Математическая логика: 2

Станислав Олегович Сперанский

Санкт-Петербургский государственный университет

Санкт-Петербург 2020

Prelude: Формализация вычислимости

Неформальное, интуитивное понятие алгоритма использовалось на протяжении практически всей истории математики.

Традиционно конкретные алгоритмы представлялись в виде конечных наборов простых инструкций, которые можно было выполнять «по шагам». Однако до XX века никаких универсальных, общепринятых языков для записи алгоритмов не существовало.

Математики были уверены: если нужный алгоритм существует, мы его найдём. Но даже если так, как узнать, существует ли алгоритм, т.е. разрешима ли задача алгоритмически?

- Мы знаем алгоритм решения линейных диофантовых уравнений над целыми числами. Как насчёт полиномиальных?
  - Можно попробовать найти алгоритм.
- Но может ли случиться так, что алгоритма не существует?
  - Наверное. В таком случае нет смысла его искать.
- Но как мы узнаем, что алгоритма не существует?
  - Можно попытаться показать, что никакой алгоритм не способен решить интересующую нас задачу.
- Но как перебрать все возможные алгоритмы?... И, вообще, что такое алгоритм как абстрактно-математическое понятие?...

Мораль

Если мы хотим уметь доказывать алгоритмическую неразрешимость, интуитивному, неформальному понятию алгоритма необходимо дать строгое математическое, формальное определение.

«Математизация» алгоритмов была осуществлена логиками в 1930х, где стоит особо отметить труды Гёделя, Тьюринга и Чёрча.

Впоследствии эти труды приведут к созданию архитектуры современного ПО и различных языков программирования.

В 1930х появились первые примеры алгоритмически неразрешимых задач, которые затем многократно применялись для доказательства неразрешимости задач в алгебре, топологии и так далее.

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

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

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

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

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

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

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 полухарактеристической функцией A.

Предложение

Для любого $A \subseteq \mathbb{N}$,

$$A \text{ перечислимо} \iff \chi_A^* \text{ вычислима.}$$

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 1, т.е. $1 = \lambda n.[1]$. Тогда

$$\chi_A^* \;=\; f \circ 1.$$

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. $\square$

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 $B \leqslant A$; 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

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

$$\mathsf{NP} \;:=\; \begin{array}{l}\text{класс всех множеств, характеристические функции}\\ \text{которых вычислимы за пол. время посредством}\\ \textit{недетерминированных}\text{ машин Тьюринга.}\end{array}$$

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

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

в силу 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

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.

Яркий пример

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

Диофантова проблема над $\mathbb{Z}$

Обозначим за Poly множество всех полиномов с коэффициентами из $\mathbb{Z}$ от произвольного числа переменных. **Задача**: по данному $p \in \mathrm{Poly}$ понять, имеет ли уравнение $p = 0$ решение в $\mathbb{Z}$.

Этой проблеме соответствует множество

$$\mathrm{DE}(\mathbb{Z}) := \{p \in \mathrm{Poly} \mid p = 0 \text{ имеет решение в } \mathbb{Z}\},$$

которое можно отождествить с подходящим подмножеством $\mathbb{N}$.

Легко убедиться, что $\mathrm{DE}(\mathbb{Z})$ перечислимо.

Десятая проблема Гильберта над $\mathbb{Z}$

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

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

$\mathrm{DE}(\mathbb{Z}) \equiv \mathrm{Halt}$. *В частности,* $\mathrm{DE}(\mathbb{Z})$ *неразрешимо.*

По аналогии с $\mathrm{DE}(\mathbb{Z})$ можно определить $\mathrm{DE}(\mathbb{Q})$, которое, как легко видеть, перечислимо. Известный открытый вопрос:

Десятая проблема Гильберта над $\mathbb{Q}$

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

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]

Общие комментарии

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

Некоторая литература

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 базовой теории вычислимости. Посвежее: Soare, R. I. *Turing Computability*. Springer, 2016.