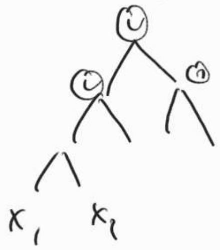
$f:\{0,1\}^n \to \{0,1\}$ $\qquad f: 2^{[n]} \to \{0,1\}$

$Th^n_k(S) = \begin{cases} 1, & |S| \geq k \\ 0, & \text{иначе} \end{cases}$

<u>Теорема</u> В $\forall$ монотонной ф-ле для Th^n_2 $\geq \lceil n \log n \rceil$ листьев



<u>Д-во</u>

Мера на вершинах ф-лы

$\begin{cases} \mu(\text{корень}) = \log n \\ \mu(\text{лист}) = 1/n \\ \mu(u) \leq \mu(v) + \mu(w) \end{cases}$

$f: 2^{[n]} \to \{0,1\}$ $\qquad (f)_i = \left\{ S \subseteq [n] \ \ |S| = i : \ \ f(S)=1 \atop \forall T \subsetneq S \ \ f(T)=0 \right\}$

$(f)_1$

$(f)_2$ – граф на $[n]$

$(f_u)_2 \subseteq (f_v)_2 \cup (f_w)_2$ $\qquad f_u = f_v \cup f_w$

$\ni S$

$(f_u)_2 \subseteq (f_v)_2 \cup (f_w)_2 \cup \big((f_v)_1 \setminus (f_w)_1\big) \times \big((f_w)_1 \setminus (f_v)_1\big)$

$\ni S = \{i, j\}$

$f_u = f_v \wedge f_w$

$(f_u)_2 \subseteq (f_v)_2 \cup (f_w)_2 \cup T_{v,w}$ $\qquad H(T_{v,w}) \leq 1$

Граф $T_{v,w}$ соед. верш. только из $(f_v)_1 \triangle (f_w)_1$

$H(T_{v,w}) \leq \dfrac{|(f_v)_1 \triangle (f_w)_1|}{n}$

$\mu(f) = H((f)_2) + \dfrac{|(f)_1|}{n}$

1) $\mu(Th^n_2) = \log n$

2) $\mu(x_i) = 1/n$

3) a) $f_u = f_v \cup f_w$ $\qquad (f_u)_2 \subseteq (f_v)_2 \cup (f_w)_2$

$$\mu(f_u) = H((f_u)_2) + \frac{|(f_u)_1|}{n} \le H((f_v)_2) + H((f_w)_2) + \frac{|(f_u)_1|}{n} \le H((f_v)_2) + H((f_w)_2) + \frac{|(f_v)_1|}{n} + \frac{|(f_w)_1|}{n} = \mu(f_v) + \mu(f_w)$$

$(f_u)_2 \subseteq (f_v)_2 \cup (f_w)_2 \cup T_{v,w}$

б) $f_u = f_v \wedge f_w$

$$\mu(f_u) = H((f_u)_2) + \frac{|(f_u)_1|}{n} \le H((f_v)_2) + H((f_w)_2) + \frac{|(f_v)_1 \Delta (f_w)_1|}{n} + \frac{|(f_v)_1 \cap (f_w)_1|}{n} \le H((f_v)_2) + H((f_w)_2) + \frac{|(f_v)_1|}{n} + \frac{|(f_w)_1|}{n} = \mu(f_v) + \mu(f_w).$$

Коды Уолша – Адамара

$WH: \{0,1\}^n \to \{0,1\}^{2^n}$

$WH(x) = (\langle x, a \rangle)_{a \in \{0,1\}^n}$

$e_i = (0 \ldots \underset{i}{1} \ldots 0)$

1% координат испорчены

$x_i = \langle x, a \rangle + \langle x, a + e_i \rangle = \langle x, e_i \rangle = x_i$

a – случайно

(Самородницкий)

Теорема. $\forall$ линей. код, декодир. с двумя запросами имеет длину код. слова $\ge 2^{\Omega(n)}$.

