Математические основы Computer Science
Часть 1: Теория алгоритмов. Лекция 4.

Дмитрий Ицыксон

ПОМИ РАН

4 октября 2009

Содержание лекции

1. Арифметичность вычислимых функций.
2. Арифметическая иерархия.
3. m-сводимость
4. Универсальные множества.
5. Теоремы Тарского и Геделя.

В прошлый раз

- Арифметика:
  - Сигнатура: $\mathfrak{P} = \{=\}, \mathfrak{F} = \{+, \times\}$
  - Интерпретация: $\mathbb{N} = \{0, 1, 2, \dots\}$
- Выразимые в арифметике предикаты: арифметичные.
- $x = 0$ $\forall y(x \leq y)$
- $x = 1$ $\forall y(x \times y = y)$
- $x = k$ $\exists x_1 \dots x_k (x_1 = 1) \wedge \dots \wedge (x_k = 1) \wedge (x = x_1 + \dots + x_k)$
- $x \vdots y$ $\exists z(x = y \times z)$
- x — простое число
  $\neg(x = 1) \wedge ((x \vdots y) \implies ((y = 1) \vee (x = y)))$
- $r = a \bmod b$ $\exists q(a = b \times q + r \wedge (r < b))$

Кодирование конечных последовательностей

Лемма. Для любого целого k найдется сколь угодно большое b, что $b+1, 2b+1, \ldots, kb+1$ — попарно взаимно простые числа.

Лемма. Для любой последовательности $x_0, x_1, \ldots, x_n$ натуральных чисел можно найти такие числа a и b, что $x_i = a \bmod b(i+1)+1$.

- $\exists <x_0, x_2, \ldots, x_n> (\forall i \leq n)[\ldots x_i \ldots]$
- $\exists a, b, n \forall i (i \leq n) \rightarrow [\ldots a \bmod b(i+1)+1 \ldots]$
- $\beta(a, b, i) = a \bmod b(i+1)+1$ — β-функция Геделя.
- x — степень 6.
- $\exists a, b, n(\beta(a, b, 0) = 1) \wedge \forall i (i+1 \leq n) \rightarrow (\beta(a, b, i+1) = 6 \times \beta(a, b, i)) \wedge x = \beta(a, b, n)$

Арифметичные предикаты

- Наша ближайшая цель доказать, что график вычислимой функции арифметичен.
- Кодирование пары (x, y):
  - Код: $p = (x + y)^2 + x$
  - x — первый элемент пары p:
    $\exists d(p > d^2) \wedge (p < (d+1)^2) \wedge d^2 + x = p$.
  - y — второй элемент пары:
    $\exists x(x$ — первый элемент пары $p) \wedge p = (x + y)^2 + x$.

Кодирование стека

- Стек $\{c_1, c_2, \ldots, c_n\}$ можно кодировать так: $\ell = p_1^{c_1+1} p_2^{c_2+1} \ldots p_k^{c_k+1}$, p_i — это i-ое простое число.
- Выдать последний элемент стека (top):
  - Найти максимальное простое число p, на которое делится ℓ
  - Найти максимальную степень d, что $\ell \vdots p^d$.
  - $top + 1 = d$
- Удалить верхний элемент из стека (pop):
  - Найти максимальное простое число p, на которое делится ℓ
  - Найти максимальную степень d, что $\ell \vdots p^d$.
  - $pop \times p^d = \ell$
- Добавить элемент c в стек (push):
  - Найти первое простое число p, на которое не делится ℓ
  - $push = \ell \times p^{c+1}$

Кодирование машины Тьюринга

- Конфигурация МТ: (q, ℓ, c, r)
- q — текущее состояние
- ℓ — список символов до головки
- c — символ, на который указывает головка
- r — список символов от конца ленты до головки (в обратном порядке)
- $Step(t_1, t_2)$: за один шаг МТ из конфигурации t_1 попадает в конфигурацию t_2.
- $t_1 = (q_1, \ell_1, c_1, r_1)$, $t_2 = (q_2, \ell_2, c_2, r_2)$
- Для правила $(q, c) \mapsto (q', c', \rightarrow)$
- $(q = q_1 \wedge c = c_1) \rightarrow$
  $((q_2 = q') \wedge l_2 = push(l_1, c') \wedge c_2 = top(r_1) \wedge r_2 = pop(r_2))$
- $t_0 = (q_0, \ell_0, c_0, r_0)$ — начальная конфигурация.
- (q, ℓ, c, r) — конечная конфигурация, если $q = q_f$.

