Открытие неразрешимости 3:
Сводимость между алгоритмическими проблемами

Станислав Олегович Сперанский

ФМКН СПбГУ

12 декабря 2020

Напоминаю, что вычислимая $U :\subseteq \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ называется универсальной для $\mathscr{F}^\sharp$, если

$$\{U_n \mid n \in \mathbb{N}\} \;=\; \mathscr{F}^\sharp.$$

Кроме того, стандартным образом построенная U (из предыдущей лекции) обладает дополнительным полезным свойством:

- **!** для любой вычислимой $V :\subseteq \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ найдётся $\tau \in \mathscr{F}$ такая, что $V_k = U_{\tau(k)}$ для всех $k \in \mathbb{N}$.

Интуитивно τ представляет собой своего рода транслятор системы $\langle V_k : k \in \mathbb{N}\rangle$ в систему $\langle U_k : k \in \mathbb{N}\rangle$.

Утверждение

Существуют два полуразрешимых непересекающихся множества нат. чисел, которые нельзя отделить разрешимым множеством.

Доказательство.

Рассмотрим непересекающиеся множества

$$A := \{n \in \mathbb{N} \mid U(n,n) = 0\} \quad \text{и} \quad B := \{n \in \mathbb{N} \mid U(n,n) > 1\}.$$

Как можно убедиться, A и B полуразрешимы. Пусть $C \subseteq \mathbb{N}$ отделяет A и B, т.е.

$$A \subseteq C \quad \text{и} \quad B \subseteq \overline{C}.$$

Заметим, что $\chi_C \neq U_n$ для каждого $n \in \mathbb{N}$. Если C разрешимо, то χ_C вычислима — противоречие. □

Зафиксируем какую-нибудь универсальную вычислимую функцию U для $\mathscr{F}^\sharp$, обладающую полезным свойством. Для $F \subseteq \mathscr{F}^\sharp$ положим

$$[\![F]\!] := \{n \in \mathbb{N} \mid U_n \in F\}.$$

Когда $F = \{f\}$, мы пишем $[\![f]\!]$ вместо $[\![\{f\}]\!]$ для краткости.

Утверждение

Пусть $f, g \in \mathscr{F}^\sharp$, причём $f \neq g$. Тогда $[\![f]\!]$ и $[\![g]\!]$ нельзя отделить разрешимым множеством.

Доказательство.

Пусть A и B — непересекающиеся полуразрешимые множества натур. чисел, которые нельзя отделить разрешимым множеством. ...

Доказательство (продолжение).

Рассмотрим $V : \subseteq \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, действующую по правилу

$$V(k,n) := \begin{cases} f(n) & \text{если } k \in A \\ g(n) & \text{если } k \in B \\ \uparrow & \text{иначе.} \end{cases}$$

Нетрудно убедиться, что V вычислима, причём для любого $k \in \mathbb{N}$:

- если $k \in A$, то $V_k = f$;
- если $k \in B$, то $V_k = g$.

Далее, в силу полезного свойства, найдется $\tau \in \mathscr{F}$ такая, что

$$V_k = U_{\tau(k)} \quad \text{для всех } k \in \mathbb{N}.$$

Пусть $C \subseteq \mathbb{N}$ отделяет $[\![f]\!]$ и $[\![g]\!]$. Тогда $\tau^{-1}[C]$ отделяет A и B. Если C разрешимо, то $\tau^{-1}[C]$ разрешимо — противоречие. $\square$

Следствие («Теорема Райса»)

Пусть $F \subseteq \mathscr{F}^\sharp$, причём $F \neq \varnothing$ и $F \neq \mathscr{F}^\sharp$. Тогда $[\![F]\!]$ неразрешимо.

Доказательство.

Пусть $f \in F$ и $g \in \mathscr{F}^\sharp \setminus F$. Ясно, что

$$[\![f]\!] \subseteq [\![F]\!] \quad \text{и} \quad [\![g]\!] \subseteq \overline{[\![F]\!]}.$$

Очевидно, $[\![F]\!]$ отделяет $[\![f]\!]$ и $[\![g]\!]$, а потому оно неразрешимо. $\square$

Замечание

На самом деле, множества вида $[\![F]\!]$ нередко даже не являются полуразрешимыми. Например, известно, что $[\![\mathscr{F}]\!]$ не полуразрешимо.

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 $n \in \mathbb{N}$,

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

Например, Self $\leqslant$ Halt. Далее, пишут $A \equiv B$, называя A и B эквивалентными, если $A \leqslant B$ и $B \leqslant A$. Наконец, под степенями понимают классы эквивалентности по $\equiv$.

Замечание

На самом деле, с помощью полезного свойства можно показать, что Halt $\leqslant$ Self, откуда Halt $\equiv$ Self.

Замечание (продолжение)

Рассмотрим $V : \subseteq \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, действующую по правилу

$$V(k, n) := \begin{cases} 1 & \text{если } k \in \mathrm{Halt} \\ \uparrow & \text{иначе.} \end{cases}$$

Нетрудно убедиться, что V вычислима, причём для любого $k \in \mathbb{N}$:

- если $k \in \mathrm{Halt}$, то $V_k = \mathbf{1}$;
- если $k \notin \mathrm{Halt}$, то V_k — «пустая функция».

