Def Булева схема — directed acyclic graph with n sources and one sink.

~~Все вершины~~ Все не истоки вершины называются гейтами и помечены символами $\vee, \wedge, \neg$.

$\neg$ - входит одно ребро

$\wedge, \vee$ - входят два ребра.

Для схемы C, выход $C(x)$ вычисляется естественным способом.

Def $T: \mathbb{N} \to \mathbb{N}$. $T(n)$ - size семейство схем ~~C~~ - это последовательность схем C_n, таких что $|C_n| \leq T(n)$.

Мы говорим, что $L \in Size[T(n)]$ если для L $\exists$ ~~...~~ семейство схем размера $T(n)$. таких что $\forall x \in \{0,1\}^n$ $x \in L$ iff $C(x) = 1$.

Example $\{1^n, n \in \mathbb{Z}\}$, $\{(m, n, n+m) \mid n, m \in \mathbb{N}\}$

~~Опред~~ Def $P_{/poly}$ - класс языков распознающихся с помощью полиномиальных схем.

т.е. $P_{/poly} = \bigcup_{c} Size(n^c)$

Теорема $P \subseteq P_{/poly}$.

Док-во Пусть $L \in P$ построим для L схему полином. размера.

$L \in P \Rightarrow \exists$ ~~oblivious~~ oblivious машина Тьюринга.

~~$x_1, x_2, \ldots x_n$ — вход~~

~~Закодируем вход~~

$x_1, x_2, \ldots x_n$ - вход

~~q_1 — то~~ q_1 - начальное состояние

~~$z_1 = f(q_1, x_1)$~~ $\boxtimes$

$(q_1, z_1) = f(q_{start}, x_1)$

$(q_2, z_2) = f(q_1, y_1)$

$(q_3, z_3) = f(q_2, y_2)$

$\vdots$

$(q_n, z_n) = f(q_{n-1}, y_{n-1})$

Output z_n $\boxtimes$

Утв. Если $L \subseteq \{0,1\}^*$ - унарный язык, то $L \in P_{/poly}$. $\{1^n / \ldots\}$

Док-во. Схема это или 0 или AND всего. $\boxtimes$

$UHALT = \{1^n \mid n$ кодирует $\langle M, x \rangle$ и M останавливается на $x\}$.

$\Rightarrow P_{/poly} \neq P$, т.е. $P \subsetneq P_{/poly}$.

Если показать, что $NP \not\subseteq P_{/poly} \Rightarrow NP \neq P$.

т.е. если для $L \in NP$ как-то экспон. ~~нижнюю~~ оценку на схему то $P \neq NP$!

Машины Тьюринга с советом.

<u>Определение</u>: $T, a : \mathbb{N} \to \mathbb{N}$. класс языков раздели~~мый~~ с помощью ~~T(n) машина~~ ~~маш~~ $T(n)$-time машиной Тьюринга, обозначается $DTime(T(n))/a(n)$ содержит все L, такие что $\exists$ последов.

$\{\alpha_n\}_{n=1}^{\infty}$, что

$$x \in L \text{ iff } M(x, \alpha_n) = 1$$

M - работает $T(n)$ времени.

<u>Пример</u> $\forall$ унарный язык можно решить с однобитной подсказкой.

<u>Теорема</u>

$$P/_{poly} = \bigcup_{c,d} DTime(n^c)/n^d.$$

<u>Док-во</u> $P/_{poly} \subseteq \bigcup DTime(n^c)/n^d$

$L \in P/_{poly}$, возьмем в качестве подсказки схему C и просто посчитаем $C(x)$ с помощью машины Тьюринга. ~~Т~~

Пусть $L \in DTime(n^c)/n^d \Rightarrow \exists$ МТ M ~~т.~~ ч.

$$x \in L \text{ iff } \underbrace{M(x, \alpha_{|x|})}_{} = 1$$

по пред. теореме для этого выражения существует схема, только с зависимостью от $\alpha_{|x|}$, но ~~они~~ $\alpha_{|x|}$ постоянно $\forall x$

$\Rightarrow$ можно просто зафиксировать эти данные и получим схему для L.

$P/poly$ и NP

$SAT \in P/poly$?

