Введение в математическую логику (осень 2018)

В.Б. Шехтман

Лекция 15

Алгоритмы

Свойства алгоритмов (вычислительных устройств), неформально.

1. Алгоритмы работают со словами. *Слово* — это конечная последовательность символов (букв), взятых из некоторого конечного алфавита. Слово может быть пустым.

2. Алгоритм основан на программе. Программа — конечный набор команд, которые записываются словами.

3. Алгоритм содержит "процессор", который обращается к программе и изменяет текущее состояние (слово).

4. Имеется начальное слово (вход) и заключительное слово (выход). Если заключительное слово не появляется, алгоритм работает бесконечно долго (зацикливание).

5. Вычисление разбивается на дискретные шаги.

6. Вычисление детерминированно (т.е. каждый следующий шаг однозначно определен) и не обращается к случайным данным.

Имеется несколько точных определений алгоритма (рекурсивные функции, машины Тьюринга, абстрактные RAM и др.). Все они оказываются эквивалентными. Философский *тезис Чёрча — Тьюринга* утверждает, что они полностью соответствуют интуитивному пониманию вычислимости.

Вычислимые функции

Будем записывать положительные натуральные числа как последовательности единиц, нуль - как 0. Конечный кортеж натуральных чисел $(n_1, \ldots, n_k)$ записывается как $n_1 \sharp \ldots \sharp n_k$, где $\sharp$ — специальный символ (разделитель).

Рассматриваем частичные функции f из $\mathbf{N}^k$ в $\mathbf{N}$. Это записывается так: $f : \mathbf{N}^k \tilde{\longrightarrow} \mathbf{N}$. Если функция всюду определена (тотальна), пишем $f : \mathbf{N}^k \longrightarrow \mathbf{N}$.

Также рассматриваем функции на словах. Если Δ — конечный алфавит, Δ^* — множество всех слов в нем, то рассматриваем частичные функции f из Δ^* в Δ^*. Обозначения аналогичны: $f : \Delta^* \tilde{\longrightarrow} \Delta^*$, $f : \Delta^* \longrightarrow \Delta^*$.

Область определения f обозначается $dom\, f$, область значений — $im\, f$. В частности, возможно, что $dom\, f = \varnothing$ (пустая функция).

Определение 1. *Функция $f : \mathbf{N}^k \tilde{\longrightarrow} \mathbf{N}$ или $f : \Delta^* \tilde{\longrightarrow} \Delta^*$ называется* вычислимой*, если существует алгоритм M со следующими свойствами.*

- *Если $x \in dom\, f$, то M на входе x заканчивает работу и выдает $f(x)$. Это записывается так: $M : x \mid\Rightarrow f(x)$*
- *Если $x \notin dom\, f$, то M на входе x зацикливается. Это записывается так: $M : x \mid\Rightarrow$*

Разрешимость и перечислимость

Определение 2. *Множество слов $A \subseteq \Delta^*$ называется* разрешимым*, если его характеристическая функция χ_A вычислима.*

(Функция $\chi_A : \Delta^* \longrightarrow \{0, 1\}$ принимает значение 1 на A и 0 на его дополнении.)

Аналогично определяются разрешимые подмножества $\mathbf{N}^k$.

Предложение 15.1. *(1) Если A разрешимо, то его дополнение $(-A)$ (до Δ^* или $\mathbf{N}^k$) разрешимо.*

(2) Если A и B разрешимы, то $A \cap B$, $A \cup B$ разрешимы.

Следствие 15.2. *Конечные множества разрешимы.*

Определение 3. *Множество слов $A \subseteq \Delta^*$ (или $A \subseteq \mathbf{N}^k$) называется* полуразрешимым*, если его полухарактеристическая функция χ_A^- вычислима.*

(Частичная функция $\chi_A^- : \Delta^* \tilde{\longrightarrow} \{1\}$ принимает значение 1 на A и не определена на его дополнении.)

Предложение 15.3. *Если A и B полуразрешимы, то $A \cap B$, $A \cup B$ полуразрешимы.*

Теорема 15.4. *(теорема Поста) Множество слов $A \subseteq \Delta^*$ разрешимо $\Leftrightarrow$ A и $-A$ полуразрешимы.*

Определение 4. *Множество $A \subseteq \Delta^*$ (или $A \subseteq \mathbf{N}^k$) называется* перечислимым*, если оно пусто или является множеством значений некоторой вычислимой последовательности, т.е. тотальной функции $\mathbf{N} \longrightarrow \Delta^*$.*

Теорема 15.5. *Существуют вычислимые биекции $\mathbf{N} \longrightarrow \mathbf{N}^k$ и $\mathbf{N} \longrightarrow \Delta^*$ (для конечного Δ), причем обратные биекции тоже вычислимы.*

Теорема 15.6. *Множество $A \subseteq \Delta^*$ (или $A \subseteq \mathbf{N}^k$) перечислимо, если только если оно полуразрешимо.*

Доказательство Рассмотрим сначала случай $A \subseteq \mathbf{N}$.

