Коллоквиум по Дискретной математике, 2 курс

Залялов Александр, @bcategorytheory,
Солодовников Никита, @applied_memes
Шморгунов Александр, @Owlus

Содержание

1 Определение вычислимой частичной функции из $\mathbb{N}$ в $\mathbb{N}$. Счётность семейства частичных вычислимых функций, и существование невычислимых функций. Разрешимые и перечислимые подмножества $\mathbb{N}$. Счётность семейства перечислимых множеств, существование неперечислимых множеств.

Здесь не даётся формального определения алгоритма. В нашем случае "алгоритм" — некоторый чёрный ящик, принимающий на вход конструктивный объект (натуральное число или же объект, который можно закодировать как натуральное число), производящий некоторый результат (также конструктивный объект), а также работающий по шагам (некоторые атомарные действия вроде сложения).

Rule of thumb для вопроса "Алгоритм ли это?" — можно написать как программу на каком-нибудь языке программирования.

Определение. Функция $f : \mathbb{N} \to \mathbb{N}$ называется *частичной*, если $\mathrm{Dom}\, f \subseteq \mathbb{N}$.

Определение. Функция $f : \mathbb{N} \to \mathbb{N}$ называется *тотальной*, если $\mathrm{Dom}\, f = \mathbb{N}$.

Определение. Алгоритм $\mathcal{A}$ *вычисляет* частичную функцию $f : \mathbb{N} \to \mathbb{N}$, если

$$\begin{cases} \mathcal{A}(x) = f(x), & \text{если } x \in \mathrm{Dom}\, f, \\ \mathcal{A}(x) \text{ не определено} & \text{иначе.} \end{cases}$$

Определение. Частичная функция $f : \mathbb{N} \to \mathbb{N}$ называется *вычислимой*, если существует алгоритм, её вычисляющий.

Утверждение. *Множество частичных вычислимых функций не более, чем счётно.*

Доказательство. Действительно, всякой вычислимой функции можно поставить в соответствие некоторый алгоритм, причём различные функции вычисляются различными алгоритмами. Алгоритм — это программа, то есть конечная строка. Конечных строк (а следовательно, алгоритмов) всего лишь счётное число. Существует инъекция из множества вычислимых функций в множество алгоритмов, значит, количество вычислимых функций не более, чем счётно. □

Теорема. *Существуют невычислимые функции $f : \mathbb{N} \to \mathbb{N}$.*

Доказательство. Мощность множества вычислимых функций меньше мощности множества всех функций из $\mathbb{N} \to \mathbb{N}$, а значит, его дополнение не пусто. □

Определение. Множество $A \subseteq \mathbb{N}$ называется *разрешимым*, если существует алгоритм, вычисляющий его характеристическую функцию $\chi_A(x)$, то есть функцию такую, что

$$\chi_A(x) = \begin{cases} 1, & \text{если } x \in A, \\ 0 & \text{иначе.} \end{cases}$$

Определение. Множество $A \subseteq \mathbb{N}$ называется *перечислимым*, если существует алгоритм (не принимающий никаких входных данных), который выводит последовательность a_n такую, что множество всех элементов этой последовательности равно A.

Утверждение. *Множество перечислимых подмножеств $\mathbb{N}$ не более, чем счётно.*

Доказательство. Всякому перечислимому множеству соответствует алгоритм, его перечисляющий, причём различные множества перечисляются различными алгоритмами. Отсюда следует, что мощность множества перечислимых множеств не превосходит мощности множества алгоритмов, которое, в свою очередь, является счётным. □

Теорема. *Существуют неперечислимые множества $A \subseteq \mathbb{N}$.*

Доказательство. Множество перечислимых множеств имеет мощность меньшую, чем $2^{\mathbb{N}}$. Значит, его дополнение не пусто. □

2 Эквивалентные определения перечислимости: полуразрешимость, область определения вычислимой функции, множество значений вычислимой функции.

