Open Problem Set

Given by Andrew Yao

Sept. 12th, 2002

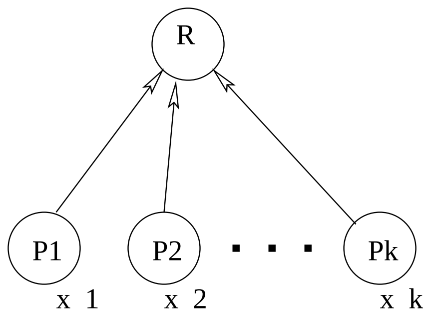
Randomized Lower Bound in Simultaneous Message Model

Definition These are $k,\ k \geq 2$ computational unlimited parties,$P_1, P_2, \cdots P_k$ in the communication game, each party holds a n-bit integer $x_i \quad i = 1 \cdots k$ and does not know any other's integer. They can only send message to the *referee*,R. The referee, which initially knows nothing about x_i,need to compute the function

$$f(x_1, x_2, \cdots x_k) = \begin{cases} 1 & : \quad x_1 \oplus x_2 \oplus \cdots \oplus x_k = 0 \\ 0 & : \quad otherwise \end{cases}$$

by the binary message sent by those parties.

The communication complexity $C^k(f)$ is defined as $max_{1 \leq i \leq k}\,(c_i)$ where c_i denotes the number of bits P_i send to R who compute f deterministicly.



The randomized communication complexity $C_\epsilon^k(f)$ is defined as $max_{1 \leq i \leq k}\,(r_i)$ where r_i denotes the number of bits P_i send to R who compute f using a 1-sided randomized algorithm.

Existence Protocol When $k = 2$,$C_\epsilon^2(f) = \Theta(n^{\frac{1}{2}}$

Open Problem When $k > 2$, whether $C_\epsilon^k(f) = \Omega(n^{1-\frac{1}{k}})$

Scribed by $Li\ \ Yunpeng$