Конспект по теории сложности
III семестр
Современное программирование, факультет математики и компьютерных наук, СПбГУ
(лекции Гирша Эдуарда Алексеевича)

Тамарин Вячеслав

January 19, 2021

Contents

Index

Chapter 1

Введение в теорию сложности вычислений

Лекция 1: †

5 nov

1.1 Машины Тьюринга

1.1.1 Напоминания

Обсудим, что мы решаем.

Обозначение.

- *Алфавит будет бинарный* $\{0,1\}$*;*
- *Множество всех слов длины* n *:* $\{0,1\}^n$*;*
- *Множество всех слов конечной длины* $\{0,1\}^*$*;*
- *Длина слова* x*:* $|x|$.

Определение 1

Язык (задача распознавания, decision problem) — $L \subseteq \{0,1\}^*$.

Индивидуальная задача — пара, первым элементом которой является условие, а второй – решение; принадлежит $\{0,1\}^* \times \{0,1\}^*$.

Массовая задача — некоторое множество индивидуальных задач, то есть бинарное отношение на $\{0,1\}^*$.

Определение 2

Будем говорить, что алгоритм **решает задачу поиска** для массовой задачи R, если для условия x он находит решение w, удовлетворяющее $(x,w) \in R$.

Можем сопоставить массовой задаче, заданной отношением R, язык

$$L(R) = \{x \mid \exists w\colon (x,w) \in R\}.$$

Пример 1.1.1 (Массовая задача и соответствующий язык)**.**

$$\texttt{FACTOR} = \{(n,d) \mid d|n,\ 1 < d < n\}.$$

Здесь условием задачи является натуральное число n, а решением некоторый (не 1, и не n) делитель числа n.

Данной задаче соответствует язык

$$L(\texttt{FACTOR}) = \text{множество всех составных чисел.}$$

1.1.2 Детерминированная машина Тьюринга

Определение 3: Детерминированная машина Тьюринга

Детерминированная машина Тьюринга —

- конечный алфавит (с началом ленты и пробелом): $\Sigma = \{0, 1, \triangleright, \_\}$;
- несколько лент, бесконечных в одну сторону;
- читающие/пишущие головки, по одной на каждую ленту;
- конечное множество состояний, в том числе начальное (q_S/q_0), принимающее (q_Y/q_{acc}) и отвергающее (q_N/q_{rej});
- управляющее устройство (программа), содержащее для каждых $q, c_1, \dots c_k$ одну инструкцию вида

$$(q, c_1, \dots c_k) \mapsto (q', c_1', \dots c_k', d_1, \dots d_k),$$

где $q, q' \in Q$ — состояния, $c_i, c_i' \in \Sigma$ — символы, обозреваемые головками, $d_i \in \{\rightarrow, \leftarrow, \cdot\}$ — направления движения головок.

ДМТ **принимает** входное слово, если заканчивает работу в q_{acc}, и **отвергает**, если заканчивает в q_{rej}.

ДМТ M **распознает язык** A, если принимает все $x \in A$ и отвергает все $x \notin A$.

$$A = L(M).$$

Замечание. Обычно есть отдельная лента только для чтения, куда записаны входные данные, и лента только для вывода, куда нужно поместить ответ. Остальные ленты будут рабочими.

Замечание. Изначально на входной ленте вход и пробелы, на остальных пробелы, головки в крайней левой позиции, а состояние есть q_s.

Определение 4

Время работы машины M на входе x — количество шагов (применений инструкций) до достижения q_{acc} или q_{rej}.

Используемая память — суммарное крайнее правое положение всех головок на *рабочих* лентах.

Теорема 1.1.1. Для любого $k \in \mathbb{N}$, работу ДМТ M с k рабочими лентами, работающую t шагов, можно промоделировать на ДМТ с двумя рабочими лентами за время $\mathcal{O}(t \log t)$, где константа $\mathcal{O}(\dots)$ зависит только от размеров записи машины M.

□

- Перестроим исходную МТ:
  - Запишем все ленты в одну строку по символу из всех лент по очереди.
  - Будем бегать «лентой по головке»: выровняем все ленты, чтобы головки стояли друг над другом и далее будем сдвигать нужную ленту.
  - Заметим, что двустороннюю ленту можно смоделировать на односторонней, причем с увеличением количества операций в константу раз:
    разрезаем двустороннюю пополам и записываем элементы через один.

- Теперь поймем, как экономично сдвигать ленты в однострочной записи.

  Разобьем строку на блоки начиная от позиции головки в две стороны: справа блоки R_i, слева L_i. При этом $|L_i| = |R_i| = 2^i$. Раздвинем символы, заполняя пустоту специальными символами пустоты, так, чтобы в каждом блоке ровно половина элементов были пустыми.

  Далее будем поддерживать такое условие:

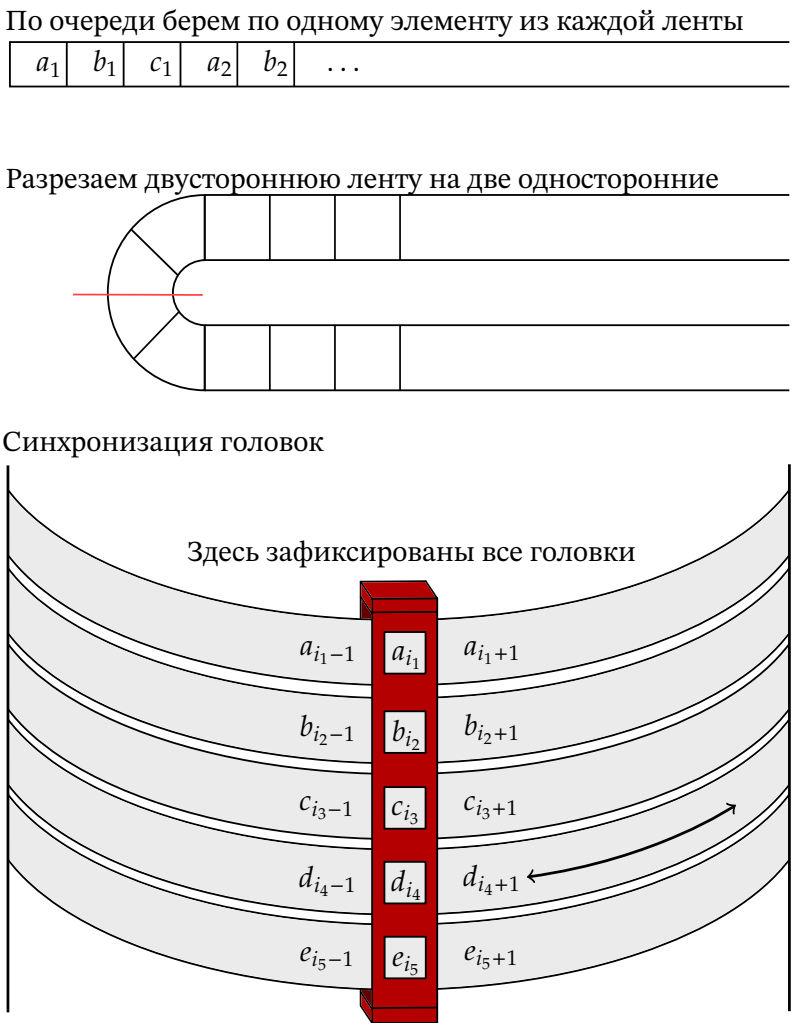


Figure 1.1: Построение новой МТ

1. В блоке либо информация, либо пусто, либо наполовину (ровно) пусто
2. L_i пустой, когда R_i полный
3. L_i наполовину пустой, когда R_i наполовину полный
4. L_i полный, когда R_i пустой

Пусть нужно подвинуть головку влево. Найдем слева первый не пустой блок L_i. Возьмем из него правую половину и разложим по пустым $L_{<i}$ так, чтобы порядок сохранился и каждый из $L_{<i}$ стал полупустым, а первый символ попал под головку.

Так получится сделать, так как всего перемещаемых символов 2^{i-1}, а в j-й блок будет помещено 2^{j-1} символов, поэтому всего в $L_{<i}$ поместится

$$1 + 2 + 4 + \ldots + 2^{i-2} = 2^{i-1} - 1.$$

И один символ под головку.

Чтобы инвариант сохранился нужно теперь исправить правую часть.

Так как первые $i-1$ левых блоков были пусты, первые $i-1$ правых блоков полны, а R_i пуст (либо наполовину полон, в зависимости от первоначального состояния L_i). Заполним половину в R_i символами из R_{i-1}. Теперь R_{i-1} пустой, а меньшие полные. Проделаем ту же операцию еще раз для $i-1$, потом для $i-2$ и так далее. Заметим, что по отношению к R_i все сохранилось: если L_i был наполовину полон, то стал пуст, а R_i - полон (так как до этого был наполовину полон). Полностью аналогичный случай, если бы L_i был полон.

Когда мы дойдем до R_1, положим туда элемент из-под головки.

Итого, инвариант сохранился.

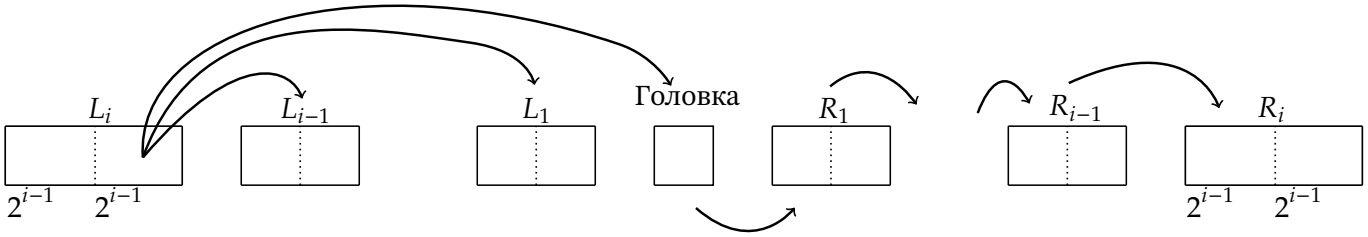


Figure 1.2: Структура блоков

- Посчитаем количество операций. В алгоритме переносим различные отрезки из одного места в другое. Чтобы делать это за линию, сначала скопируем нужный участок на вторую ленту, а затем запишем с нее.

  Тогда при перераспределении происходит $c \cdot 2^i$ операций:
  каждый символ переносили константное число раз (на вторую ленту, со второй ленты) плюс линейное перемещение от L_i к R_i несколько раз (символов всего 2^{i-1} в каждой половине, итого суммарно перенесли 2^i символов).

  Докажем, что с i-м блоком происходят изменения не чаще 2^{i-1} шагов. Пусть L_i хотя бы наполовину заполнен. Когда мы забрали половину из него, мы заполнили все $L_{<i}$ и $R_{<i}$ наполовину.

  Поэтому, чтобы изменить L_i еще раз, нужно сначала опустошить все $L_{<i}$. При перераспределении в левой части становится на один элемент меньше, а всего там 2^{i-1} заполненное место. Для того, чтобы все они ушли из левой половины, придется совершить 2^{i-1} сдвигов.

  Итого, для t шагов исходной машины будет

$$\sum_{i}^{\log t} c \cdot 2^i \cdot \frac{t}{2^{i-1}} = \mathcal{O}(t \log t).$$

  Почему сумма до логарифма? Заметим, что так как мы сделали не более чем t шагов изначально, то мы не можем на каждой ленте занять более чем t ячеек. В таком случае, самый большой блок не будет больше t. А его индекс, соответственно не будет больше, чем $\log t$.

  Замечание. Так как до этого у нас было k лент и все сдвиги могли происходить одновременно, то здесь мы делаем сдвиг каждой ленты по очереди. То есть на самом деле мы получаем $\mathcal{O}(k \cdot t \log t)$, но k в данном случае просто константа (почти точно константа может стать намного больше, чем k, но всё равно останется константой).

