Открытие неразрешимости 2:
Полуразрешимые множества

Станислав Олегович Сперанский

ФМКН СПбГУ

12 декабря 2020

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 понимаются р-машины, например.

В наших 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 регистровой машины.

Пусть $\mathcal{D}$ — дискретный «тип данных», и нас интересуют элементы $\mathcal{D}$, обладающие определённым свойством $\mathscr{P}$. Иными словами, нас волнует решение следующей задачи:

По данному $d \in \mathcal{D}$ понять, обладает ли оно свойством $\mathscr{P}$.

Этой задаче соответствует множество

$$\{d \in \mathcal{D} \mid d \text{ обладает свойством } \mathscr{P}\},$$

которое можно отождествить с подходящим подмножеством $\mathbb{N}^{\ell}$ посредством какой-нибудь эффективной кодирующей процедуры.

Функции vs. множества

Для $f :\subseteq \mathbb{N}^\ell \to \mathbb{N}$ положим

$$\Gamma_f \;:=\; \{(\vec{n}, m) \in \mathbb{N}^\ell \times \mathbb{N} \mid f(\vec{n}) = m\},$$

т.е. Γ_f — это график частичной функции f.

Замечание

Если $\mathcal{A}$ — алгоритм, то для каждого $\vec{n} \in \mathbb{N}^\ell$ через $\mathcal{A}(\vec{n})$ мы будем обозначать результат, который выдаёт $\mathcal{A}$ на входе $\vec{n}$.

$A \subseteq \mathbb{N}^\ell$ называется разрешимым, если χ_A вычислима, и полуразрешимым, если χ_A^* вычислима. При этом нетрудно убедиться, что из разрешимости следует полуразрешимость.

Утверждение

$f : \mathbb{N}^\ell \to \mathbb{N}$ *вычислима, если и только если* Γ_f *разрешимо.*

Доказательство.

Для наглядности давайте считать, что $\ell = 1$.

$\boxed{\Longrightarrow}$ Тривиально.

$\boxed{\Longleftarrow}$ Пусть χ_{Γ_f} вычисляется посредством некот. алгоритма $\mathcal{A}$. Тогда f вычисляется посредством следующего алгоритма.

?: На входе — произвольное n.

0: Положим $k := 0$.

1: Если $\mathcal{A}(n, k) = 1$, то выдадим k.

2: Положим $k := k + 1$. GoTo 1. $\square$

Утверждение

$f :\subseteq \mathbb{N}^{\ell} \to \mathbb{N}$ *вычислима, если и только если* Γ_f *полуразрешимо.*

Доказательство.

Для наглядности давайте считать, что $\ell = 1$.

$\Longrightarrow$ Тривиально.

$\Longleftarrow$ Пусть $\chi^*_{\Gamma_f}$ вычисляется посредством некот. алгоритма $\mathcal{A}$. Тогда f вычисляется посредством следующего алгоритма.

?: На входе — произвольное n.

0: Положим $k := 0$.

1: Перебираем i, j от 0 до k: если $\mathcal{A}$ останавливается на входе (n, i) после j шагов, то выдадим i.

2: Положим $k := k + 1$. `GoTo 1`. $\square$

По поводу дополнений

Пусть $A \subseteq \mathbb{N}^\ell$. Под дополнением A относительно $\mathbb{N}^\ell$ понимают

$$\overline{A} \;:=\; \{\vec{n} \in \mathbb{N}^\ell \mid \vec{n} \notin A\}.$$

Когда из контекста ясно, о каком $\mathbb{N}^\ell$ идёт речь, уточнение «относительно $\mathbb{N}^\ell$» обычно опускают.

Утверждение

$A \subseteq \mathbb{N}^\ell$ разрешимо, если и только если $\overline{A}$ разрешимо.

Доказательство.

