Fooling Sets

Jake Kinsella

March 24, 2021

Consider a two-party protocol for determining whether two inputs are equal:

$$EQ(x,y) = \begin{cases} 1 \text{ if x=y} \\ 0 \text{ otherwise} \end{cases} \tag{1}$$

The "obvious protocol" is for Player 1 to send it's entire input to Player 2 and let Player 2 compare the values itself.

Protocol Π

Player 1	Player 2
$x = 111$ $P_1(x) \longrightarrow$ $p_2 = 0$	$y = 110$ $p_1 = 111$ $\longleftarrow P_2(y,p_1) = P_2(110,111) = 0$

In this example, 4 bits are communicated. More generally the $C(\Pi) = |x| + 1$, the cost for Player 1 to communicate x plus one bit for Player 2 to communicate the answer.

Theorem: $C(EQ) \geq n$

Claim: For any (x,x) and (x',x'), if on both inputs, both Players communicate the exact same sequence of bits, then $f(x,x) = f(x',x') = f(x,x') = f(x',x)$

(x,x)

Player 1	Player 2
x $P_1(x) \longrightarrow$ p_2	x p_1 $\longleftarrow P_2(x,p_1)$

(x',x')

Player 1	Player 2
x $P_1(x') \longrightarrow$ p'_2	x p'_1 $\longleftarrow P_2(x',p'_1)$

$p_1 = p'_1$ and $p_2 = p'_2$ $p_2 = p'_2$ is the final answer.

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

If they produce the same sequence of bits, then they agree on the output (as the output is just the final bit).

Proof: $C(EQ) \geq n$

Assume a protocol Π' with complexity $n-1$ exists that solves EQ.

Π' has 2^{n-1} $(0,1$ over $n-1$ bits) possible communication patterns if it can communicate a max $n-1$ bits.

However, there are 2^n input pairs (x,x) ($|x| = n$, $0,1$ over n bits)

Π' has 2^{n-1} possible communication patterns. However there are 2^n equal input pairs.
Thus there exists some: (x,x) and (x',x') where $x \neq x'$ that have the same communication protocol

This is a contradiction.
$EQ(x,x') = 0 \neq EQ(x,x)$

Thus: $C(EQ) \geq n$

Lemma (generalization of the above theorem): Given some $f: 0,1^n \times 0,1^n \to 0,1$. f has a M-sized fooling set if there exists an M-sized subset $S \subset 0,1^n \times 0,1^n$ and a value $b \in 0,1$ such that:
1) $\forall (x,y) \in S, f(x,y) = b$
2) $\forall distinct(x,y),(x',y') \in S, either f(x,y') \neq b or f(x',y) \neq b$
If f has a size-M fooling set, then $C(f) \geq log(M)$

Example:
Determining whether two sets are disjoint across two parties.
$x,y \subset 1,2,\ldots,n$

$$DISJ(x,y) = \begin{cases} 1 \text{ if } x \cap y = \varnothing \\ 0 \text{ otherwise} \end{cases} \tag{2}$$

Fooling set for $DISJ$:
$S = (A,\overline{A}) | A \subset 1,2,\ldots,n$
1) $\forall A, DISJ(A,\overline{A}) = 1$
2) $\forall (A,\overline{A}),(B,\overline{B}), either DISJ(A,\overline{B}) = 0 or DISJ(B,\overline{A}) = 0$

There are 2^n possible A sets

Thus S is a 2^n-sized fooling set

Therefore $C(DISJ) \geq log(M) \geq n$