Математическая логика и теория вычислимости Лекция 12. Неразрешимые множества и их свойства

Денис Николаевич Москвин

Совместная магистратура JetBrains и ИТМО
Разработка ПО / Software Engineering

12.05.2021

План лекции

1. Неразрешимые и неперечислимые множества
2. Теорема Успенского-Райса
3. Теорема Клини о неподвижной точке

План лекции

Неразрешимые и неперечислимые множества

- Существуют ли неразрешимые и/или неперечислимые множества?

Неразрешимые и неперечислимые множества

- Существуют ли неразрешимые и/или неперечислимые множества? Да.
- Разрешимых (и перечислимых) множеств — счетное число, поскольку они определены через алгоритмы.
- С другой стороны мощность множества всех подмножеств $\mathbb{N}$ строго больше мощности счетного множества.
- Этот факт доказывается канторовской диагональной конструкцией. (Пишем характеристические функции подмножеств как последовательности нулей и единиц.)
- Существуют ли неразрешимые, но перечислимые множества?

Универсальная функция

- Функция $\mathcal{U} : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ называется *универсальной* (для класса унарных вычислимых функций), если
  1. для каждого n ее сечение
  $$\mathcal{U}_n : x \mapsto \mathcal{U}(n, x)$$
  является унарной вычислимой функцией;
  2. все унарные вычислимые функции встречаются среди $\mathcal{U}_n$.
- **Утверждение.** Существует бинарная вычислимая функция, являющаяся универсальной для класса унарных вычислимых функций.
- **Доказательство.** Перенумеруем все алгоритмы (например, по длине). Будем обозначать через $\langle i \rangle$ алгоритм с номером i, а через $\sharp A$ — номер алгоритма A. Положим
$$\mathcal{U}(i, x) = \langle i \rangle(x) \qquad \blacksquare$$
- Фактически, универсальная функция — это интерпретатор.

Диагональная функция

- Рассмотрим так называемую *диагональную* функцию $\mathfrak{u}(\mathfrak{n}) = \mathfrak{U}(\mathfrak{n}, \mathfrak{n})$.
- Свойства
  1. $\mathfrak{u}(\mathfrak{n})$ является вычислимой функцией;
  2. $\mathfrak{u}(\mathfrak{n})$ определена не при всех значениях аргумента (поскольку есть никогда не завершающиеся алгоритмы);
  3. $\mathfrak{u}(\mathfrak{n})$ невозможно продолжить до всюду определенной вычислимой функции.

Докажем последнее. Пусть существует всюду определенная $\mathfrak{u}'(\mathfrak{n})$, такая что $\mathfrak{u}'(\mathfrak{n}) = \mathfrak{u}(\mathfrak{n})$ всюду, где $\mathfrak{u}(\mathfrak{n})$ определена. Рассмотрим всюду определенную вычислимую функцию

$$\mathfrak{d}(\mathfrak{n}) = \mathfrak{u}'(\mathfrak{n}) + 1$$

Она вычислима, поэтому есть вычисляющий ее алгоритм $\mathfrak{D}$ (всюду останавливающийся). Пусть $\mathfrak{k} = \sharp\mathfrak{D}$. Рассмотрим

$$\mathfrak{u}(\mathfrak{k}) = \mathfrak{U}(\mathfrak{k}, \mathfrak{k}) = \mathfrak{d}(\mathfrak{k}) = \mathfrak{u}'(\mathfrak{k}) + 1$$

Но $\mathfrak{u}'(\mathfrak{k}) = \mathfrak{u}(\mathfrak{k})$. Противоречие. ■

Неразрешимое, но перечислимое множество

- Рассмотрим область определения диагональной функции $\mathfrak{u}(\mathfrak{n}) = \mathfrak{U}(\mathfrak{n}, \mathfrak{n})$

$$W = \{\mathfrak{n} \mid \langle \mathfrak{n} \rangle(\mathfrak{n}) \neq \perp\}$$

- Множество W перечислимо, как область определения вычислимой функции.

