Утв. $\Pr[\pi(A,B) = A\wedge B] \le \frac{1}{2} + \sqrt{IC^{int}_{\tilde{A},\tilde{B}}(\pi)/d}$

Д-во для π без общих случ. битов.

$$\Pr[\pi(A,B) = A\wedge B] = \mathop{E}_{r}\left[\Pr[\pi_r(A,B) = A\wedge B]\right] \le$$

$$\mathop{E}_{r}\left[\frac{1}{2} + \sqrt{\frac{IC_{\tilde{A},\tilde{B}}(\pi_r)}{d}}\right] = \frac{1}{2} + \sqrt{\mathop{E}_{r}\left[IC_{\tilde{A},\tilde{B}}(\pi_r)\right]/d}$$

$$= \frac{1}{2} + \sqrt{E\left[IC_{\tilde{A},\tilde{B}}(\pi)\right]/d}$$

$$\Delta\left((A,B), A\times B\right) \le \sqrt{\frac{I(A:B)\ln 2}{2}}$$ нер-во Пинскера

$$(A,B) \;\|\; \mathop{E}_{b\sim B}\left[A|_{B=b}, A\right)$$

$$\underbrace{f(x_1,y_1)\; f(x_2,y_2) \;-\; f(x_k,y_k)}_{k}$$

$\frac{k}{n}$ $\qquad$ $IC \le D$

к.сл. ℓ

π протокол для задачи f

$IC(\pi) = A$

$\Downarrow$ протокол π' для f

с $D(\pi') \approx \sqrt{A\,\ell} > A$

A

сжатие протоколов

Теорема $f(x,y)$ μ – распр. на x,y

π – вероятн. протокол высоты ℓ, кот. вычисляет f с ошибкой $\le \delta$ (по всем случ. битам и входам)

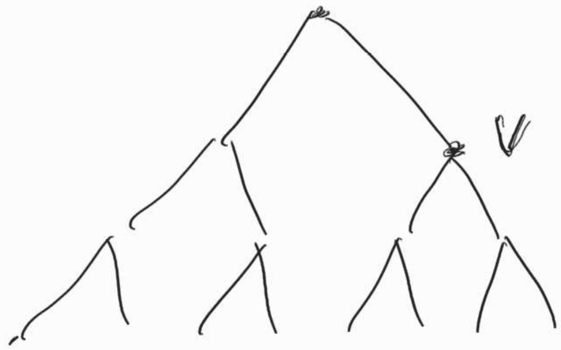
Тогда $\forall \varepsilon > 0$ $\exists$ протокол для f со средней длиной коммуникации

$O\left(\sqrt{IC_\mu(f)\cdot \ell}\cdot \log\left(\frac{\ell}{\varepsilon}\right)\right)$ и вер-тью ошибки $\le \delta+\varepsilon$.

<u>Д-во</u> 1. Сначала докажем для протоколов без публичных случ. битов.

$\pi_r \longrightarrow \pi'_r$ $\qquad x, y$

$\delta_r \qquad\quad \delta_r+\varepsilon$



$r_v \in [0;1]$

случ. число $P_{i,v,x,y}$

$= \Pr[M_i=1 \mid M_{<i}=v, X=x, Y=y]$

$= \Pr[M_i=1 \mid M_{<i}=v, X=x]$

Если $r_v < P_{i,v,x,y}$ тогда идем по 1

Если $r_v \ge P_{i,v,x,y}$ тогда идем по 0.

<u>Лемма</u> LCP

Алиса $x\in\{0,1\}^n$ найти $\max\{i \mid x_{\le i}=y_{\le i}\}$

Боб $y\in\{0,1\}^n$

$\exists$ вероятн. ком. протокол для LCP с ошибкой ε сл-ти $O\left(\log\left(\frac{n}{\varepsilon}\right)\right)$