■

Теорема 1.1.2 (Об универсальной МТ)**.** Существует ДМТ U, выдающая на входе $(M,\ x)$ тот же результат, что дала бы машина M на входе x, за время $\mathcal{O}(t \log t)$, где t — время работы M на входе x.

□ Используем прием из прошлой теоремы 1.1.1. ■

Замечание. Единственный способ узнать результат машины M на строке x, это промоделировать вычисление машины M на входе. Мы никогда не можем заранее сказать результат этого вычисления, и заканчивается ли оно вообще. Поэтому, моделировать вычисления (т.е. иметь универсальную машину Тьюринга) можно, но, например, нельзя иметь машину, которая по записи машины M' скажет, принимает ли M' пустую строку, можно лишь повести себя как M' на пустой строке.

1.2 Классы сложности

1.2.1 Классы DTime и P

Определение 5: Конструируемая по времени функция

Функция $t\colon \mathbb{N} \to \mathbb{N}$ называется **конструируемой по времени**, если

- $t(n) \geqslant n$;
- двоичную запись $t(|x|)$ можно найти по входу x на ДМТ за $t(|x|)$ шагов.

Замечание. Все стандартные функции (многочлены, экспоненты) конструируемы по времени.

Неконструируемыми являются вырожденные, специально построенные случаи.

Определение 6: Класс DTime

Язык L принадлежит классу $\mathbf{DTime}[t(n)]$, если существует ДМТ M, принимающая L за время $\mathcal{O}(t(n))$, где t конструируема по времени.

Константа может зависеть от языка, но не от длины входа.

Определение 7: Класс P

Класс языков, распознаваемых за полиномиальное время на ДМТ —

$$\mathbf{P} = \bigcup_c \mathbf{DTime}[n^c].$$

Будем обозначать задачи, заданные отношениями волной.

Определение 8

Массовая задача R **полиномиально ограничена**, если существует полином p, ограничивающий длину кратчайшего решения:

$$\forall x \left(\exists u\colon (x,u) \in R \Longrightarrow \exists w\colon \big((x,w) \in R \wedge |w| \leqslant p(|x|)\big)\right).$$

Массовая задача R **полиномиально проверяема**, если существует полином q, ограничивающий время проверки решения: для любой пары (x,w) можно проверить принадлежность $(x,w) \stackrel{?}{\in} R$ за время $q(|(x,w)|)$.

Определение 9: Класс $\widetilde{\mathbf{NP}}$

$\widetilde{\mathbf{NP}}$ — класс задач поиска, задаваемых полиномиально ограниченными полиномиально проверяемыми массовыми задачами.

Определение 10: Класс $\tilde{\mathbf{P}}$

$\tilde{\mathbf{P}}$ — класс задач поиска из $\widetilde{\mathbf{NP}}$, разрешимых за полиномиальное время.

То есть класс задач поиска, задаваемых отношениями R, что для всех $x \in \{0,1\}^*$ за полиномиальное время можно найти w, для которого $(x,w) \in R$.

Ключевой вопрос теории сложности $\tilde{\mathbf{P}} \stackrel{?}{=} \widetilde{\mathbf{NP}}$

Определение 11: Класс NP

NP — класс языков (задач распознавания), задаваемых полиномиально ограниченными полиномиально

проверяемыми массовыми задачами:

$$\mathbf{NP} = \{L(R) \mid R \in \widetilde{\mathbf{NP}}\}.$$

Замечание. $L \in \mathbf{NP}$, если существует массовая п.о.п.п.[1] задача, такая, что

$$\forall x \in \{0,1\}^* : x \in L \iff \exists w : (x, w) \in R.$$

Определение 12: Класс P

P— класс языков (задач распознавания), распознаваемых за полиномиальное время.

$$\mathbf{P} = \{L(R) \mid R \in \tilde{\mathbf{P}}\}.$$

Замечание. Очевидно, $\mathbf{P} \subseteq \mathbf{NP}$.

Ключевой вопрос теории сложности $\mathbf{P} \stackrel{?}{=} \mathbf{NP}$

Лекция 2: †

12 nov

1.3 Недетерминированная машина Тьюринга

Определение 13: Недетерминированная машина Тьюринга

Недетерминированная машина Тьюринга — машина Тьюринга, допускающая более одной инструкции для данного состояния $q \in Q$ и $c_1, \dots c_k \in \Sigma$, то есть для состояния q и символа c функция δ будет многозначной.

Из такого определения получаем **дерево вычислений** вместо последовательности состояний ДМТ.

Мы говорим, что НМТ [2] **принимает** вход, если существует путь в дереве вычислений, заканчивающийся принимающим состоянием.

Утверждение. В машины (ДМТ / НМТ) с заведомо ограниченным временем работы можно встроить **будильник** и считать время вычислений на входах одной длины всегда **одинаковым**. Для этого можем просто записать на дополнительную ленту $t(n)$ единиц и стирать по одной за ход.

Определение 14: Эквивалентное определение НМТ

Недетерминированная машина Тьюринга — ДМТ, у которой есть дополнительный аргумент – конечная (ограниченная временем работы) подсказка w на второй ленте.

Определённая таким образом НМТ M принимает вход x, если существует такая подсказка w, что соответствующая ДМТ примет такой вход, т.е. $M(x, w) = 1$.

□ Докажем эквивалентность.

- Представим дерево вычисления как бинарное дерево и пронумеруем ребра из каждой вершины 0 и 1. Теперь запишем нужную принимающую ветку на ленту-подсказку.

  По подсказке можем построить дерево, где будет нужный путь.

- Обратно: у нас есть ДМТ, которая ожидает вход из самого входа x (который мы знаем – всегда одинаков) и подсказки w. Считаем, что мы знаем оценку верхнюю на длину подсказки. Построим теперь НМТ: бинарное дерево 0 и 1.

  Отработав какой-то путь в таком дереве, мы получим возможную подсказку, которую отдадим в качестве w ДМТ. Тогда приниматься будет тогда и только тогда, когда существует подсказка.

[1] полиномиально ограниченная полиномиально проверяемая

[2] недетерминированная машина Тьюринга

■

Определение 15

Еще одно определение класса **NP** — класс языков, принимаемых полиномиальными по времени НМТ.

Замечание. Это определение класса **NP**, можно считать двумя, так как у нас есть два определения НМТ.

1.4 Сведения и сводимости

Определение 16: Сведение по Карпу

Язык L_1 **сводится по Карпу** к языку L_2, если существует полиномиально вычислимая функция f такая, что

$$\forall x: x \in L_1 \iff f(x) \in L_2.$$

Определение 17: Сведение по Левину

Задача поиска (отношение) R_1 **сводится по Левину** к задаче R_2, если существуют функции f, g, h такие, что для всех x_1, y_1, y_2 верно

- $R_1(x_1, y_1) \Longrightarrow R_2(f(x_1), g(x_1, y_1))$;
- $R_1(x_1, h(f(x_1), y_2)) \Longleftarrow R_2(f(x_1), y_2)$;
- f, g, h полиномиально вычислимые.

Замечание. Первое условие нужно для того, чтобы образы каждого входа, имеющего решение первой задачи, имели решение и второй задачи.

Теорема 1.4.1. Классы $\mathbf{P}, \mathbf{NP}, \tilde{\mathbf{P}}, \widetilde{\mathbf{NP}}$ замкнуты относительно этих сведений.
То есть если $R_2 \in \tilde{\mathbf{P}}, R_1 \to R_2 \Rightarrow R_1 \in \tilde{\mathbf{P}}$

▢ Пусть есть два языка или две задачи поиска R_1, R_2, R_2 принадлежит классу $C \in \{\mathbf{P}, \tilde{\mathbf{P}}, \mathbf{NP}, \widetilde{\mathbf{NP}}\}$ и R_1 сводится к R_2. Чтобы проверить принадлежность $R_1 \in C$, нам нужно:

- Проверить полиномиальную ограниченность и полиномиальную проверяемость, тогда R_2 будет в **NP** или $\widetilde{\mathbf{NP}}$.
- Если $C \in \{\mathbf{P}, \tilde{\mathbf{P}}\}$, то еще проверить, что для R_1 есть полиномиальный алгоритм.

Задачи поиска. R_2 задано п.о.п.п. отношением. Что можно узнать про R_1?

Если есть решение для R_1, то функция g дает решение R_2, которое не на много длиннее.

Еще есть h, которая позволяет из решения R_2 обратно быстро построить решение R_1.

- **Полиномиальная ограниченность.** Пусть есть некоторое решение y_1 для задачи R_1. Для него можно получить некоторое решение R_2 – $g(x_1, y_1)$.
  Так как существует **какое-то** решение $g(x_1, y_1)$, то (по определению п.о.) есть решение y_2, которое ограничено полиномом. В таком случае его можно перевести в $h(f(x_1), y_2)$ – решение для R_1. Оно тоже будет ограничено полиномом, так как h – полиномиально вычислимо (и как следствие – полиномиально ограничена).
- **Полиномиальная проверяемость.** Проверяется аналогично.
- **Полиномиальный алгоритм.** Если есть алгоритм для R_2 и x_1, сначала перегоняем $x_1 \to f(x_1)$, далее применяем алгоритм, получаем y_2, а далее, используя h, перегоняем обратно в R_1.

Языки. Пусть есть $L_1 \to L_2$, $L_2 \in C$.

- $C = \mathbf{P}$. Хотим проверить $x \in L_1$. Сначала можем за полином посчитать $f(x)$, а затем опять за полином проверить $f(x) \in L2$.
- $C = \mathbf{NP}$. У нас есть алгоритм проверки решения для L_2 за полином. Так как $L_1 \to L_2$, если $x \in L_1$, то $f(x) \in L_2$, поэтому можем проверить решение в L_2.

■

Утверждение. Если задача R_1 сводится по Левину к R_2, то язык $L(R_1)$ сводится по Карпу к $L(R_2)$.

□ Функция f для сведения по Карпу будет взята из сведения по Левину. Разберем два случая:

- $x \in L(R_1)$. Тогда мы точно знаем, что есть некоторый y_1, причем $(x, y_1) \in R_1$. Следовательно, по сведению по Левину есть такой $y_2 = g(x_1, y_1)$, что $(f(x_2), y_2) \in R_2$. Значит, $x \in L(R_1) \implies f(x) \in L(R_2)$.
- $x \notin L(R_1)$. Хотим показать, что тогда $f(x) \notin L(R_2)$. Пусть это не так. Тогда есть некоторый y_2 такой, что $(f(x), y_2) \in R_2$. Тогда из сведения по Левину знаем, что $(f(x), h(f(x), y_2)) \in R_1$, то есть $x \in L(R_1)$, противоречие.

■

Определение 18: Оракульная МТ

Оракульная МТ — МТ с доступом к оракулу, который за один шаг дает ответ на некоторый вопрос.

Обозначение. *При переходе в состояние q_{in} происходит «фантастический переход» в состояние q_{out}, заменяющий содержимое некоторой ленты на ответ оракула.*
M^B — оракульная машина M, которой дали оракул B.

Определение 19: Сведение по Тьюрингу

Язык или задача A **сводится по Тьюрингу** к B, если существует оракульная машина полиномиальная по времени $M^\bullet$ такая, что M^B решает A.
Например, если A — язык, $A = L(M^B)$.

Пример 1.4.1. Классы $\mathbf{P}$ и $\tilde{\mathbf{P}}$ замкнуты относительно сведений по Тьюрингу. А $\mathbf{NP}$ и $\widetilde{\mathbf{NP}}$ могут быть незамкнуты: если $A = \texttt{UNSAT}$, $B = \texttt{SAT}$, $M^O(x) = \overline{(x \in O)}$, и A сводится по Тьюрингу к B, но $B \in \mathbf{NP}$, а про A не известно.