Достаточно заметить, что $\chi_{\overline{A}}(\vec{n}) = 1 - \chi_A(\vec{n})$ для всех $\vec{n} \in \mathbb{N}^\ell$. □

Теорема («Теорема Поста»)

$A \subseteq \mathbb{N}^{\ell}$ *разрешимо, если и только если* A *и* $\overline{A}$ *полуразрешимы.*

Доказательство.

Для наглядности давайте считать, что $\ell = 1$.

$\boxed{\Longrightarrow}$ Тривиально.

$\boxed{\Longleftarrow}$ Пусть χ^*_A, $\chi^*_{\overline{A}}$ вычисляются посредством некот. алгоритмов $\mathcal{A}$, $\overline{\mathcal{A}}$. Тогда χ_A вычисляется посредством следующего алгоритма.

?: На входе — произвольное n.

0: Положим $k := 0$.

1: Если $\mathcal{A}$ ост. на входе n после k шагов, то выдадим 1.

2: Если $\overline{\mathcal{A}}$ ост. на входе n после k шагов, то выдадим 0.

3: Положим $k := k + 1$. `GoTo 1`. $\square$

Замечание

Стало быть, для любого полуразрешимого $A \subseteq \mathbb{N}^\ell$,

$$\overline{A} \text{ полуразрешимо} \quad \Longleftrightarrow \quad A \text{ разрешимо.}$$

Поэтому, если A полуразрешимо, но не разрешимо, то дополнение A не полуразрешимо. Вскоре мы убедимся, что такие множества действительно существуют.

Interlude: Перечислимость

$A \subseteq \mathbb{N}$ называют перечислимым, если либо A пусто, либо найдётся вычислимая $f : \mathbb{N} \to \mathbb{N}$ такая, что

$$A = \{ f(0), f(1), \dots \},$$

т.е. A совпадает с областью значений f, обозначаемой range f.

Утверждение

Для любого $A \subseteq \mathbb{N}$,

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

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^* вычисляется посредством следующего алгоритма.

?: На входе — произвольное n.

0: Положим $k := 0$.

1: Вычислим $f(k)$. Если $f(k) = n$, то выдадим 1.

2: Положим $k := k + 1$. GoTo 1.

...

Доказательство (продолжение).

$\Longleftarrow$ Пусть χ_A^* вычисляется посредством некот. алгоритма $\mathcal{A}$. Легко убедиться, что существуют вычислимые $h_1, h_2 : \mathbb{N} \to \mathbb{N}$ такие, что

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

Зафиксируем какой-нибудь $a \in A$. Теперь рассмотрим $f : \mathbb{N} \to \mathbb{N}$, вычисляемую посредством следующего алгоритма.

?: На входе — произвольное n.

0: Вычислим $h_1(n)$ и $h_2(n)$. Если $\mathcal{A}$ останавливается на входе $h_1(n)$ за $h_2(n)$ шагов, то выдадим $h_1(n)$. Иначе выдадим a.

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

Следствие

$A \subseteq \mathbb{N}$ перечислимо, если и только если $A = \operatorname{dom} f$ для некоторой 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, если и только если $A = \operatorname{range} f$ для некоторой 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. $\square$

Упражнение

$A \subseteq \mathbb{N}$ перечислимо, е.т.е. существует разрешимое $S \subseteq \mathbb{N}^2$ такое, что

$$A = \{n \in \mathbb{N} \mid \exists m\, S(m, n)\}.$$

Значит, полуразрешимые подмножества $\mathbb{N}$ суть в точности проекции разрешимых подмножеств $\mathbb{N}^2$.

Замечание

Вместе с тем полуразрешимые множества в целом замкнуты относительно проекций: проекция каждого полуразрешимого подмножества $\mathbb{N}^2$ является полуразрешимым подмножеством $\mathbb{N}$.

Замечание

Определим $\text{pair} : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ 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 $\text{left}, \text{right} : \mathbb{N} \to \mathbb{N}$ 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 $\ell\text{-tuple}$ из $\mathbb{N}^\ell$ на $\mathbb{N}$:

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

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

Замечание

В литературе немалую популярность приобрела функция

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

называемая канторовской нумерующей функцией. Можно проверить, что она также является биекцией из $\mathbb{N}\times\mathbb{N}$ на $\mathbb{N}$.

