

FINAL MODULE

INFORMATION THEORY AND COMMUNICATION COMPLEXITY

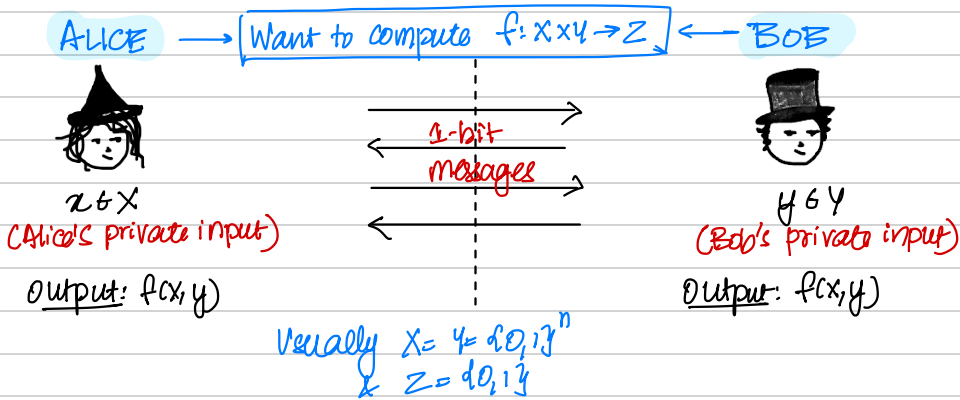
Today ↗

References

- Ryan's lecture 23
- Communication Complexity by Alexander Razborov
- Book → Kushilevitz & Nisan
- Lecture notes → Foundations of communication complexity by Toniann Pitassi

Recall: we spoke briefly about it in Lecture 10.

2-party Communication complexity



Key problem: Minimize the number of bits of communication assuming that computation is free.

Examples

① (From Lecture 10) $f = \text{EQUALITY}_n: \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}$

Deterministically: $(n+1)$ -bits of communication sufficient and necessary.

without any additional power (like randomness) need to communicate x itself.

Alice sends x
& Bob sends back $f(x, y)$

Randomized: (deamuelo) $\rightarrow$ show that $O(\log n)$ -bits suffice, w.h.p. $\forall x, y$.

② $f = \text{PARITY}_{2n} : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}$ $f(x,y) = x_1 \oplus \dots \oplus x_n \oplus y_1 \oplus \dots \oplus y_n$
only need to communicate 2-bits.

Alice sends $\bigoplus_{i=1}^n x_i$ & Bob $\bigoplus_{i=1}^n y_i$

③ Alice gets $A \subseteq [n]$, Bob gets $B \subseteq [n]$

Subsets are like bit-string

(each bit indicates whether the corresponding element in $[n]$ is in A or not)

e.g. $\{1, 3\} = A$ is 10100 $\underbrace{\hspace{1cm}}_{n\text{-bits}}$

a) Alice & Bob want to compute $\text{median}(A \cup B)$

How many bits sufficient to compute this?

Naïve solution: Alice sends A (n -bits) & Bob sends $\text{median}(A \cup B)$, which is a location ($\log n$ -bits) i.e. $(n + \log n)$ -bits

Can do better: $O(\log^2 n) \rightarrow$ using binary search.

Remark: Protocols with $\text{poly}(\log n)$ considered "efficient" and $n^{\Omega(1)}$ considered "inefficient"

b) $f = \text{DISJOINTNESS}_n : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}$

$f(A, B) = 1$ if and only if $A \cap B = \emptyset$

$= \neg \text{OR}_n(x_1 \wedge y_1, x_2 \wedge y_2, \dots, x_n \wedge y_n)$

(Remark: Similar to how SAT is fundamental problem of study in complexity theory, disjointness is a fundamental problem in communication complexity)

Deterministic: $n+1$ (also necessary)

$\hookrightarrow$ Alice sends A & Bob sends back $f(A, B)$.

