Lower Bounds

ε

$f:[N]\to[N]$

1. Compression
2. Presampling
3. Concentration technique (Russell's trick)

$P:[N]\to[N]$

$A_0(P) \to s$ bits

A_1: T queries

$$\Pr_{P,\,y}\left[A_1^P(A_0(P), y) = P^{-1}(y)\right] = \varepsilon$$

$\forall\, z \in \{0,1\}^s$

$$\Pr_P\left[\Pr_y\left[A_1^P(z, y) = P^{-1}(y)\right] \geq \varepsilon_2\right] < 2^{-s}\cdot\varepsilon_2$$

X_y : $A_i(z, y) = P^{-1}(y)$

$$\Pr_P\left[\frac{1}{N}\sum X_y \geq \varepsilon_1\right] < 2^{-s} \cdot \varepsilon_2$$

$$E_P[X_y] = \Pr_P[A_i^P(z, y) = P^{-1}(y)]$$

$$\leq \frac{T}{N}$$

want: $\varepsilon_1 = \frac{sT}{N}$

$X_1, \ldots, X_N$ $\{0,1\}$ variables

{ ① what conditions
② variables $\Rightarrow$ conditions

$$\Pr\left[X_1 + \cdots + X_N \geq N\varepsilon\right] \leq 2^{-s}$$

① $\Pr[X_i = 1] \leq \varepsilon$, $Q \subseteq [n]$

$$\Pr\left[\bigwedge_{i \in Q} X_i = 1\right] \leq \varepsilon^{|Q|}$$

$Q \subseteq_k [n]$ $|Q| = k$

$$E[\#\text{ of set of size } k \text{ s.t. } X_Q = 1]$$

$$\geq E[\# \cdots \mid X_1 + \cdots + X_n \geq \varepsilon \cdot N] \cdot \Pr[X_1 + \cdots + X_n \geq \varepsilon \cdot N]$$

$$\leq \frac{E[\# \cdots]}{E[\# \cdots \mid X_1 + \cdots + X_N \geq \varepsilon \cdot N]}$$

$E[X_i] = \delta$

$E[\#\text{ of sets of size } k \text{ s.t. } X_{\alpha^{-1}}]$

$\leq \binom{N}{k} \cdot \delta^k$

$E[\# \cdots \mid X_1 + \cdots + X_N \geq \varepsilon \cdot N]$

$\geq \binom{\varepsilon \cdot N}{k}$ $\quad \varepsilon \cdot N \geq s$

$$\Pr[X_1 + \cdots + X_N \geq \varepsilon \cdot N]$$

$$\leq \frac{\binom{N}{k} \cdot \varepsilon^k}{\binom{\varepsilon \cdot N}{k}} \leq \frac{\left(\frac{Ne}{k} \cdot \varepsilon\right)^k}{\left(\frac{\varepsilon N}{k}\right)^k}$$

$$\left(\left(\frac{N}{j}\right)^j \leq \binom{N}{j} \leq \left(\frac{eN}{j}\right)^j\right)$$

$$= \left(\frac{e\varepsilon}{\varepsilon}\right)^k \qquad \varepsilon = 2e\varepsilon$$