Определение. Множество $A \subseteq \mathbb{N}$ называется *полуразрешимым*, если существует алгоритм, вычисляющий его полухарактеристическую функцию $\xi_A(x)$, то есть функцию такую, что

$$\xi_A(x) = \begin{cases} 1, & \text{если } x \in A, \\ \text{не определено} & \text{иначе.} \end{cases}$$

Теорема. *Следующие утверждения эквивалентны:*

1. *Множество A перечислимо.*
2. *Множество A полуразрешимо.*
3. *Существует частичная вычислимая функция $f : \mathbb{N} \to \mathbb{N}$ такая, что $A = \operatorname{Dom} f$.*
4. *Существует частичная вычислимая функция $f : \mathbb{N} \to \mathbb{N}$ такая, что $A = \operatorname{Ran} f$.*

Доказательство. Чтобы показать эквивалентность всех этих утверждений, докажем несколько импликаций.

(1) $\implies$ (2)

Множество A перечислимо, докажем его полуразрешимость.

Модифицируем алгоритм $\mathcal{A}$ перечисления множества A следующим образом: если для входа x при перечислении мы встретили x, вернём ответ 1, иначе продолжим работу, ничего не возвращая. Так как в последовательности, получаемой алгоритмом, рано или поздно встретится каждый из элементов A, положительный ответ будет дан за конечное число шагов. В случае, если $x \notin A$, алгоритм зациклится без вывода, что вполне устраивает нас в рамках нашей задачи.

(2) $\implies$ (3)

Множество A полуразрешимо, докажем, что найдётся вычислимая функция, для которой A — область значений.

Этой частичной вычислимой функцией был ~~Альберт Эйнштейн~~ $\xi_A(x)$. Действительно, знаем, что $\xi_A(x)$ вычислима, а $\operatorname{Dom} \xi_A = A$. Значит, мы нашли искомую функцию.

(3) $\implies$ (4)

Множество A является областью определения некоторой вычислимой функции f, докажем, что оно также является областью значений некоторой другой вычислимой функции.

Определим функцию $g(x)$:

$$g(x) = \begin{cases} x, & \text{если } x \in \operatorname{Dom} f, \\ \text{не определено} & \text{иначе.} \end{cases}$$

Эта функция вычислима. Алгоритм, её вычисляющий, должен попытаться вычислить $f(x)$ и затем просто вывести x. Кроме того, $\operatorname{Ran} g = \operatorname{Dom} f$, а значит, мы нашли искомую функцию.

(4) $\implies$ (1)

Множество A является областью значений некоторой вычислимой функции, докажем его перечислимость.

Известно, что существует алгоритм $\mathcal{F}$, вычисляющий функцию f, область значений которой совпадает с A. Чтобы перечислить элементы множества A, будем бесконечно производить итерации следующего вида: на n-той итерации запустим по очереди на n шагов $\mathcal{F}(i)$ для каждого $0 \leqslant i \leqslant n$. Таким образом, для всех i алгоритм $\mathcal{F}(i)$ будет рано или поздно запущен на число шагов, необходимое для завершения. Значит, на всех x из $\operatorname{Dom} f$ мы вычислим (и выведем) $f(x)$. Таким образом будут выведены все элементы $\operatorname{Ran} f$, равного A.

Из каждого утверждения следуют все остальные. Значит, утверждения эквивалентны. □

3 Теорема Поста. Теорема о графике.

Теорема Поста. Множества A и $\mathbb{N} \setminus A$ перечислимы тогда и только тогда, когда A разрешимо.

Доказательство.

$\implies$

Перечислимость множества эквивалентна его полуразрешимости. Будем использовать алгоритмы $\mathcal{A}$ и $\mathcal{B}$, вычисляющие $\xi_A(x)$ и $\xi_{\mathbb{N}\setminus A}(x)$ соответственно.

Алгоритм $\mathcal{C}$, находящий $\chi_A(x)$, будет по очереди запускать $\mathcal{A}(x)$ и $\mathcal{B}(x)$ на некоторое число шагов. Как только один из этих алгоритмов завершится, можно будет дать ответ: если $x \in A$, вернуть 1, в противном случае вернуть 0.