1.4.1 Трудные и полные задачи

Определение 20: Трудные и полные задачи

Задача A называется **трудной** для класса $\mathbf{C}$, если $\forall C \in \mathbf{C}$: $C \to A$.
Задача A называется **полной** для класса $\mathbf{C}$, если она трудная и принадлежит $\mathbf{C}$.

Замечание. Если не упомянуто другое, имеется ввиду сводимость по Карпу.

Теорема 1.4.2. Если A — $\mathbf{NP}$-трудная и $A \in \mathbf{P}$, то $\mathbf{P} = \mathbf{NP}$.

Следствие 1. Если A — $\mathbf{NP}$-полная, то $A \in \mathbf{P} \iff \mathbf{P} = \mathbf{NP}$.

Задача об ограниченной остановке

Определение 21: BH

Определим задачу об ограниченной остановке $\widetilde{\texttt{BH}}(\langle M, x, 1^t\rangle, w)$ [a] так: дана НМТ M и вход x, требуется найти такую подсказку w, чтобы M распознавала x не более чем за t шагов.

Соответствующая задача распознавания — ответить, существует ли такая подсказка.

[a] здесь 1^t — служебные t единиц, ограничивающие время работы МТ

Теорема 1.4.3. Задача об ограниченной остановке $\widetilde{\mathbf{NP}}$-полная, а соответствующий язык **NP**-полный.

□

- Принадлежность $\widetilde{\mathbf{NP}}$ и **NP** следует из существования универсальной ДМТ, которая за $\mathcal{O}(t \log t)$ промоделирует вычисление ДМТ, описание которой дано ей на вход. После этого нужно проверить, что M успевает за t шагов закончить.
- Проверим, что язык **NP**-трудный. Пусть язык L принадлежит **NP**. По определению **NP** существует для соответствующего отношения R машина Тьюринга $M^*(x, w)$, которая работает за $p(|x|)$ – полином.

  Сведем L к задаче BH. Рассмотрим тройку $\langle M^*, x, 1^{p(|x|)}\rangle$. Пусть функция $f(x)$ будет равна этой тройке.

  В таком случае условие распознавание тройки равносильно тому, что x из языка $L(M^*)$
- Аналогично для задач поиска.

■

1.4.2 Булевы схемы

Определение 22: Булева схема

Булева схема — ориентированный граф без циклов, в вершинах которого записаны бинарные, унарные или нульарные операции над битами ($\wedge, \vee, \oplus$), при этом есть специальные вершины-входы и вершины-выходы.

Определение 23: CIRCUIT_SAT

$$\widetilde{\texttt{CIRCUIT\_SAT}} = \{(C, w) \mid C \text{ — булева схема}, C(w) = 1\}.$$

Соответственно, $C \in$ CIRCUIT_SAT, если существует такой вход w, что схема возвращает 1.

Очевидно, что CIRCUIT_SAT $\in$ **NP**. Чтобы доказать **NP**-трудность, сведем BH $\to$ CIRCUIT_SAT: будем рисовать конфигурацию МТ на схемах.

- Пусть каждый этаж схемы — конфигурация ДМТ. Всего этажей будет столько же, сколько шагов в МТ, то есть t. Если в последнем этаже q_{acc}, то результат 1.
- **Пересчет конфигураций.** Заметим, что при переходе от одной конфигурации к другой меняются только гейты рядом с положением головки.

  Выделим подсхему, которая должна по состоянию и элементу рядом с головкой получить новое состояние, положение головки и поменять элемент, а остальные символы скопировать. Так мы построим новый уровень с измененными элементами.

  Для хранения головки будем после каждого символа с ленты хранить d_i равное единице, если головка на символе c_i перед ним.

Если $d_i = 0$, то новый $c_i' = c_i$, иначе нужно заменить c_i на c_i' из программы МТ:

$$(q, c_{i-1}, c_i, c_{i+1}, d_{i-1}, d_i, d_{i+1}) \mapsto (q', c_i', d_i').$$

- Так как входная строка x нам дана, «запаяем» ее в схему: подключим входные гейты с элементами x к нужным входам.

  Тогда оставшимся входом схемы останется подсказка w для НМТ, а выходом — попадание в q_{acc}.

Таким образом, мы по $\langle M, x, t\rangle$ построили схему $C(w)$.

Лекция 3: †

19 nov

1.5 Теорема Кука-Левина

$\widetilde{\texttt{3-SAT}} = \{(F, A) \mid F$ — в 3-КНФ, $F(A) = 1\}$.

Пример 1.5.1.
$$\big((\neg x \vee \neg y \vee \neg z) \wedge (y \vee \neg z) \wedge (z), [x = 0, y = 1, z = 1]\big) \in \widetilde{\texttt{3-SAT}}.$$

Теорема 1.5.1 (Кук-Левин)**.** $\widetilde{\texttt{3-SAT}}$ — $\widetilde{\mathbf{NP}}$-полная задача.

□ Мы уже доказали полноту задач выполнимости булевых схем, поэтому будем сводить к ней.

Пусть у нас есть некоторая схема. Для каждого гейта заведем по переменной, которая обозначает результат операции в этом гейте. Входы тоже остаются гейтами в схеме.

Запишем для гейтов клозы длины 3, которые выражают результат в зависимости от аргументов.

Например, для входов x, y и операции $\oplus = g(x, y)$,

$$(x \vee y \vee \neg g)$$
$$(\neg x \vee \neg y \vee \neg g)$$
$$(x \vee \neg y \vee g)$$
$$(\neg x \vee y \vee g)$$

Еще для последнего гейта g (выходного) запишем клоз (g).

Значение в полученной схеме будет соответствовать результату конъюнкции всех клозов и наоборот: по формуле можем построить булеву схему и входные переменные выполняют ее. ■

Теорема 1.5.2. Пусть $R \in \widetilde{\mathbf{NP}}$, и соответствующий язык $L(R)$ — $\mathbf{NP}$-полон. Тогда R сводится по Тьюрингу к $L(R)$.

□ Во-первых, задача поиска из $\mathbf{NP}$ сводится к $\widetilde{\texttt{SAT}}$. При этом $\texttt{SAT}$ сводится к $L(R)$.

Осталось свести $\widetilde{\texttt{SAT}} \to \texttt{SAT}$. Для этого нужно построить МТ с оракулом $\texttt{SAT}$ будет решать $\widetilde{\texttt{SAT}}$.

Пусть нам дали формулу F и мы хотим найти выполняющий набор. Предполагается, что она выполнима.

Подставим первую переменную x_1 как 0 и как 1 в F (это тоже будут формулы) и спросим у оракула $\texttt{SAT}$ про $F[x_1 = 0] \in \texttt{SAT}$ и $F[x_1 = 1] \in \texttt{SAT}$.

Так как F выполнима, хотя бы одна из полученных схем выполнима. Выберем ее и продолжим подставлять в нее. Так мы дойдем до конечной истиной формулы. Следовательно, последовательность подставляемых значений x_i и будет выполняющим набором. ■

1.5.1 Оптимальный алгоритм для $\widetilde{\mathbf{NP}}$-задачи

Пусть мы хотим решить задачу, заданную отношениям R, с входом x. Давайте переберем все машины (не только полиномиальные) и, если какая-то машина выдала результат y, то проверим его $R(x, y)$ за полином.

Если ответ подошел, то просто заканчиваем работу, иначе продолжаем ждать других результатов.

Если машины были бы запущены параллельно, то мы бы нашли ответ за время самой быстрой машины на данном входе.

А мы будем делать шаги «змейкой»: выделим для l-ой машины 2^{-l} времени удельно.

На очередном этапе $2^l(1 + 2k) = 2^l + 2^{l+1}k$ будем моделировать k-ый шаг машины M_l. То есть для l-той машины первый шаг (нулевой) будет сделан на 2^l-том реальном шаге, и каждый следующий будет совершаться каждые 2^{l+1} шаг.

Так, например, будет выглядеть табличка для первых машин (указаны этапы моделирования, на которых будет выполнен соответствующий шаг):

№ МТ	0 шаг	1 шаг	2 шаг	3 шаг
0	1	3	5	7
1	2	6	10	14
2	4	12	20	28
3	8	24	40	56

Посчитаем замедление алгоритма. Мы хотим выдать ответ не сильно позже, чем самая быстрая машина. Но заметим, что такая машина одна[3], поэтому l это константа, следовательно, множитель 2^l тоже константа.

Как моделировать эти машины? Если было бы быстрое обращение к каждому элементу памяти, то $t(x) \leqslant \text{const}_i \cdot t_i + p(|x|)$, где i - номер самой быстрой машины ($p(|x|)$ на проверку).

Но у нас ДМТ, поэтому получаем $t(x) \leqslant \text{const}_i \cdot p(t_i(x))$ из-за необходимости хранить на одной ленте несколько МТ и следовательно тратить время на «переключения» между ними.

Замечание. Если $\mathbf{P} = \mathbf{NP}$, то построенный алгоритм может решить SAT за полиномиальное от времени работы самой быстрой машины $p(t_i(x))$, но и оно полиномиально в случае $\mathbf{P} = \mathbf{NP}$.

Теорема 1.5.3. Если $\mathbf{P} \neq \mathbf{NP}$, то существует язык $L \in \mathbf{NP} \setminus \mathbf{P}$, **не** являющийся $\mathbf{NP}$-полным.

□ Найдем задачу, которая и не в $\mathbf{P}$ и не является $\mathbf{NP}$-полной.

Занумеруем все полиномиальные ДМТ с полиномиальными будильниками[4]:

$$M_1, M_2, \ldots.$$

Аналогично пронумеруем полиномиальные сведения с будильниками, про которые мы будем думать, как про машины Тьюринга.

$$R_1, R_2, \ldots.$$

Построим следующий язык $\mathcal{K} = \{x \mid x \in \text{SAT} \wedge f(|x|) \equiv 0 \pmod 2\}$, где $f(n)$ ведет себя следующим образом:

1. за n шагов вычисляем $f(0), f(1), \ldots f(i) =: k$ (k — последнее значение, которое мы успели вычислить).
2. тоже за n шагов:
   (a) если $k \equiv 0 \pmod 2$, то проверим, что $\exists z$: $M_{k/2}(z) \neq \mathcal{K}(z)$, и в случае успеха вернем $k + 1$, иначе (или истратили n шагов) k;

[3] Кажется, здесь важно просто, что такая есть и она имеет какой-то номер l.

[4] то есть настроенными на полиномиальное время

(b) если $k \equiv 1 \pmod 2$, проверим, что очередное $R_{\frac{k-1}{2}}$ правильно сводит $\texttt{SAT}$ к R: если $\exists z\colon \mathcal{K}(R_{\frac{k-1}{2}}(z)) \neq \texttt{SAT}(z)$, возвращаем $k+1$, в любом другом случае — k.

По факту в пункте (a) мы проверяем, что рассматриваемая машина Тьюринга не решает задачу $\mathcal{K}$. Такое вычисление точно остановится, т.к. ограничено число шагов, т.е., если нынешняя МТ вдруг решала бы задачу $\mathcal{K}$, то число k просто и вернулось бы. Здесь первый пункт проверяет $\mathcal{K} \in \mathbf{P}$, а второй — $\texttt{SAT} \to \mathcal{K}$, то есть $\mathcal{K}$ $\mathbf{NP}$-трудная.

Для какого-то огромного n найдутся контр-примеры и мы получим $k+1$.

3. $f(0) = 0$

Заметим, что $\mathcal{K} \in \mathbf{NP}$, так как выполняющий набор можно проверить принадлежность $\texttt{SAT}$ за полином и подставить в f, которая тоже работает полином ($2n$ шагов).