Неразрешимое, но перечислимое множество

- Рассмотрим область определения диагональной функции $\mathfrak{u}(\mathfrak{n}) = \mathfrak{U}(\mathfrak{n}, \mathfrak{n})$

$$W = \{\mathfrak{n} \mid \langle \mathfrak{n} \rangle(\mathfrak{n}) \neq \perp\}$$

- Множество W перечислимо, как область определения вычислимой функции.
- Множество W неразрешимо. Действительно, если бы оно было разрешимым, то мы легко могли бы продолжить $\mathfrak{u}$ до всюду определенной вычислимой функции.

Неразрешимое, но перечислимое множество

- Рассмотрим область определения диагональной функции $\mathfrak{u}(\mathfrak{n}) = \mathfrak{U}(\mathfrak{n}, \mathfrak{n})$

$$W = \{\mathfrak{n} \mid \langle \mathfrak{n} \rangle(\mathfrak{n}) \neq \perp\}$$

- Множество W перечислимо, как область определения вычислимой функции.
- Множество W неразрешимо. Действительно, если бы оно было разрешимым, то мы легко могли бы продолжить $\mathfrak{u}$ до всюду определенной вычислимой функции.
- А можно ли построить пример неперечислимого множества?

Неразрешимое, но перечислимое множество

- Рассмотрим область определения диагональной функции $\mathfrak{u}(\mathfrak{n}) = \mathfrak{U}(\mathfrak{n}, \mathfrak{n})$

$$W = \{\mathfrak{n} \mid \langle \mathfrak{n} \rangle(\mathfrak{n}) \neq \perp\}$$

- Множество W перечислимо, как область определения вычислимой функции.
- Множество W неразрешимо. Действительно, если бы оно было разрешимым, то мы легко могли бы продолжить $\mathfrak{u}$ до всюду определенной вычислимой функции.
- А можно ли построить пример неперечислимого множества? Да. Теорема Поста.

$$W' = \mathbb{N} \setminus W = \{\mathfrak{n} \mid \langle \mathfrak{n} \rangle(\mathfrak{n}) = \perp\}$$

Пример: последовательность Шпеккера

- Мы доказали неразрешимость и перечислимость множества

$$W = \{n \mid \langle n \rangle(n) \neq \perp\}$$

- Запустим перечисляющий алгоритм, получим последовательность

$$w_1, w_2, w_3, \ldots$$

Пример: последовательность Шпеккера

- Мы доказали неразрешимость и перечислимость множества
$$W = \{n \mid \langle n \rangle(n) \neq \perp\}$$
- Запустим перечисляющий алгоритм, получим последовательность
$$w_1, w_2, w_3, \ldots$$
- Частичные суммы ряда
$$\sum_{n=1}^{\infty} 10^{-w_n}$$
называют последовательностью Шпеккера (Specker sequence). Ее предел невычислим.
- Придумал Ernst Specker, 1949.

Неразрешимость W, другое доказательство

- Пусть
$$W = \{n \mid \langle n \rangle(n) \neq \perp\}$$
разрешимо, тогда разрешимо (и, следовательно, полуразрешимо)
$$W' = \mathbb{N} \setminus W = \{n \mid \langle n \rangle(n) = \perp\}$$
- Пусть A — полуразрешающий алгоритм для W' и $\sharp A = k$.
- Какому из множеств принадлежит k?

$$k \in W' \to \langle k \rangle(k) = \perp \to A(k) = \perp \to k \notin W'$$
$$k \in W \to \langle k \rangle(k) \neq \perp \to A(k) \neq \perp \to k \in W' \to k \notin W$$

Противоречие. ■

План лекции

1. Неразрешимые и неперечислимые множества
2. Теорема Успенского-Райса
3. Теорема Клини о неподвижной точке

Проблема остановки

- Рассмотрим множество

$$\mathrm{H} = \{(\mathfrak{n}, \mathfrak{x}) \mid \langle \mathfrak{n} \rangle(\mathfrak{x}) \neq \perp\}$$

- Множество H является неразрешимым.