Докажем корректность построенного алгоритма. Во-первых, он действительно даёт правильный ответ на всех $x \in \mathbb{N}$, а во-вторых, всегда завершается, так как всякое натуральное число лежит либо в множестве A, либо в его дополнении. Оба вспомогательных алгоритма могут при необходимости отработать бесконечное число шагов, значит, если какой-то из них завершается на данном входе, он завершится.

$\Longleftarrow$

Если множество разрешимо, его дополнение также разрешимо. Разрешимость влечёт перечислимость. □

Определение. Пусть задана функция f. Множество $\Gamma_f = \{(x, f(x)) \mid x \in \operatorname{Dom} f\}$ называется *графиком* функции f.

Теорема о графике. Функция f вычислима тогда и только тогда, когда Γ_f перечислимо.

Доказательство.

$\Longrightarrow$

Умея вычислять функцию f, хотим перечислить Γ_f.

Будем бесконечно производить итерации следующего вида: на n-той итерации попытаемся вычислить $f(x)$ для всех $0 \leqslant x \leqslant n$ не более, чем за n шагов. Если удастся, выведем пару $(x, f(x))$ в противном случае остановим вычисление $f(x)$ и перейдём к следующему i. Для каждого $x \in \operatorname{Dom} f$ рано или поздно мы произведём достаточное число шагов, чтобы вычислить $f(x)$, так как алгоритм, вычисляющий $f(x)$, должен завершаться за конечное число шагов. Значит, Γ_f таким образом действительно будет перечислено.

$\Longleftarrow$

Умея перечислять Γ_f, хотим вычислить $f(x)$.

Будем перечислять Γ_f, пока не найдём пару, в которой первый элемент равен x. Действительно, если функция определена на x, то такая пара найдётся в Γ_f, а значит, будет выведена алгоритмом его перечисления за конечное число шагов. Далее просто выведем второй элемент этой пары и завершим работу.

□

4 Универсальные вычислимые функции (нумерации) для семейства частичных вычислимых функций натурального аргумента. Несуществование универсальной вычислимой функции для семейства тотальных вычислимых функций натурального аргумента (диагональное рассуждение). Главные универсальные функции.

Известно, что множество частичных вычислимых функций счётно. Значит, все эти функции можно каким-то способом занумеровать.

Определение. Пусть φ_n — последовательность вычислимых частичных функций. Такая последовательность называется *универсальной нумерацией*. Функция $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ такая, что $f(n, x) = \varphi_n(x)$, называется *универсальной функцией*.

Теорема. *Существует вычислимая нумерация (универсальная функция).*

Доказательство. Определим следующий порядок на двоичных словах: если слово a короче слова b, $a \prec b$, если наоборот — $b \prec a$, в случае же равной длины будем сравнивать слова лексикографически. Последовательность двоичных слов в таком порядке будет выглядеть как $\{\bot, 0, 1, 00, 01, 10, 11, \ldots\}$. Таким образом множество окажется вполне упорядоченным. Теперь каждому натуральному числу можно поставить в соответствие некоторое двоичное слово.

Без ограничения общности будем считать, что алгоритм можно записать некоторым двоичным словом.

Определим теперь функцию $f(n, x)$ следующим образом: интерпретируем двоичное слово с номером n (в нашем порядке $\prec$) как код (запись машины Тьюринга, программу на C, whatever) для алгоритма $\mathcal{A}$, и положим $f(n, x) = \mathcal{A}(x)$. Если двоичное слово с номером n не является корректной записью алгоритма, будем считать, что $f(n, x)$ не определена для всех x.

Описанная функция вычислима. Она также является универсальной, так как пробегает по всем возможным алгоритмам (и, как следствие, всем возможным вычислимым функциям). Значит, мы построили вычислимую универсальную функцию. □

Может показаться, что универсальная функция может существовать и для семейства тотальных вычислимых функций. Однако, это неверно.

