Communication Complexity

Sushovan Majhi

April 26, 2016

Andrew Chi-Chih Yao
姚期智

Born	December 24, 1946 (age 69) Shanghai, China
Residence	Beijing
Citizenship	United States Taiwan
Fields	Computer science
Institutions	Stanford University Princeton University Tsinghua University Chinese University of Hong Kong
Alma mater	National Taiwan University (BS) Harvard University (AM, PhD) University of Illinois at Urbana–Champaign (PhD)
Known for	Yao's Principle
Notable awards	Pólya Prize (SIAM) (1987) Knuth Prize (1996) Turing Award (2000)

Communication Everywhere

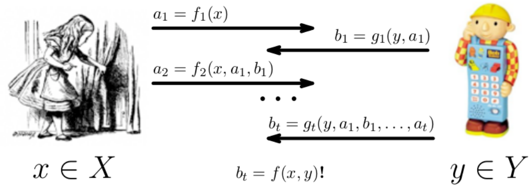
Communcation exists because of the limitation of resources in a single system

Setting Up The Stage

Given a boolean function

$$f : X \times Y \to \{0, 1\}$$

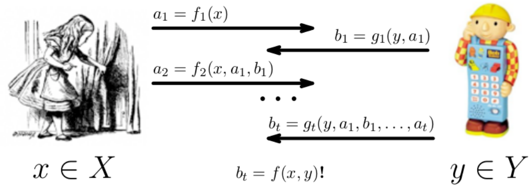
that both Alice and Bob want to compute on an input(x,y).
Let's take $X = Y = \{0, 1\}^n$.



Given a boolean function

$$f : X \times Y \to \{0, 1\}$$

that both Alice and Bob want to compute on an input(x,y).
Let's take $X = Y = \{0, 1\}^n$.



Assumptions

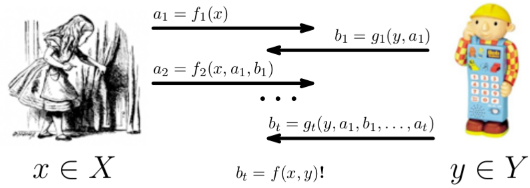
i) We have a two "party" or "player" communication system.

Setting Up The Stage

Given a boolean function

$$f : X \times Y \to \{0, 1\}$$

that both Alice and Bob want to compute on an input(x,y).
Let's take $X = Y = \{0, 1\}^n$.



Assumptions

i) We have a two "party" or "player" communication system.

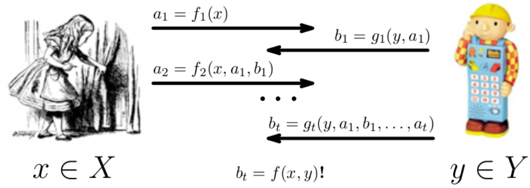
ii) The communication channel is completely secure and noiseless.

Setting Up The Stage

Given a boolean function

$$f : X \times Y \to \{0, 1\}$$

that both Alice and Bob want to compute on an input(x,y).
Let's take $X = Y = \{0, 1\}^n$.



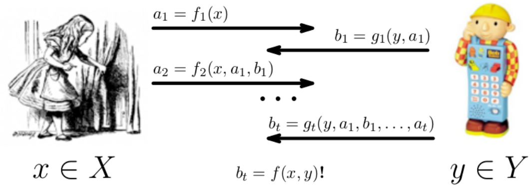
Assumptions

i) We have a two "party" or "player" communication system.
ii) The communication channel is completely secure and noiseless.
iii) The parties have unbounded/infinte computational power.

Given a boolean function

$$f : X \times Y \to \{0,1\}$$

that both Alice and Bob want to compute on an input(x,y).
Let's take $X = Y = \{0,1\}^n$.



Assumptions

i) We have a two "party" or "player" communication system.
ii) The communication channel is completely secure and noiseless.
iii) The parties have unbounded/infinte computational power.
iv) The number of rounds or the size of the sets X, Y are not that important to us.

Measuring The Cost

We are interested in $\mu(A)$ =the number of bits exchanged between Alice and Bob by a protocol A to successfully transmit $f(x, y)$ in the last round for all possbile inputs x and y.