Далее, в силу полезного свойства, найдется $\tau \in \mathscr{F}$ такая, что

$$V_k = U_{\tau(k)} \quad \text{для всех } k \in \mathbb{N}.$$

Легко понять, что τ сводит Halt к Self.

Утверждение

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

Доказательство.

Пусть f сводит A к B, а g — B к C. Тогда для любого $n \in \mathbb{N}$,

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

Стало быть, $f \circ g$ сводит A к C. □

Значит, $\leqslant$ — предпорядок на подмножествах $\mathbb{N}$, который, разумеется, индуцирует (частичный) порядок на степенях подмножеств $\mathbb{N}$.

Утверждение

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

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

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

Доказательство.

Пусть f сводит A к B. Заметим, 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^*. □

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. С другой стороны:

Теорема

Всякое полуразрешимое множество натур. чисел сводится к Halt.

Доказательство.

Пусть $A \subseteq \mathbb{N}$ полуразрешимо. Значит, существует $f \in \mathscr{F}^\sharp$ такая, что $A = \operatorname{dom} f$. Далее, $f = U_k$ для некоторого $k \in \mathbb{N}$, в силу универсальности U для $\mathscr{F}^\sharp$. Тогда для любого $n \in \mathbb{N}$,

$$\begin{aligned} n \in A &\iff n \in \operatorname{dom} f \\ &\iff U_k(n)\downarrow \\ &\iff 2^k \cdot 3^n \in \text{Halt}. \end{aligned}$$

Стало быть, $\lambda n.\left[2^k \cdot 3^n\right]$ сводит A к Halt. □

Ввиду этого результата, говорят, что Halt является полным в классе всех полуразрешимых множеств.

$10^{\text{ая}}$ проблема Гильберта

Вопросы об алгоритмической разрешимости разнообразных математических проблем обычно можно переформулировать как вопросы о разрешимости подходящих подмножеств $\mathbb{N}$.

Диофантова проблема над $\mathbb{N}$

Обозначим через Poly множество всех полиномов с коэффициентами из $\mathbb{N}$ от произвольного числа переменных. **Задача:** по данным $p, q \in \mathrm{Poly}$ понять, имеет ли уравнение $p = q$ решение в $\mathbb{N}$.

Этой проблеме соответствует множество

$$\mathrm{DE}(\mathbb{N}) := \left\{(p, q) \in \mathrm{Poly}^2 \mid p = q \text{ имеет решение в } \mathbb{N}\right\},$$

которое можно отождествить с подходящим числовым множеством.

По аналогии для $F \subseteq \mathbb{R}$ можно рассмотреть

$$\mathrm{DE}(F) := \{(p, q) \in \mathrm{Poly}^2 \mid p = q \text{ имеет решение в } F\}.$$

В частности, естественным образом возникают следующие вопросы.

$10^{\text{ая}}$ проблема Гильберта над $\mathbb{N}$

Разрешимо ли $\mathrm{DE}(\mathbb{N})$?

$10^{\text{ая}}$ проблема Гильберта над $\mathbb{Z}$

Разрешимо ли $\mathrm{DE}(\mathbb{Z})$?

$10^{\text{ая}}$ проблема Гильберта над $\mathbb{Q}$

Разрешимо ли $\mathrm{DE}(\mathbb{Q})$?

При этом легко видеть, что $\mathrm{DE}(\mathbb{N})$, $\mathrm{DE}(\mathbb{Z})$ и $\mathrm{DE}(\mathbb{Q})$ полуразрешимы.

$A \subseteq \mathbb{N}^\ell$ называют диофантовым, если существуют полиномы

$$\mathrm{p}\left(x_1, \ldots, x_\ell, \vec{y}\right) \quad \text{и} \quad \mathrm{q}\left(x_1, \ldots, x_\ell, \vec{y}\right)$$

с коэффициентами из $\mathbb{N}$ такие, что

$$A = \left\{ (n_1, \ldots, n_\ell) \in \mathbb{N}^\ell \mid \begin{array}{c} \mathrm{p}\left(n_1, \ldots, n_\ell, \vec{y}\right) = \mathrm{q}\left(n_1, \ldots, n_\ell, \vec{y}\right) \\ \text{для некоторых } \vec{y} \text{ из } \mathbb{N}. \end{array} \right\}.$$

Имеет место следующий важный результат.

Теорема Матиясевича–Робинсон–Дэвиса–Патнэма; без док-ва

Для любого $A \subseteq \mathbb{N}^\ell$,

$$A \text{ полуразрешимо} \iff A \text{ диофантово.}$$

Следствие

$\mathrm{DE}(\mathbb{N}) \equiv \mathrm{Halt}$, *а потому* $\mathrm{DE}(\mathbb{N})$ *неразрешимо.*

Доказательство.