Теорема. *Не существует вычислимой нумерации (универсальной функции) для семейства тотальных вычислимых функций.*

Доказательство. Допустим, что существует вычислимая нумерация ψ_n тотальных вычислимых функций. Значит, будет тотальной и вычислимой функция следующего вида

$$f(x) = \psi_x(x) + 1.$$

Так как функция f тотальна и вычислима, должно найтись n такое, что $\psi_n(x) = f(x)$. Однако, если поставить $x = n$:

$$\psi_n(n) = f(n) = \psi_n(n) + 1.$$

Произошло противоречие [1]...

□

Определение. Нумерация φ называется *главной*, если для любой вычислимой частичной функции $V(n, x)$ существует тотальная вычислимая функция $s(n)$ такая, что $V(n, x) = \varphi_{s(n)}(x)$.

Теорема. *Существует главная нумерация (универсальная функция).*

Доказательство. Рассмотрим построенную выше нумерацию. Для функции $V(n, x)$ построим алгоритм $\mathcal{S}(m)$, который "вшивает" в алгоритм $\mathcal{V}(n, x)$, вычисляющий $V(n, x)$, константу m вместо переменной n. Такой алгоритм, очевидно, всегда будет завершаться. Значит, он вычисляет некоторую тотальную функцию $s(n)$. □

5 Вычислимая функция, не имеющая тотального вычислимого продолжения. Перечислимое неразрешимое множество. Неразрешимость проблемы применимости.

Определение. Функция g является *продолжением* функции f, если $\mathrm{Dom}\, f \subset \mathrm{Dom}\, g$ и $\forall x \in \mathrm{Dom}\, f\ g(x) = f(x)$.

Теорема. *Существует вычислимая частичная функция, не имеющая всюду определённого продолжения.*

Доказательство. Определим функцию f:

$$f(x) = \varphi_x(x) + 1.$$

Пусть мы вычислимо продолжили функцию f функцией φ_n (продолжение вычислимо, а потому будет присутствовать в главной нумерации). Запишем уравнение:

$$\varphi_x(x) + 1 = \varphi_n(x).$$

Это уравнение, вообще говоря, неверно, так как левая часть может быть не определена, но при этом при подстановке $x = n$ получаем слева вполне определённое выражение (напомню, φ_n всюду определена), а вместе с ним и противоречие:

$$\varphi_n(n) + 1 = \varphi_n(n).$$

Значит, для функции f не существует всюду определённого вычислимого продолжения. □

Теорема. *Множество $A = \{x \mid \varphi_x(x)$ определено$\}$ неразрешимо.*

[1] Такая конструкция не будет приводить к противоречию, если говорить о частичных функциях, а не тотальных. Действительно, построенная нами функция $f = \varphi_n$ просто не будет определена в точке n.

Доказательство. Вернёмся вновь к нашей любимой функции f:

$$f(x) = \varphi_x(x) + 1.$$

Продолжим эту функцию самым простым способом — везде вне её области определения её продолжение будет равно нулю. Нетрудно было бы реализовать это продолжение, умея разрешать множество A: просто вычислим $\varphi_x(x) + 1$, если это значение определено, и вернём ноль иначе.

Однако мы уже знаем, что продолжение функции f не может быть вычислимым. Значит, вычислимость χ_A приводит к противоречию. □

Определение. Задача разрешения множества $\{(n, x) \mid \varphi_n(x) \text{ определено}\}$ называется *проблемой остановки (применимости).*

Теорема. *Проблема остановки неразрешима.*

Доказательство. Пусть χ_A вычисляется алгоритмом $\mathcal{A}$. Запустив $\mathcal{A}(x, x)$, можно разрешить множество $\{x \mid \varphi_x(x) \text{ определено}\}$, для которого уже доказана неразрешимость. □

6 Теорема Поста. Существование перечислимого множества, дополнение которого неперечислимо. Перечислимые неотделимые множества.

Теорема Поста была доказана здесь.

Теорема. *Существует перечислимое множество с неперечислимым дополнением.*

Доказательство. Уже знакомое нам множество $\{x \mid \varphi_x(x) \text{ определено}\}$ является неразрешимым. Однако же, это множество очевидно полуразрешимо, а значит, и перечислимо.