$C(x) = \langle a^1, x \rangle, \langle a^2, x \rangle, \ldots \langle a^m, x \rangle$

$a^j + a^k = e_i$

$x_i = \langle x, a^j \rangle + \langle x, a^k \rangle$

$i \quad M_i = \{ (j,k) \mid a^j + a^k = e_i \}$

$\forall i$

Утв. $|M_i| \ge \frac{m}{200}$

$a^1, a^2, \ldots, a^m \in \{0,1\}^n$

Подграф Булевого куба, индуц $\{a^1, a^2, \dots, a^n\}$ содержит $\geq \frac{n}{200}$ ребер в напр. e_i $\forall i \in [n]$.

Лемма $S \subseteq \{0,1\}^n$. Тогда в $S \leq \frac{|S| \log(S)}{2}$ ребер $\{0,1\}^n$

$$\frac{m \log m}{2} \geq \frac{m \cdot n}{200} \text{ ребер.}$$

$$\log m \geq \frac{n}{100} \Rightarrow m \geq 2^{n/100}$$

Д-во (леммы) $X_1 X_2 \dots X_n$ равномерно распр. на S

$x_2, \dots, x_n \in \{0,1\}^{n-1}$ $\quad * x_2 \dots x_n \in S$

$$H(X_1 \mid X_2 = x_2, X_3 = x_3, \dots, X_n = x_n) = \begin{cases} 1, & \text{если есть ребро в напр. } e_1 \\ 0, & \text{иначе} \end{cases}$$

$$H(X_1 \mid X_2, X_3, \dots, X_n) = \frac{2}{|S|} (\text{число ребер в } S \text{ в напр. } e_1)$$

$$\text{Число ребер в } S = \frac{|S|}{2} \sum_{i=1}^{n} H(X_i \mid X_{\neq i})$$

$$\leq \frac{|S|}{2} \left(H(X_1) + H(X_2 \mid X_1) + H(X_3 \mid X_1 X_2) + \dots + H(X_n \mid X_1 \dots X_{n-1}) \right)$$

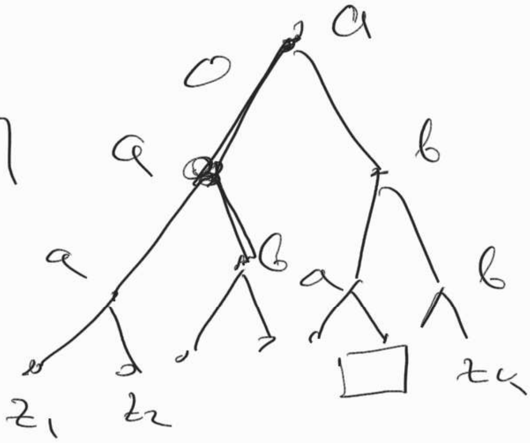
$$= \frac{|S|}{2} H(X_1, \dots, X_n) = \frac{|S|}{2} \log |S|.$$

§ Применение теории инф. в ком. сложности.

$$f: X \times Y \to Z$$

$$\underset{x \in X}{A} \quad \rightleftarrows \quad \underset{y \in Y}{Б}$$

Π



$a_v : X \to \{0,1\}$

$b_v : Y \to \{0,1\}$

$R \subseteq (X, Y, Z)$

x, y ? z:

$(x, y, z) \in R$

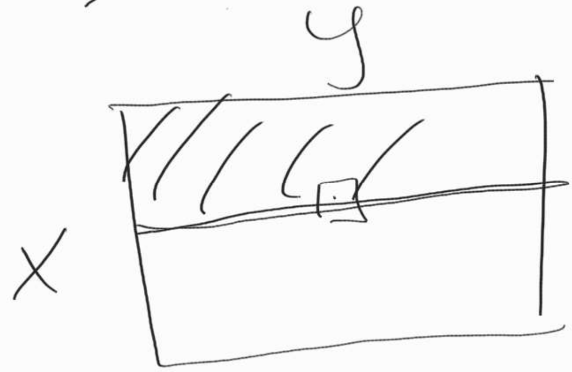
$D(\Pi)$ глубина

$L(\Pi)$ число листьев

$f : X \times Y \to Z$

$L(\Pi) \le 2^{D(\Pi)}$

$CC(f) = \min\limits_{\Pi} D(\Pi)$



$A \times B$ $\quad A \subseteq X$

$B \subseteq Y$

Формульная сложность ф-ции $f : \{0,1\}^n \to \{0,1\}$ в базисе $\wedge, \vee, \neg$