- Пусть $\mathcal{K} \in \mathbf{P}$, тогда есть полиномиальная машина M, которая принимает этот язык. Поэтому в пункте (a) мы дальше этой машины не пройдем, так как контр-примера там нет. То есть с некоторого момента $f(n) \equiv 0 \pmod 2$, по определению с некоторого места $\mathcal{K} = \texttt{SAT}$, кроме конечного числа случаев, их можно разобрать отдельно. Тогда $\mathcal{K} \in \mathbf{NP\text{-}complete}$ и $\mathcal{K} \in \mathbf{P}$, поэтому $\mathbf{P} = \mathbf{NP}$.
- Если $\mathcal{K} \in \mathbf{NP\text{-}complete}$, то с некоторого момента мы не пройдем пункт (b), так как у нас действительно будет сводимость к $\mathcal{K}$. С некоторого места $f(n) \equiv 1 \pmod 2$, а тогда $|\mathcal{K}| < \infty$. Следовательно, $\mathcal{K} \in \mathbf{P}$. Опять противоречие.

■

1.6 Полиномиальная иерархия

Обозначение. *Пусть есть два класса языков $\mathcal{C}, \mathcal{D}$. Можно построить класс $\mathcal{C}^{\mathcal{D}}$, который состоит из языков вида C^D, где $D \in \mathcal{D}$ и C — машина для языка из $\mathcal{C}$.*

Определение 24: Класс дополнений

$$\mathbf{co}\text{-}\mathcal{C} = \{L \mid \overline{L} \in \mathcal{C}\}.$$

Пример 1.6.1. $\texttt{SAT} \in \mathbf{NP}$, дополнение к $\texttt{SAT}$, то есть всюду ложные формулы (или записи, которые вообще формулами не являются, но их легко проверить полиномиально) $\in \mathbf{co\text{-}NP}$.

1.6.1 Полиномиальная иерархия

Самый нижний класс иерархии — $\mathbf{P}$. Остальные классы строятся также из $\mathbf{NP}$ и $\mathbf{co\text{-}NP}$.

$$\Sigma^0\mathbf{P} = \Pi^0\mathbf{P} = \Delta^0\mathbf{P} = \mathbf{P}$$
$$\Sigma^{i+1}\mathbf{P} = \mathbf{NP}^{\Pi^i\mathbf{P}}$$
$$\Pi^{i+1}\mathbf{P} = \mathbf{co\text{-}NP}^{\Sigma^i\mathbf{P}}$$
$$\Delta^{i+1}\mathbf{P} = \mathbf{P}^{\Sigma^i\mathbf{P}}$$
$$\mathbf{PH} = \bigcup_{i \geqslant 0} \Sigma^i\mathbf{P}$$

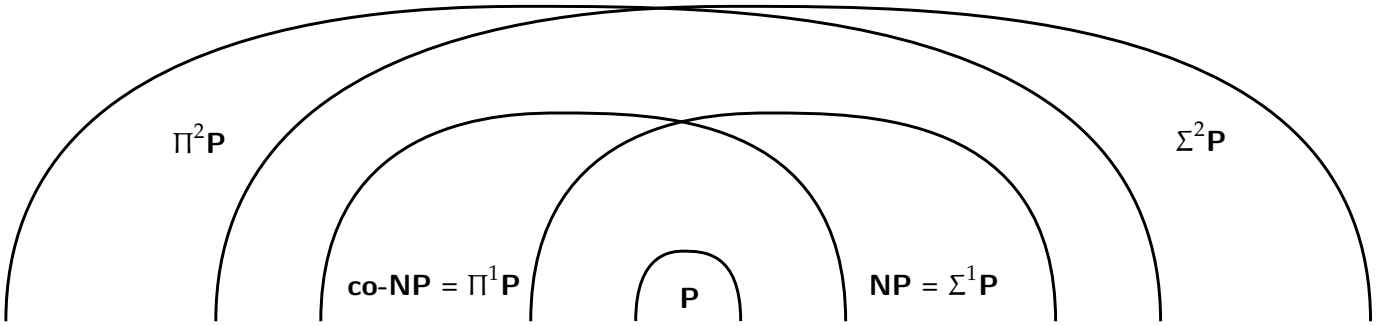


Figure 1.3: Полиномиальная иерархия

Лемма 1. $\mathbf{NP}^{\Pi^i\mathbf{P}} = \mathbf{NP}^{\Sigma^i\mathbf{P}}$

□ Пусть есть машина M с оракулом A. Рассмотрим оракул $\overline{A}$ и построим машину M', чтобы $M'^{\overline{A}}$ вела себя аналогично M^A. Для этого просто M' будет переворачивать любой ответ, полученный от оракула, все остальные действия повторяем за M.

Теперь докажем по индукции утверждение леммы, база очевидна. Переход такой: можно поменять оракула $\Pi^i\mathbf{P}$ на оракула $\overline{\Pi^i\mathbf{P}} = \mathbf{NP}^{\Sigma^{i-1}\mathbf{P}} = \mathbf{NP}^{\Pi^{i-1}\mathbf{P}} = \Sigma^i\mathbf{P}$. ■

Теорема 1.6.1. $L \in \Sigma^k\mathbf{P}$, согда[a] существует полиномиально ограниченное отношение $R \in \Pi^{k-1}\mathbf{P}$ такое, что для всех x :

$$x \in L \iff \exists y\colon R(x,y).$$

[a] тогда и только тогда, когда

□

⇒ Докажем по индукции.

- **База:** по определению $\Sigma^1\mathbf{P} = \mathbf{NP}^{\mathbf{P}} = \mathbf{NP}$.
- **Переход:** $k-1 \to k$. Пусть $L = L(M^O)$, где M — полиномиальная НМТ, $O \in \Sigma^{k-1}\mathbf{P}$.
  По предположению индукции для O существует полиномиально ограниченное $S \in \Pi^{k-2}\mathbf{P}$ такое, что $\forall q\colon q \in O \iff \exists w\colon S(q,w)$.
  Сконструируем из этого R:
  - $R(x,y) = 1$, если y — принимающая ветвь вычисления M^O (то есть последовательность $0,1$ – идти налево или направо), при этом положительные ответы оракула должны быть снабжены сертификатами $w\colon S(q,w) = 1$.
    То есть все переходы, основанные на ответе оракула «да», должны дополнительно содержать «доказательство».
    Проверим, что это отношение из $\Pi^{k-1}\mathbf{P}$, и, что оно задает язык L.
  - $R \in \Pi^{k-1}\mathbf{P}$: детерминировано проверяем корректность y, а далее проверяем, что ответы оракула были верными.
    Для ответов «нет» нужно проверить, что O для него равно нулю (запускаем $\Pi^{k-1}\mathbf{P}$ вычисление), а для ответов «да» — что S равно 1, то есть проверить сертификат ($\Pi^{k-2}\mathbf{P}$ вычисление).
    Нужно, чтобы все $\Pi^{k-1}\mathbf{P}$ и $\Pi^{k-2}\mathbf{P}$ (это частный случай $k-1$) вычисления вернули «да».
    Для этого построим схему: присоединим к большой конъюнкции все вычисления, чтобы ответ был положительным, нужно, чтобы все ветки $\Pi^{k-1}\mathbf{P}$ (то есть **co-NP**) вернули одно и то же, при этом мы остаемся в $\Pi^k\mathbf{P}$.

Для машины M существует принимающее вычисление и оно может быть дано в качестве y.
Наоборот, если у нас есть корректное вычисление машины M, то оно и будет принадлежать L.

$\boxed{\Leftarrow}$ Пусть у нас есть отношение R. Возьмем машину с оракулом R.
Она будет недетерминировано выбирать y и проверять, то есть спрашивать у оракула, $R(x, y)$.
Эта машина и будет распознавать наш язык L.

■

Аналогично можно доказать следующую теорему

Теорема 1.6.2. $L \in \Pi^k\mathbf{P}$, согда существует полиномиально ограниченное отношение $R \in \Sigma^{k-1}\mathbf{P}$ такое, что для всех x :

$$x \in L \iff \forall y\colon R(x, y).$$

Следствие 2. $L \in \Sigma^k\mathbf{P}$, согда существует полиномиально ограниченное отношение $R \in \mathbf{P}$ такое, что для всех x:

$$x \in L \iff \exists y_1 \forall y_2 \exists y_3 \ldots R(x, y_1, y_2, \ldots y_k).$$

Следствие 3. $L \in \Pi^k\mathbf{P}$, согда существует полиномиально ограниченное отношение $R \in \mathbf{P}$ такое, что для всех x:

$$x \in L \iff \forall y_1 \exists y_2 \forall y_3 \ldots R(x, y_1, y_2, \ldots y_k).$$

Лекция 4: †

26 nov

1.7 $\Sigma^k\mathbf{P}$-полная задача

Определение 25: Язык $\mathtt{QBF}_k$

Язык $\mathtt{QBF}_k$ — язык, состоящий из замкнутых истинных формул вида

$$\exists X_1 \forall X_2 \exists X_3 \ldots X_k \varphi,$$

где φ — формула в КНФ или ДНФ, а $\{X_i\}_{i=1}^k$ — разбиение множества переменных этой формулы на непустые подмножества.

Теорема 1.7.1. $\mathtt{QBF}_k$ — $\Sigma^k\mathbf{P}$-полный язык.

□

- Во-первых, проверим принадлежность.

  По следствию из прошлой теоремы достаточно найти полиномиально ограниченное отношение $R \in \mathbf{P}$ такое, что $\forall x\colon x \in \mathtt{QBF}_k \iff \exists y_1 \forall y_2 \exists y_3 \ldots R(x, y_1, y_2, y_3, \ldots)$.

  Возьмем просто R, которое для R(формула с $\varphi, x_1, x_2, \ldots$) выдает результат подстановки x_i в φ.

  Проверка будет работать за полином, то есть $R \in \mathbf{P}$.

- Докажем, что к этой задаче сводится любой язык из $\Sigma^k\mathbf{P}$.

  Пусть есть язык $L \in \Sigma^k\mathbf{P}$. Тогда существует полиномиально ограниченное отношение $R \in \mathbf{P}$:

  $$\forall x\colon x \in L \iff \exists y_1 \forall y_2 \exists y_3 \ldots R(x, y_1, y_2, \ldots).$$

– Если в конце формулы идет квантор $\exists$, то запишем язык R в таком виде (как в теореме Кука-Левина):

$$R(z) \iff \exists w \Phi(z, w).$$

Тогда определение языка будет иметь следующий вид:

$$\forall x\colon x \in L \iff \exists y_1 \forall y_2 \exists y_3 \dots \exists y_k \exists w \Phi(x, y_1, y_2, \dots, y_k, w).$$

Но так как последние два квантора можно объединить в один, получаем формулу из $\texttt{QBF}_k$.

– Иначе запишем $\overline{R}$ в виде булевой формулы Ψ, как в теореме Кука-Левина:

$$\overline{R}(z) \iff \exists w \Psi(z, w).$$

Тогда определение языка будет иметь следующий вид:

$$\forall x\colon x \in L \iff \exists y_1 \forall y_2 \exists y_3 \dots \forall y_k \forall w \overline{\Psi}(x, y_1, y_2, \dots, y_k, w).$$

Аналогично можно объединить последние два квантора.

■

Следствие 4. Если в определении $\texttt{QBF}_k$ заменить кванторы существования на кванторы всеобщности и наоборот, то получится $\Pi^k\mathbf{P}$-полный язык.

1.7.1 Коллапс полиномиальной иерархии

Теорема 1.7.2. Если $\Sigma^k\mathbf{P} = \Pi^k\mathbf{P}$, то $\mathbf{PH} = \Sigma^k\mathbf{P}$.