Предположим теперь, что дополнение данного множества перечислимо. В таком случае, согласно теореме Поста, само множество разрешимо. Противоречие. □

Определение. Множества A, B называются *отделимыми*, если существует множество C такое, что $A \subseteq C$ и $B \cap C = \varnothing$.

Теорема. *Существуют непересекающиеся перечислимые множества, которые нельзя отделить разрешимым множеством.*

Доказательство. Рассмотрим множества $A = \{x \mid \varphi_x(x) = 0\}$ и $B = \{x \mid \varphi_x(x) = 42\}$. Они, очевидно, перечислимы и не пересекаются.

Допустим, существует разрешимое C, отделяющее A и B. Пусть оно содержит в себе множество A. Тогда:

$$\chi_C(x) = \begin{cases} 1, & \text{если } \varphi_x(x) = 0, \\ 0, & \text{если } \varphi_x(x) = 42, \\ \text{и что-то ещё на других числах.} \end{cases}$$

χ_C вычислима. Значит, $\exists n\ \chi_C(x) = \varphi_n(x)$ Но пусть тогда $x = n$. Получаем:

$$\varphi_n(n) = \begin{cases} 1, & \text{если } \varphi_n(n) = 0, \\ 0, & \text{если } \varphi_x(n) = 42, \\ \text{и что-то ещё на других числах.} \end{cases}$$

Получили противоречие. □

7 Сводимости: m-сводимость и Тьюрингова сводимость. Свойства. Полные перечислимые множества.

Определение. Множество A *m-сводится* к множеству B, если существует тотальная вычислимая функция f такая, что $\forall x\ x \in A \iff f(x) \in B$. Обозначается как $A \leqslant_m B$.

m-сводимость позволяет построить алгоритм разрешения множества A, если есть алгоритм разрешения множества B. Строго говоря, $\chi_A(x) = \chi_B(f(x))$.

Свойства m-сводимости:

- $A \leqslant_m A$ (рефлексивность),
- $A \leqslant_m B \wedge B \leqslant_m C \implies A \leqslant_m C$ (транзитивность),
- $\left.\begin{array}{l} B \text{ разрешимо} \\ A \leqslant_m B \end{array}\right\} \implies A$ разрешимо,
- $\left.\begin{array}{l} A \text{ неразрешимо} \\ A \leqslant_m B \end{array}\right\} \implies B$ неразрешимо.

Определение. Множество A *T-сводится* (сводится по Тьюрингу) к множеству B, если при помощи алгоритма вычисления χ_B (не обязательно существующего) можно вычислить χ_A. Обозначается как $A \leqslant_T B$ [2].

Тьюринова сводимость обладает теми же свойствами, что и m-сводимость. Однако же, $A \leqslant_m B \implies A \leqslant_T B$, а обратное утверждение неверно.

Тьюрингова сводимость обладает ещё одним свойством: $A \leqslant_T \mathbb{N} \setminus A$. Однако же данное утверждение не будет верно для m-сводимости. К примеру, множество $\mathbb{N}$ не может быть m-сведено к своему дополнению.

Определение. Перечислимое множество, к которому m-сводится любое другое перечислимое множество, называется *полным перечислимым множеством.*

Теорема. *Существует полное перечислимое множество.*

Доказательство. Рассмотрим множество $A = \{(n, x) \mid \varphi_n(x) \text{ определено}\}$. Заметим, что оно перечислимо.

Пусть мы хотим свести некоторое перечислимое множество B к множеству A. Знаем, что в силу перечислимости существует вычислимая частичная функция f такая, что $B = \operatorname{Dom} f$. Эта функция должна присутствовать в универсальной нумерации. Пусть это φ_n. Тогда для того, чтобы проверить принадлежность $x \in B$, достаточно проверить принадлежность $(n, x) \in A$. Сводящая функция в данном случае выглядит как $m(x) = (n, x)$. □

8 Теорема Клини о неподвижной точке.

Теорема. *Для всякой тотальной вычислимой функции f и главной нумерации φ_n найдётся n такое, что $\varphi_n = \varphi_{f(n)}$* [3].