$$k = s$$

$$= 2^{-s}$$

ε-security against

s-bit advice

$\varepsilon^{|S|}$-security in

S-wise multi-instance

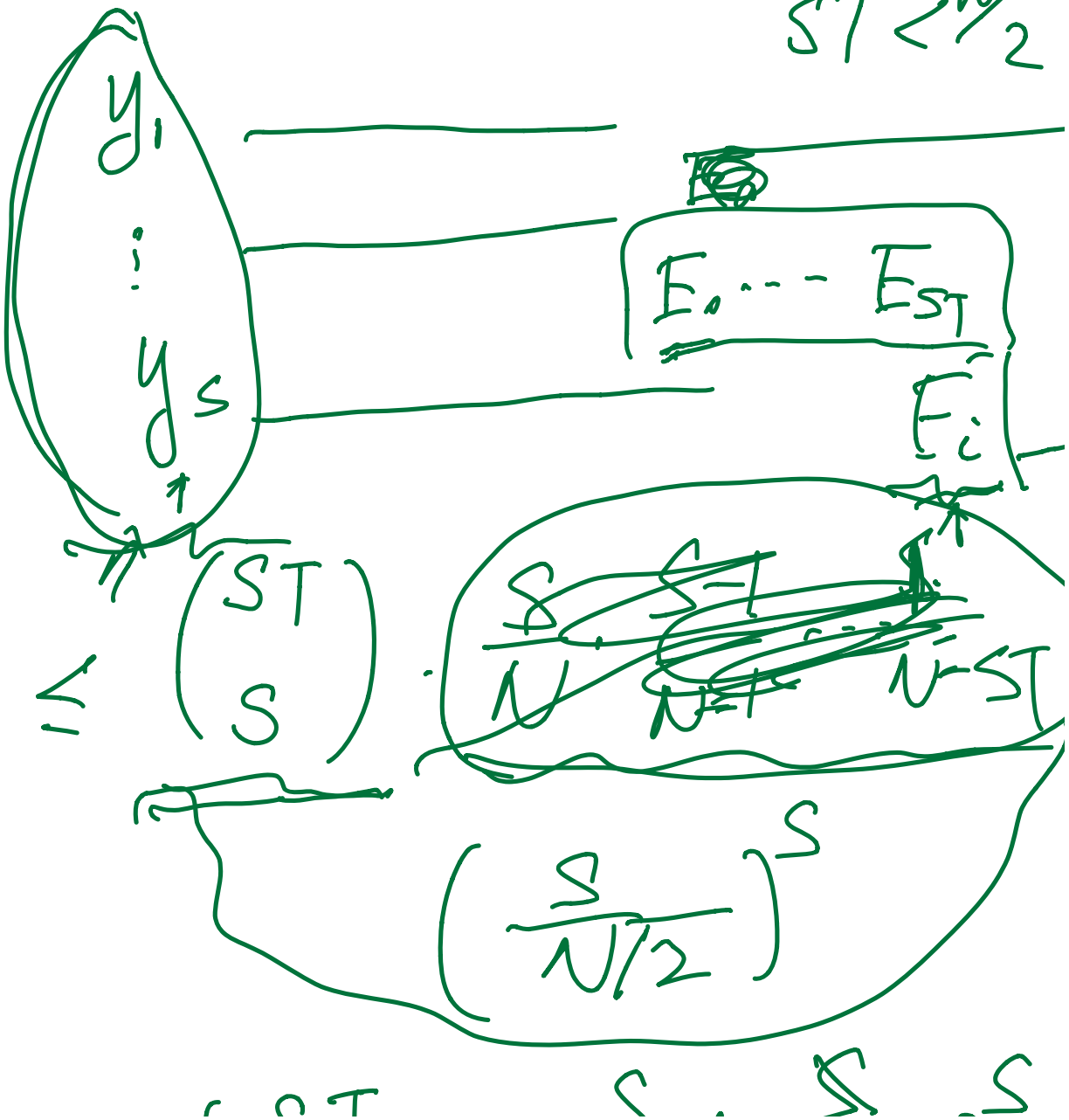
game

(against 0 advice)