□ Достаточно показать, что следующий уровень равен текущему: $\Sigma^{k+1}\mathbf{P} = \Pi^k\mathbf{P}$.

Пусть $L \in \Sigma^{k+1}\mathbf{P}$, то есть $L = \{x \mid \exists y\colon R(x, y)\}$ для $R \in \Pi^k\mathbf{P} = \Sigma^k\mathbf{P}$.

Тогда существует $S \in \Pi^{k-1}\mathbf{P}$ такое, что

$$R(x, y) \iff \exists z\colon S(x, y, z).$$

После подстановки получаем

$$x \in L \iff \underbrace{\exists y \exists z}_{\exists t}\colon \underbrace{S(x, y, z)}_{S(x,t)}.$$

То есть $L \in \Sigma^k\mathbf{P}$.

Замечание. Доказали про следующие Σ классы, но из этого следует и, что Π классы тоже будут совпадать.

■

Следствие 5. Если существует $\mathbf{PH}$-полная задача, полиномиальная иерархия коллапсирует (конечна).

□ Полный язык лежит в каком-то конкретном $\Sigma^k\mathbf{P}$ (потому что $\mathbf{PH}$ есть их объединение), при этом все остальные к нему сводятся, следовательно, они тоже лежат в $\Sigma^k\mathbf{P}$. ■

1.8 Классы, ограниченные по времени и памяти

Определение 26: DSpace

$$\mathbf{DSpace}[f(n)] = \{L \mid L \text{ принимается ДМТ с памятью } \mathcal{O}(f(n))\},$$

где $f(n)$ должна быть неубывающей и вычислимой с памятью $\mathcal{O}(f(n))$ (на входе 1^n, на выходе двоичное

представление $f(n))$[a].

$$\mathbf{PSPACE} = \bigcup_{k \geqslant 0} \mathbf{DSpace}[n^k].$$

[a]Это определение конструируемой по памяти функции

1.8.1 PSPACE-полная задача

Определение 27: Язык QBF

Язык QBF — язык, состоящий из замкнутых истинных формул вида

$$q_1 x_1 q_2 x_2 \ldots \varphi,$$

где φ — формула в КНФ, $q_i \in \{\forall, \exists\}$.

Теорема 1.8.1. Язык QBF **PSPACE**-полон.

□

- QBF $\in$ **PSPACE**. Рассмотрим дерево перебора всех значений переменных. Когда мы дойдем до листа этого дерева и подставим значения переменных с ветки, получим значение функции. Значение

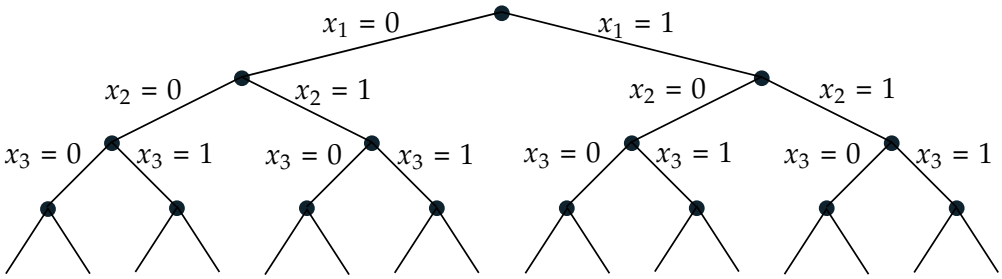


Figure 1.4: Дерево перебора

булевой формулы можем вычислить поиском в глубину.

Для этого понадобится память равная глубине дерева, то есть пропорциональная количеству кванторов, еще нужна память для вычисления значения φ, для этого тоже вполне хватит полинома.

- Сведем $L \in$ **PSPACE** к QBF. Для языка L есть МТ.

  Модифицируем ее немного: если у нее было много принимающих состояний, например, из-за каких-то рабочих данных на других лентах, будем перед переходом в принимающее состояние очищать все, кроме q_{acc}.

  Теперь построим граф, где конфигурации будут вершинами, а ребро между конфигурациями будет означать, что из одной можно получить другую.

  Так как МТ детерминированная, выходить будет ровно одно ребро (кроме конечной).

  Поскольку память полиномиальна, всего вершин будет $2^{p(n)}$, где $p(n)$ — некоторый полином.

  Длина пути точно не более $2^{p(n)} + 1$, либо он зацикливается.

  Запишем теперь это в формулу. Пусть

$$\varphi_i(c_1, c_2) = \text{существует путь из } c_1 \text{ в } c_2 \text{ длины } \leqslant 2^i.$$

Возьмем вершину d посередине пути $c_1 \to c_2$. Заметим, что можно записать так

$$\varphi_i(c_1, c_2) = \exists d\ \forall x \forall y\colon \big((x = c_1 \wedge y = d) \vee (x = d \wedge y = c_2)\big) \Longrightarrow \varphi_{i-1}(x, y).$$

Формула, которую мы будем получать рекурсивно подставляя в $\varphi_{p(n)}(q_0, q_{acc})$, будет иметь длину $p^2(n)$ (всего шагов $p(n)$, на каждом записываем вектора длины $p(n)$), то есть полином.

$$\varphi_0(c_1, c_2) = \text{можно ли из первого состояния за один шаг получить второе.}$$

Так мы получили формулу из `QBF`.

Замечание. После построения формулы нужно будет привести ее к нужному виду, а именно, перенести кванторы в начало, перевести формулы в КНФ.

■

Следствие 6. Если **PH** = **PSPACE**, то **PH** коллапсирует.

1.8.2 Иерархия по памяти

Полезная ссылка: Статья Охотина

Теорема 1.8.2 (Об иерархии по памяти)**.** **DSpace**$[s(n)] \neq$ **DSpace**$[S(n)]$, где $s(n) = o(S(n))$ и для всех $n > n_0$: $S(n) \geqslant \log n$.

□ Рассмотрим следующий язык:

$$L = \left\{ x = M01^k \;\middle|\; \begin{array}{l} k \in \mathbb{N} \cup \{0\}, \\ |M| < S(|x|), \\ M \text{ отвергает } x \text{ с памятью } \leqslant S(|x|) \end{array} \right\}.$$

Заметим, что $L \in$ **DSpace**$[S(n)]$, так как можем промоделировать работу на универсальной машине Тьюринга, а памяти дополнительной она почти не использует.

Докажем, что $L \notin$ **DSpace**$[s(n)]$. Пусть M_* распознает L с памятью $s_*(|x|) = \mathcal{O}(s(|x|))$.

Выберем N_1 таким, что $\forall n > N_1$: $s_*(n) < S(n)$.

Еще найдем такое $N_* > \max(N_1, 2^{|M_*|})$.

Теперь посмотрим как себя ведет M_*. Пусть $x = M_*01^{N_* - |M_*| - 1}$.

Заметим, что M_* использует не более $s_*(|x|) < S(|x|)$ памяти. Кроме этого по построению $|x| = N_*$.

- Если $M_*(x) = 0$, третье условие выполнено, первое тоже. Пусть второе условие не выполнено. Тогда: $N_* > 2^{|M_*|} \geqslant 2^{S(|x|)} \geqslant |x| = N_*$, так как $S(n) \geqslant \log n$. Противоречие.
- Если $M_*(x) = 1$, то не выполняется третье условия языка L.

Противоречие. Получили, что **DSpace**$[s(n)] \subsetneq$ **DSpace**$[S(n)]$. ■

1.8.3 Если памяти совсем мало...

Две теоремы без доказательств для общего развития.

Теорема 1.8.3. **DSpace**$[\log \log n] \neq$ **DSpace**$[\mathcal{O}(1)]$

Теорема 1.8.4. $\mathbf{DSpace}[(\log\log n)^{1-\varepsilon}] = \mathbf{DSpace}[\mathcal{O}(1)]$

1.8.4 Иерархия по времени

Теорема 1.8.5 (Об иерархии по времени)**.** $\mathbf{DTime}[t(n)] \neq \mathbf{DTime}[T(n)]$, где $t(n)\log t(n) = o(T(n))$, $T(n) = \Omega(n)$.

□ Аналогично ситуации с памятью рассмотрим следующий язык:

$$L = \left\{ x = M01^k \;\middle|\; \begin{array}{l} k \in \mathbb{N} \cup \{0\}, \\ |M| < T(|x|), \\ M \text{ отвергает } x \text{ за время } \leqslant \dfrac{T(|x|)}{\log T(|x|)} \end{array} \right\}.$$

Также за счет универсальной МТ получаем принадлежность $\mathbf{DTime}[T(|x|)]$ (именно из-за этого нам нужен логарифм), она $f(n)$ шагов произвольной МТ моделирует за $\mathcal{O}(f(n)\log f(n))$ шагов.

Остальное полностью аналогично иерархии по памяти. ■

$$\mathbf{P} \subseteq \mathbf{NP} \subseteq \ldots \subseteq \mathbf{PSPACE} \subseteq \mathbf{EXP} = \bigcup_{k\geqslant 0} \mathbf{DTime}[2^{n^k}].$$

Про $\mathbf{P}$ и $\mathbf{EXP}$ мы знаем (по теореме об иерархии по времени), что есть неравенство. Следовательно, в каком-то из этих включений тоже должно быть строгое, но пока не известно какое.

1.9 Полиномиальные схемы

Определение 28: Size

$L \in \mathbf{Size}[f(n)]$, если существует семейство булевых схем $\{C_n\}_{n\in\mathbb{N}}$ такое, что

- $\forall n\colon |C_n| \leqslant f(n)$;
- $\forall x\colon x \in L \iff C_{|x|}(x) = 1$.

Определение 29: Полиномиальные схемы

$$\mathbf{P/poly} = \bigcup_{k\in\mathbb{N}} \mathbf{Size}[n^k].$$

Утверждение. $\mathbf{P} \subsetneq \mathbf{P/poly}$.

□ Включение очевидно: любой ДМТ соответствует схема (этажи и всё такое, как мы делали раньше). Почему нет равенства точно? Например, $L = \{1^n \mid n$ — номер останавливающейся МТ, $M_n(M_n) = 1\}$. $L \notin \mathbf{P}$, но легко вычисляется схемами

$$C_n(x) = \begin{cases} 0, & 1^n \notin L \\ 0, & x \neq 1^n \\ 1, & 1^n \in L \end{cases}$$

■

Определение 30: Альтернативное определение P/poly

$L \in \mathbf{P/poly}$, если имеются $R \in \mathbf{P}$ и последовательность строк (подсказок) $\{y_n\}_{n\in\mathbb{N}}$ полиномиальной

длины (по одной, для каждой длины входа) таких, что

$$\forall x\colon x \in L \iff R(x, y_{|x|}) = 1.$$

Замечание (связь определений).

$\boxed{1 \Longrightarrow 2}$ $\{C_n\}$ — подсказки, $R(x, C_{|x|}) = C_{|x|}(x)$.
$\boxed{2 \Longrightarrow 1}$ Берем R, строим $C_n = C'_n(\dots, y_n)$ — подставили y_n (можем по Куку-Левину).

Лекция 5: †

3 dec

Теорема 1.9.1 (Карп-Липтон). $\mathbf{NP} \subseteq \mathbf{P/poly} \Longrightarrow \mathbf{PH} = \Sigma^2\mathbf{P}$.

▢ Покажем, что $\Sigma^3\mathbf{P}$-полный язык лежит в $\Sigma^2\mathbf{P}$. Тогда все следующие классы тоже схлопываются. Мы знаем $\Sigma^3\mathbf{P}$-полный язык

$$\mathtt{QBF}_3 = \{F \text{ — формула в КНФ} \mid \exists x \forall y \exists z\, F(x, y, z)\}.$$

Докажем, что он лежит в $\Sigma^2\mathbf{P}$.

