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
$x=111$	$y=110$
$P_1(x) \longrightarrow$	$p_1=111$
$p_2=0 \longleftarrow$	$P_2(y,p_1)$

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 $f(x,x) = f(x',x') = f(x,x') = f(x',x)$

(x,x)

P1	P2
$P_1(x) \rightarrow$	p_1
$p_2 \leftarrow$	$P_2(x,p_1)$

(x',x')

P1	P2
$P_1(x') \rightarrow$	p_1'
$p_2' \leftarrow$	$P_2(x',p_1')$

$$p_1 = p_1' \qquad \underbrace{p_2 = p_2'}_{\text{final answer}}$$

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 $\underbrace{2^{n-1}}_{\{0,1\} \text{ over } n-1 \text{ bits}}$ communication patterns

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

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 <u>same</u> communication protocol

This is a contradiction

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

$C(EQ) \geq n$

This proof generalizes to:

Lemma:

$f: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$

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

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

Fooling set for DISJ:
$S = \{(A, \bar{A}) : A \subseteq \{1, 2, \ldots, n\}\}$

$\forall A$, $DISJ(A, \bar{A}) = 1$
$\forall (A, \bar{A}), (B, \bar{B})$ either
$DISJ(A, \bar{B}) = 0$
$DISJ(B, \bar{A}) = 0$

There are 2^n possible A sets.
Thus S is a 2^n-sized fooling set
$C(DISJ) \geq \log(M)$
$\geq n$