**Value discovery in complete graphs**

**Group 43**

**Shivneshwar Velayutham and Madhumitha Venkatesan**

The protocol for a processor Pi to find it’s secret si is as below.

**First step**

All processors have read access to the secret value of all other processors. So, they can start by taking the first secret they can read and do an XOR operation on it with the next secret that they can read. The output of the previous operation should be XORed with the next secret and so on and so forth until all processor’s secrets (except the original processor’s secret of course) have been XORed upon. Write the final result of the operations to ri.

Therefore, every ri contains the following:

ri = s1 xor s2 … xor si-1 xor si+1 xor si+2 … xor sn

**Second step**

Once all processors are done with the first step, Pi can now look at another processor Pj and read the secret in sj and the output of previous step in rj. So now Pi will be able to compute the following:

rj xor sj = s1 xor s2 xor s3 … xor sn

The important property of XOR is the fact that XOR is commutative (ie. the order in which XOR is applied does not matter and the result is always the same). Below is the truth table of XOR and it’s quite easy to see if A and B are switched, we would get the same output.

|  |  |  |
| --- | --- | --- |
| **Input** | | **Output** |
| A | B | A XOR B |
| 0 | 0 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |

**Third step**

The other important property of XOR is that it’s possible to undo XOR. For example, the way to undo addition would be to use subtraction therefore making subtraction the inverse of addition. Similarly, the inverse of XOR is actually XOR. Below is the proof of the same and uses the fact which we proved earlier that XOR is commutative.

x = a xor b

x xor a = a xor b xor a

x xor a = a xor a xor b (Using commutative property)

Using the truth table above we can see that XORing same bits we get the result as 0. So,

a xor a = 0

x xor a = 0 xor b

Using the truth table above we can see that 0 xor 0 = 0 and 1 xor 0 = 1. So 0 is XOR’s identity value that doesn’t change the value of the other operand similar to how 0 is the additive identity and 1 is the multiplicative identity.

Therefore,

x xor a = b proving that xor is the inverse of xor.

Since we have the result of the XORs of all the secret from the previous step and Pi has the XORs of all the secrets except its own secret from the first step. It’s possible to calculate its secret by doing the following operation.

si = rj xor sj xorri

**Done**