

Введение в математическую логику и теорию алгоритмов

Семинар № 8: Теория алгоритмов: невычислимые функции, неразрешимые и неперечислимые множества (см. книгу: Верещагин, Шень «Вычислимые функции», гл. 2)

Разбор домашних задач

1. Семейство перечислимых множеств замкнуто относительно \cap и \cup .

Указание. Нужно доказать, что если A и B перечислимы, то $A \cap B$ и $A \cup B$ перечислимы. Задачу можно решать, используя (для $A, B, A \cap B, A \cup B$) различные варианты определения перечислимости множеств.

Используя полухарактеристические функции. Пусть даны программы для вычисления \mathcal{P}_A и \mathcal{P}_B . Функция $\mathcal{P}_{A \cap B}(n)$ вычисляется очевидным образом: вычислить последовательно $\mathcal{P}_A(n)$ и $\mathcal{P}_B(n)$; если оба выдали результат, то выдать 1. Функция $\mathcal{P}_{A \cup B}(n)$ вычисляется так: для описания алгоритма ее вычисления можно использовать метафору «запустить параллельно программы для вычисления $\mathcal{P}_A(n)$ и $\mathcal{P}_B(n)$; если хотя бы одно из вычислений завершилось, то выдать 1». Такого рода (параллельные) вычисления реализуются (на устройстве, позволяющем выполнять лишь одну программу) так: сделать один шаг вычисления $\mathcal{P}_A(n)$, один шаг вычисления $\mathcal{P}_B(n)$, два шага вычисления $\mathcal{P}_A(n)$, два шага вычисления $\mathcal{P}_B(n)$, и т.д.; если какое-то из вычислений завершилось, то выдать 1. То есть «параллельное» вычисление реализуется попеременным выполнением программ.

Используя вычислимые последовательности. Если $A = \{f(0), f(1), \dots\}$ и $B = \{g(0), g(1), \dots\}$ — вычислимые последовательности, то $A \cup B = \{h(0), h(1), \dots\}$, где h — следующая тотальная вычислимая функция: $h(n) = f(k)$, если $n = 2k$; $h(n) = g(k)$, если $n = 2k + 1$.

Придумайте тотальную вычислимую функцию $h: \mathbb{N} \rightarrow \mathbb{N}$, такую что $A \cap B = \{h(0), h(1), \dots\}$. Обратите внимание, что $A \cap B$ может быть пустым или конечным.

2. **Теорема Поста:** A и \bar{A} перечислимы $\iff A$ разрешимо.

Указание. (\Leftarrow): очевидно. (\Rightarrow): чтобы вычислить $\chi_A(n)$, «параллельно» вычисляем $\mathcal{P}_A(n)$ и $\mathcal{P}_{\bar{A}}(n)$.

3. **Теорема о графике:** частичная функция $f: \mathbb{N} \rightarrow \mathbb{N}$ вычислима \iff ее график перечислим.

График функции f обозначим $A := \Gamma_f = \{\langle n, k \rangle \in \mathbb{N} \times \mathbb{N} \mid f(n) = k\}$.

Указание. (\Rightarrow) Для вычисления $\mathcal{P}_A(n, k)$ запустить вычисление $f(n)$ и ответ сравним с k ; если $f(n) = k$, выдать 1, иначе зациклимся.

(\Leftarrow) Если $A = \emptyset$, то f нигде не определена и потому вычислима. Пусть теперь $A = \{h(0), h(1), \dots\}$ — вычислимая последовательность, то есть $h: \mathbb{N} \rightarrow \mathbb{N} \times \mathbb{N}$ — тотальная вычислимая функция, перечисляющая пары чисел, составляющие график функции f . Опишем алгоритм вычисления $f(n)$:

вычислять $h(0), h(1), \dots$, если встретилась пара с первой компонентой n , то есть $h(i) = \langle n, k \rangle$, то выдать k .

Убедитесь, что данный алгоритм вычисляет функцию f .

Решите также этот пункт (\Leftarrow), используя другое определение перечислимости A — вычислимость \mathcal{P}_A .

4. Проекция множества $B \subseteq \mathbb{N}^2$: $p_1(B) = \{n \in \mathbb{N} \mid \exists m \in \mathbb{N}: \langle n, m \rangle \in B\}$.

а) Проекция перечислимого множества $B \subseteq \mathbb{N} \times \mathbb{N}$ перечислима.

