Введение в математическую логику и теорию алгоритмов

Семинар № 7: Теория алгоритмов: вычислимые функции, разрешимые и перечислимые множества

(см. книгу: Верещагин, Шень «Вычислимые функции», гл. 1)

Алгоритм (интуитивное понятие) — это конечный набор инструкций, указывающих, какие операции (и в каком порядке) нужно выполнять над *входными данными* для получения *результата вычислений*. Всякий алгоритм, будучи примененным к произвольным входным данным, выполняется *по шагам*, каждый шаг элементарен (его выполнение можно поручить машине) и занимает конечное время, то есть если на входных данных вычисление длится бесконечно долго, то это возможно лишь по причине того, что выполняется бесконечно много шагов. Можно представлять, что выполнение алгоритма (то есть вычисление) происходит на абстрактном вычислительном устройстве («компьютере»), отличающегося от реальных компьютеров тем, что предполагается, что у него нет ограничения по *объему памяти*, требуемого для выполнения вычисления.

Для описания алгоритмов придумано множество *языков программирования*; конечный набор инструкций на каждом таком языке называется *программой*. Описывать языки, на которых реально программируют, довольно сложная работа; вместо этого в математике описывают *модель вычислений*, то есть чрезвычайно упрощенный язык, который, тем не менее, позволяет написать программу для вычисления любой (!) функции, вычислимой на любых других языках программирования. Несмотря на относительную простоту, такая модель даёт точное (математическое) понятие, соответствующее интуитивному понятию «алгоритм»; однако, ввиду упрощённости языка программировать на нем сложнее, чем на «языках высокого уровня».

В этом курсе принимаем **соглашение:** когда требуется описать алгоритм для вычисления чего-либо, мы будем предъявлять описание, которое каждый из нас, имеющий опыт программирования, сможет легко реализовать на своем любимом языке программирования.

Вычислимые функции

Мы будем интересоваться вычислением функций двух видов (и даже сконцентрируемся лишь на первом):

- *числовые* функции $f\colon \mathbb{N} \to \mathbb{N}$; здесь $\mathbb{N} = \{0, 1, 2, \ldots\}$ — множество натуральных чисел;
- *словарные* функции $f\colon \Sigma^* \to \Sigma^*$; здесь $\Sigma = \{a_1, \ldots, a_n\}$ — конечный *алфавит* (то есть конечное множество), Σ^* — множество всех *слов* в алфавите Σ (*слово* — это конечная (!) последовательность символов из Σ), включая пустое слово, которое мы обозначаем Λ. Очевидно, множество Σ^* счётно.

Вообще говоря, алгоритмы на некоторых входных данных могут не останавливаться. Поэтому и мы вынуждены рассматривать *частичные функции*,[1] то есть определенные не обязательно на всём $\mathbb{N}$ или Σ^*. Все даваемые ниже определения легко дать и для функций нескольких аргументов $f\colon \mathbb{N}^k \to \mathbb{N}$ или $f\colon (\Sigma^*)^k \to \Sigma^*$.

Определение 1. Частичная функция $f\colon \mathbb{N} \to \mathbb{N}$ называется ***вычислимой***, если существует алгоритм, *вычисляющий* функцию f. Здесь использовано следующее понятие: алгоритм $\mathfrak{A}$ *вычисляет* частичную функцию $f\colon \mathbb{N} \to \mathbb{N}$, если для каждого натурального числа $n \in \mathbb{N}$ алгоритм $\mathfrak{A}$ на входном данном n останавливается тогда и только тогда, когда функция f определена на числе n, то есть $n \in \mathsf{Dom}(f)$, и в случае остановки алгоритм $\mathfrak{A}$ на входе n выдает в качестве результата число $f(n)$.

Упражнение. Сформулируйте определения вычислимых словарных функций и функций k (числовых или словарных) аргументов.
Упражнение. Функций $f\colon \mathbb{N} \to \mathbb{N}$ — континуум. Почему вычислимых функций — счётное множество?

