Round elimination

6.897
L11.3
Mar. 10, 2005

Variation on problem f: $f^{(k)}$

- Alice has k inputs $x_1, x_2, \ldots, x_k$
- Bob has 2 inputs y, $i \in \{1, 2, \ldots, k\}$
  & already knows $x_1, x_2, \ldots, x_{i-1}$
- goal: compute $f(x_i, y)$

Intuition:

- first message sent by Alice with $\leq a$ bits $\ll k$ inputs is useless — unlikely to send anything useful about x_k
- $\Rightarrow$ can start comm. protocol at second message — eliminate first message
- repeat in Bob $\rightarrow$ Alice direction $\Rightarrow$ eliminate round

Lemma: if there is a protocol for $f^{(k)}$ where Alice speaks first using m messages and with error probability δ then there is a protocol for f where Bob speaks first using $m-1$ messages and with error prob. $\delta + O(\sqrt{a/k})$

Intuition: (not a proof)

- if i were chosen uniformly at random, then expect a/k bits to be "about" x_i
- Bob can guess these bits randomly
- $\Pr[\text{correct guess}] = 1/2^{a/k}$

$\Rightarrow$ error increase $= 1 - 1/2^{a/k}$ (by union bound)

$\approx a/k$ $(1 - 1/e^x \approx x)$

$\sqrt{a/k}$ is bigger $\Rightarrow$ safer & "more correct" ☺

- real proof uses information theory