$$KW_f = \{(x, y, i) \mid x \in f^{-1}(0),\ y \in f^{-1}(1),\ x_i \ne y_i\}$$

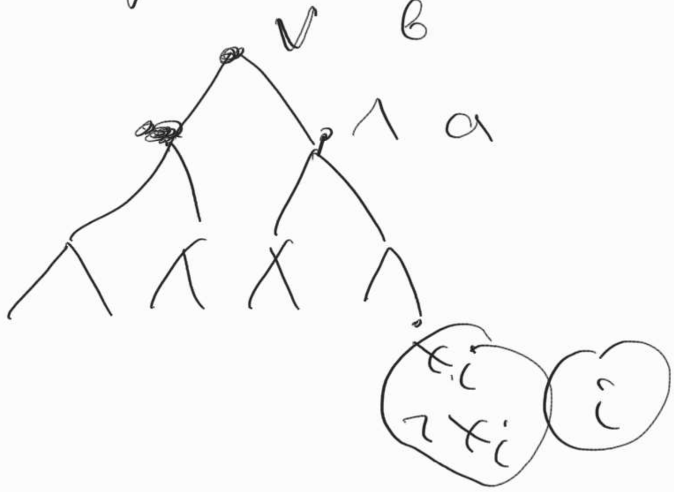
$x \in f^{-1}(0)$ $\qquad y \in f^{-1}(1)$

<u>Теорема</u> (Карчмер – Вигдерсон)

Миним. число листьев в формуле вычисл. f = мин. числу листьев в ком. протоколе для KW_f.

Д-во (в одну сторону)

Ф-ла $\Longrightarrow$ протокол



$x \in f^{-1}(0)$

$y \in f^{-1}(1)$

Disj

Parity_n

Информационное разглашение коммуникационного протокола

Π – комм. протокол

μ – распределение на (X, Y)

Внешнее информ. разглашение

$$IC_\mu^{ext}(\Pi) = I\big(\Pi(X,Y) : X, Y\big) = \left[= H\big(\overbrace{\Pi(X,Y)}^{\text{посланные биты в протоколе}}\big) - \underbrace{H\big(\Pi(X,Y) \mid X,Y\big)}_{=0}\right]$$

Внутр. инфо. разглашение

$$IC^{int}_{\mu}(\Pi) = I(\Pi(X,Y):X \mid Y) + I(\Pi(X,Y):Y \mid X)$$

$$\left[= H(\Pi(X,Y) \mid X) + H(\Pi(X,Y) \mid Y)\right]$$

<u>Теорема</u> Π комм. протокол, μ — распр. на (X,Y). Тогда $D(\Pi) \underset{(1)}{\geq} \log L(\Pi) \underset{(2)}{\geq} IC^{ext}_{\mu}(\Pi) \underset{(3)}{\geq} IC^{int}_{\mu}(\Pi)$. $\exists \mu$: в (2) достигается рав-во для мин. протоколов.

<u>Д-во</u> (1) очевидно

(2) $IC^{ext}_{\mu}(\Pi) = I(\Pi(X,Y):X,Y)$

$= H(\Pi(X,Y)) \leq \log L(\Pi)$

(3) будет потом

<u>Теорема</u> (Храпченко)

В ф-ле для $Parity_n$ $\geq n^2$ листьев

<u>Д-во</u> KW_{Parity_n}

μ — равном. распр. на парах, отличающ. ровно в 1 бите строк из $\{0,1\}^n$ (X,Y)

Π протокол для KW_{parity_n}

$\log L(\Pi) \geq IC^{ext}_{\mu}(\Pi) \geq IC^{int}_{\mu}(\Pi) =$

$$= I(\Pi(X,Y) : X \mid Y) + I(\Pi(X,Y) : Y \mid X) = 2\log n$$

$$\boxed{I(\Pi(X,Y) : X \mid Y)} = H(\overset{\log n}{X \mid Y}) - H(X \mid \underset{0}{Y, \Pi(X,Y)})$$

$= \log n -$

$$\boxed{L(\Pi) \geq n^2}$$

IC