Проблема остановки

- Рассмотрим множество

$$\mathrm{H} = \{(\mathfrak{n}, \mathfrak{x}) \mid \langle \mathfrak{n} \rangle(\mathfrak{x}) \neq \perp\}$$

- Множество H является неразрешимым.
- Действительно, если бы был разрешающий алгоритм для H, то его запуск на входах $(\mathfrak{n}, \mathfrak{n})$ сделали бы множество W разрешимым.
- *Проблема остановки* заданного алгоритма на заданном входе является алгоритмически неразрешимой (Алан Тьюринг, 1936).
- Этот метод доказательства неразрешимости можно обобщить.

$\mathfrak{m}$-сведение

- Говорят, что множество A $\mathfrak{m}$-*сводится* к множеству B, нотация $A \leqslant_{\mathfrak{m}} B$, если существует всюду определенная вычислимая функция f, такая что

$$\forall x(x \in A \leftrightarrow f(x) \in B)$$

- **Утверждение.** Если $A \leqslant_{\mathfrak{m}} B$ и B — разрешимо, то A — разрешимо.
- **Пример.** $W \leqslant_{\mathfrak{m}} H$. Действительно, в качестве f мы можем взять $n \mapsto (n, n)$. Если бы H было разрешимо, то и W тоже, что неверно.
- Множество с известной неразрешимостью сводят к изучаемому, а не наоборот!

$\mathfrak{m}$-сведение: свойства

- **Утверждение.** Если $A \leqslant_{\mathfrak{m}} B$ и B — перечислимо, то A — перечислимо.
- **Утверждение.** Сведение транзитивно.
- **Утверждение.** Любое разрешимое множество $\mathfrak{m}$-сводится к любому множеству, отличному от $\mathbb{N}$ и пустого.

Алгоритмы, останавливающиеся на нулевом входе

- Рассмотрим
$$\mathrm{H}_0 = \{\mathbf{n} \mid \langle \mathbf{n} \rangle(0) \neq \perp\}$$
- Является ли H_0 неразрашимым?

Алгоритмы, останавливающиеся на нулевом входе

- Рассмотрим
$$\mathrm{H}_0 = \{\mathrm{n} \mid \langle \mathrm{n} \rangle(0) \neq \perp\}$$
- Является ли H_0 неразрашимым? Да.
- Покажем, что
$$\mathrm{H} \leqslant_\mathrm{m} \mathrm{H}_0$$

Алгоритмы, останавливающиеся на нулевом входе

- Рассмотрим
$$H_0 = \{n \mid \langle n \rangle(0) \neq \perp\}$$
- Является ли H_0 неразрашимым? Да.
- Покажем, что
$$H \leqslant_m H_0$$

- В качестве f возьмем $(n, x) \mapsto \sharp A$, где алгоритм A игнорирует свой вход и запускает $\langle n \rangle(x)$.

Алгоритмы, кодирующие тождественный ноль

- Рассмотрим
$$I_0 = \{n \mid \forall x.\langle n \rangle(x) = 0\}$$
- Покажем, что
$$W \leqslant_m I_0$$
- В качестве f возьмем $n \mapsto \sharp A$, где алгоритм A вычисляет $\langle n \rangle(n)$ и возвращает 0.

Эквивалентные алгоритмы

- Два алгоритма A и B называют *эквивалентными*, нотация $A \sim B$, если результат их работы совпадает:

$$\forall x. \quad (A(x) = \bot \to B(x) = \bot) \wedge \\ (A(x) \neq \bot \to B(x) \neq \bot \wedge A(x) = B(x))$$

- Эквивалентные алгоритмы задают одну и ту же вычислимую функцию.
- Число шагов может отличаться.
- Сколько разных алгоритмов может задавать некоторую вычислимую функцию?