Заметим, что корректность некоторой схемы $G \in \mathtt{SAT}$ можно проверить так: сначала подставим в первую переменную 0, а потом 1 и проверим полученные схемы. Исходная корректна, согда хотя бы одна из полученных корректна.

Можно записать это так:

$$\forall G\colon C_{|G|} = C_{|G[x_1 := 0]|}\left(G[x_1 := 0]\right) \vee C_{|G[x_1 := 1]|}\left(G[x_1 := 1]\right).$$

Хотим доказать, что $\mathtt{QBF}_3$ можно уложить в два квантора. Сделаем это следующим образом:

$$\begin{aligned}\left(\exists x \forall y \exists z\, F\right) \in \mathtt{QBF}_3 \iff\ & \exists \text{ схемы } C_1, \dots C_{|F|} \text{ размера, ограниченного полиномом} \\ & \exists x \\ & \forall y \\ & \forall G \text{ — булева формула длина не более } |F| \\ & (\text{семейство } \{C_i\} \text{ корректно для } G) \wedge C_{|F|}(F(x, y, z)) = 1\end{aligned}$$

Такая запись принадлежит $\Sigma^2\mathbf{P}$.

Замечание. $\mathbf{NP} \subseteq \mathbf{P/poly}$ используем, когда проверяем схему из $\mathtt{SAT}$ за полином.

■

1.9.1 Схемы фиксированного полиномиального размера

Теорема 1.9.2. $\forall k\colon \Sigma^4\mathbf{P} \notin \mathbf{Size}[n^k]$

▢ Заметим, что существует функция $f\colon \{0,1\}^n \to \{0,1\}$, зависящая только от первых $c \cdot k \cdot \log n$ битов, для которой нет булевой схемы размера n^k, так как всего функций с ограничением на биты $2^{2^{c \cdot k \cdot \log n}}$, а схем $\mathcal{O}(2^{n^k \log n})$ (для каждого из n^k гейтов нужно задать два числа, каждое задается $\log n^k = \mathcal{O}(\log n)$).

Найдем такую в $\Sigma^4\mathbf{P}$:

$$y \in L \iff \exists f\ \forall c\ (\text{схемы размера } n^k)\ \forall f'\ \exists x \exists c'\ (\text{схема размера } n^k)\ \forall x'\colon$$
$$\underbrace{f(x) \neq c(x)}_{\text{не принимается схемой}} \wedge \underbrace{\left((f < f') \vee f'(x') = c'(x')\right)}_{\text{лексикографически первая } f} \wedge \underbrace{\left(f(y) = 1\right)}_{\text{значение}}$$

Все кванторы имеют полиномиальные размеры. ■

Следствие 7. $\forall k\colon \Sigma^2\mathbf{P} \cap \Pi^2\mathbf{P} \not\subseteq \mathbf{Size}[n^k]$[a].

[a]Здесь берется пересечение, так как схемам все равно, выдавать 0 или 1

□ Пусть $\Sigma^2\mathbf{P} \cap \Pi^2\mathbf{P} \subseteq \mathbf{Size}[n^k]$. Тогда $\mathbf{NP} \subseteq \mathbf{P/poly}$, поэтому можно применить теорему Карпа-Липтона:

$$\mathbf{PH} = \Sigma^2\mathbf{P} \cap \Pi^2\mathbf{P} \subseteq \mathbf{Size}[n^k].$$

Но $\Sigma^4\mathbf{P} \subseteq \mathbf{PH} \subseteq \mathbf{Size}[n^k]$. Противоречие. ■

1.9.2 Класс NSpace

Определение 31: NSpace

$\mathbf{NSpace}[f(n)] = \{L \mid L$ принимается НМТ с памятью $\mathcal{O}(f(n))\}$.

Замечание.

- $f(n)$ должна быть конструируемая по памяти;
- входная лента read-only, выходная лента write-only, память на них не учитывается;
- **ленту подсказки** можно читать только слева направо.

$$\mathbf{NPSPACE} = \bigcup_{k\geqslant 0} \mathbf{NSpace}[n^k].$$

1.10 Логарифмическая память

Определение 32

$\texttt{STCON} = \{(G, s, t) \mid G$ — ориентированный граф, $\exists\, s \rightsquigarrow t\}$.

Лемма 2. $\texttt{STCON} \in \mathbf{DSpace}[\log^2 n]$.

□ Будем делить путь пополам и искать путь от начала до середины и от середины до конца.

Пусть $\mathrm{PATH}(x, y, i)$ равно 1, если есть путь из x в y длины не более 2^i.

$$\begin{aligned}
\mathrm{PATH}(x, y, 0) &= (x, y) \in E \\
\mathrm{PATH}(x, x, 1) &= 1 \\
\mathrm{PATH}(x, y, i) &= \bigvee_z \big(\mathrm{PATH}(x, z, i-1) \wedge \mathrm{PATH}(z, y, i-1)\big)
\end{aligned}$$

Перебираем промежуточную вершину. Будем хранить «задания» (пары, для которых проверяем путь, и еще логарифм длины пути) в стеке. Достаем оттуда одно «задание» и заменяем его на два меньших. Когда-то мы либо найдем 1, тогда нужно вернуться к проверке второй половины, либо 0, тогда нужно перейти к следующей промежуточной вершине, так как с текущей пути нет.

Чтобы получить ответ, посчитаем $\mathrm{PATH}(s, t, \log|V|)$.

Оценим память: на счетчик промежуточных вершин и на элемент стека нужен логарифм, максимальная глубина стека тоже $\log n$. Тогда всего не более $\log^2 n$. ■

Теорема 1.10.1. $\mathbf{NSpace}[f(n)] \subseteq \mathbf{DSpace}[f^2(n)]$ для $f(n) = \Omega(\log n)$.

□ Пусть язык $L \in \mathbf{NSpace}[f(n)]$. Это значит, что есть НМТ , которая принимает его с памятью $\mathcal{O}(f(n))$. Построим детерминированный алгоритм, который выполнит ту же работу за $\mathcal{O}(f^2(n))$.

Построим граф псеводоконфигураций: вершина — состояние, содержимое *рабочих* лент и положение *всех* головок.

Всего памяти для хранения псевдоконфигураций требуется $2^{f(n)\cdot k}$ памяти: всего состояний конечное число, положение занимает $\log n$, остается содержимое.

Считаем, что у нас только одно принимающее состояние.

Заметим, что граф нам нужен, когда хотим выяснить достижимость за один шаг.

Делаем такой же стек, как и выше, на него уходит порядка $f(n)$ памяти (на каждую «задачу» три числа: начало, конец и длина).

Теперь посмотрим на «задачу» $(z, t, 0)$, до которой мы в какой-то момент дошли. Мы хотим выяснить, есть ли переход из z в t, но явного графа у нас нет. Для этого сравниваем конфигурации посимвольно, кроме состояния (и, возможно, текущего символа).

Вспоминаем, что наша задача — проверить, что НМТ M принимает данный вход.

Поэтому для сравнения z и t осталось посмотреть табличку перехода M (константного размера) и на текущий символ на входной ленте (его индекс хранится вместе с рабочими индексами) и понять, можно ли из z получить t.

Так как один стек занимает $\mathcal{O}(f(n))$ памяти, то для всей работы достаточно $\mathcal{O}(f^2(n))$.

Итого, мы построили нужный детерминированный алгоритм. ■

Следствие 8. $\mathbf{PSPACE} = \mathbf{NPSPACE}$

Определение 33: L и NL

Класс языков **L** — множество языков, разрешимых на детерминированной машине Тьюринга с использованием $\mathcal{O}(\log n)$ дополнительной памяти для входа длиной n.

Класс языков **NL** — множество языков, разрешимых на недетерминированной машине Тьюринга с использованием $\mathcal{O}(\log n)$ дополнительной памяти для входа длиной n.

Лемма 3. `STCON` является **NL**-полной (относительно logspace-сведений, то есть сводящая функция использует логарифмическую память).

□

- Принадлежность **NL**: храним только текущую вершину и угадываем следующее состояние, пока не дойдем до конца.
- Полнота: если есть задача из **NL**, то есть НМТ M, которая использует логарифмическую память.

  M принимает вход, если в дереве вычислений есть путь от стартовой вершины до принимающей:

  $$M(x) = 1 \iff start \rightsquigarrow accept.$$

  Поэтому функция сведения должна построить граф по машине Тьюринга для данного входа x.

■

Утверждение. Для неориентированного графа алгоритм гораздо сложнее: `USTCON` $\in$ **L** (Reingold, 2004).

Утверждение. Все задачи из **L** являются **L**-полными (относительно logspace сводимости).

1.11 Равномерные полиномиальные схемы

Определение 34

Семейство схем $\{C_n\}_{n\in\mathbb{N}}$ **равномерно**, если существует полиномиальный алгоритм A такой, что $A(1^n) = C_n$.

Лемма 4. Равномерные схемы задают класс **P**.

□ Полиномиальная МТ на входе x сначала запускает $A(|x|)$, потом запускает полученную схему $C(x)$.

Наоборот, пусть дана полиномиальная МТ, про вход мы знаем, что $|x| = n$, тогда можно нарисовать схему из состояний, которая будет работать как МТ. Каждый уровень можно породить алгоритмом, который будет их пересчитывать по функции перехода. ■

Определение 35

Семейство схем $\{C_n\}_{n\in\mathbb{N}}$ logspace-**равномерно**, если существует полиномиальный алгоритм A, использующий $\mathcal{O}(\log n)$ памяти, такой, что $A(1^n) = C_n$.

Глубина булевой схемы — время параллельного вычисления.

Определение 36: Nick's class

Класс $\mathbf{NC}^i = \left\{L \mid \text{для } L \text{ есть logspace-равномерные схемы глубины } \mathcal{O}(\log^i n)\right\}$.

Класс $\mathbf{NC} = \bigcup_i \mathbf{NC}^i \subseteq \mathbf{P}$.

Замечание. Еще есть класс $\mathbf{AC}^i$, который определяется аналогично $\mathbf{NC}^i$, только разрешает степень входа гейта больше двух.

Лемма 5. Композиция двух logspace-функций $f_2(f_1(x))$ принадлежит logspace.

□ Будем запускать[5] и f_1 и f_2. Храним счетчики позиций на лентах: для f_1 на выходе и для f_2 на входе.

Пусть f_2 нужен очередной бит входа с номером y_i. Запускаем f_1, как только ее счетчик достигает y_i, останавливаем f_1, продолжаем работу f_2.

Если f_2 требуется новый y_j (возможно $j < i$), то мы запускаем f_1 снова (с самого начала).

В итоге у нас хранится только вход для f_1 и индексы, а он не входит в рабочую память.

И так пока f_2 не закончит. Во время работы f_1, f_2 запущено только два экземпляра, поэтому память логарифмическая (для счетчиков – логарифм размера ленты).

Замечание. f_1 мы моделируем без выходной ленты, помним только последний символ.

■

Теорема 1.11.1. Если L — **P**-полный (относительно logspace-сводимости), то $L \in \mathbf{L} \iff \mathbf{P} = \mathbf{L}$.

□

- Докажем, что $L \in \mathbf{L} \Rightarrow \mathbf{P} = \mathbf{L}$. Если $L' \in \mathbf{P}$, то он сводится к L, так как второй **P**-полный. А L решается logspace-алгоритмом. Получили две функции, обе logspace, значит, по доказанной лемме их композиция тоже logspace, поэтому $L' \in \mathbf{L}$.

  С другой стороны, $\mathbf{L} \subset \mathbf{P}$, так как $L \in \mathbf{P}$ и L является **L**-полной.

- В обратную сторону. Пусть $\mathbf{P} = \mathbf{L}$, по условию L — **P**-полный, поэтому $L \in \mathbf{L} = \mathbf{P}$.