В силу теоремы М.–Р.–Д.–П., найдутся полиномы $\mathrm{p}(x, \vec{y})$ и $\mathrm{q}(x, \vec{y})$ с коэффициентами из $\mathbb{N}$ такие, что для любого $n \in \mathbb{N}$,

$$\begin{aligned} n \in \mathrm{Halt} &\iff \mathrm{p}(n, \vec{y}) = \mathrm{q}(n, \vec{y}) \text{ для нек. } \vec{y} \text{ из } \mathbb{N} \\ &\iff (\mathrm{p}_n^x(\vec{y}), \mathrm{q}_n^x(\vec{y})) \in \mathrm{DE}(\mathbb{N}). \end{aligned}$$

Стало быть, $\mathrm{Halt} \leqslant \mathrm{DE}(\mathbb{N})$. Кроме того, всякое полуразрешимое множество сводится к Halt, откуда $\mathrm{DE}(\mathbb{N}) \leqslant \mathrm{Halt}$. □

Следствие

$\mathrm{DE}(\mathbb{Z}) \equiv \mathrm{DE}(\mathbb{N})$, *а потому* $\mathrm{DE}(\mathbb{Z})$ *неразрешимо.*

Доказательство.

Сначала сведём $\mathrm{DE}(\mathbb{Z})$ к $\mathrm{DE}(\mathbb{N})$. Нужно построить вычислимую процедуру, которая по любым $p, q \in \mathrm{Poly}$ строит $p', q' \in \mathrm{Poly}$ так, чтобы

$$(p, q) \in \mathrm{DE}(\mathbb{Z}) \iff (p', q') \in \mathrm{DE}(\mathbb{N}).$$

Пусть $p(x_1, \ldots, x_k)$ и $q(x_1, \ldots, x_k)$ суть полиномы с коэффициентами из $\mathbb{N}$. Рассмотрим равенство

$$p(u_1 - v_1, \ldots, u_k - v_k) = q(u_1 - v_1, \ldots, u_1 - v_1).$$

Очевидно, его можно эффективно привести к виду $p' = q'$, где p' и q' суть полиномы от $u_1, \ldots, u_k, v_1, \ldots, v_k$ с коэффициентами из $\mathbb{N}$. ...

Доказательство (продолжение).

Давайте сведём $\mathrm{DE}(\mathbb{N})$ к $\mathrm{DE}(\mathbb{Z})$. Нужно построить вычислимую процедуру, которая по любым $\mathrm{p}, \mathrm{q} \in \mathrm{Poly}$ строит $\mathrm{p}', \mathrm{q}' \in \mathrm{Poly}$ так, чтобы

$$(\mathrm{p}, \mathrm{q}) \in \mathrm{DE}(\mathbb{N}) \iff (\mathrm{p}', \mathrm{q}') \in \mathrm{DE}(\mathbb{Z}).$$

Пусть $\mathrm{p}(x_1, \ldots, x_k)$ и $\mathrm{q}(x_1, \ldots, x_k)$ суть полиномы с коэффициентами из $\mathbb{N}$. Рассмотрим равенство

$$\mathrm{p}\left(t_1^2 + u_1^2 + v_1^2 + w_1^2, \ldots, t_k^2 + u_k^2 + v_k^2 + w_k^2\right) = \mathrm{q}\left(t_1^2 + u_1^2 + v_1^2 + w_1^2, \ldots, t_k^2 + u_k^2 + v_k^2 + w_k^2\right).$$

В качестве p' и q' возьмём его левую и правую части. □

Замечание

Вместе с тем $10^{\text{ая}}$ проблема Гильберта над $\mathbb{Q}$ остаётся открытой.

Общие комментарии

- Теория вычислимости, также известная как теория рекурсии / теория алгоритмов, — глубокий предмет. Так, про одни только перечислимые множества можно написать увесистую книгу.
- Результаты и методы теории вычислимости во многом вдохновили то, что происходит в теории вычислит. сложности.
- В основе теории вычислимости лежат работы пионеров матем. логики и информатики, таких как Гёдель, Карри, Клини, фон Нейман, Петер, Пост, Тьюринг и Чёрч.

Postlude: Историческая справка

Советские математики внесли большой вклад в применение методов теории вычислимости в алгебре. В частности:

- П. С. Новиков, С. И. Адян и др. получили ключевые результаты в алгоритмической теории групп. [Мск]
- А. И. Мальцев, Ю. Л. Ершов и др. получили важные теоремы о теориях классов колец, решёток и так далее. [Нск]
- Ю. В. Матиясевич завершил доказательство неразрешимости проблемы Диофанта над целыми числами. [СПб]

Базовая литература

Enderton, H. *Computability Theory*. Academic Press, 2011.

Неплохое пособие на английском.

Когабаев, Н. Т. *Лекции по теории алгоритмов*. Изд-во НГУ, 2009.

Здесь можно найти аккуратное построение универсальной функции, а также доказательство результата об эквивалентности некоторых моделей вычислимости.

Роджерс, Х. *Теория рекурсивных функций и эффективная вычислимость*. — Пер. с англ. — Мир, 1972.

Классический - пусть и несколько устаревший - учебник по теории вычислимости.