Эквивалентные алгоритмы

- Два алгоритма A и B называют *эквивалентными*, нотация $A \sim B$, если результат их работы совпадает:

$$\forall x. \quad (A(x) = \bot \to B(x) = \bot) \wedge \\ (A(x) \neq \bot \to B(x) \neq \bot \wedge A(x) = B(x))$$

- Эквивалентные алгоритмы задают одну и ту же вычислимую функцию.
- Число шагов может отличаться.
- Сколько разных алгоритмов может задавать некоторую вычислимую функцию? Бесконечно много.

Теорема Успенского-Райса

- Два натуральных числа $\mathfrak{m}, \mathfrak{n} \in \mathbb{N}$ называют *эквивалентными*, нотация $\mathfrak{m} \equiv \mathfrak{n}$, если $\langle \mathfrak{m} \rangle \sim \langle \mathfrak{n} \rangle$.
- Множество $S \subset \mathbb{N}$ называют *инвариантным*, если оно вместе с любым своим элементом содержит его класс эквивалентности по отношению $\equiv$.

$$\forall \mathfrak{m}. \forall \mathfrak{n}. (\mathfrak{m} \equiv \mathfrak{n}) \to (\mathfrak{m} \in S \wedge \mathfrak{n} \in S) \vee (\mathfrak{m} \notin S \wedge \mathfrak{n} \notin S)$$

- **Утверждение.** Если S — инвариантно, то $\mathbb{N} \setminus S$ тоже инвариантно.
- Числовое множество назовем *тривиальным*, если оно пусто или совпадает с $\mathbb{N}$.
- **Теорема (Успенского-Райса).** Если инвариантное множество разрешимо, то оно тривиально.
- Иначе: Невозможно по номеру алгоритма выяснить, обладает ли вычисляемая им функция любым нетривиальным свойством.

Доказательство теоремы Успенского-Райса

(От противного). Пусть S — инвариантно, нетривиально, но разрешимо. Рассмотрим два алгоритма L и A со свойствами:

$$\forall x.\ \mathrm{L}(x) = \bot \qquad \exists x.\ \mathrm{A}(x) \neq \bot$$

Пусть $\sharp\mathrm{A} \in S$, $\sharp\mathrm{L} \in \mathbb{N}\setminus S$. Рассмотрим произвольное неразрешимое перечислимое W и зададим функцию

$$\nu(n, x) = \begin{cases} \mathrm{A}(x), & n \in W, \\ \bot, & n \notin W. \end{cases}$$

ν вычислима: полуразрешающий алгоритм для W, потом $\mathrm{A}(x)$. Ее сечения $\nu_n(x)$ вычислимы для любого n; вот алгоритм

$$V_n = \begin{cases} \mathrm{A}, & n \in W, \\ \mathrm{L}, & n \notin W. \end{cases}$$

При $n \in W$ имеем $\sharp V_n \equiv \sharp\mathrm{A}$; т.к. $\sharp\mathrm{A} \in S$ и S инвариантно. (При $n \notin W$ имеем $\sharp V_n \equiv \sharp\mathrm{L}$, поэтому $\sharp V_n \in \mathbb{N}\setminus S$.)

$$n \in W \leftrightarrow \sharp V_n \in S\ , \qquad W \leqslant_m S. \quad \blacksquare$$

План лекции

Лемма о продолжении

Лемма. Пусть $f : D \to \mathbb{N}$ — вычислимая функция. Тогда существует всюду определенная функция $g(x)$ — продолжение функции $f(x)$ по отношению $\equiv$, то есть для всех $x \in D$:

$$f(x) \equiv g(x)$$

Доказательство. Рассмотрим алгоритм $A(n, x)$ с «кодом»

$$\begin{aligned} &k := f(n) \\ &\texttt{return } \langle k \rangle(x) \end{aligned}$$

