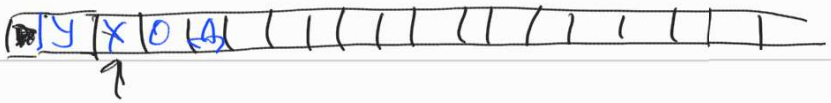
Вычисл. задачи
- время
- память

Нижние оценки
- Криптография
- глубокое изучение
- Нижние оценки
  }
  Верхние оценки
- Нижние оценки
  ⊆
  Аффтоматизация

Алгоритм

Машины Тьюринга 1930-е гг

Одноленточная Машина Тьюринга



конечное мн-во
Σ входной алфавит
$\Delta, \sqcup \notin \Sigma$

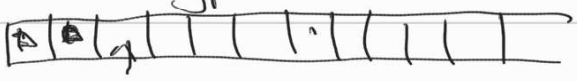
Q - мн-во состояний
q_0 - нач. сост.
q_f - финальное

$\delta : Q \times \Sigma \mapsto Q \times \Sigma \times \{\leftarrow, \cdot, \rightarrow\}$

$q_0 \to q_1$ $\quad (q_0, \Delta) \longmapsto (q_1, Y, \rightarrow)$
(q_1, Y)

$\begin{bmatrix} q_{yes} \\ q_{no} \end{bmatrix}$ - два фин. сост.

МТ, расп. проверяет битовое слово на палиндром.



$(q_0, 0) \longmapsto (q_2, \Delta, \rightarrow)$
$(q_0, 1) \longmapsto (q_3, \Delta, \rightarrow)$
$\left(\frac{q_2}{q_3}, \frac{0}{1}\right) \longmapsto \left(\frac{q_2}{q_3}, \frac{0}{1}, \rightarrow\right)$

$(q_4, 1) \to (q_{no}, \sqcup, \cdot)$
$(q_5, 0) \to$
$(q_4, 0) \to (q_6, \sqcup, \leftarrow)$
$(q_5, 1) \to$

$(q_2, \sqcup) \mapsto (q_4, \sqcup, \leftarrow)$

$(q_3, \sqcup) \mapsto (q_5, \sqcup, \leftarrow)$

$(q_0, \sqcup) \mapsto (q_{yes}, \sqcup, \cdot)$

$(q_6, \overline{1}) \to (q_6, \overline{1})$

$(q_6, \triangleright) \to (q_0, \triangleright, \to)$

$(q_4, \blacksquare) \to (q_{yes}, \triangleright, \cdot)$

$(q_5, \triangleright) \mapsto (q_{yes}, \triangleright, \cdot)$

$X \quad |X| = n$

$$n + (n-2) + (n-4) + (n-6) + \ldots = \Theta(n^2)$$

$$\frac{n^2}{C}$$

Теорема $\forall$ одноленточная МТ, кот. расп. бинарные цепочки $\exists\, C : \forall n \exists$ слово $x \in \{0,1\}^n$: $M(x)$ раб. $\geq Cn^2$ шагов.

Д-во

Принцип нескимаемости

$S: \{0,1\}^n \to \{0,1\}^*$ - инъекция

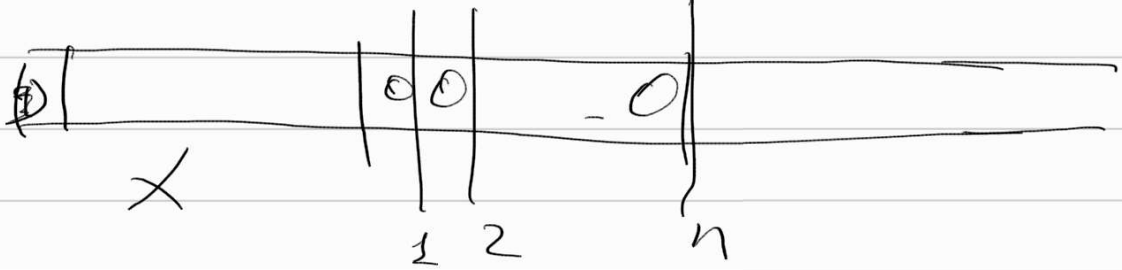
$\exists\, x \in \{0,1\}^n$: $|S(x)| \geq n$.

$2^n \qquad 2^n - 1$

$(+2^n + \ldots + 1)^{n-1}$

$|x| = n \qquad x \circ^n x^{rev} \qquad x \in \{0,1\}^n$

$T(x)$ время работы $M(x \circ^n x^{rev})$



- ∃ перегородка i : $M(x0^i x^{rev})$ головка пересекает i-ую перегородку $\leq \frac{T(x)}{n}$ раз

- $f: x \longmapsto (i, q_1, q_2, \dots, q_k)$

$k \leq \frac{T(x)}{n}$ посл-ть состояний, в которых головка пересек. перегор.

