МФТИ, сложность вычислений, осень 2023
Семинар 01. Модели вычислений

Определение. (Детерминированной многоленточной) машиной Тьюринга называется кортеж объектов $\langle \Sigma, \Gamma, Q, q_{start}, q_{accept}, q_{reject}, k, \delta \rangle$, такой что Σ, Γ, Q — непустые конечные множества, $\Sigma \subset \Gamma$, k — целое положительное число, $q_{start}, q_{accept}, q_{reject}$ — три различных элемента Q, $\delta : (Q \setminus \{q_{accept}, q_{reject}\}) \times \Gamma^k \to Q \times \Gamma^k \times \{L, N, R\}^k$. В таком случае Σ называется входным алфавитом, Γ — ленточным алфавитом, Q — множеством состояний, q_{start} — начальным состоянием, q_{accept} и q_{reject} — принимающим и отвергающим состоянием соответственно, k — числом лент, δ — функцией перехода.
Определение. Язык $L \subset \Sigma^*$ распознаётся машиной Тьюринга M, если для каждого $x \in \Sigma^*$ вычисление $M(x)$ останавливается и $M(x) = L(x)$, где $L(x)$ — характеристическая функция языка L.
Определение. Язык $L \subset \Sigma^*$ распознаётся машиной Тьюринга M за время $O(T(n))$ (или просто $T(n)$), если M распознает L, а также существует глобальная константа C, такая что для каждого $x \in \Sigma^*$ вычисление $M(x)$ останавливается не более чем за $C \cdot T(|x|)$ шагов, то есть за $O(T(n))$ шагов, где $n = |x|$.
Определение. Если $T(n) : \mathbb{N} \to \mathbb{N}$ — функция, то класс $\mathbf{DTIME}(T(n))$ состоит в точности из тех языков, которые распознаются хоть какой-нибудь машиной Тьюринга за время $T(n)$.
Определение. $\mathbf{P} = \bigcup\limits_{c=1}^{\infty} \mathbf{DTIME}(n^c)$.
Тезис Чёрча—Тьюринга. Любой физический вычислитель можно смоделировать на машине Тьюринга.
Тезис Чёрча—Тьюринга в сильной форме. Любой физический вычислитель можно смоделировать на машине Тьюринга с не более чем полиномиальным замедлением.

---

1. Конфигурацией машины Тьюринга M назовём набор $\langle \alpha_1, \ldots, \alpha_k, \beta_1, \ldots, \beta_k, q \rangle$. В нём α_i — строка, находящаяся на i-й ленте (нестрого) левее позиции указателя, β_i — строка правее этой позиции, а q — текущее состояние. Формально определите, что значит, что $M(x) = 0$, $M(x) = 1$ и $M(x) = \perp$.
2. Как на многоленточной машине Тьюринга смоделировать
а) вычисление функции, а не распознавание языка;
б) вычисление функции многих аргументов;
в) запрет на движение влево на входной ленте (одноразовое чтение);
г) использование случайных битов?
3. Опишите класс разрешимых языков $\mathbf{R}$, если в определении машины Тьюринга убрать требование конечности множества состояний Q. Проделайте то же для Σ и Γ.
4. Докажите, что класс $\mathbf{P}$ не изменяется, если вместо многоленточной машины Тьюринга использовать
а) машину с ленточным алфавитом $\Gamma = \Sigma \cup \{\#\}$ (обычно $\Sigma = \{0, 1\}$);
б) непоседливую машину (ту, которая на каждом шаге должна сдвинуться на каждой из лент);
в) машину, в которой ленты бесконечны только в одну сторону;
г) одноленточную машину Тьюринга ($k = 1$);
д) RAM-машину (random access memory).
5. Чтобы не рассматривать различные входные алфавиты Σ и чтобы уметь задавать вопросы о комбинаторных объектах, а не только строках, достаточно научиться кодировать все данные в бинарном алфавите. Предъявите какое-нибудь эффективное (с быстрым кодированием и декодированием) инъективное сюръективное соответствие следующих множеств объектов на $\{0, 1\}^*$:
а) пары бинарных строк (можно ли потратить $|x| + |y| + \log|x| + 2\log\log|x| + O(1)$ битов для кодирования пары строк (x, y)?);
б) натуральные числа;
в) булевы формулы;
г) рациональные числа (можно ли вещественные?);
д) матрицы;
е) графы.