Randomized : $\Omega(n)$ [Kalyanasundaram-Schnitger '92]

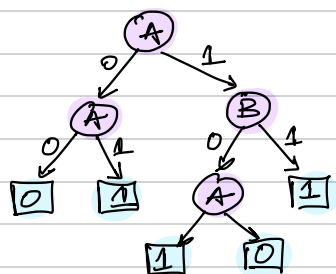
Formal Definition of a "communication protocol" π

Tree-view :

Each internal node labelled either by

- A : function from $X \rightarrow \{0,1\}$
- B : function from $Y \rightarrow \{0,1\}$

Each leaf node labelled with an element from $Z = \{0,1\}$



Value of protocol π on input (x,y) is the label of the leaf reached by starting from the root, and traversing the tree.

Cost of protocol π : (height of the tree)

$$\text{cost}(\pi) = \max \{ \text{cost}(x,y) : x \in X, y \in Y \}$$

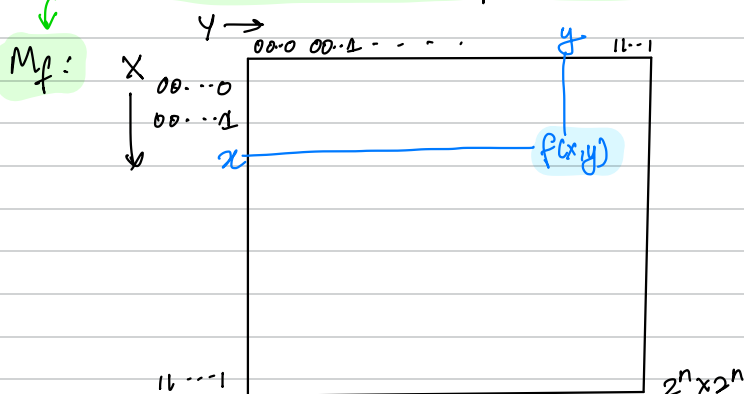
where $\text{cost}(x,y) = \text{path length on input } (x,y)$

Deterministic communication complexity of $f: X \times Y \rightarrow Z$ is

$$D(f) = \min_{\pi_f} \text{cost}(\pi_f)$$

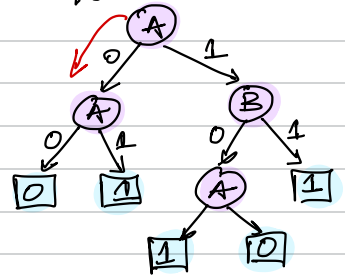
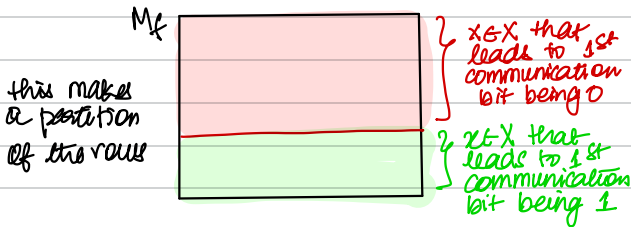
minimum over all protocols π computing f

Communication Matrix to compute $f: X \times Y \rightarrow Z$



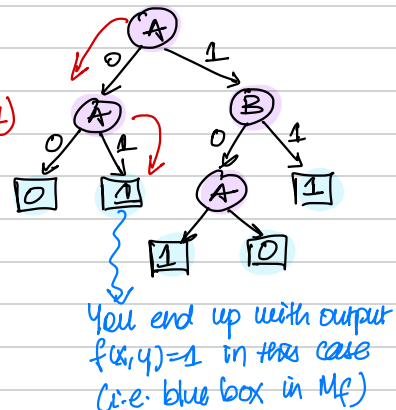
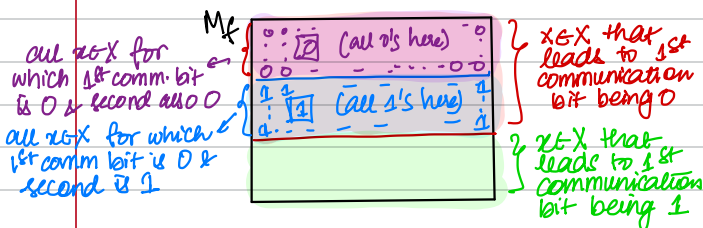
$X = \{0,1\}^n$
 $Y = \{0,1\}^n$
 $Z = \{0,1\}$

Step 1 of the: Say Alice on her input $x \in \{0,1\}^n$ decides to send 0 or 1 (say she sends 0)