■

[5] считаем, что функции — МТ, которые принимают аргумент на входной ленте и возвращают результат на выходной

Лекция 6: †

10 dec

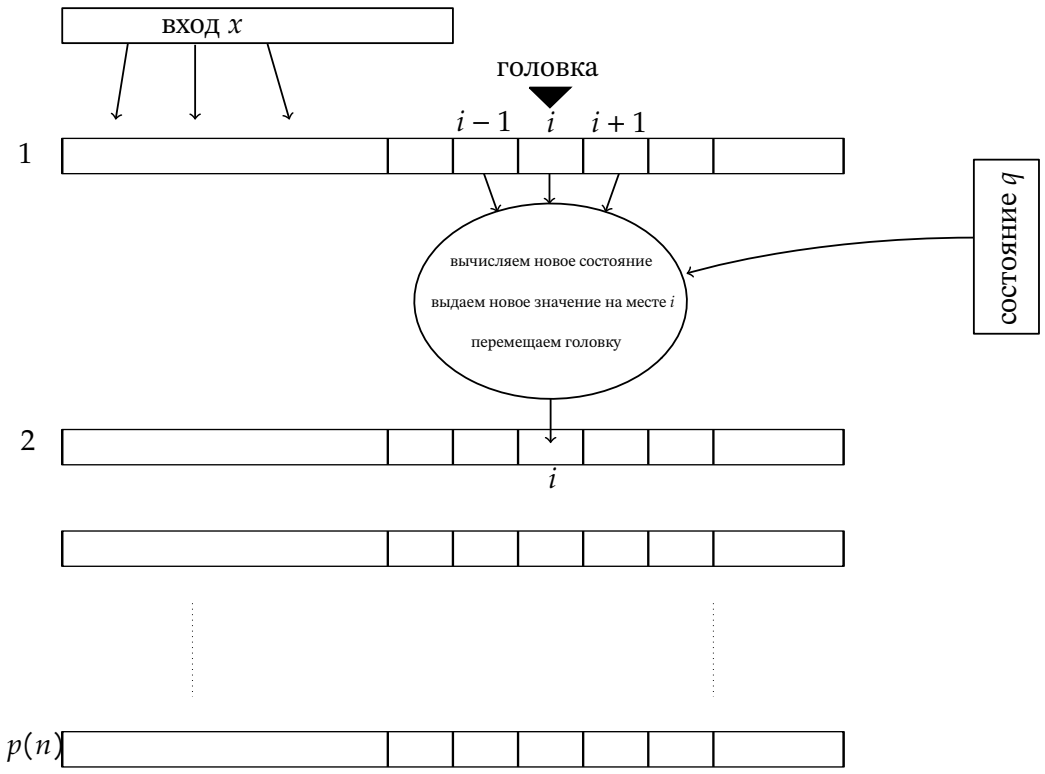


Figure 1.5: Построение схемы по ДМТ

Пример 1.11.1 (**P**-полный язык)**.** Приведем пример **P**-полного языка.

$$\texttt{CIRCUIT\_EVAL} = \{(\text{схема } C, \text{вход } x) \mid C(x) = 1\}.$$

Нам уже дан вход, остается только его проверить. Это легко и быстро сделать.

Докажем полноту. Вспомним, как строили схему по недетерминированной МТ в доказательстве теоремы Кука-Левина. Построим аналогично по детерминированной: каждый слой отвечает за состояние, переход к следующему – маленькие подсхемки, на вход только x.

Единственное, что нужно проверить — что нарисовать можно с логарифмической памятью.

Описание машины — константа. От x нам нужна только длина, чтобы узнать количество этажей.

На каждом уровне, чтобы построить следующий, нам нужно знать положение головки, три бита прошлой строки и состояние. Будем хранить t — номер уровня, i — положение головки, логарифма для этого хватит.

Теорема 1.11.2. $\mathbf{NC}^1 \subseteq \mathbf{L} \subseteq \mathbf{NL} \subseteq \mathbf{NC}^2$.

□

1. $\mathbf{NL} \subseteq \mathbf{NC}^2$. Начнем с последнего включения. У нас есть недетерминированная машина, которая использует логарифмическую память, хотим ее параллелизовать.

   Вспомним про граф псевдоконфигураций нашей детерминированной машины. Так как память логарифмическая, конфигураций полиномиальное число.

   Можем задать допустимые переходы НМТ матрицей смежности A ($k \times k$). Чтобы найти пути длины k (а больше нам не нужно), возведем булево в степень k.

   Это $\log k$ последовательных умножений: $A^2, (A^2)^2, \ldots$, причем каждое умножение пары булевых матриц вычисляется схемой глубины $\mathcal{O}(\log k)$.

Тогда общая глубина $\log^2 k$, из чего следует последнее включение.

2. $\mathbf{L} \subseteq \mathbf{NL}$. Среднее включение тривиально.

3. $\mathbf{NC}^1 \subseteq \mathbf{L}$. Докажем первое. Мы знаем, что logspace функции можно комбинировать и получится тоже logspace.

   Сейчас находимся в $\mathbf{NC}^1$, поэтому у нас есть семейство схем $\{C_n\}$, каждая вычисляется с логарифмической памятью.

   Построим композицию трех функций:

   - Первая функция вычисляет схему. Заметим, что эта схема будет логарифмической глубины (так как мы в $\mathbf{NC}^1$).
   - Докажем, что эту схему можно преобразовать в формулу тоже с логарифмической памятью.
     Пусть есть некоторая схема. Склонируем все гейты, которые используются два раза в следующих гейтах. Так как глубина логарифмическая, больше полинома вершин в полученном дереве не окажется. Научимся делать это формально с logspace. Запустим dfs от выхода схемы и

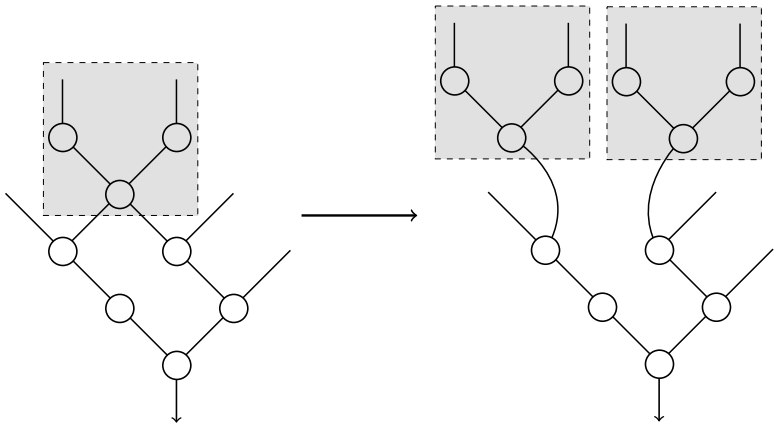


Figure 1.6: Схема → дерево

     будем записывать все пути. Заметим, что каждый путь представляет из себя как раз одну из полученных веток с клонированными уникальными гейтами.

     После построения одного пути, начинаем из корня, храним только текущую вершину. «Сам путь нам подскажет, где мы ходили налево, а где еще нет»[6].
   - Теперь вычисляем значение формулы на входе x. Аналогично запускаем dfs, храним текущую вершину и результаты в поддеревьях, когда обошли оба поддерева, поднимемся выше и передадим результат операции гейта.

■

Теорема 1.11.3. Если L — $\mathbf{P}$-полный, то все параллелизуется

$$L \in \mathbf{NC} \iff \mathbf{P} = \mathbf{NC}.$$

□ Если $L' \in \mathbf{P}$, его можно свести к L (logspace), а $L \in \mathbf{NC}$. То есть $\exists i\colon L \in \mathbf{NC}^i$.

Логарифмические вычисления мы умеем превращать в параллельные с $\log^2$, поэтому $L' \in \mathbf{NC}^{i+2}$. ■

[6] Тогда уж «сила подскажет», кажется, можно сделать так: храним еще одну примерно $\log n$-битную переменную, в которой i-й бит равен 1, если на i-ом уровне мы уже ходили в левое поддерево.

1.11.1 Замкнутость NSpace относительно дополнения

Теорема 1.11.4 (Immerman, Szelepcsényi). $\texttt{STCON} \in$ **co-NL**. Альтернативная формулировка $\overline{\texttt{STCON}} \in$ **NL**.

Хотим: недетерменированно с логарифмической памятью принимать те, где нет пути в орграфе

□ Придумаем такие подсказки, которые будут нас убеждать, что пути между s и t нет.

Пусть S_i — множество вершин на расстоянии не более i от s.

Сертификат того, что $x \in S_i$ — последовательность вершин от s до x.

Так как подсказки будут в недетерминированной подсказке, память занимать они не будут.

Теперь посмотрим на такой сертификат *непринадлежности* ($x \notin S_i$):

- все вершины S_i с сертификатами принадлежности,
- размер S_i[7]

Теперь нужно проверить все вершины из S_i, что ни одна из них не совпала с x, и, что их столько, сколько нужно.

Будем строить сертификат $|S_i|$ индуктивно так:

- $|S_{i-1}|$ мы знаем,
- переберем все u и проверим, что $u \in S_i$ так:
  - переберем все v (нам интересно, могли ли они быть предыдущими на пути), проверяя $(v, u) \in E$, и, если такое ребро есть, проверяем сертификат принадлежности (то есть путь) для $v \in S_{i-1}$,
  - в процессе проверки, подсчитываем количество правильных сертификатов, в итоге должно сойтись с $|S_{i-1}|$.

Теперь мы знаем общее число вершин из S_i.

Ответом будет $t \notin S_{|V|-1}$.

Замечание. Что мы храним? Храним номера вершин и счетчики, поддерживаем простые арифметические операции. Еще нужно хранить обращение к входу (несколько счетчиков для поиска ребер), считаем, что граф записан в нормальном виде, например, как перечисление ребер или матрица смежности.

■

Следствие 9. Если $s(n) = \Omega(\log n)$, то **NSpace**$[s(n)]$ = **coNSpace**$[s(n)]$.

□ Пусть есть МТ M для языка из **NSpace**$[s(n)]$. Тогда нас интересует достижимость в графе конфигураций из $2^{s(n)}$ состояний.

Только что мы научились проверять достижимость в классе **co-NL**, то есть доказывать недостижимость в классе **NL**.

$$\log 2^{s(n)} \approx s(n).$$

Поэтому теперь мы можем запустить алгоритм из прошлой теоремы, единственное, что нужно изменить — теперь не нужно читать граф с входной ленты, а нужно проверять смежность двух конфигураций. ■

Лекция 7: †

17 dec

1.12 Вероятностные вычисления

1.12.1 Классы с односторонней ошибкой

[7]Это тоже нужно сертифицировать и об этом будет написано ниже.

Определение 37: Класс RP

$L \in \mathbf{RP}$, если существует п.о.п.п. отношение R такое, что $\forall x \in \{0,1\}^*$:

$$x \notin L \implies \forall w\colon (x,w) \notin R$$
$$x \in L \implies \frac{|\{w \mid (x,w) \in R\}|}{|\{\text{все } w\}|} > \frac{1}{2}$$

Определение 38: Классы без ошибки

$\mathbf{ZPP} = \mathbf{RP} \cap \mathbf{co\text{-}RP}$.