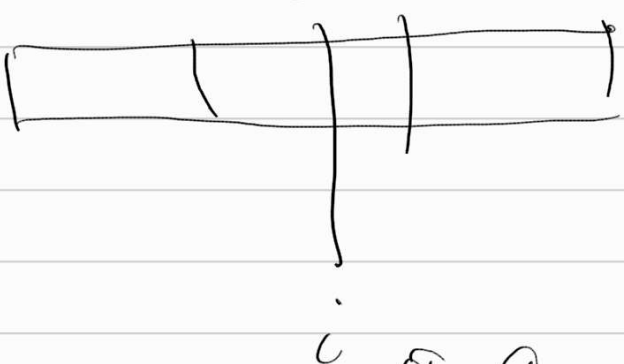
$x \longmapsto (i, q_1, q_2 \dots, q_k)$

$y \longmapsto (i, q_1, q_2, \dots, q_k)$

$x 0^n y^{rev}$ не пом-ся, если $x \neq y$

- $x 0^n x^{rev}$

$y 0^n y^{rev}$



$\exists x \in \{0,1\}^*$:

$$|f(x)| \geq n$$

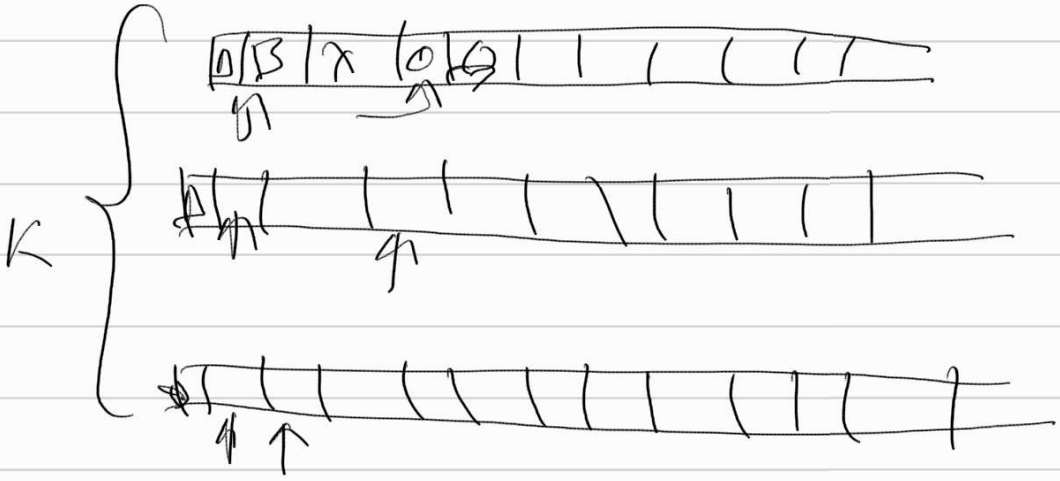
$$2\log n + C \cdot K + C_2$$

$$2\log n + C \cdot \frac{T(x)}{n} + C_2$$

$$T(x) \geq \frac{n(n - 2\log n - C_2)}{C}$$

$$= \Omega(n^2)$$

Многоленточная МТ



Q

$\delta : Q \times \Sigma \to Q \times \Sigma \times \{\leftarrow, \cdot, \rightarrow\}$

$O(n)$

Факт Класс. МТ. можно смоделир. на 1-лент. с квадратичным замедл.

$T(x)$ $O(T(x)^2)$

$T(x) \cdot T(x)$

---

k лент $T(n)$ — 2 ленты $O(T(n) \log T(n))$

$DTime[f(n)]$ — мн-во языков, кот можно распозн. на многолент. МТ за время $O(f(n))$

$f: \mathbb{N} \to \mathbb{N}$

$\Sigma = \{0, 1\}$ $\forall$ входа

$L \subseteq \Sigma^*$ x вр. [illegible]

на $x \le O(f(|x|))$

$$P = \bigcup_{c>0} DTime[n^c]$$

Булевы схемы

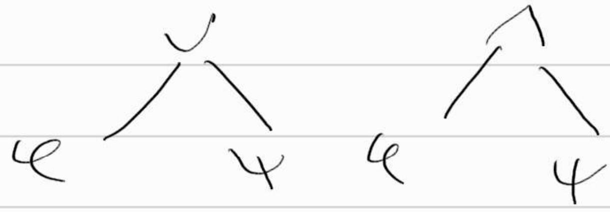
$f: \{0,1\}^n \to \{0,1\}$

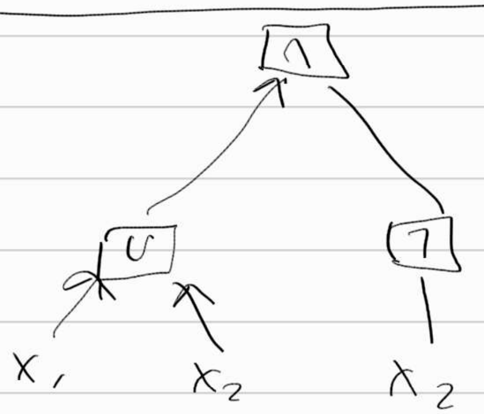
- т.и. 2^n
- формулами
- КНФ / ДНФ

$x_1, x_2, \ldots x_n$

$\vee, \wedge, \neg$

- пер. ф-ла
- φ $\neg\varphi$
- φ ψ





$(x_1 \vee x_2) \wedge (\neg x_2)$

КНФ $\underbrace{(x_1 \vee \bar{x}_2 \vee x_3 \vee x_4)}_{\text{дизъюнкт clause}} \wedge (x_1 \vee x_2) \wedge (\ldots)$

Булева схема

Размер схемы — число рёбер

$L \subseteq \{0,1\}^*$

$\{C_n\}_{n=1}^{\infty}$ – сем-во булевых схем C_i имеет i входов.

Опр. $\{C_n\}_{n=1}^{\infty}$ распознает язык $L \iff \forall x \in \{0,1\}^*$

$x \in L \iff C_{|x|}(x) = 1$

$Size[f(n)]$ – это кл-во таких языков L, для которых $\exists$ сем-во схем $\{C_n\}$, расп. этот язык и при этом $|C_n| \le f(n)$. $\forall n$

$$P/poly = \bigcup_{c>0} Size[n^c]$$