Обозначим $A = p_1(B)$. Пусть $B = \{h(0), h(1), \dots\}$, где $h: \mathbb{N} \rightarrow \mathbb{N} \times \mathbb{N}$ — тотальная вычислимая функция. Тогда алгоритм для $\mathcal{P}_A(n)$:

вычислять $h(0), h(1), \dots$; если встретилась пара с первой компонентой n , то есть $h(i) = \langle n, k \rangle$, то выдать 1.

Убедитесь, что этот алгоритм действительно вычисляет полухарактеристическую функцию множества A .

б) Всякое перечислимое множество $A \subseteq \mathbb{N}$ является проекцией некоторого разрешимого $B \subseteq \mathbb{N} \times \mathbb{N}$.

Дано: функцию \mathcal{P}_A вычисляет программа P .

Докажите, что $A = p_1(B)$, где разрешимое множество B таково:

$$B = \{\langle n, t \rangle \in \mathbb{N} \times \mathbb{N} \mid$$

вычисление программы P на входе n останавливается за $\leq t$ шагов\}.

Нумерация вычислимых функций

Фиксируем некоторый универсальный язык программирования (то есть на котором можно запрограммировать любую вычислимую функцию). Каждая программа на этом языке представляет собой слово в некотором алфавите Σ . Очевидно, что по слову в алфавите Σ можно распознать, является ли оно программой на данном языке.¹ Итак, множество всех программ является *разрешимым* подмножеством Σ^* . Следовательно, оно является перечислимым, и тем самым имеет вычислимый пересчет всех программ.

Таким образом, мы имеем нумерацию программ, то есть вычислимую биекцию² $n \mapsto P_n$ между множеством натуральных чисел \mathbb{N} и множеством всех программ $\{P_n \mid n \in \mathbb{N}\} \subseteq \Sigma^*$. Каждой программе P_n сопоставим вычисляемую ею частичную функцию $\varphi_n: \mathbb{N} \rightarrow \mathbb{N}$; если программа P_n требует более одного аргумента или выдает (на некотором входе x) «нечисловой» результат, то будем считать, что значение $\varphi_n(x)$ не определено.

Итак, мы занумеровали *все* вычислимые функции $\mathbb{N} \rightarrow \mathbb{N}$; n -я вычислимая функция обозначена φ_n .

Факт. “Универсальная” функция $U(n, x) = \varphi_n(x)$ — вычислима.

Введем удобное обозначение: запись $!f(n)$ означает, что частичная функция f определена на числе n .

¹Именно проверкой того, является ли данный текст программой, занимается в начале своей работы компилятор.

²Обратная биекция — по программе узнать ее номер — очевидно, тоже вычислима.

Пусть $f, g: \mathbb{N} \rightarrow \mathbb{N}$ — частичные функции. Функция g называется *продолжением* функции f , если

$$\forall n \in \mathbb{N} (!f(n) \implies !g(n) \text{ и } f(n) = g(n)).$$

Поскольку функция и ее график — это одно и то же, то можно сказать иначе: функция g — продолжение функции f , если $f \subseteq g$.

Задачи

5. Рассмотрим функцию $f(n) = \begin{cases} \varphi_n(n) + 1, & \text{если } !\varphi_n(n); \\ \text{неопр.}, & \text{иначе.} \end{cases}$

а) Функция f вычислима. \triangleright Она есть $U(n, n) + 1$. \triangleleft

б) Функция f не имеет тотальных вычислимых продолжений.

\triangleright Допустим g — тотальное вычислимое продолжение функции f . Каждая вычислимая функция имеет номер; пусть k — номер функции g , то есть $g = \varphi_k$. Тогда $!g(k)$, значит $!\varphi_k(k)$, значит $!f(k)$, и наконец, $f(k) = \varphi_k(k) + 1$. Но g — продолжение f , поэтому $f(k) = g(k) = \varphi_k(k)$. Противоречие: $\varphi_k(k) + 1 = \varphi_k(k)$. \triangleleft

6. Множество $K := \{n \in \mathbb{N} \mid !\varphi_n(n)\}$ — перечислимо, но не разрешимо.

\triangleright Множество K перечислимо как область определения вычислимой функции f из предыдущей задачи. Очевидно, что следующая функция является тотальным продолжением функции f :

$$g(n) = \begin{cases} f(n), & \text{если } n \in K; \\ 0, & \text{если } n \notin K. \end{cases}$$

Если бы множество K было разрешимым, то функция g была бы вычислима (как?), а значит, была бы тотальным вычислимым продолжением функции f , что невозможно по предыдущей задаче. \triangleleft

7. **Проблема остановки** $\{\langle n, k \rangle \mid !\varphi_n(k)\}$ неразрешима.