(Только если). $\varnothing$ разрешимо.

Пусть $A = im\, f$ для вычислимой $f : \mathbf{N} \longrightarrow \mathbf{N}$. Тогда χ_A^- вычислима по следующему алгоритму.

0. Пусть на входе дано n.

1. Полагаем $i := 0$.

2. В цикле по i проверяем, верно ли $f(i) = n$. Если да, выдаем 1 и заканчиваем работу. Если нет, полагаем $i := i + 1$ и продолжаем цикл.

(Если). $\varnothing$ перечислимо.

Пусть $A \neq \varnothing$. Выберем $a_0 \in A$.

Пусть $\gamma : \mathbf{N} \longrightarrow \mathbf{N} \times \mathbf{N}$ — вычислимая биекция (теорема 15.5). Пусть $\gamma(n) = (\alpha(n), \beta(n))$. Тогда α и β тоже вычислимы.

Построим последовательность f, перечисляющую A следующим образом. Для нахождения $f(n)$ делаем $\beta(n)$ шагов в вычислении $\chi_A^-(\alpha(n))$ (или меньше, если вычисление заканчивается раньше). Если за это время вычисление закончилось, полагаем $f(n) := \alpha(n)$. Иначе полагаем $f(n) := a_0$.

Тогда $im\, f = A$. Действительно, включение $\subseteq$ очевидно (почему?).

Обратно, пусть $a \in A$. Тогда $\chi_A^-(a)$ вычислится через сколько-то (k) шагов. Т.к. γ — биекция, имеем $\gamma(n) = (a, k)$ для некоторого n. Т.е. $\alpha(n) = a,\ \beta(n) = k$. По построению тогда $f(n) = a$.

Общий случай сводится к случаю $A \subseteq \mathbf{N}$ с помощью теоремы 15.5. ■

Теорема 15.7. *Пусть $h : \Delta^* \longrightarrow \Delta^*$ — вычислимая тотальная функция.*

(1) Если $A \subseteq \Delta^*$ разрешимо, то $h^{-1}(A)$ разрешимо.

(2) Если $A \subseteq \Delta^*$ перечислимо, то $h[A]$ (образ A) и $h^{-1}(A)$ перечислимы.

Доказательство

(1) $\chi_{h^{-1}(A)} = \chi_A \cdot h$, а композиция вычислимых функций вычислима.

(2) Для прообраза: $\chi^-_{h^{-1}(A)} = \chi_A^- \cdot h$. И используем предыдущую теорему.

Для образа. Если $A = \varnothing$, все очевидно. Если $A = im\, f$ для вычислимой f, то $h[A] = im\,(h \cdot f)$. ■

Универсальная вычислимая функция. Неразрешимость

Ключевой результат теории алгоритмов следующий:

Теорема 15.8. *(об универсальной вычислимой функции) Существует вычислимая функция* $F : \mathbf{N}^2 \tilde{\longrightarrow} \mathbf{N}$ *такая, что для любой вычислимой* $f : \mathbf{N} \tilde{\longrightarrow} \mathbf{N}$ *существует* m *такое, что*

$$\text{для всех } n \; F(m,n) \simeq f(n).$$

Здесь $\simeq$ *означает условное равенство, т.е. обе части определены одновременно и равны, когда определены.*

Идея доказательства: нумеруем программы, работающие с натуральными числами. F вычисляется компьютером, который по номеру программы восстанавливает саму программу и запускает ее на различных входах. Т.е. $F(m,n)$ — результат работы программы с номером m на входе n (если этот результат существует).

Обозначим через φ_m вычислимую функцию с номером m, т.е.

$$\varphi_m(n) \simeq F(m,n).$$

Тогда всякая вычислимая $f : \mathbf{N} \tilde{\longrightarrow} \mathbf{N}$ совпадает с φ_m, где m — номер программы, вычисляющей f.

Теорема 15.9. *Существует перечислимое неразрешимое подмножество в* $\mathbf{N}$.

