Семинар 6.
Схемная сложность

Составил Р. Делла Пиетра

21.3.20

1 Определения

В этом разделе рассматриваем другую систему распознавания языков: булевы схемы.
Считается, что семейство схем $\{C_n\}$ распознают некоторый язык L, если $x \in L \iff C_{|x|}(x) = 1$,
то есть для каждой длины входного слова есть схема, которая распознаёт слова из языка данной длинны.
Понятия невычислимой схемы не существует, т.к. корректное описание схемы (ориентированный граф без циклов, переменные используются однажды, далее операции отрицания, конъюнкции и дизъюнкции) не допускает «неостанавливающейся» схемы.

$$SIZE(s(n)) = \{L \mid L \text{ распознаётся семейством схем } \{C_n\} : \ |C_n| = O(s(n))\}$$

$$\mathcal{P}/poly = \bigcup_{c \in \mathbb{N}} SIZE(n^c) \quad \text{(схемное определение)}$$

$$DTIME(t(n))/a(n) = \{L \mid L \text{ распознаётся за } O(t(|x|)) \text{ с подсказкой } a(|x|)\}$$

$$\mathcal{P}/poly = \{L \mid \exists R(\cdot,\cdot) \in \mathfrak{F}_p(|x|)\ \exists h(\cdot) : \ x \in L \iff R(x, h(|x|)) = 1\} \quad \text{(определение через подсказку)}$$

Сравним определение $\mathcal{P}/poly$ через подсказку и определение $\mathcal{NP}$:

$$\mathcal{NP} = \{L \mid \exists R(\cdot,\cdot) \in \mathfrak{F}_p(|x|) : \ x \in L \iff \exists y : R(x,y) = 1,\ |y| = poly(|x|)\}$$

Существенное различие состоит в y против $h(|x|)$.
y — полиномиальная по длине подсказка, может быть подобрана своя для каждого x.
$h(|x|)$ — некоторая абстрактная функция (может не быть вычислимой), подсказка одновременно для всех x фиксированной длины.

$$DEPTH(d(n)) = \{L \mid L \text{ распознаётся семейством схем } \{C_n\} : \ C_n \text{ глубины } O(d(n))\}$$

$\mathbf{NC}^d = DEPTH(\log^d n)$, у узлов с конъюнкциями и дизъюнкциями входная степень 2

$\mathbf{AC}^d = DEPTH(\log^d n)$, у узлов с конъюнкциями и дизъюнкциями входная степень любая

$$\mathbf{NC}^d \subseteq \mathbf{AC}^d \subseteq \mathbf{NC}^{d+1} \implies \mathbf{NC} = \bigcup_{d \in \mathbb{N}} \mathbf{NC}^d = \mathbf{AC}$$

2 Унарные языки

Покажем, что любой унарный язык $L_A = \{\underbrace{11\ldots1}_{n} \mid n \in A \subseteq \mathbb{N}\}$ лежит в $\mathcal{P}/poly$.

Воспользуемся определением через подсказку: $h(|x|) = |x| \in^? A$. Тогда предикату достаточно проверить, что x состоит из одних единиц и $h(|x|)$ верно.
Также можно воспользоваться схемным определением: если $n \notin A$, C_n выдаёт всегда отрицательный ответ, иначе C_n просто конъюнкция всех битов входа.
Таким образом, любой унарный язык лежит в $\mathcal{P}/poly$.
Возьмём $A = \{$номера машин Тьюринга, которые не останавливаются на пустом входе$\}$, тогда L_A неразрешим.
Как известно, любые языки из $\mathcal{P}$, $\mathcal{NP}$ и других классов, которые мы рассматривали, разрешимы, поэтому $\mathcal{P}/poly \neq \mathcal{P}, \mathcal{NP}$.

3 Задачи

3.1 Существуют ли функции, требующие схемы, размер которых растёт быстрее, чем $\frac{2^n}{10n}$?

Сделаем грубую оценку сверху, сколько различных функций определяют схемы размера $\frac{2^n}{10n}$. Для этого оценим, сколько памяти нам потребуется, чтобы описать схему такого размера. Каждая вершина требует не более двух номеров вершин — предков и два бита для описания типа: переменная, отрицание, конъюнкция или дизъюнкция. Если $\frac{2^n}{10n} = T(n)$, для каждой вершины понадобится $2\log T(n)+2$ бита, или грубо $3\log T(n)$, то есть вся схема кодируется не более $3T(n)\log T(n) = 3\frac{2^n}{10n}\log\left(\frac{2^n}{10n}\right) < 3\frac{2^n}{10n}\log 2^n = \frac{3}{10}2^n$. Всего различных функций, описываемых такими схемами, будет не более $2^{\frac{3}{10}2^n}$, в то время как всего булевых функций от n переменных 2^{2^n}, что асимптотически значительно больше, чем $2^{\frac{3}{10}2^n}$. Таким образом, такие функции существуют, потому что любую булеву функцию от n переменных можно представить в виде схемы.

3.2 $\mathbf{NC}^d \subseteq \mathbf{AC}^d \subseteq \mathbf{NC}^{d+1}$

Первая часть тривиальна, любая схема, лежащая в $\mathbf{NC}^d$, лежит в $\mathbf{AC}^d$ в том же виде.
$\mathbf{AC}^d \subseteq \mathbf{NC}^{d+1}$: это тоже легко понять, если вспомнить, что многопараметрическую конъюнкцию можно выразить через $O(\log n)$ двухпараметрических. Аналогично для дизъюнкций.

3.3 Как сложить два числа с помощью булевой схемы?

Для начала научимся складывать 2 бита: результат сложения двух бит a и b состоит также из двух бит, младший $a \oplus b = (a \wedge \overline{b}) \vee (b \wedge \overline{a})$, второй $a \wedge b$. Для этого несложно построить схему.
Теперь 3 бита a, b и c: ответ также состоит из двух бит, младший $a \oplus b \oplus c$, старший $(a \wedge b) \vee (b \wedge c) \vee (c \wedge a)$. В итоге для сложения двух чисел складываем младшие биты, получаем младший бит ответа и бит переноса, складываем вторые биты и перенос от первого и тд.

3.4 Равны ли $\mathbf{AC}^0$ и $\mathbf{NC}^0$?

Задача конъюнкции всех входов лежит в $\mathbf{AC}^0$, т.к. требует схему, состоящую из одной конъюнкции, но не в $\mathbf{NC}^0$, т.к. нельзя построить схему константной глубины, обрабатывающую вход произвольной длины, пользуясь только двухпараметрическими конъюнкциями и дизъюнкциями.

3.5 Равны ли $\mathbf{AC}^0$ и $\mathbf{NC}^1$?

Задача $PARITY = \{(x_0, \ldots, x_n) : \bigoplus_{i=1}^{n} x_i = 1\}$ лежит в $\mathbf{NC}^1$, т.к. требует $O(\log n)$ схем для $\oplus$.

Можно найти большое количество доказательств того, что $PARITY$ не лежит в $\mathbf{AC}^0$, вот одно из самых простых.