Кодирование машины Тьюринга

- $$\exists n \exists x_0 x_2 \dots x_n ((x_1 = t_0) \wedge \forall i ((i + 1 \leq n) \to Step(x_i, x_{i+1})) \\ \wedge\, x_n \text{ — конечная конфигурация})$$

- Надо вход поместить в t_0.
- $k_0 = x, k_i = 2k_{i+1} + k_i \bmod 2, k_n = 1$
- $l_0 = 1, l_{i+1} = p_i^{1+(k_i \bmod 2)}$
- p_i — это максимальное простое число, на которое делится l_i.
- Упражнение. Нужно результат на ленте записать в натуральное число.

Итог

- f — вычислимая функция, M — машина Тьюринга, вычисляющая f
- (x, y) принадлежит графику f:
  - t_0 — начальная конфигурация
  - $t_1, t_2, \ldots, t_n$
  - $Step(t_{i-1}, t_i)$
  - Конфигурация t_n содержит конечное состояние
  - y соответствует тому, что записано на ленте в t_n

Арифметичность перечислимых и разрешимых множеств

Следствие. Перечислимое множество арифметично.

Доказательство. Перечислимое множество S — это множество значений вычислимой функции f. $\varphi(x, y)$ — задает график f. $y \in S \iff \exists x \varphi(x, y)$.

Следствие. Разрешимое множество арифметично.

Предваренная форма

- Переименуем связанные переменные так, чтобы их имена не совпадали ни с одной свободной переменной. И у связанных переменных, соответсвующих разным кванторам были бы разные имена.
- Вынесем все кванторы вперед, руководствуясь правилами
  - $(\forall x A) \vee B$ эквивалентно $\forall x(A \vee B)$,
  - $(\forall x A) \wedge B$ эквивалентно $\forall x(A \wedge B)$,
  - $(\exists x A) \vee B$ эквивалентно $\exists x(A \vee B)$,
  - $(\exists x A) \wedge B$ эквивалентно $\exists x(A \wedge B)$.

Пример. $(p(f(x)) \vee \forall x q(g(x))) \wedge \exists y q(y)$

- Переименовываем переменные $(p(f(x)) \vee \forall z q(g(z))) \wedge \exists y q(y)$
- $(\forall z(p(f(x)) \vee q(g(z)))) \wedge \exists y q(y)$
- $\forall z(((p(f(x)) \vee q(g(z)))) \wedge \exists y q(y))$
- $\forall z \exists y(\forall z(p(f(x)) \vee q(g(z))) \wedge q(y))$

Арифметическая иерархия

- $\Sigma_0 = \Pi_0$ — множество разрешимых предикатов.
- Σ_1 — множество предикатов, которые представляются в виде $\exists x P(x, y)$, где $P \in \Pi_0$.
- $\Pi_1 : \forall x P(x, y)$, где $P \in \Sigma_0$.
- Σ_k — множество предикатов, которые представляются в виде $\exists x P(x, y)$, где $P \in \Pi_{k-1}$.
- $\Pi_k : \forall x P(x, y)$, где $P \in \Sigma_{k-1}$.
- $\Sigma_k :$ $\underbrace{\exists x_1 \forall x_2 \exists x_3 \ldots}_{k \text{ перемен кванторов}}$ $P(x_1, \ldots, x_k, y)$, P — разрешимый предикат.
- $\Pi_k :$ $\underbrace{\forall x_1 \exists x_2 \forall x_3 \ldots}_{k \text{ перемен кванторов}}$ $P(x_1, \ldots, x_k, y)$, P — разрешимый предикат.