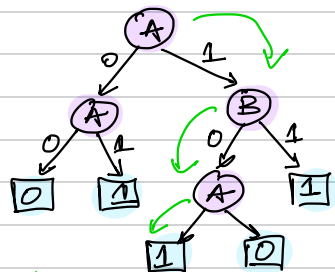
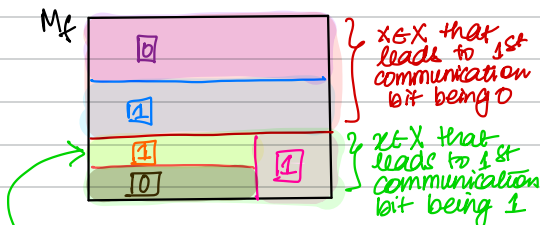


Remark: these need not be consecutive rows, these could be any subset of rows corresponding to 0 & 1.
(Just for illustration, taking consecutive rows)

Step 2 of the: If 0 was the 1st bit communicated by Alice, then the the says she goes again $\rightarrow$ (say she sends 1)



Alternatively: Alice sends 1, Bob sends 0



You will end up with output $f(x,y)=1$ in this case (i.e. yellow box in M_f)

∴ In particular, the colored rectangles above are called "combinatorial rectangles": $R = K \times L$ is a sub-matrix of M_f containing some $K \subseteq X$ & columns $L \subseteq Y$ that are formed based on the particular direction (left (0) or right (1)) taken in the tree corresponding to π .

(Recall remark above: K & L need not be contiguous)

At the end of this partitioning of M_f , the sub-matrix of same color is a constant matrix of all 0's or all 1's.

Theorem I: Any c -bit correct, deterministic protocol for $f: X \times Y \rightarrow \mathbb{Z}$ partitions M_f into $\leq 2^c$ combinatorial rectangles, each of which is " f -monochromatic".

↳ meaning f is constantly 0 or 1 on the rectangle.

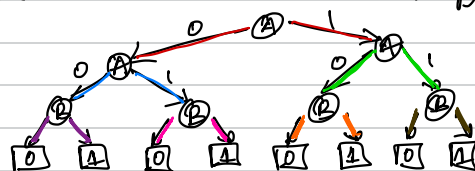
Example: $f = EG_2: \{0,1\}^2 \times \{0,1\}^2 \rightarrow \{0,1\}$

	00	01	10	11
00	1	0	0	0
01	0	1	0	0
10	0	0	1	0
11	0	0	0	1

M_f

(the naïve protocol)

Alice sets x & then Bob sends $f(x,y)$



The naïve protocol leads to $8 (=2^3)$ partitions & has 3-bits of communication.

Theorem $D(EG_n) \geq n+1$ (hence $=n+1$)

Pf: what we will show is that it is not possible to color M_{EG_n} to get small number of combinatorial rectangles.

A general comm-matrix for EG_n has 2^n 1's in the diagonal (just by correctness)

$\{00\} \times \{00\}$
 $\{00\} \times \{01, 10, 11\}$
 $\{01\} \times \{00, 10, 11\}$
 $\{01\} \times \{01\}$
 $\{10\} \times \{00, 01, 11\}$
 $\{10\} \times \{10\}$
 $\{11\} \times \{00, 01, 10\}$
 $\{11\} \times \{11\}$

Clearly, every 1 has to be in its own 1×1 combinatorial rectangle. Why? $\downarrow$

Exercise $\rightarrow$ Simple to prove claim: R is a combinatorial rectangle if and only if whenever $(x, y), (x', y') \in R$, then $(x', y), (x, y') \in R$.

Now, for the 0's we also require ≥ 1 rectangle.

$\Rightarrow \geq 2^{n+1}$ combinatorial rectangles needed.

$\Rightarrow c \geq \lceil \log_2(2^n + 1) \rceil > n \Rightarrow c \geq n+1$ (by Thm I)

Theorem (General lower bound for $D(f)$) Σ Melhorn-Schmidt '82

$$D(f) \geq \log_2 (2 \cdot \text{rank}(M_f) - 1)$$

Proof:

Fix a partition $X \times Y = \bigcup_{i=1}^c R_i$, where $c = D(f)$. Let R_0 & R_1 be sets of all 0-monochromatic rectangles and 1-monochromatic rectangles, respectively, among $R_1, R_2, \dots, R_c$.