Доказательство. Педагогический трюк для лучшего запоминания: сначала попытаемся доказать ложное утверждение о том, что у всякой тотальной вычислимой функции есть неподвижная точка, то есть число n такое, что $n = f(n)$.

Функция f вычислима, функция $\varphi_x(x)$ вычислима, значит, вычислима их композиция. То есть, существует m такое, что

$$f(\varphi_x(x)) = \varphi_m(x).$$

Подставляя $x = m$, получаем

$$f(\varphi_m(m)) = \varphi_m(m),$$

то есть $n = \varphi_m(m)$.

И всё бы было хорошо, если бы $\varphi_m(m)$ было всегда определено. Но вернёмся в суровую реальность и докажем истинное утверждение теоремы Клини.

Вместо равенства чисел нужно рассматривать эквивалентность следующего вида: $n \sim m$, если $\varphi_n = \varphi_m$.

Рассмотрим вычислимую функцию

$$V(m, x) = \varphi_{f(\varphi_m(m))}(x).$$

По свойству главности нумерации φ найдётся тотальная вычислимая функция s такая, что

$$V(m, x) = \varphi_{s(m)}(x).$$

[2] Это — старая добрая сводимость из курса алгоритмов. Классы задач P и NP машут ручкой.

[3] Неформально: существует программа, которая может напечатать свой код.

Значит, можем записать, что

$$f(\varphi_m(m)) \sim s(m).$$

Важно отметить, что $s(m)$ тотальна. Какое бы значение m мы не подставили, наше утверждение сохранит истинность в силу того, что правая часть уравнения определена.

Теперь, зная, что $s(m)$ вычислима, запишем её как $\varphi_k(m)$

$$f(\varphi_m(m)) \sim \varphi_k(m),$$

и подставим $m = k$

$$f(\varphi_k(k)) \sim \varphi_k(k).$$

Чудесным образом получили слева и справа вполне определённые значения, так как и f, и φ_k являются тотальными функциями. То есть, неподвижной точкой (в смысле определённой нами эквивалентности, а не обычного равенства) функции f является $\varphi_k(k)$, совершенно точно определённое значение. □

9 Теорема Райса-Успенского.

Теорема. *Пусть множество F является собственным подмножеством множества частичных вычислимых функций (то есть, F не пусто и не совпадает с множеством всех частичных вычислимых функций). Тогда множество $\{i \mid \varphi_i \in F\}$ неразрешимо* [4].

Доказательство. Обозначим нигде не определённую функцию как $\zeta(x)$. Рассмотрим два случая.

- $\zeta \notin F, f \in F$

  Пусть A — перечислимое неразрешимое множество. Хотим m-свести A к F. Для этого определим функцию $V(n, x)$ следующим образом:

  $$V(n,x) = \begin{cases} f(x), & n \in A, \\ \zeta(x), & \text{иначе.} \end{cases}$$

  Так как полухарактеристическая функция A вычислима, $V(n, x)$ также вычислима. Кроме того, в главной нумерации φ найдётся тотальная вычислимая функция s такая, что $V(n, x) = \varphi_{s(n)}(x)$. Запишем:

  $$\varphi_{s(n)}(x) = \begin{cases} f(x), & n \in A, \\ \zeta(x), & \text{иначе.} \end{cases}$$

  Но теперь мы получили, что $n \in A \iff s(n) \in F$. Значит, неразрешимое множество A m-сводится к нашему множеству F. Значит, и F является неразрешимым.

- $\zeta \in F, f \notin F$

  Построив всё аналогично предыдущему пункту, мы получаем, что $n \in A \iff s(n) \notin F$. Это значит, что дополнение F неразрешимо. Само F в таком случае также неразрешимо.

□

[4] Неформально эту теорему можно понимать так: по алгоритму вычисления функции нельзя понять (алгоритмически), обладает ли она каким-либо свойством. То есть, к примеру, нельзя написать алгоритм, решающий, монотонна ли функция, по коду, её вычисляющему.