Задачи

1. Докажите, что существуют вычислимые биекции (то есть опишите алгоритм вычисления биекции)
   – между $\mathbb{N}$ и $\mathbb{N} \times \mathbb{N}$;
   – между $\mathbb{N}$ и Σ^*;
   – между Σ^* и $\Sigma^* \times \Sigma^*$ (используйте первые два пункта).

   Эта задача показывает, что достаточно ограничиться рассмотрением вычислимых *числовых* функций.[2]

[1] Обычно в математике *функцией* $f\colon A \to B$ называется произвольное подмножество декартова произведения $F \subseteq A \times B$, такое что $\forall x \in A\ \exists! y \in B\colon \langle x, y\rangle \in F$; этот y называется *значением* функции f на аргументе x и обозначается $y = f(x)$. *Частичная* же функция отличается тем, что для каждого $x \in A$ существует *не более одного* $y \in B$, такого что $\langle x, y\rangle \in F$. Это равносильно следующему определению.
Частичной функцией $f\colon A \to B$ называется произвольное подмножество декартова произведения $F \subseteq A \times B$, такое что $\forall x \in A\ \forall y_1, y_2 \in B\ \big((\langle x, y_1\rangle \in F \text{ и } \langle x, y_2\rangle \in F) \Rightarrow y_1 = y_2\big)$. Всюду далее, если мы пишем $f\colon A \to B$, мы будем понимать, что f — частичная функция. *Область определения* функции f обозначаем $\mathsf{Dom}(f)$; *область значений* — $\mathsf{Ran}(f)$; дайте их определения.

[2] Стоит заметить, что числа зачастую даются на вход программе в виде десятичной или двоичной записи, которая сама является словом в соответствующем алфавите. То есть словарные функции — более общее понятие. Но математикам более привычно иметь дело с числовыми функциями, поэтому мы будем рассматривать именно их.

Разрешимые множества

Определение 2. Множество $A \subseteq \mathbb{N}$ называется ***разрешимым***, если вычислима его *характеристическая функция*:

$$\boxed{\chi_A(n) = \begin{cases} 1, & n \in A; \\ 0, & n \notin A. \end{cases}}$$

Задачи

2. Произвольных множеств $A \subseteq \mathbb{N}$ — континуум.
   Почему разрешимых множеств $A \subseteq \mathbb{N}$ счётное число?

3. Всякое конечное множество $A \subseteq \mathbb{N}$ разрешимо.

4. Докажите, что разрешимыми являются множества: четных чисел; простых чисел; чисел, представимых в виде суммы квадратов двух натуральных чисел; четверок натуральных чисел, задающих обратимые $2{\times}2$ матрицы; множество начальных десятичных разложений числа π: $\{3, 31, 314, 3141, 31415, \ldots\}$; множество слов-палиндромов (читающихся слева направо и справа налево одинаково).

5. Семейство разрешимых множеств замкнуто относительно пересечения, объединения, дополнения:
   если A и B — разрешимы, то разрешимы $A \cap B$, $A \cup B$, $\overline{A} = \mathbb{N} \setminus A$.

Перечислимые множества

Мы дадим четыре эквивалентных определения.

Определение 3. Множество $A \subseteq \mathbb{N}$ называется ***перечислимым***, если

(1a) вычислима его *полухарактеристическая функция*:

$$\boxed{\pi_A(n) = \begin{cases} 1, & n \in A; \\ \text{неопр.}, & n \notin A. \end{cases}}$$

(1b) A есть область определения $A = \mathsf{Dom}(f)$
некоторой вычислимой функции $f\colon \mathbb{N} \to \mathbb{N}$;

(2a) A есть область значений $A = \mathsf{Ran}(f)$
некоторой вычислимой функции $f\colon \mathbb{N} \to \mathbb{N}$;

(2b) A есть область значений $A = \mathsf{Ran}(f)$
некоторой *тотальной*[3] вычислимой функции $f\colon \mathbb{N} \to \mathbb{N}$, или $A = \varnothing$.