Доказательство Пусть

$$d(x) \simeq F(x,x) \simeq \varphi_x(x).$$

Рассмотрим

$$K := dom\, d.$$

Ясно, что K полуразрешимо, т.е. перечислимо. Докажем, что $(-K)$ не перечислимо.

Допустим противное. Тогда $-K = dom\, \varphi_n$, где $\varphi_n = \chi^{-}_{-K}$. Тогда для любого x

$$x \notin K \Leftrightarrow x \in dom\, \varphi_n.$$

В частности,

$$n \notin K \Leftrightarrow n \in dom\, \varphi_n.$$

Но по определению K

$$n \in K \Leftrightarrow n \in dom\, \varphi_n.$$

Таким образом,

$$n \in K \Leftrightarrow n \notin K.$$

Противоречие, аналогичное парадоксу Рассела и доказательству теоремы Кантора. ■

О разрешимости теорий первого порядка

Рассмотрим теории в конечной сигнатуре Ω.

Лемма 15.10. *Множества Fm_Ω, CFm_Ω разрешимы.*

Для теории $T \subseteq CFm_\Omega$ обозначим через $[T]$ множество всех ее замкнутых теорем, т.е. $[T] = \{A \in CFm_\Omega \mid T \vdash A\}$.

Теорема 15.11. *Если T — разрешимое множество, то множество $[T]$ перечислимо.*

Доказательство Будем записывать доказательства в T в виде $A_1 \sharp \ldots \sharp A_n$. Пусть Док$(T)$ — множество всех этих доказательств.

Заметим, что Док(T) разрешимо: по любой последовательности формул можно узнать, является ли она правильно построенным доказательством, т.к. элементы T и аксиомы исчисления предикатов распознаются алгоритмически, а применения правил вывода — также.

Имеем: $[T] = h[\text{Док}(T)] \cap CFm_\Omega$, где h — вычислимая функция, выбирающая последний член кортежа. По теореме 15.7 множество $h[\text{Док}(T)]$ перечислимо. По лемме 15.10 CFm_Ω разрешимо и следовательно, перечислимо. Пересечение сохраняет перечислимость по предложению 15.3. ■

Теорема 15.12. *Если T — разрешимое множество и T полна, то множество $[T]$ разрешимо.*

Доказательство По теореме 15.11 это множество перечислимо. Поэтому достаточно доказать перечислимость его дополнения и применить теорему Поста.

Имеем:

$$-[T] = -CFm_\Omega \cup (CFm_\Omega \backslash [T]).$$

Первое множество перечислимо, ввиду разрешимости CFm_Ω. Поскольку T полна,

$$CFm_\Omega \backslash [T] = \{A \in CFm_\Omega \mid T \vdash \neg A\}.$$

Тогда это множество равно $f^{-1}([T])$, где f — вычислимая функция, которая добавляет в начале слова знак $\neg$. По теореме 15.7 оно перечислимо. Объединение сохраняет перечислимость. ■

Теорема Гёделя о неполноте

Напомним, что определимые подмножества стандартной модели $\mathbf{N}$ называются *арифметическими*.

Теорема 15.13. *(Гёделя об определимости) Всякое перечислимое подмножество* $\mathbf{N}$ *является арифметическим.*

Теорема 15.14. *(первая теорема Гёделя о неполноте) Пусть* T *— теория в сигнатуре* PA *с разрешимым множеством аксиом, причем* $\mathbf{N} \models T$*. Тогда* T *неполна. В частности,* PA *неполна.*

Доказательство Допустим, что T полна. По теореме 15.12 $[T]$ разрешимо. Поскольку $\mathbf{N} \models T$, получаем $[T] = Th(\mathbf{N})$ и значит, $Th(\mathbf{N})$ разрешима.

Рассмотрим теперь множество K, построенное в теореме 15.9. По теореме 15.13 существует формула A такая, что для всех n

$$n \in K \Leftrightarrow \mathbf{N} \models A(n).$$

Здесь $A(n)$ — формула, оцененная в $\mathbf{N}$. Заметим, что

$$\mathbf{N} \models A(n) \Leftrightarrow \mathbf{N} \models A(\underline{n}),$$

где $\underline{n}$ — терм (сумма единиц); это следует из леммы 12.1. Таким образом,

$$n \in K \Leftrightarrow A(\underline{n}) \in Th(\mathbf{N}).$$

Поэтому

$$K = h^{-1}(Th(\mathbf{N})),$$

где h — вычислимая функция, переводящая число n в формулу $A(\underline{n})$. По теореме 15.7 K разрешимо. Противоречие.

Итак, T неполна. ■