6*. Докажите, что язык $\mathsf{PAL} = \{x \in \{0,1\}^* \mid x = x^R\}$ всех палиндромов над бинарным алфавитом нельзя распознать на одноленточной машине за $o(n^2)$, но можно распознать на многоленточной за $O(n)$.

7. Рассмотрим язык $\{0^n1^n \mid n$ — целое положительное число$\}$. Докажите, что его можно распознать на одноленточной машине за $O(n \log n)$.

1. Здесь нужно выделить символы под всеми k указателями и разобрать случаи переходов влево, вправо и стояния на месте на каждой из лент. Также понадобится сформулировать понятие стартовой конфигурации.

2.

а) Заведите отдельную выходную ленту, на которой записывается ответ.

б) Аргументы можно подавать на разных лентах.

в) Достаточно немного изменить определение δ.

г) На отдельной ленте можно подавать случайную строку. Тогда вероятность выдать какой-то ответ равна доле тех случайных строк, на которых этот ответ достигается.

3. Покажите, что при бесконечном Q или Γ все языки становятся разрешимыми.

4.

а) Можно перекодировать старый ленточный алфавит через $\Sigma \cup \{\#\}$ и выписывать на лентах закодированные данные. Для чтения может понадобиться расширить множество состояний (чтобы запоминать прочитанные биты). Замедление должно получиться в константное число раз (константа зависит от структуры исходной машины M).

б) Случай $k = 1$ можно разобрать отдельно, тогда вместо стояния на месте можно сходить влево-вправо (внимательно проследите за состояниями). В общем случае можно разнести все значимые ячейки и печатать между ними бланки (#). Тогда N заменяется на LR, L заменяется на LL, а R — на RR. Остаётся понять, как внести бланки между буквами входного слова x.

в) Ленту, бесконечную в две стороны, можно согнуть в некоторой точке. Теперь в ячейках следует писать пары символов из Γ, а в состоянии также поддерживать номер половины ленты.

г) На машине с k лентами пронумеруйте ячейки i-й ленты числами $i, i+k, i+2k, \ldots$. На одной новой ленте храните ячейки в полученном порядке $(1, 2, \ldots)$. Для поддержания позиций старых указателей символы надо размножить на две группы: те, на которые указывают головки машины, и те, на которые не указывают. Один такт на старой машине превращается в проход по всей ленте. Если время работы было $T(n)$, то станет $k \cdot T^2(n)$.

д) В этой модели в паре с каждой лентой есть адресная лента, на которой можно вписывать номер (уже когда-либо использованной) ячейки. Переход в выделенное состояние совершит мгновенное перемещение в заданную ячейку ленты. Для симуляции RAM-машины на обычной машине достаточно делать переходы последовательными шагами L или R.

5.

а) Простейший метод — раздваивание символов и вставка маркера-разделителя 01 между строками x и y. Для экономии числа бит можно выписать длину x в таком раздвоенном виде, после чего записать x и y без разделителей. Также можно выписать длину длины x.

б) Натуральные числа эффективно кодируются в двоичной системе счисления.

в) Достаточно все допустимые символы закодировать коротким набором бит.

г) Рациональные числа — отношение двух целых. Вещественные числа закодировать нельзя (инъекций из континуального в счётное не существует).

д) Можно ввести какой-нибудь разделитель между элементами матрицы.

е) Граф однозначно задаётся матрицей смежности.

6*. Рассмотрим слова вида $x0^{2n}y^R$, где $|x| = |y| = n$, предположим, что PAL распознаётся некоторой одноленточной машиной. Пусть протокол в точке i — это описание всех переходов (состояния и направление движения) между i-й и $(i+1)$-й ячейками. Тогда при $x \neq z$ и для любого $i : n \leqslant i \leqslant 3n$, протоколы работы машины на словах $x0^{2n}x^R$ и $z0^{2n}z^R$ различны. Далее, существует некоторое i, т.ч. протокол в точке i — самый короткий (среди всех $2n+1$ протоколов) хотя бы для $2^n/(2n+1)$ слов. Для всех этих слов протоколы в i различны, так что есть слово с минимальной длиной протокола $\Omega(n)$. Наконец, каждому действию каждого протокола соответствует такт работы машины. Значит, тактов хотя бы на одном слове совершается $\Omega(n^2)$.

7. Каждый раз отмечайте половину нулей и единиц использованными.