Рассмотрим его проекции $A_n(x) = A(n, x)$ и положим

$$g(n) = \sharp A_n$$

Эта функция вычислима, всюду определена и эквивалентна f. Действительно, для произвольного y

$$\langle g(n) \rangle(y) = A_n(y) = A(n, y) = \langle f(n) \rangle(y) \quad \blacksquare$$

Теорема Роджерса о неподвижной точке

Теорема Кли́ни (о неподвижной точке). Пусть h — всюду определенная вычислимая функция. Тогда существует такое m, что

$$\mathrm{h}(\mathrm{m}) \equiv \mathrm{m}$$

Доказательство. Пусть $\mathrm{u}(\mathrm{n}) = \langle \mathrm{n} \rangle(\mathrm{n})$, а $\mathrm{g}(\mathrm{n})$ — ее $\equiv$-продолжение до всюду определенной функции. Рассмотрим всюду определенную вычислимую

$$\mathrm{t}(\mathrm{n}) = \mathrm{h}(\mathrm{g}(\mathrm{n}))$$

Докажем, что неподвижная точка $\mathrm{m} = \mathrm{g}(\sharp \mathrm{t})$:

$$\mathrm{h}(\mathrm{m}) = \mathrm{h}(\mathrm{g}(\sharp \mathrm{t})) = \mathrm{t}(\sharp \mathrm{t}) = \mathrm{u}(\sharp \mathrm{t}) \equiv \mathrm{g}(\sharp \mathrm{t}) = \mathrm{m} \quad \blacksquare$$

Главная универсальная функция

- У нас имеется вычислимая универсальная функция $\mathcal{U}(n, x) = \langle n \rangle(x)$.
- Легко показать, что для любой другой вычислимой $\mathcal{V}(n, x)$ верно, что существует всюду определенная вычислимая функция f, такая что

$$\mathcal{V}(n, x) = \mathcal{U}(f(n), x)$$

- Функции, обладающими подобным свойством, называются *главными* или *гёделевыми*.

Теорема Кли́ни о неподвижной точке

Теорема Кли́ни (о неподвижной точке). Пусть $\mathcal{U}(n, x)$ — главная вычислимая универсальная функция, а $V(n, x)$ — произвольная вычислимая функция. Тогда $\mathcal{U}$ и V совпадают на некотором сечении $\mathcal{U}_p = V_p$, то есть

$$\exists p.\, \forall x.\, \mathcal{U}(p, x) = V(p, x)$$

Доказательство. Поскольку $\mathcal{U}$ — главная, то для любых n и x верно

$$V(n, x) = \mathcal{U}(h(n), x)$$

Берем за p неподвижную точку функции h. ■
В частности, для произвольной вычислимой $V(n, x)$ верно

$$\exists p.\, \forall x.\, \langle p \rangle(x) = V(p, x)$$

Количество неподвижных точек

- Сколько всего у вычислимой функции неподвижных точек?

Количество неподвижных точек

- Сколько всего у вычислимой функции неподвижных точек?
- Бесконечно много.
- Если бы была одна, мы могли бы переопределить ее значение в этой точке, не теряя вычислимости.
- То же рассуждение верно для случая конечного числа неподвижных точек.

Другое доказательство теоремы Успенского-Райса

- Пусть множество S инвариантно, нетривиально, но разрешимо.
- Пусть $p \in S$, $q \notin S$.
- Рассмотрим всюду определенную и вычислимую (из-за разрешимости S) функцию

$$h(x) = \begin{cases} q, & x \in S, \\ p, & x \notin S. \end{cases}$$

- Она не имеет неподвижной точки (из-за инвариантности $p \not\equiv q$). Противоречие. ■

Квайны

- Квайн (quine) — программа, которая печатает свой текст.
- Название — в честь американского логика Уилларда Куайна (Willard Quine).
- Такая программа обязательно существует, иначе бы не имело неподвижной точки преобразование:

$$\mathfrak{m} \mapsto \sharp A$$

где алгоритм A игнорирует свой вход и печатает $\langle \mathfrak{m} \rangle$.