Теорема Если $NP \subseteq P/poly \Rightarrow PH = \Sigma_2^P$

Док-во Чтобы доказать $PH = \Sigma_2^P$, достаточно док-ть $\Pi_2^P \subseteq \Sigma_2^P$.

$\Rightarrow$ достаточно док-ть

$\Pi_2 SAT \in \Sigma_2^P$

$\exists$ такие φ, что:

~~$\forall u \, \exists v$~~ $\forall u \in \{0,1\}^n \; \exists v \in \{0,1\}^n \; \varphi(u, v) = 1$.

Если $NP \subseteq P/poly$, то $\exists$ ~~р схем~~ семейство C_n схем размера $p(n)$ таких, ~~что~~ $\forall \varphi$ и $\forall u$

$C_n(\varphi, u) = 1$ iff $\exists v$ т. ч. $\varphi(u, v) = 1$,

то есть схема ~~решает~~ отвечает вопрос принадлежности для задачи SAT. Знаем есть polynomial алгоритм для ~~вып~~ нахождения вып. набора если есть доступ к black boxy, говорящему на формула выполнима или нет. ~~Все По такому~~ По алгоритму можно построить схему, а оракульный доступ заменить на подсхему. $\Rightarrow \exists$ схема которая по SAT выдает вып. набор.

Верно ~~след~~ следующее.

$\exists w \in \{0,1\}^{10q(n)^2}$ $\forall u$: w - задает схему C' и

схема размера $q(n)$ $\qquad \varphi(u, C'(\varphi, u)) = 1$.

и все вычисления

можно проводить для полинома

(1) $\forall u \; \exists v \quad \varphi(u, v) = 1$

$\Updownarrow \qquad \Downarrow$ по построению

(2) $\exists w \; \forall u : \varphi(u, C'(\varphi, u)) = 1$

Если (1) неверно то $\exists u \; \forall v \quad \varphi(u, v) = 0$, то

и (2) неверно.

$\boxtimes$

<u>Теорема</u> Если $EXP \subseteq P_{/poly} \Rightarrow EXP = \Sigma_2^P$

<u>Без док-ва.</u>

Если $P = NP$, то $EXP \not\subseteq P_{/poly}$.

Предположим противное

$EXP \subseteq P_{/poly} \Rightarrow EXP = \Sigma_2^P$, но $P = NP \Rightarrow P = \Sigma_2^P$

$\Rightarrow P = EXP$ - противоречие.

Circuit lower bound

<u>Теорема</u> $\forall n > 1\ \exists f:\{0,1\}^n \to \{0,1\}$ не вычислимая схемой размера $\frac{2^n}{10n}$.

~~Док~~-во было на 1 курсе.

<u>Теорема о "иерархии"</u>

$\forall T, T': \mathbb{N} \to \mathbb{N}$ таких что $\frac{2^n}{n} > T'(n) > 10T(n) > n$

$$\mathrm{size}(T(n)) \subsetneq \mathrm{size}(T'(n))$$

<u>Док-во:</u> Диагонализация не работает кажется :(

Для иллюстрации докажем

$$\mathrm{size}(n) \subsetneq \mathrm{size}(n^2)$$

$f: \{0,1\}^\ell \to \{0,1\}$ и f - не вычислима за $\frac{2^\ell}{10\ell}$.

С другой стороны f выч. инф размера

$2^\ell \cdot 10\ell$. Возьмем $\ell = 1.1 \log n$, ~~тогда~~ и $g|_{\text{первые биты}} = f$

$g \in \mathrm{size}(2^\ell 10\ell) = \mathrm{size}(11 n^{1.1} \cdot \log n) \subseteq \mathrm{size}(n^2)$

$g \notin \mathrm{size}\left(\frac{2^\ell}{10\ell}\right) = \mathrm{size}\left(\frac{n^{1.1}}{11 \log n}\right) \supseteq \mathrm{size}(n)$

$\boxtimes$

Класс NC и класс AC

Def $L \in NC^d$ если L решается с помощью полином схем глубины $O(\log^d n)$.

$$NC = \bigcup_{i \geq 1} NC^i$$

Def AC^d — то же что и NC^d, только fan-in — unbounded.

Утв $NC^d \subseteq AC^d \subseteq NC^{d+1}$

$$\underbrace{NC^0 \subsetneq AC^0 \subsetneq NC^1}_{\text{без док-ва}}.$$