1

Thu 3/28

## Communication Complexity (CC)

Q: How many bits do 2 (or more) parties need to exchange to compute a function on their inputs.

* Whole book written in 1997
  much more work done since then.

CC vs Inf. Theory.

CC → Starting Point: Some problem to be solved (e.g. compute a+b where a, b are the 2 parties).
Q. What needs to be communicated?

Inf. Theory → Starting point: Certain communication needs to take place.
Q. How to carry out the communication? (what code to use, etc).

* Recently, many connections emerged between CC and I.T.

"Most lower bound techniques for CC actually lower bound the information exchange."
(not just # bits exchanged, which could be greater).

Q: Can you make "Most" "all"? (Open Question)

Today: Classic C.C.

Two party CC (Yao '79)

| Alice | | Bob |
|---|---|---|
| has $x$ | $\rightleftarrows$ ⋮ | has $y$ |

(for fixed $f(\cdot,\cdot)$)

in the end both should know $f(x,y)$.

We'll focus on $f: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$.

Q: How many bits need to be exchanged?

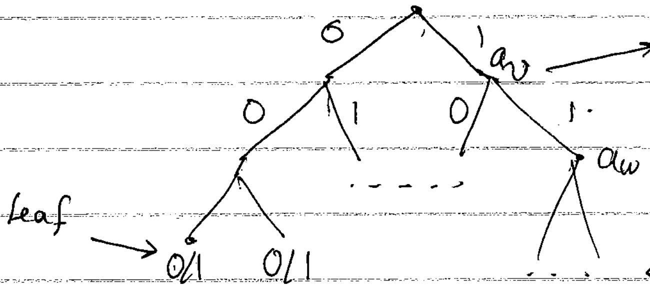
Trivial protocol: Alice sends $x$ to Bob.
Bob responds $f(x,y)$.
$\Rightarrow n+1$ bits.

* CC is useful in:
- Circuit Complexity
- Streaming Computation
- Data structure lower bounds

etc.

* Define a communication protocol (deterministic).
Sequence of instructions:
Given a party's inputs and the bits exchanged so far, determine which bit to send, or output 0/1 for the value of function.

③




labeled by $a_v$ or $b_v$ depending on whose turn it is.

$$\begin{cases} a_v \text{ depends on } (x, \text{transcript}) \\ b_v \quad " \quad " \quad (y, \quad " \quad ) \end{cases}$$

$v$

Protocol $\pi$ correctly computes $f$ if

$\forall (x,y)$, following $\pi$ leads to a leaf

labeled by $f(x,y)$.

For a protocol $\pi$ that correctly computes $f$,

define $CC(\pi, f)$ = depth of the tree.

= max # bits exchanged for any $(x,y)$.

<u>Def.</u> The deterministic CC of $f$,

$$\mathcal{D}(f) = \min_{\substack{\pi \\ \pi \text{ computes } f}} CC(\pi, f).$$

We already saw, $\mathcal{D}(f) \le n+1$.

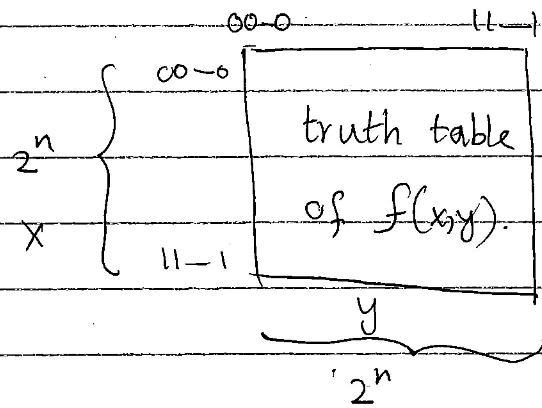
Ex. $f(x,y) = (x = 0^n \text{ or } y = 1^n) \Rightarrow \mathcal{D}(f) \le 2$.

Ex. $f(x,y) = \underbrace{\bigoplus_i x_i}_{\text{Alice knows}} \overbrace{\bigoplus_i y_i}^{\text{Bob knows}}$ , $\mathcal{D}(f) \le 2$.

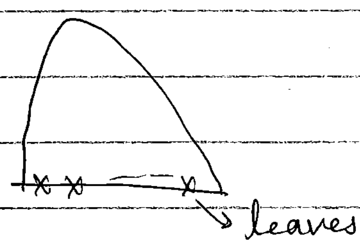
Ex. $f(x,y) = EQ(x,y) = \begin{cases} 1 & x = y \\ 0 & \text{else.} \end{cases}$

Pigeonhole principle shows $n$ bits needed.

Communication problem as a matrix




To prove a lower bound on the depth, it suffices to 〃 〃 〃 〃 〃 〃 # leaves.