$y \to p^{-1}(y)$

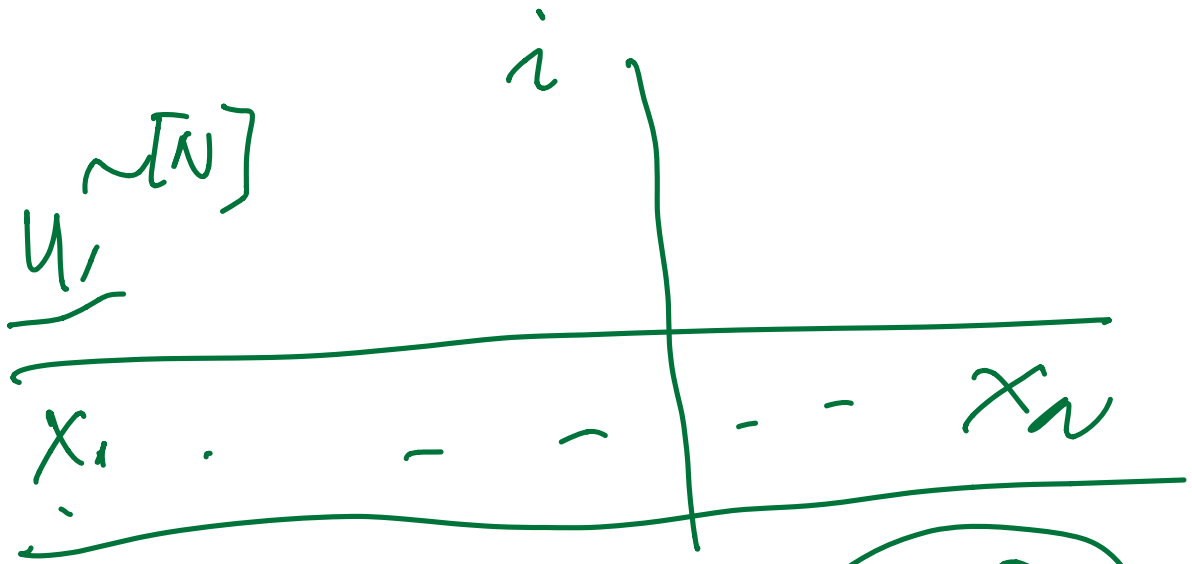
$y_1, \dots, y_s$ ST queries to P

$ST < N/2$



$$= \left(\frac{S!}{S} \cdot e\right)^{-} \left(\frac{}{N/2}\right)$$

$$= \left(2e \cdot \frac{ST}{N}\right)^{S}$$



QED

$N^{2/3}$ $N^{1/2}$

— non-adaptive

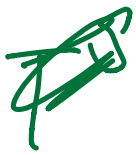
v.s. adaptive

upper lower

$T = N$ $\sqrt{N}$

y_1 X_{11} --- X_{1T}

y_s X_{s1} -- X_{sT}

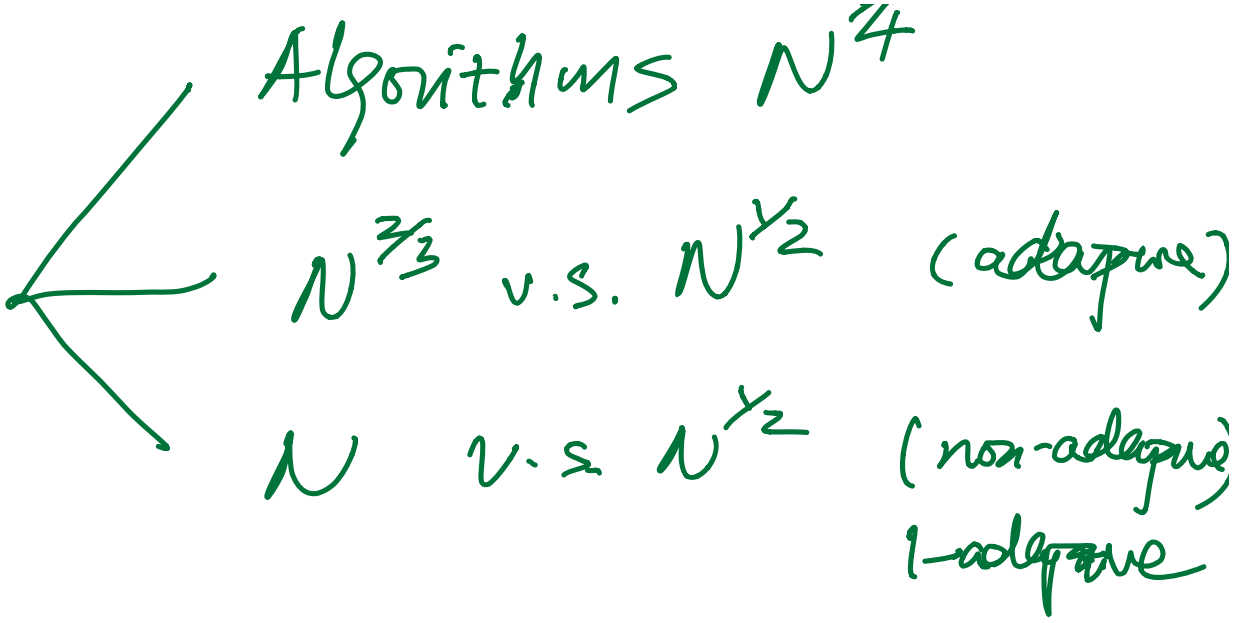


$$\sum_{j_1,\dots,j_S \in [T]} \Pr\left[X_{1,j_1} = P^{-1}(y_1) \wedge \cdots \wedge X_{S,j_S} = P^{-1}(y_S) \right]$$

$$T^S \cdot \frac{1}{N} \cdot \frac{1}{N-1} \cdot \frac{1}{N-2} \cdots \frac{1}{N-S}$$

$$\leq \left(\frac{T}{N-S} \right)^S$$

$$\left(\frac{T+S}{N} \right)^S$$


Algorithms N^{4}
$N^{2/3}$ v.s. $N^{1/2}$ (adaptive)
N v.s. $N^{1/2}$ (non-adaptive)
1-adaptive