Определение 39: Классы с двусторонней ошибкой

$L \in \mathbf{BPP}$, если существует п.о.п.п. отношение R такое, что $\forall x \in \{0,1\}^*$:

$$x \notin L \implies \frac{|\{w \mid (x,w) \in R\}|}{|\{\text{все } w\}|} < \frac{1}{3}$$
$$x \in L \implies \frac{|\{w \mid (x,w) \in R\}|}{|\{\text{все } w\}|} > \frac{2}{3}$$

Лемма 6. Пусть некоторый язык принадлежит **RP**. Запустим соответствующий алгоритм k раз. Тогда

$$\Pr[k \text{ неудач}] \leqslant \frac{1}{2^k}.$$

▢ Очевидно ■

Лемма 7. Пусть некоторый язык принадлежит **BPP**. Запустим соответствующий алгоритм k раз, вернем самый частый ответ. Тогда

$$\Pr[\text{ошибок более } \tfrac{k}{2}] \leqslant \frac{1}{2^{\Omega(k)}}.$$

▢

Утверждение (Неравенство Чернова, без доказательства)**.**

$$\Pr[X > (1+\varepsilon)pk] < \left(\frac{e^{\varepsilon}}{(1+\varepsilon)^{1+\varepsilon}}\right)^{pk} \leqslant e^{-\frac{pk\varepsilon^2}{4}},$$

где $X = \sum_{i=1}^{k} x_i$, x_i — независимые случайные величины, принимающие 1 с вероятностью p и 0 с вероятностью $1-p$.

В данной задаче x_i — наличие ошибки при i-ом вычислении, $p = \frac{1}{3}$, $\varepsilon = \frac{1}{2}$. ■

Определение 40: Альтернативное определение ZPP

ZPP — алгоритмы без ошибок с полиномиальным матожиданием времени работы.

▢

- Пусть есть два алгоритма: один **RP**, второй **co-RP**. Пока первый выдает 0, мы не уверены в ответе, и, пока второй выдает 1 мы не уверены.

  Когда-то один из них выдаст правильный ответ. Тогда матожидание равно

  $$\mathbb{E} = \mathcal{O}\left(\left(\tfrac{1}{2} + 2\cdot\tfrac{1}{4} + 3\cdot\tfrac{1}{8} + 4\cdot\tfrac{1}{16} + \ldots\right)t(n)\right) = \mathcal{O}(t(n)),$$

где $t(n)$ — время самого долгого из алгоритмов.

- Пусть есть алгоритм A, для которого $\mathbb{E}t_A(n) \leqslant p(n)$.

  Запустим его $k \cdot p(n)$ раз и прервем. Тогда вероятность неверного ответа по неравенству МАРКОВА, меньше $\frac{1}{k}$, а время на выполнения все еще полиномиально.

■

1.12.2 Связь с другими классами

Теорема 1.12.1. $\mathbf{BPP} \subset \mathbf{P/poly}$.

□

- Вероятностный алгоритм дополнительно получает случайную строку (подсказку)[8].

  Назовем ее *хорошей* подсказкой для входа x, если она приводит к правильному ответу, и *плохой* иначе.

  Давайте уменьшим ошибку до $\frac{1}{4^n}$.

- Хотелось бы найти хорошую строку для всех входов x. Входов длины n всего 2^n штук.

  Заметим, что $\frac{1}{4^n} \cdot 2^n < 1$, поэтому доля плохих строк для всех входов точно меньше единицы, поэтому есть хорошая для всех входов.

- Построим булеву схему по нашему алгоритму.

  BPP задается полиномиальным алгоритмом, у которого два аргумента: вход и случайная строка. Тогда это просто НМТ. По теореме Кука-Левина мы можем построить булеву схему, соответствующую НМТ. У этой схемы есть часть входов для x и часть для случайной строки w. Просто зашьем вместо

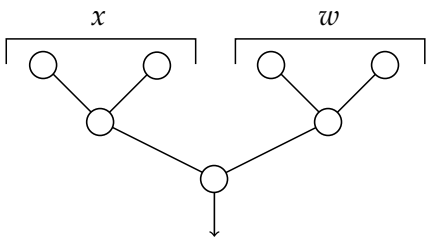


Figure 1.7: Булева схема для **BPP**

  w одну из хороших для всех входов строку.

■

Теорема 1.12.2. $\mathbf{BPP} \subseteq \Sigma^2\mathbf{P}$.

□ Пусть есть язык $R \in \mathbf{BPP}$. Пусть вероятность ошибки мы уже уменьшили до 2^{-n}.

$$A_x = \{w \in \{0,1\}^{p(n)} \mid R(x,w) = 1\}.$$

Построим формулу с двумя кванторами.

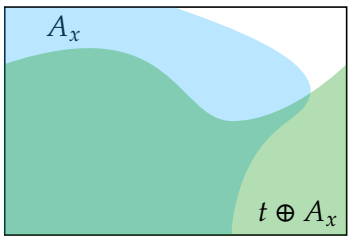
[8] Всегда можно считать, что ее длина не больше времени работы, так как дальше мы ее просто не прочитаем. Еще можно считать, что длины всех случайных срок равны.

- $x \in L$. Будем покрывать все возможные случаи строки $U = \{0,1\}^{p(n)}$ копиями A_x.

  Если мы покроем полиномиальным количеством копий, то получим следующее:

$$\exists \{t_i\}_{i=1}^{k} \; \forall r \in U \bigvee_{i=1}^{k} (r \in A_x \oplus t_i).$$

  После первого квантора полином битов, после второго тоже, поэтому, чтобы данная схема была из



$\{0,1\}^{p(n)}$

$t \oplus A_x = \{t \oplus w \mid w \in A_x\}$

Figure 1.8: Покрытие случайных строк

  $\Sigma^2\mathbf{P}$, нужно проверить, что все вычисления работают полином.

- $x \notin L$. В этом случае за полином A_x мы не покроем все U, так как их доля $\frac{1}{2^n}$.

Для первого случая осталось доказать, что, во-первых, можно найти полиномиальное множество $\{t_i\}$, а, во-вторых, вычисления можно провести за полиномиальное время.

1. Выберем случайно множество $\{t_i\}_i$ и убедимся, что вероятность полного покрытия больше нуля.

   Запишем вероятность того, что мы не покрыли все строки:

$$\Pr\left[\neg\left(\forall r \in U \bigvee_{i=1}^{k} (r \in A_x \oplus t_i)\right)\right] = \Pr\left[\exists r \in U \bigwedge_{i=1}^{k} (r \notin A_x \oplus t_i)\right] \leqslant$$

$$\leqslant \sum_{r \in U} \Pr\left[\bigwedge_{i=1}^{k} (r \notin A_x \oplus t_i)\right] \overset{\text{выбирали независимо}}{=} \sum_{r \in U} \prod_{i=1}^{k} \Pr[r \notin A_x \oplus t_i] \leqslant$$

$$\leqslant \frac{1}{2^{nk}} \cdot 2^{p(n)}$$

   Чтобы сделать $\frac{2^{p(n)}}{2^{nk}} < 1$, возьмем, например, $k = p(n)$.

2. Посчитать $\vee$ для k значений легко. Заметим, что

$$r \in A_x \oplus t_i \iff r \oplus t_i \in A_x.$$

   Чтобы выяснить последнее нужно запустить $R(x, r \oplus t_i)$, так как A_x — как раз строки, на которых R выдает единицу.

   R работает полином, следовательно, все вычисления будут работать тоже полином.

■

Замечание. Так как $\mathbf{BPP} = \mathbf{co\text{-}BPP}$, $\mathbf{BPP} \subseteq \Pi^2\mathbf{P}$, а тогда $\mathbf{BPP} \subseteq \Sigma^2\mathbf{P} \cap \Pi^2\mathbf{P}$.

1.13 Общая картина

Ничего не известно про связь **BPP** с **NP** и **co-NP**

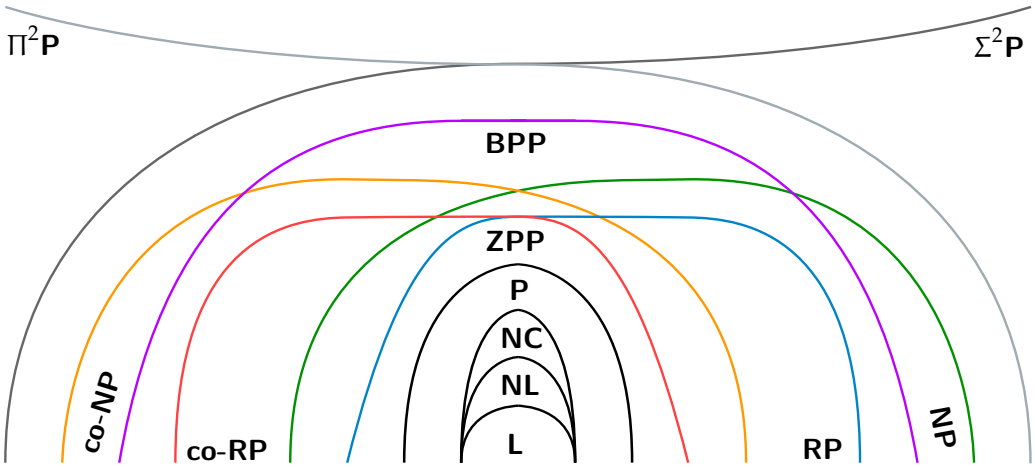


Figure 1.9: Общая картина иерархии

1.14 Квантовые вычисления

Недетерминированные МТ

Посмотрим на вычисления как на матрицы: $A(u,v) = 1 \iff u \overset{\text{шаг МТ}}{\longrightarrow} v$.

Заметим, что не любая матрица подойдет под описание МТ. Это объясняется тем, что при переходе от одной конфигурации меняется константное число битов и один символ на ленте. И поэтому много участков памяти остаются прежними.

Детерминированные МТ

Мы аналогично можем записать все в матрицу, но в каждой строке будет ровно одна единица ($\sum_j a_{ij} = 1$), так как мы точно должны знать, куда попадем на следующем шаге.

Текущее состояние можно записать как строку $x = (0, \dots 0, 1, 0, \dots 0)$, где 1 на i-ом месте говорит, что мы сейчас в i-ом состоянии.

Теперь мы можем умножать транспонированный вектор на матрицу и получать следующее состояние.

$$x \longmapsto xA \longmapsto xA^2 \longmapsto \dots.$$

Вероятностные МТ

С вероятностными МТ можно в матрице писать в возможных переходах писать вероятность $\frac{1}{2}$ (так как у нас случайные биты, всего два варианта развития событий).

Аналогично, $\sum_j a_{ij} = 1$. Такая матрица называется **стохастической**.

$$\delta(q,a,0) = (q', b, \rightarrow / \leftarrow)$$
$$\delta(q,a,1) = (q'', c, \rightarrow / \leftarrow)$$

Теперь можно думать о состоянии, как о «сумме состояний»: сумма произведений вероятности на прошлое состояние.

Квантовые МТ

Теперь в матрице записаны некоторые комплексные числа, которые называются **амплитудами**.

Матрица должна быть унитарной, $AA^* = A^*A = E$.

Наше текущее положение дел также записано в строку матрицы.

Смешанное состояние — линейная комбинация чистых конфигураций с амплитудами

$$\sum_i x_i \cdot s_i.$$

Вероятность — $|x_i|^2$, это примерно длина вектора.

Эволюция происходит аналогично, домножаем строку на матрицу. Эволюция происходит пока мы не захотим получить ответ.

Матрица все равно должна быть получена из МТ или другого устройства, мы не можем осуществлять какие-то нелогичные переходы, не понятна их реализация.

Преобразования тоже должны быть унитарными с небольшим числом бит.

О квантовых МТ можно думать, как о булевых схемах с маленькими унитарными преобразованиями.

Пример 1.14.1. Пусть таким переходом будет матрица 2×2, применяем к $(1, 0)$.

$$\begin{pmatrix} 1 & 0 \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}.$$

Результатом будет 1 с вероятностью $\frac{1}{2}$ и 0 с вероятностью $\frac{1}{2}$.

Если же применить дважды, так как матрица обратная к себе, получим только 0.

Определение 41

BQP — класс решаемых квантовым компьютером за полиномиальное время с ограниченной ошибкой.