Примечания:
1) Множества $A \subseteq \mathbb{N}$, удовлетворяющие условию **(1a)**, еще называют ***полуразрешимыми***. Поскольку мы докажем эквивалентность всех четырех условий, это — лишь синоним ***перечислимого*** множества.
2) В пункте **(2b)**, если $A = \mathsf{Ran}(f)$ для некоторой тотальной вычислимой функции f, то фактически имеем: $A = \{f(0), f(1), f(2), \ldots\}$. Тем самым функция f «перечисляет» все элементы множества A (быть может, с повторениями); отсюда и название таких множеств — ***перечислимые***. Таким образом, это определение можно сформулировать так: множество A *перечислимо*, если оно представимо в виде *вычислимой последовательности*.

[3] В теории алгоритмов *тотальными* называют всюду определенные функции.

Задачи

6. Почему перечислимых множеств $A \subseteq \mathbb{N}$ счетное число?

7. Докажите: A разрешимое $\Longrightarrow$ A перечислимое. (Обратное не верно.)

8. Множество натуральных чисел, представимых в виде разности квадратов натуральных чисел, перечислимо.

9. **(1a)** $\Longrightarrow$ **(1b)** A есть область определения своей полухарактеристической функции: $A = \mathsf{Dom}(\pi_A)$.

10. **(1b)** $\Longrightarrow$ **(1a)** Пусть $A = \mathsf{Dom}(f)$; опишите алгоритм вычисления π_A.

11. **(2b)** $\Longrightarrow$ **(2a)** Тривиально; в частности, $\varnothing = \mathsf{Ran}(f)$, где f — нигде не определенная функция.

12. **(1a)** $\Longrightarrow$ **(2a)** Если π_A вычислима, то вычислима и следующая функция f, причем $A = \mathsf{Ran}(f)$:

$$f(n) = \begin{cases} n, & n \in A; \\ \text{неопр.}, & n \notin A. \end{cases}$$

13. **(2b)** $\Longrightarrow$ **(1a)** Если $A = \varnothing$, то конечно же функция π_A (нигде не определенная!) вычислима. Пусть $A \neq \varnothing$ и тотальная вычислимая функция $f\colon \mathbb{N} \to \mathbb{N}$ перечисляет множество A, то есть $A = \mathsf{Ran}(f)$. Описываем алгоритм вычисления $\pi_A(n)$:

    > вычислять $f(0), f(1), f(2), \ldots$, пока не встретится $f(k) = n$;
    > если встретилось, выдать результат 1.

    Убедимся, что этот алгоритм действительно вычисляет функцию π_A. Если $n \in A$, то такое k, что $f(k) = n$, обязательно встретится, и описанный выше алгоритм выдаст 1 (это и требовалось, ведь $\pi_A(n) = 1$). Если же $n \notin A$, то такого k заведомо не встретится и алгоритм будет работать бесконечно долго (а это и требовалось, ведь и функция π_A для данного числа n не определена).

14. **(2a)** $\Longrightarrow$ **(2b)** Дано: $A = \mathsf{Ran}(f)$ для некоторой вычислимой (частичной!) функции $f\colon \mathbb{N} \to \mathbb{N}$. Пусть ее вычисляет программа P. Случай $A = \varnothing$ тривиален. Пусть $A \neq \varnothing$. Фиксируем какое-нибудь $n_0 \in A$. Опишем алгоритм вычисления некоторой *тотальной* функции $h\colon \mathbb{N} \to \mathbb{N}$:

    > На вход дали число $n \in \mathbb{N}$. Преобразовать n в пару натуральных чисел $(k, t) \in \mathbb{N} \times \mathbb{N}$, используя вычислимую биекцию из задачи 1. Запустить программу P, вычисляющую f, на входе k и (главное!) проделать лишь t шагов этого вычисления. Если оно завершилось за $\leqslant t$ шагов, то выдать вычисленное значение $f(k)$. В противном случае выдать число n_0.