Пусть дан набор чисел

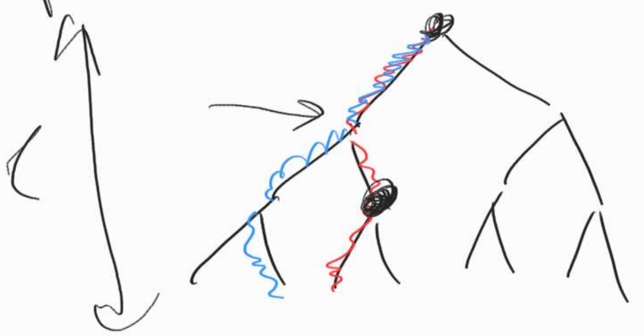
r_v,

Алиса и Боб моделируют протокол,

используя свои вер-ти

$\Pr[M_i = 1 \mid M_{<i} = v, X = x]$ вместо $p_{i,v,x,y}$

$\Pr[M_i = 1 \mid M_{<i} = v, Y = y]$ вместо $p_{i,v,x,y}$



С помощью протокола для $LCP(l, \frac{\varepsilon}{l^2})$ Алиса и Боб находят точку расхождения

и перемещают фишку в верш. следующую после. Затем повторяют проц.

Продолжают, пока не придут в лист.

Если LCP не врёт, то мы пришли в тот же лист, что и реальные.

$\leq l$ вызовов LCP

$\Rightarrow$ вер-ть ≥ 1 ошибка была у LCP $\leq \frac{\varepsilon}{l^2} \cdot l \leq \varepsilon$

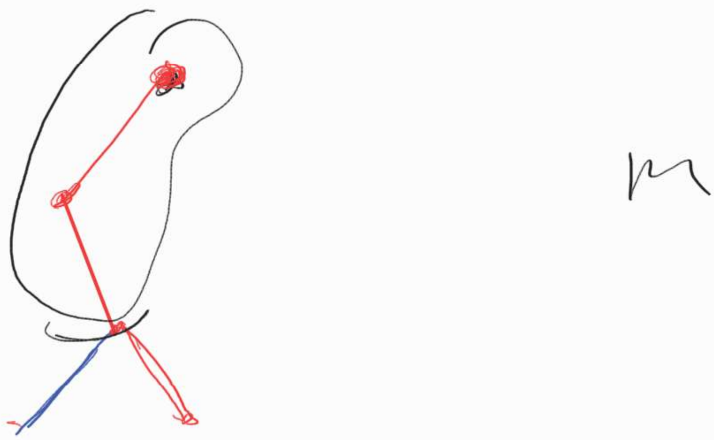
$\delta + \varepsilon$

Среднее число переданных битов $\leq \underbrace{\#\text{ вызовов LCP}}$: $O(\log \frac{\ell}{\varepsilon})$

Оценим
в предп., что LCP не делает ошибки

В предп., что LCP делает ошибки.

$$\frac{\varepsilon}{\ell} \cdot \underbrace{\ell} \leq \varepsilon$$



Среднее число вызовов LCP = среднему числу номеров i, что $C_{Alice}(m_{<i})$ отлич. от $C_{Bob}(m_{<i})$ в бите i.

Средн. число вызовов LCP

$$\le \mathop{E}_{m} \sum_{i=1}^{\ell} \Big[\Pr \big[C_{Alice}(m_{<i}) \text{ в } i\text{-м отлич. от } C_{Bob}(m_{<i}) \text{ бите} \big] \Big] = \sum_{i=1}^{\ell} \Big[\mathop{E}_{\substack{v \leftarrow \text{случ. на высоте } i \\ x,y}} \Big[\Delta\big((M_i \mid M_{<i} = v, X = x), (M_i \mid M_{<i} = v, Y = y) \big) \Big] \Big]$$

Лемма Среднее по v на высоте i и по x, y

$$\Delta\big((M_i \mid M_{<i} = v, X = x), M_i \mid M_{<i} = v, Y = y \big) \le$$

$$\le \sqrt{I(M_i : X \mid M_{<i}, Y) + I(M_i : Y \mid M_{<i}, X)}$$

Д-во Достаточно док-ть для фикс. v.