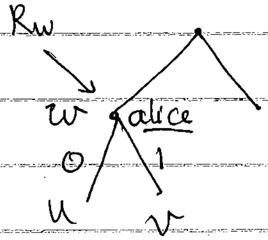

$R_\ell := \{ (x,y) \mid \Pi \text{ leads to } \ell \text{ on input } (x,y) \}$.

Claim, $\forall$ leaves $\ell$, $R_\ell$ is a rectangle.

NB. $R_\ell \subseteq X \times Y$ is a rectangle if $R_\ell = S \times T$ for $S \subseteq X$, $T \subseteq Y$.

In fact, this is true for all nodes and not only leaves!

Proof by induction: (on depth) It's true for the root $R_{root} = X \times Y$.




Now, $R_u = \{(x,y) : (x,y) \in R_w, a_w(x) = 0\}$

Obviously a rectangle! $\square$

Another view: $R$ is a rectangle $\Longleftrightarrow$

$$(x_1,y_1) \in R \wedge (x_2,y_2) \in R \Rightarrow (x_1,y_2) \in R \wedge (x_2,y_1) \in R.$$

This view also proves the claim.

assume $(x_1,y_1),(x_2,y_2) \in R$. Argue that the state of protocol is unchanged for $(x_1,y_2)$ and $(x_2,y_1)$.

$\square$

⑥

Now, lower bound for EQ

Def. A rectangle is $f$-monochromatic if

$\exists b \in \{0,1\}, \forall (x,y) \in R, \quad f(x,y) = b.$

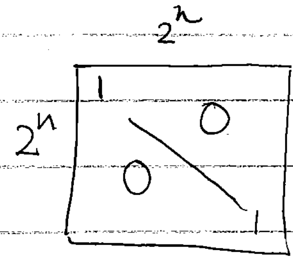
$\Rightarrow$ ① $f$ partitions the space $X \times Y$ into monochromatic rectangles.

② If $\pi$ correctly computes $f$, then each $R_\ell$ (corresponding to leaf $\ell$) must be $f$-monochromatic.

$\therefore$ If $D(f) = c$, then $\exists$ partition of $X \times Y$ into $\underbrace{\ }_{\leq 2^c}$ $f$-monochromatic rectangles.

Contrapositive (Thm): If any partition of $X \times Y$ into $f$-chromatic rectangles needs $\geq t$ rectangles, then $D(f) \geq \lceil \log_2 t \rceil$.

Ex. 1 $\mathcal{D}(EQ)$




Need $\geq 2^n$ rectangles to cover all ones (i.e., we have "a fooling set")

$$\Rightarrow \mathcal{D}(EQ) \geq \lceil \log_2 (2^n + 1) \rceil = n+1.$$

$\square$

**Def.** "Fooling set"

A 0-fooling set is a set of pairs $(x, y) \in f^{-1}(0)$ such that no two of them together are in a monochromatic rectangle.

**Def.** $FS_0(f)$ = max size of a 0-fooling set.

(same for $0 \to 1$).

**Thm:** $\mathcal{D}(f) \geq \lceil \log_2 ( FS_0(f) + FS_1(f)) \rceil$.

(Obvious) $\square$

Exercise: $\mathcal{D}(GT) = n+1$, $GT(x,y) = \begin{cases} 1 & \text{if } x > y \\ 0 & \text{else} \end{cases}$

$(x \in \{0, \dots, 2^n - 1\})$.

Disjointness ("3SAT of CC") (DISJ)

$$DISJ(x,y) = \begin{cases} 1 & \text{if } x \cap y = \phi \\ 0 & \text{else} \end{cases} \quad \text{(as characteristic sets)}$$

also, $DISJ(x,y) = \overline{(x_1 \wedge y_1) \vee (x_2 \wedge y_2) \vee \cdots \vee (x_n \wedge y_n)}$.

Thm: $\mathcal{D}(DISJ) = n+1$.

Proof: Let us prove $FS_1(DISJ)$ is large.

$$\begin{bmatrix} (A,\bar{A}) & ↯ \\ ↯ & (B,\bar{B}) \end{bmatrix} \Rightarrow \{(A,\bar{A}) : A \subseteq \{1,\dots,n\} \text{ is a 1-fooling set}\}$$

$$\Rightarrow \begin{cases} FS_1(DISJ) \geq 2^n \\ FS_0(DISJ) \geq 1 \end{cases}$$

$$\Rightarrow \mathcal{D}(DISJ) \geq \lceil \log_2(2^n + 1) \rceil = n+1.$$

$\square$

* Next time: $IP(x,y) = x_1 y_1 \oplus \cdots \oplus x_n y_n$.

again, $\mathcal{D}(IP) = n+1$.