    Ясно, что данный алгоритм останавливается на каждом входе $n \in \mathbb{N}$, то есть он вычисляет некоторую тотальную функцию $h\colon \mathbb{N} \to \mathbb{N}$. Осталось убедиться, что $A = \mathsf{Ran}(h)$. Очевидно включение $\supseteq$, ведь наш алгоритм всегда выдает либо $f(k) \in A$, либо $n_0 \in A$. Почему верно включение $\subseteq$, то есть почему каждый элемент $a \in A$ когда-либо будет выдан функцией h? Для любого $a \in A$ имеем: $a \in \mathsf{Ran}(f)$, значит, существует такое число k, что $f(k)$ определено и равно числу a; поэтому вычисление программы P на входе k завершается за какое-то конечное число (скажем, T) шагов. Но тогда функция h выдаст это число a, если ей на вход подать число n, являющееся «кодом» пары (k, T).

Домашнее задание

15. Докажите: семейство перечислимых множеств замкнуто относительно пересечения и объединения. Решите эту задачу, используя разные варианты определения перечислимого множества.
(Замкнутости относительно дополнения нет, см. задачи ниже.)

16. Докажите **Теорему Поста**: A и $\overline{A}$ перечислимы $\iff$ A разрешимо.

    Указание: как из алгоритмов для вычисления полухарактеристических функций для A и $\overline{A}$ «собрать» алгоритм для вычисления характеристической функции множества A?

17. Пусть тотальная вычислимая функция $f\colon \mathbb{N} \to \mathbb{N}$ *строго монотонна*, то есть если $m < n$, то $f(m) < f(n)$. Докажите, что множество $\mathsf{Ran}(f)$ является (не только перечислимым, но и) разрешимым.

18. *Проекцией* множества $B \subseteq \mathbb{N}\times\mathbb{N}$ *на первую координату* называется множество его первых компонентов:

$$p_1(B) = \{n \in \mathbb{N} \mid \exists m \in \mathbb{N}\colon\ \langle n, m\rangle \in B\}.$$

    Докажите:
    а) Проекция перечислимого множества $B \subseteq \mathbb{N}\times\mathbb{N}$ перечислима.
    б) Всякое перечислимое множество $A \subseteq \mathbb{N}$ является проекцией некоторого разрешимого $B \subseteq \mathbb{N}\times\mathbb{N}$.

    Указание: в пункте (б) действуйте по аналогии с задачей 14: представьте $A = \mathsf{Dom}(f)$ в виде проекции разрешимого множества, используя в качестве «второй координаты» количество шагов вычисления $f(k)$.

19. Функцию $g\colon \mathbb{N} \to \mathbb{N}$ называют *продолжением* функции $f\colon \mathbb{N} \to \mathbb{N}$, если $\mathsf{Dom}(f) \subseteq \mathsf{Dom}(g)$ и на множестве $\mathsf{Dom}(f)$ их значения совпадают.

    Пусть $f\colon \mathbb{N} \to \mathbb{N}$ — вычислимая частичная функция, *не имеющая* вычислимого тотального продолжения.[4] Докажите, что множество $\mathsf{Dom}(f)$ является ***неразрешимым*** (но перечислимым).

    (Это первый пример перечислимого, но не разрешимого множества!)

20. Докажите **Теорему о графике:** частичная функция $f\colon \mathbb{N} \to \mathbb{N}$ является вычислимой $\iff$ ее *график* $\Gamma_f = \{\langle a, b\rangle \in \mathbb{N}\times\mathbb{N} \mid f(a) = b\}$ является перечислимым подмножеством $\mathbb{N}\times\mathbb{N}$.

[4] Пример такой функции будет построен на лекции (и на следующем семинаре).