

Fooling Set Proof

Consider a two-party protocol for:

$$EQ = \begin{cases} 1 & \text{if } x=y \\ 0 & \text{otherwise} \end{cases}$$

Simplest Protocol:

Send the entire input and compare the values

Protocol Π

Player 1	Player 2
$x=111$	$y=110$
$P_1(x)$	$P_1=111$
$P_2=0$	$P_2(y, P_1)$

4 bits = $|x|+1$ communicated

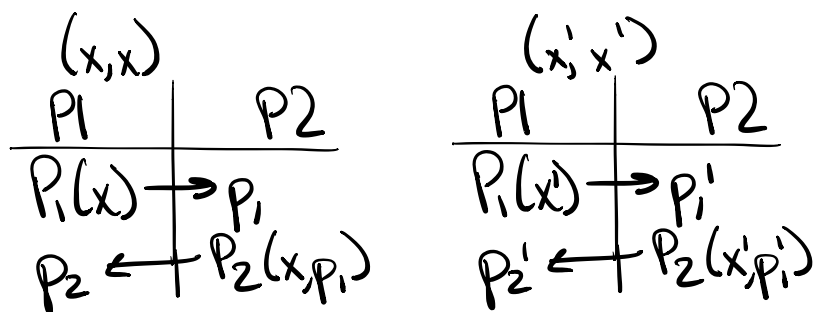
$$C(\Pi) = n+1$$

Theorem: $C(EQ) \geq n$


Proof (via the fooling set method):

Claim: For any (x, x) and (x', x') , if both inputs

communicate the exact same sequence of bits, then $F(x,x) = F(x',x') = F(x,x') = F(x',x)$



$$P_1 = P_1' \quad P_2 = P_2'$$

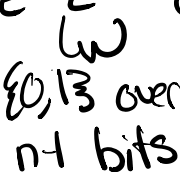


If (x, x) and (x', x') have the same communication pattern, then it doesn't matter which way they are mixed, each x and x' produce the same bits.

If they produce the same sequence of bits, then they agree on the output.

Claim: $C(EQ) \geq n$

Assume a protocol with complexity $n-1$ exists

Thus there are 2^{n-1} communication patterns


However, there are 2^n input pairs (x, x)
 $|x| = 2^n$

2^{n-1} communication patterns

2^n equal input pairs

Thus there exists:

(x, x) and (x', x') where $x \neq x'$

that have the same communication protocol

This is a contradiction

$$EQ(x, x') = 0 \neq EQ(x, x)$$

$$C(EQ) \geq n$$

This proof generalizes to:

Lemma:

$$F: \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}$$

F has a M -sized fooling set if:

\exists M -sized subset $S \subseteq \{0, 1\}^n \times \{0, 1\}^n$
and value $b \in \{0, 1\}$ s.t.:

1) $\forall \langle x, y \rangle \in S, F(x, y) = b$

2) \forall distinct $\langle x, y \rangle, \langle x', y' \rangle \in S$,
either $F(x, y') \neq b$ or $F(x', y) \neq b$

If F has a size- M fooling set,
then $C(F) \geq \log M$

Example:

$\langle x, y \rangle: x, y \subseteq \{1, 2, \dots, n\}$

$$\text{DISJ}(x, y) = \begin{cases} 1 & x \cap y = \emptyset \\ 0 & \text{otherwise} \end{cases}$$

Fooling set for DISJ:

$$S = \{(A, \bar{A}) : A \subseteq \{1, 2, \dots, n\}\}$$

$$\forall A, \text{DISJ}(A, \bar{A}) = 1$$

$\forall (A, \bar{A}), (B, \bar{B})$ either

$$\text{DISJ}(A, \bar{B}) = 0$$

$$\text{DISJ}(B, \bar{A}) = 0$$

There are 2^n possible A sets.

Thus S is a 2^n -sized fooling set

$$\begin{aligned} C(\text{DISJ}) &\geq \log(M) \\ &\geq n \end{aligned}$$