1) v — вершина Алисы $\Rightarrow I(M_i : Y \mid M_{<i}, X) = 0$

$$\mathop{E}_{x} \Delta\big(M_i \mid M_{<i} = v, X = x, Y = y, M_i \mid M_{<i}, Y = y \big) =$$

$$= \Delta\Big(M_i|_{M_{<i}=v,\, Y=y} \times X|_{M_{<i}=v,\, Y=y},$$

$$(M_i|_{M_{<i}=v, Y=y}, X_{M_{<i}=v,\, Y=y})\Big)$$

$$\leq \sqrt{\frac{\ln 2}{2} I(M_i : X \mid M_{<i}=v, Y=y)}$$

$$E_{x,y}\Delta \leq \sqrt{I(M_i : X \mid M_{<i}, Y)}$$

среднее

\# выз. $LCP \leq$

$$\sum_{i=1}^{\ell} \sqrt{I(M_i : X \mid M_{<i}, Y) + I(M_i : Y \mid M_{<i}, X)} \leq$$

$$\leq \sqrt{\ell\Big(\sum_{i=1}^{m} I(M_i : X \mid M_{<i}, Y) + \ldots\Big)}$$

$$\leq \sqrt{\ell\, IC_\mu(\pi)}$$

$$O\Big(\Big(\sqrt{\ell\, IC_\mu(\pi)} + 1\Big)\log\Big(\frac{\ell}{\varepsilon}\Big)\Big)$$

Дивергенция Кульбака-Лейблера

P и Q распр на U конечное мн-во

$$D(P\|Q) = \sum_{x \in U} P(x) \log \frac{P(x)}{Q(x)}$$

<u>Лемма</u> $D(P\|Q) \geq 0$

$D(P\|Q) = 0 \iff P = Q$

Д-во <u>упр</u>

<u>Лемма</u> $I(X:Y) = D((X,Y)\|X \times Y)$

$$= -\sum_{x,y} \Pr[X=x, Y=y] \log \frac{\Pr\{X=x\} \Pr\{Y=y\}}{\Pr[X=x, Y=y]}$$

<u>Теорема</u> (нер-во Пинскера)

$$D(P\|Q) \geq \frac{1}{2\ln 2} \|P-Q\|_1^2 = \frac{2}{\ln 2} \Delta(P,Q)^2$$

<u>Сл-ие</u> $\underset{I(X:Y)}{\underset{\|}{D((X,Y)\|X \times Y)}} \geq \frac{2}{\ln 2} \Delta((X,Y), X \times Y)^2$

Св-ва 1) KL-дивергенции

$$D((X,Y)\|(Z,T)) \geq D(X\|Z)$$

2) α - ф-ция

$$D(\alpha(X)\|\alpha(Y)) \leq D(\alpha(X),X\|\alpha(Y),Y)$$

$$= D(X\|Y)$$

Теорема (нер-во Пинскера)

$$D(P\|Q) \geq \frac{1}{2\ln 2}\|P-Q\|_1^2 =$$

Д-во

1) $P = \begin{cases} 1, & p \\ 0 & 1-p \end{cases}$ $Q = \begin{cases} 1, & q \\ 0, & 1-q \end{cases}$

$f(p,q)$

$$p\log\frac{p}{q} + (1-p)\log\frac{1-p}{1-q} - \frac{1}{2\ln 2}(2(p-q))^2 \geq 0$$

$f(p,p) = 0$ $\qquad$ $f(p,q) = f(1-p, 1-q)$

$p \geq q$ $\qquad$ $\frac{\partial f}{\partial q} \leq 0$ при $p \geq q$

2) P и Q распр на U.

$$A = \{ x \mid P(x) \geq Q(x) \}$$

$$P_A = \begin{cases} 1, & P(A) = \sum_{x \in A} P(x) \\ 0, & 1 - P(A) \end{cases}$$

$$Q_A = \begin{cases} 1 & Q(A) = \sum_{x \in A} Q(x) \\ 0 & 1 - Q(A) \end{cases}$$

$$\|P - Q\|_1 = \|P_A - Q_A\|_1 \leftarrow \underline{\text{упр.}}$$

$$\alpha(x) = \begin{cases} 1, & x \in A \\ 0, & x \notin A \end{cases}$$

$$D(P\|Q) \geq D(\alpha(P)\|\alpha(Q)) =$$

$$= D(P_A\|Q_A) \geq \frac{1}{2\ln 2} \|P_A - Q_A\|_1^2$$

$$= \frac{1}{2\ln 2} \|P - Q\|_1^2 .$$