Введение в математическую логику и теорию алгоритмов

Семинар № 8: Теория алгоритмов:
невычислимые функции, неразрешимые и неперечислимые множества
(все детали — в книге: Верещагин, Шень «Вычислимые функции», гл. 2)

Разбор домашних задач

1. Семейство перечислимых множеств замкнуто относительно пересечения и объединения.

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

   Используя вычислимые последовательности. Если $A = \{f(0), f(1), \ldots\}$ и $B = \{g(0), g(1), \ldots\}$ — вычислимые последовательности, то $A \cup B = \{h(0), h(1), \ldots\}$, 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 $h\colon \mathbb{N} \to \mathbb{N}$, такую что $A \cap B = \{h(0), h(1), \ldots\}$. Обратите внимание, что $A \cap B$ может быть пустым или конечным.

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

   Указание. ($\Longleftarrow$): очевидно. ($\Longrightarrow$): чтобы вычислить $\chi_A(n)$, «параллельно» вычисляем $\pi_A(n)$ и $\pi_{\overline{A}}(n)$.

3. **Теорема о графике:** частичная функция $f\colon \mathbb{N} \to \mathbb{N}$ 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. ($\Longrightarrow$) Для вычисления $\pi_A(n, k)$ нужно запустить вычисление $f(n)$ и результат сравнить с k; если $f(n) = k$, выдать 1, иначе зациклиться.

   ($\Longleftarrow$) Если $A = \varnothing$, то f нигде не определена и потому вычислима. Пусть теперь $A = \{h(0), h(1), \ldots\}$ — вычислимая последовательность, то есть $h\colon \mathbb{N} \to \mathbb{N}\times\mathbb{N}$ — тотальная вычислимая функция, перечисляющая пары чисел, составляющие график функции f. Описываем алгоритм вычисления $f(n)$:

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

   Убедитесь, что данный алгоритм вычисляет функцию f.

   Решите также этот пункт ($\Longleftarrow$), используя другое определение перечислимости A — вычислимость π_A.

4. *Проекция* множества $B \subseteq \mathbb{N}\times\mathbb{N}$ — это $p_1(B) = \{n \in \mathbb{N} \mid \exists m \in \mathbb{N}\colon\ \langle n, m\rangle \in B\}$.

   а) Проекция перечислимого множества $B \subseteq \mathbb{N}\times\mathbb{N}$ перечислима. Обозначим $A = p_1(B)$.

   Пусть $B = \{h(0), h(1), \ldots\}$, где $h\colon \mathbb{N} \to \mathbb{N}\times\mathbb{N}$ — тотальная вычислимая функция. Алгоритм для $\pi_A(n)$:

   > вычислять $h(0)$, $h(1)$, $\ldots$; если встретилась пара с первой компонентой n, то есть $h(i) = \langle n, k\rangle$ для какого-то k, 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 π_A вычисляет программа P. Докажите, что $A = p_1(B)$, где разрешимое B таково:

   $$B \;=\; \{\langle n, t\rangle \in \mathbb{N}\times\mathbb{N} \;\mid\; \text{вычисление программы } P \text{ на входе } n \text{ останавливается за } \leqslant t \text{ шагов}\}.$$

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 имеется вычислимый пересчет всех программ.

Таким образом, мы имеем нумерацию программ, то есть вычислимую биекцию[2] $n \mapsto P_n$ 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 $\varphi_n \colon \mathbb{N} \to \mathbb{N}$; 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 $\mathbb{N} \to \mathbb{N}$; n-я вычислимая функция обозначена φ_n.
Число n называется номером или *индексом* вычислимой функции φ_n.

Факт. *Функция $U(n,x) = \varphi_n(x)$ — вычислима.* Она называется *универсальной.*

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

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

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

Поскольку функция и ее график — это одно и то же, то g — продолжение 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: $\varphi_k(k) + 1 = \varphi_k(k)$. $\triangleleft$

   Обозначим $K := \{n \in \mathbb{N} \mid\ !\varphi_n(n)\}$ — множество номеров программ, останавливающихся на своих номерах.

6. Невычислима следующая (всюду определенная!) функция: $g(n) = \begin{cases} f(n), & \text{если } n \in K; \\ 0, & \text{если } n \notin K. \end{cases}$

   $\triangleright$ Ибо она тотальная и является продолжением функции f. Далее пользуемся предыдущей задачей. $\triangleleft$

7. 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 задачи выше. Если бы K было разрешимым, то существовал бы алгоритм для вычисления функции g: сначала распознать, принадлежит ли n множеству K и либо выдать 0, либо вычислить и выдать $f(n)$. $\triangleleft$

8. **Проблема остановки** $\{\langle n,k \rangle \mid\ !\varphi_n(k)\}$ неразрешима. $\triangleright$ Иначе множество K было бы разрешимым. $\triangleleft$

9. Семейство перечислимых множеств *не замкнуто* относительно взятия дополнения.
   $\triangleright$ K перечислимо; $\overline{K}$ не перечислимо, иначе бы K было разрешимым по теореме Поста. $\triangleleft$

[1] Именно проверкой того, является ли данный текст программой, занимается в начале своей работы компилятор.
[2] Обратная биекция — по программе узнать ее номер — очевидно, тоже вычислима.

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

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 $\mathsf{Dom}(f) \neq \varnothing$), все определенные на 0 функции из $\mathcal{B}$. Семейство $\mathcal{F} \subseteq \mathcal{B}$ будем называть *нетривиальным*, если $\mathcal{F} \neq \varnothing$ и $\mathcal{F} \neq \mathcal{B}$.

Индексное множество семейства $\mathcal{F} \subseteq \mathcal{B}$ — это множество всех[3] номеров функций этого семейства:

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

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

Задачи

10. Следующие множества натуральных чисел неразрешимы, согласно теореме Успенского–Райса:

    (a) $\{n \mid\ !\varphi_n(0)\}$,
    (b) $\{n \mid \varphi_n(3) = 2017\}$,
    (c) $\{n \mid \text{функция } \varphi_n \text{ тотальна, то есть } \mathsf{Dom}(\varphi_n) = \mathbb{N}\}$,
    (d) $\{n \mid \text{функция } \varphi_n \text{ нигде не определена, то есть } \mathsf{Dom}(\varphi_n) = \varnothing\}$,
    (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 фиксированной вычислимой функции[4] $f \in \mathcal{B}$.

    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:

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

    Это никак не противоречит теореме Успенского–Райса, поскольку данное свойство не сохранится, если мы от одной программы, останавливавшейся 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).

11. Следующие множества натуральных 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, ибо 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: $\varphi(0)$, $\varphi(1)$, ... 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 (b) и (c), не прибегая к метафоре о «параллельных вычислениях».

12. 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. Но доказательство этого выходит за рамки данного курса.

---

[3]Очевидно, 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.

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

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: $\mathcal{F} \subseteq \mathcal{B}$ *нетривиально* $\Rightarrow$ $I_{\mathcal{F}}$ *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 дополнению[6] $\mathcal{B} \setminus \mathcal{F}$. 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 $n \in \mathbb{N}$:

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

Если бы множество $I_{\mathcal{F}}$ было разрешимо, то следующий алгоритм вычислял бы хар. 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. ◁

[5] Поскольку функция и ее график — это одно и то же, то ζ — это фактически $\varnothing$ (с точки зрения теории множеств).

[6] Очевидно, 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.