\triangleright Иначе множество K было бы разрешимым. \triangleleft

8. Семейство перечислимых множеств *не замкнуто* отн. дополнения.

\triangleright Множество K перечислимо; однако, множество \overline{K} не перечислимо, иначе K было бы разрешимым по теореме Поста. \triangleleft

Нераспознаваемость свойств вычислимых функций по их номерам

Можно ли по номеру n узнать, что вычислимая функция φ_n тотальна? Хотя бы где-то определена? Определена хотя бы на числе 0? Инъективна? На эти и аналогичные вопросы ответ — отрицательный.

Итак, мы изучаем семейство всех вычислимых функций:

$$\mathcal{B} = \{f: \mathbb{N} \rightarrow \mathbb{N} \mid \text{функция } f \text{ вычислима}\}.$$

Рассмотрим произвольное подсемейство $\mathcal{F} \subseteq \mathcal{B}$. Например, все тотальные функции из \mathcal{B} , все хоть где-то определенные функции из \mathcal{B} (то есть у которых $\text{Dom}(f) \neq \emptyset$), все определенные на 0 функции из \mathcal{B} . Семейство $\mathcal{F} \subseteq \mathcal{B}$ будем называть *нетривиальным*, если $\mathcal{F} \neq \emptyset$ и $\mathcal{F} \neq \mathcal{B}$.

Определение. *Индексное множество* семейства $\mathcal{F} \subseteq \mathcal{B}$ — это множество всех³ номеров функций этого семейства:

$$I_{\mathcal{F}} = \{n \in \mathbb{N} \mid \varphi_n \in \mathcal{F}\}$$

Теорема Успенского–Райса.

Для всякого нетривиального семейства вычислимых функций $\mathcal{F} \subseteq \mathcal{B}$ его индексное множество $I_{\mathcal{F}}$ неразрешимо.

Задачи

9. Следующие множества неразрешимы по теореме Успенского–Райса:

- (a) $\{n \mid !\varphi_n(0)\}$,
- (b) $\{n \mid \varphi_n(3) = 2017\}$,
- (c) $\{n \mid \text{функция } \varphi_n \text{ тотальна, то есть } \text{Dom}(\varphi_n) = \mathbb{N}\}$,
- (d) $\{n \mid \text{функция } \varphi_n \text{ нигде не определена, то есть } \text{Dom}(\varphi_n) = \emptyset\}$,
- (e) $\{n \mid \text{функция } \varphi_n \text{ инъективна}\}$,
- (f) $\{n \mid \text{функция } \varphi_n \text{ сюръективна}\}$,
- (g) $\{n \mid \varphi_n = f\}$ для любой фиксир. вычислимой функции⁴ $f \in \mathcal{B}$.

Примечание. Следует отличать свойства вычислимых *функций* от свойств *программ*. Свойство программ является свойством функций, если оно сохраняется при переходе к другой программе, вычисляющей ту же самую функцию. Например, следующее множество разрешимо:

$$\{n \mid \text{вычисление } \varphi_n(0) \text{ останавливается через } \leq 1000 \text{ шагов}\}.$$

³Очевидно, что у одной и той же вычислимой функции имеется бесконечно много номеров: например, допишите к программе, вычисляющей данную функцию, в начало или конец какие-либо ничего не меняющие операторы (типа $x:=x+0$) в любом количестве.

⁴Например, по номеру (или, что равносильно, по тексту) программы узнать, что она вычисляет функцию $f(n) = n!$, невозможно. Значит, преподаватель по программированию, принимая у студентов написанные ими программы и проверяя, что они действительно вычисляют то, что он просил запрограммировать, решает неразрешимую задачу.

Это никак не противоречит теореме Успенского–Райса, поскольку данное свойство не сохранится, если мы от одной программы, остановившейся на 0 за 300 шагов, перейдем к другой программе, вычисляющей ту же функцию, но делающей, например, 2000 «лишних» действий (в начале или в конце вычисления).

10. Следующие множества чисел не являются даже перечислимыми:

- (a) $\{n \mid \neg !\varphi_n(0)\}$,
- (b) $\{n \mid \text{функция } \varphi_n \text{ нигде не определена}\}$,
- (c) $\{n \mid \text{функция } \varphi_n \text{ инъективна}\}$.

