Multi-Party Communication

Jake Kinsella

April 6, 2021

Thus far, we've dealt exclusively with functions computed via the communication of two parties

We can generalize this to functions computed by any number of parties

Two Party Setup

In two party problems, Player 1 knows nothing about Player 2's input, and Player 2 knows nothing about Player 1's input

Multi-Party Setup

1. Player i doesn't know its own input
2. Player i knows the input of every other player
3. Messages are broadcasted to each player

What does this mean?

Consider a "real-life" example

We all place a sticky note with some value on our heads. We don't have any knowledge of our own sticky note but we can see everyone else's.

Without talking, we must compute some predetermined function via a predetermined protocol. All communication must be done through the whiteboard in front of us.

The goal is for one player, after some amount of communication, to write the output of function f on the whiteboard

Let's look at an example

$f(x_1, x_2, x_3) = \oplus_{i=1}^{n} maj(x_{1i}, x_{2i}, x_{3i})$

$f(1101, 1001, 1011) =$

____

1___

10__
100_
1001
$\oplus$ 1001 = 0

Protocol Π

Player 1	Player 2	Player 3
$x_2 = 1001$ $x_3 = 1011$ $parity(10\_1)$ $p_1 = 0$	$x_1 = 1101$ $x_3 = 1011$ $parity(1\_\_1)$ $p_2 = 0$	$x_1 = 1101$ $x_2 = 1001$ $parity(1\_01)$ $p_3 = 0$
$parity(p_1p_2p_3) = parity(000) = 0$		