Define

$$M_R(x, y) = \begin{cases} 1 & \text{if } (x, y) \in R \text{ for a rectangle } R. \\ 0 & \text{otherwise} \end{cases}$$

$$\text{Then, } M_f = \sum_{R \in R_1} M_R \quad \text{and} \quad M_{\text{not}(f)} = \sum_{R \in R_0} M_R$$

By property of rank,

$$\text{rank}(M_f) \leq \sum_{R \in R_1} \text{rank}(M_R), \quad \text{rank}(M_{\text{not}(f)}) \leq \sum_{R \in R_0} \text{rank}(M_R)$$

$\therefore \text{rank}(M_R)$ is at most 1 (by def of combinatorial rectangle R)

$$\Rightarrow \text{rank}(M_f) \leq |R_1| \quad \& \quad \text{rank}(M_{\text{not}(f)}) \leq |R_0|$$

$$\Rightarrow \text{rank}(M_f) + \text{rank}(M_{\text{not}(f)}) \leq |R_0| + |R_1| = 2^c$$

$$\therefore M_{\text{not}(f)} = J - M_f \quad (J \text{ is all 1's matrix of rank } 1)$$

$$\Rightarrow 2^c \geq 2 \cdot \text{rank}(M_f) - 1$$

$$\Rightarrow D(f) \geq \log_2 (2 \cdot \text{rank}(M_f) - 1)$$

Corollary: $D(\text{DISJINCTNESS}_n) \geq n+1$

$\rightarrow$ (Exercise: write the communication matrix of DISJINCTNESS & use above theorem to prove this corollary.)

Log-Rank Conjecture Szlowski-Saks '88

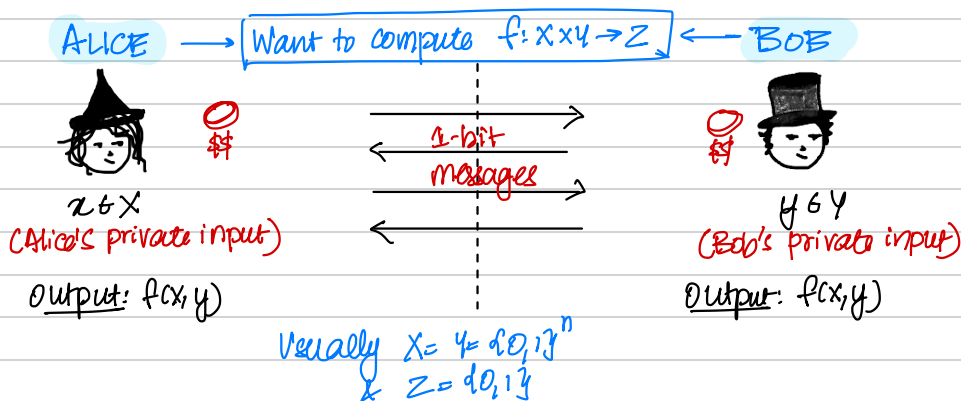
$$D(f) \leq \text{polylog}(\text{rank}(M_f))$$

What is known? (Best lower & upper bounds)

- $\forall f, D(f) \leq O(\sqrt{\text{rank}(M_f)})$ [Lovett '13]
- $\exists f \text{ s.t. } D(f) \geq \Omega(\log^2 \text{rank}(M_f))$ [Göös-Pitassi-Watson '15]

Next class!!

RANDOMIZED COMMUNICATION COMPLEXITY



- Both Alice & Bob have coin flipper in addition
- We still need that $\forall x \in X$ & $\forall y \in Y$, communication is $\leq c$ bits & output $f(x, y)$ with high probability.

Two settings

- public coins (Alice & Bob share public randomness)
- private coins (Alice & Bob have their own coins)

Defn: $R_{\epsilon, \text{priv}}(f) = \# \text{ bits communicated on worst-case input \& randomness for a "private coin" randomized protocol computing } f(x, y) \text{ with prob } \geq 1 - \epsilon \text{ on all inputs.}$

Example (Lecture 10): $R_{\frac{1}{3}, \text{priv}}(\text{EQ}_n) = O(\log n)$

Will continue next class with randomized comm. complexity....