TI-Ex-5-5-2020

5 May, 2020 15:45

200 mil. Kč

200 mil / student

20 years 50k€ / student / year

---

offline lectures - - speed-up video (150%)
[- max (320%) extreme]
- pause, skip backward

- exams - ½ half of Jaroš.

Communication complexity

$EQ(x, y) = [x \stackrel{?}{=} y]$

protocol $\leq n+1$

$n+1$

- randomized protocol?
  - pick a random bit i and compare

Alice $i, x_i \rightarrow$ Bob

$\leftarrow y_i$

$x = y$ $\quad Pr[\text{error}] = 0$

$x \neq y$ $\quad Pr[\text{error}] = 1 - \frac{\text{Ham}(x,y)}{n} = 1 - \frac{1}{n}$

repeat ℓ times

$Pr[\text{error}] \leq \left(1 - \frac{1}{n}\right)^{\ell}$

$\leq e^{-\frac{\ell}{n}}$

$\ell = n$

$\left(1 - \frac{1}{n}\right)^n \approx \frac{1}{e}$

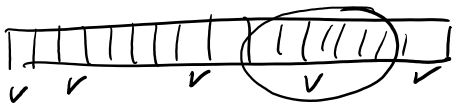
$(1-x)^{\ell} \leq e^{-x \cdot \ell}$

$\ell \approx n$

$\ell \simeq n$

- computing parities for random subset of bits

Alice → Bob



$\sum x_i \bmod 2$

$x_i = 1 \oplus y_i$

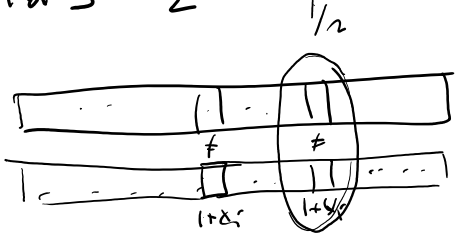
$x_i \neq y_i \iff$

$\sum y_i = \sum 1 \oplus x_i$

$= \underbrace{\sum 1}_{1} + \sum x_i$

$x = y$ $\quad Pr[error] = 0$

$x \neq y$ $\quad Pr[error] = \frac{1}{2}$

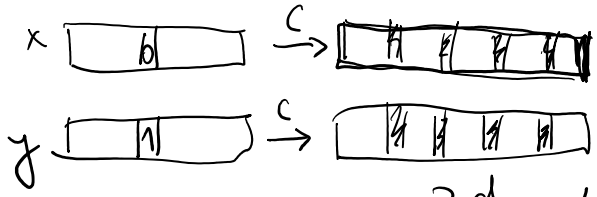


repeat ℓ-times $\quad Pr[error] = \left(\frac{1}{2}\right)^{\ell} = \frac{1}{2^{\ell}} = \frac{1}{n^2}$ ($\ell \geq \lg n$)

$\ell = 10$ $\quad 99.9\%$ $\quad$ (shared random string)

$a = 0001,0000$

$C \quad [N, n, d]$



$C(x) = x' \quad N \geq \frac{d}{N}$

$C(y) = y' \quad N$

$\geq d$

$Pr[error] \leq 1 - \frac{d}{N}$.

N

$\parallel$

$[(1+\delta)n, n, \varepsilon n]$ $\quad \delta = H(\varepsilon)$

$Pr[error] \leq 1 - \varepsilon$

$\lg N = \lg (1+\delta) n = O(\lg n)$

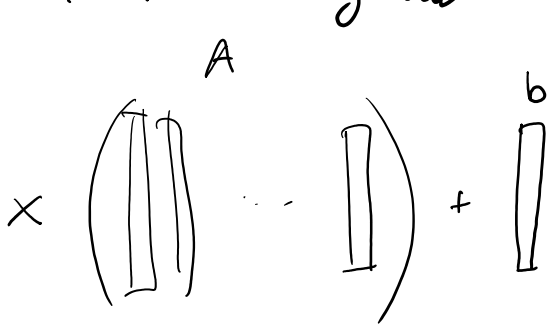
[doesn't use shared random bits]

repeat ℓ-times $\quad Pr[error] \leq (1-\varepsilon)^{\ell}$

$O(\lg n)$ $\quad O(\lg n)$ $\quad$ if $\frac{1}{n^2}$

→ $O(\lg n)$ bits

- hashing ≈ error correcting codes



$xA+b$

↳ 2 universal hash system

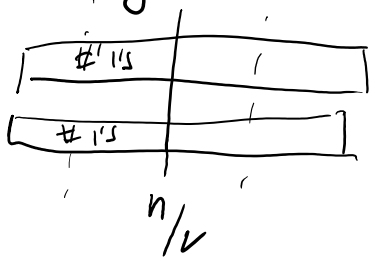
- $MED(x,y)$ = median of $x \cup y$

$y, x \subseteq \{1, \dots, n^3\}$

y has only odd #'s

x has only even #'s

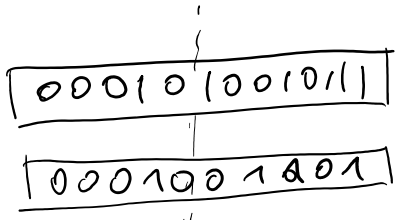
- binary search



$O(\lg^2 n)$ in total

- $GT(x,y) = [x > y]$

0001
1 0101



- binary search on to find the arbitrary position using EQ protocol. Δ

$n+1$

$2\,GT \geq EQ$

Q: • deterministic ? $\geq \frac{n}{2}$

$\lg n$ runs

EQ ptcol using $O(\lg^2 n)$ bits

error pbly $\leq \frac{1}{n^2}$

err pbly of single check $\leq \frac{1}{\lg n}$

→ error pbly of the GT-protocol $\leq \frac{\lg n}{n^2}$

error prob $\leq \frac{1}{n^2}$

$\rightarrow$ error prob of the GT-protocol $\leq \boxed{\frac{\lg n}{n^2}}$

$O(\lg^3 n)$ bit.

check $\leq \frac{1}{\lg n}$

$\{O(\lg n)$-bits$\}$