Теорема Фуетера–Полиа; без доказательства

Канторовская нумерующая функция и её симметричная версия суть единственные «квадратичные» биекции из $\mathbb{N}\times\mathbb{N}$ на $\mathbb{N}$.

Для удобства введём обозначения:

$$\mathscr{F}^{\sharp} \;:=\; \{f :\subseteq \mathbb{N} \to \mathbb{N} \mid f \text{ вычислима}\};$$
$$\mathscr{F} \;:=\; \{f : \mathbb{N} \to \mathbb{N} \mid f \text{ вычислима}\}.$$

Очевидно, $\mathscr{F} \subsetneq \mathscr{F}^{\sharp}$. С точки зрения теории вычислимости класс $\mathscr{F}^{\sharp}$ оказывается более естественным, чем класс $\mathscr{F}$.

Пусть $U :\subseteq \mathbb{N} \times \mathbb{N} \to \mathbb{N}$. Для всякого $k \in \mathbb{N}$ обозначим через U_k частичную функцию из $\mathbb{N}$ в $\mathbb{N}$, действующую по правилу

$$U_k(n) \;:=\; U(k, n).$$

Утверждение

Можно найти вычислимую $U :\subseteq \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *такую, что*

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

всякая такая функция будет называться универсальной для $\mathscr{F}^{\sharp}$.

Идея доказательства.

Повозившись, р-машины можно эффективно занумеровать натуральными числами:

$$\Pi_0, \quad \Pi_1, \quad \Pi_2, \quad \ldots$$

При этом U, которая по $(k, n) \in \mathbb{N} \times \mathbb{N}$ выдаёт результат применения Π_k к n, окажется вычислимой. □

Утверждение

Нельзя найти вычислимую $U : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *такую, что*

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

Доказательство.

Рассуждая от противного, допустим, что такая U всё же существует. Зададим $f : \mathbb{N} \to \mathbb{N}$ по правилу

$$f(n) \;:=\; U(n, n) + 1.$$

Ясно, что $f \in \mathscr{F}$. Однако $f(n) \neq U(n, n) = U_n(n)$ для любого $n \in \mathbb{N}$; поэтому $f \notin \{U_n \mid n \in \mathbb{N}\}$ — противоречие. □

Зафиксируем универсальную $U :\subseteq \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ для $\mathscr{F}^{\sharp}$. Возьмём

$$\mathrm{Self} \ := \ \{n \in \mathbb{N} \mid U(n, n) \downarrow\}.$$

Очевидно, Self полуразрешимо.

Лемма

Self *полуразрешимо, но не разрешимо.*

Доказательство.

Рассмотрим $f : \mathbb{N} \to \mathbb{N}$, действующую по правилу

$$f(n) \ := \ \begin{cases} U(n, n) + 1 & \text{если } \ n \in \mathrm{Self} \\ 0 & \text{иначе.} \end{cases}$$

Заметим, что $f \neq U_n$ для каждого $n \in \mathbb{N}$. Если χ_{Self} вычислима, то f вычислима — противоречие. □

Далее, для той же U возьмём

$$\text{Halt} \;:=\; \{2^n \cdot 3^m \mid (n, m) \in \mathbb{N}^2 \text{ и } U(n, m)\downarrow\}.$$

Очевидно, Halt полуразрешимо.

Теорема (в духе Тьюринга)

Halt *полуразрешимо, но не разрешимо.*

Доказательство.

Заметим, что для любого $n \in \mathbb{N}$,

$$n \;\in\; \text{Self} \quad\Longleftrightarrow\quad 2^n \cdot 3^n \;\in\; \text{Halt}.$$

Если χ_{Halt} вычислима, то χ_{Self} вычислима — противоречие. $\square$