Действительно, согласно теореме Успенского–Райса, каждое из этих множеств неразрешимо. Значит, по теореме Поста, либо само множество, либо его дополнение неперечислимо. Покажем, что в данных примерах *дополнение* перечислимо (а значит, само множество неперечислимо):

- (a) $\{n \mid !\varphi_n(0)\}$ перечислимо, поскольку оно является областью определения вычислимой функции $U(n, 0)$.
- (b) $\{n \mid \text{функция } \varphi_n \text{ где-то определена}\}$ перечислимо: чтобы проверить, что функция φ_n определена хотя бы на одном натуральном числе, нужно «параллельно запускать» вычисления ее на всех натуральных числах: $\varphi(0), \varphi(1), \dots$ и в случае остановки какого-либо из этих вычислений выдать 1.
- (c) $\{n \mid \text{функция } \varphi_n \text{ не инъективна}\}$ перечислимо: чтобы обнаружить не-инъективность функции φ_n , нужно «параллельно запускать» ее на всевозможных парах натуральных чисел и, в случае остановки обоих вычислений на очередной паре $\langle a, b \rangle$ проверять условие « $\varphi_n(a) = \varphi_n(b)$?». Если в каком-либо случае получили *неравенство*, то выдать 1.

Упражнение. Опишите алгоритм в пунктах (b) и (c), не прибегая к метафоре о «параллельных вычислениях».

11. Множества $\{n \mid \text{функция } \varphi_n \text{ сюръективна}\}$ и $\{n \mid \text{функция } \varphi_n \text{ тотальна}\}$ гораздо сложнее — ни сами они, ни их дополнения не являются перечислимыми. Доказательство этого выходит за рамки данного курса.

Здесь мы приведем доказательство теоремы Успенского–Райса. Но сначала — полезное наблюдение.

Факт. Если функция двух аргументов $F(x, y)$ вычислима, то существует тотальная вычислимая функция $s(x)$, которая по данному значению первого аргумента x выдает номер программы, вычисляющей получающуюся функцию от оставшегося аргумента y , то есть такая что $F(x, y) = \varphi_{s(x)}(y)$.

Обоснование. Преобразование программы, состоящее в подстановке конкретного значения n вместо аргумента x , является простым, а следовательно, его может выполнять тотальная вычислимая функция $s(n)$.

Доказательство теоремы Успенского–Райса:

Семейство $\mathcal{F} \subseteq \mathcal{B}$ нетривиально \Rightarrow множество $I_{\mathcal{F}}$ неразрешимо.

▷ Обозначим через ζ нигде не определенную функцию.⁵ Она вычислима: $\zeta \in \mathcal{B}$. Без ограничения общности $\zeta \notin \mathcal{F}$; в противном случае перейдем от \mathcal{F} к его дополнению⁶ $\mathcal{B} \setminus \mathcal{F}$. Кроме того, фиксируем какую-нибудь функцию $f \in \mathcal{F}$; очевидно, $f \neq \zeta$. Очевидно, следующая функция вычислима:

$$F(x, y) = \begin{cases} f(y), & \text{если } x \in K; \\ \text{неопр.}, & \text{если } x \notin K. \end{cases}$$

Действительно, нужно сначала запустить $U(x, x)$ и (в случае ее остановки) запустить $f(y)$. Тогда существует тотальная вычислимая функция $s(x)$, такая что $F(x, y) = \varphi_{s(x)}(y)$. Имеем импликации для любого $n \in \mathbb{N}$:

$$\begin{aligned} n \in K &\implies \varphi_{s(n)} = f \implies \varphi_{s(n)} \in \mathcal{F} \implies s(n) \in I_{\mathcal{F}} \\ n \notin K &\implies \varphi_{s(n)} = \zeta \implies \varphi_{s(n)} \notin \mathcal{F} \implies s(n) \notin I_{\mathcal{F}} \end{aligned}$$

Если бы множество $I_{\mathcal{F}}$ было разрешимо, то следующий алгоритм вычислял бы характеристическую функцию множества K :

Дано n . Вычислить $s(n)$ и проверить, принадлежит ли оно $I_{\mathcal{F}}$.
Если да — выдать 1, если нет — выдать 0.

Но мы знаем, что K неразрешимо. Значит, $I_{\mathcal{F}}$ тоже неразрешимо. ◁

⁵Поскольку функция и ее график — это одно и то же, то с точки зрения теории множеств ζ — это фактически пустое множество \emptyset .

⁶Очевидно, что индексное множество дополнения семейства функций равно дополнению индексного множества семейства функций: $I_{\mathcal{B} \setminus \mathcal{F}} = \overline{I_{\mathcal{F}}}$. Поэтому не разницы, неразрешимость какого из этих множеств доказывать.