Арифметическая иерархия

- $\Sigma_k \subseteq \Sigma_{k+1}$, $\Pi_k \subseteq \Pi_{k+1}$;
- $\Sigma_k \subseteq \Pi_{k+1}$, $\Pi_k \subseteq \Sigma_{k+1}$;
- $\Sigma_k \cup \Pi_k \subseteq \Sigma_{k+1} \cap \Pi_{k+1}$;
- $P \in \Sigma_k \iff \neg P \in \Pi_k$;
- Любой арифметичный предикат попадает в какой-нибудь уровень полиномиальной иерархии.
- Σ_1 — перичислимые предикаты.
- Π_1 — коперечислимые.
- Верно ли $\Sigma_k \subsetneq \Sigma_{k+1}$?

m-сведения

- $A \leq_m B$, если существует всюду определенная вычислимая функция f, что $\forall x, x \in A \iff f(x) \in B$.
- $A \leq_m B$, B — разрешимо $\implies$ A — разрешимо
- $A \leq_m B$, B — перечислимо $\implies$ A — перечислимо
- $A \leq_m B \iff \mathbb{N} \setminus A \leq_m \mathbb{N} \setminus B$
- $A \leq_m B$, $B \in \Sigma_k \implies A \in \Sigma_k$
  - $y \in B \iff \exists x_1 \forall x_2 \exists x_3 \ldots P(x_1, \ldots, x_k, y)$
  - $y \in A \iff \exists x_1 \forall x_2 \exists x_3 \ldots P(x_1, \ldots, x_k, f(y))$
- $A \leq_m B$, $B \in \Pi_k \implies A \in \Pi_k$
- Ω — набор множеств. $A \in \Omega$ называется m-полным, если $\forall B \in \Omega, B \leq_m A$.

Универсальные множества в арифметической иерархии

- Универсальное перечислимое множество: $U = \{(n, x) \mid < n > (x) \text{ останавливается}\}$
- A — перечислимое множество, $\mathcal{A}$ — перечисляющий алгоритм, то $A = \{x \mid (\sharp\mathcal{A}, x) \in U\}$
- Универсальное множество в Π_1 : $\overline{U} = \{(n, x) \mid (n, x) \notin U\}$.
- По индукции покажем, что универсальное множество есть в Σ_k, Π_k
- Пусть $A \in \Sigma_{k+1}$, тогда $x \in A \iff \exists y P(x, y)$, где $P \in \Pi_k$, пусть U — универсальное множество в Π_k, тогда $P = U(n_P, x, y)$.
- $x \in A \iff \exists y U(n_P, x, y)$
- $\exists y U(n, x, y)$ — универсальное множество в Σ_{k+1}.
- Дополнение универсального в Σ_k — универсальное в Π_k.

Строгость арифметической иерархии

- $T(n, x)$ — универсально Σ_k множество
- Пусть $T \in \Pi_k$
- $t(x) = T(x, x) \in \Pi_k$
- $d(x) = \neg t(x) \in \Sigma_k$, не является проекцией $T(n, x)$.
- $\Sigma_k \neq \Pi_k \subseteq \Sigma_{k+1}$
- $\Pi_k \subsetneq \Pi_{k+1}$

Теорема Тарского

- Все арифметичные предикаты содержатся в арифметической иерархии. Арифметическая иерархия состоит из арифметичных предикатов.
- Пусть T — множество номеров всех истинных замкнутых формул.
- Любое арифметичное множество m-сводится к T
- Теорема. (Тарский) T не является арифметичным
  - Пусть $T \in \Sigma_k$, тогда вся арифметическая иерархия содержится в Σ_k
- Теорема. (Гедель) Множество T не является перечислимым.

Прямое доказательство теоремы Геделя

- $Proof(m, n)$: строка с номером m является доказательством замкнутой формулы номер n.
- $Subst(m, n, k)$: m — это номер замкнутой формулы, который получается, если подставить вместо свободной переменной n-ой однопараметрической формулой число k.
- $\neg\exists z \exists p[Subst(z, x, x) \wedge Proof(p, z)]$
- Эта формула с одной свободной переменной x. Пусть ее номер N.
- Подставим N в эту формулу. Получилась формула φ.
- По построению формула φ истинна, когда недоказуема и ложна, когда доказуема.

Задачи

1. Арифметично ли множество номеров алгоритмов, которые останавливаются хотя бы на одном входе?
2. Постройте явно универсальные Σ_n и Π_n множества.
3. Покажите, что для любого N множество всех истинных замкнутых арифметических формул, содержащих не более N кванторов, арифметично.
4. Пусть свойство пар натуральных чисел $R(x, y)$ принадлежит Σ_n. Докажите, что свойство $S(x) = (\forall y \leq x) R(x, y)$ тоже принадлежит Σ_n.
5. Докажите, что нет алгоритма, который бы проверил, верно ли, что данная машина Тьюринга работает на входе длины n не более, чем $100n^2 + 200$ шагов.