) \vdash \Phi$.
- Если $\vDash \neg\Psi$, то $\mathsf{DLO} \nvdash \Psi$ и $\mathsf{Th}(\mathfrak{Q}) \nvdash \Phi$, поскольку DLO и $\mathsf{Th}(\mathfrak{Q})$ выполнимы.

$\square$

Альтернативное рассуждение.

Для каждого σ-предложения Φ,

$$\begin{aligned} \mathrm{DLO} \vdash \Phi \quad & \Longleftrightarrow \quad \Phi \text{ истинно во всех п.л.п. без концов} \\ & \Longleftrightarrow \quad \Phi \text{ истинно во всех счётных п.л.п. без концов} \\ & \Longleftrightarrow \quad \Phi \text{ истинно в } \mathfrak{Q}. \end{aligned}$$

Тут последняя эквивалентность обусловлена тем, что, как мы знаем, любой счётный п.л.п. без концов изоморфен $\mathfrak{Q}$. Этот факт ещё формулируют так: DLO категорична в мощности $\aleph_0$.

Следствие

$\mathrm{Th}(\mathfrak{Q})$ *разрешимо.*

Доказательство.

Достаточно заметить, что $\mathrm{Th}(\mathfrak{Q}) \cap \mathrm{Form}_{\sigma}^{\circ}$ разрешимо. $\square$

Альтернативное рассуждение.

Так как $\mathrm{Th}(\mathfrak{Q}) = [\mathrm{DLO}]$, $\mathrm{Th}(\mathfrak{Q})$ перечислимо, а значит, и разрешимо (ввиду своей полноты).

Более того, элиминация кванторов позволяет получать явные оценки на временную/ёмкостную сложность разрешающей процедуры, тогда как альтернативный подход такой возможности не даёт.

Следствие

Пусть $S \subseteq \mathbb{Q}$ определимо в $\mathfrak{Q}$. Тогда $S = \varnothing$ или $S = \mathbb{Q}$.

Доказательство.

Пусть $\Phi(x)$ определяет S в $\mathfrak{Q}$. Тогда $\tau(\Phi(x))$ также определяет S в $\mathfrak{Q}$. Однако $\tau(\Phi(x))$ представляет собой булеву комбинацию формул видов $x = x$ и $x < x$. Стало быть,

$$\text{либо } \mathfrak{Q} \Vdash \forall x\, \tau(\Phi(x)), \quad \text{либо } \mathfrak{Q} \Vdash \forall x\, \neg\tau(\Phi(x)).$$

□

Альтернативное рассуждение.

Как мы знаем, определимые в $\mathfrak{Q}$ множества замкнуты относительно автоморфизмов $\mathfrak{Q}$. Далее, «челночная конструкция» позволяет нам для любых $p, q \in \mathbb{Q}$ найти $\xi \in \mathrm{Aut}(\mathfrak{Q})$ такой, что $\xi(p) = q$. Поэтому, если $S \subseteq \mathbb{Q}$ замк. отн. автоморфизмов $\mathfrak{Q}$, то $S = \varnothing$ или $S = \mathbb{Q}$.

Общие комментарии

Эффективная элиминация кванторов в $\mathrm{Th}(\mathfrak{A})$, если она возможна, нередко позволяет:

- построить разрешимое множество аксиом для $\mathrm{Th}(\mathfrak{A})$;
- получить явный разрешающий алгоритм для $\mathrm{Th}(\mathfrak{A})$;
- дать исчерпывающее описание определимости в $\mathfrak{A}$.

Эффективная элиминация кванторов в Γ также нередко позволяет получить явный разрешающий алгоритм для $[\Gamma]$. Тут уже полнота может как иметь, так и не иметь места; так или иначе, бескванторные предложения куда проще, чем произвольные.

Здесь всюду речь идёт о «естественных» структурах и теориях.