Measuring The Cost

We are interested in $\mu(A)$ =the number of bits exchanged between Alice and Bob by a protocol A to successfully transmit $f(x, y)$ in the last round for all possbile inputs x and y.
We define the communication complexity of f, $C(f) := \min_A \mu(A)$.

Measuring The Cost

We are interested in $\mu(A)$ =the number of bits exchanged between Alice and Bob by a protocol A to successfully transmit $f(x, y)$ in the last round for all possbile inputs x and y.
We define the communication complexity of f, $C(f) := \min_A \mu(A)$.

A Trivial Upper Bound

For any f, $C(f) \leq n + 1$.

Measuring The Cost

We are interested in $\mu(A) =$the number of bits exchanged between Alice and Bob by a protocol A to successfully transmit $f(x, y)$ in the last round for all possbile inputs x and y.
We define the communication complexity of f, $C(f) := \min_A \mu(A)$.

A Trivial Upper Bound

For any f, $C(f) \leq n + 1$.
In the first round Alice shares her part of the input(length n).

Measuring The Cost

We are interested in $\mu(A)$ =the number of bits exchanged between Alice and Bob by a protocol A to successfully transmit $f(x, y)$ in the last round for all possbile inputs x and y.
We define the communication complexity of f, $C(f) := \min_A \mu(A)$.

A Trivial Upper Bound

For any f, $C(f) \leq n + 1$.
In the first round Alice shares her part of the input(length n).
After having access to x, Bob computes the function and shares the output of f in the second round using a single bit.

ExM:1

Given two integers(in binary) x and y of lenth n
$f(x, y)$ decides whether $x + y$ is the binary representation of an EVEN integer.
Can we have a communication protocol that uses less that $n + 1$ bits?

ExM:1

Given two integers(in binary) x and y of lenth n
$f(x, y)$ decides whether $x + y$ is the binary representation of an EVEN integer.
Can we have a communication protocol that uses less that $n + 1$ bits?
Think for a moment.......

ExM:1

Given two integers(in binary) x and y of lenth n
$f(x, y)$ decides whether $x + y$ is the binary representation of an EVEN integer.
Can we have a communication protocol that uses less that $n + 1$ bits?
Think for a moment.......
Indeed, $C(f) \leq 2$

Some Examples

ExM:1

Given two integers(in binary) x and y of lenth n
$f(x, y)$ decides whether $x + y$ is the binary representation of an EVEN integer.
Can we have a communication protocol that uses less that $n + 1$ bits?
Think for a moment.......
Indeed, $C(f) \leq 2$

ExM:2

Given two integers(in binary) x and y of lenth n, $f(x, y)$ decides whether $x + y$ is divisible by 2016.

ExM:1

Given two integers(in binary) x and y of lenth n
$f(x, y)$ decides whether $x + y$ is the binary representation of an EVEN integer.
Can we have a communication protocol that uses less that $n + 1$ bits?
Think for a moment.......
Indeed, $C(f) \leq 2$

ExM:2

Given two integers(in binary) x and y of lenth n, $f(x, y)$ decides whether $x + y$ is divisible by 2016.
Can we have a communication protocol that uses less that $n + 1$ bits?

Some Examples

ExM:1

Given two integers(in binary) x and y of lenth n
$f(x, y)$ decides whether $x + y$ is the binary representation of an EVEN integer.
Can we have a communication protocol that uses less that $n + 1$ bits?
Think for a moment.......
Indeed, $C(f) \leq 2$

ExM:2

Given two integers(in binary) x and y of lenth n, $f(x, y)$ decides whether $x + y$ is divisible by 2016.
Can we have a communication protocol that uses less that $n + 1$ bits?
Think for a moment.......

Some Examples

ExM:1

Given two integers(in binary) x and y of lenth n
$f(x, y)$ decides whether $x + y$ is the binary representation of an EVEN integer.
Can we have a communication protocol that uses less that $n + 1$ bits?
Think for a moment.......
Indeed, $C(f) \leq 2$

ExM:2

Given two integers(in binary) x and y of lenth n, $f(x, y)$ decides whether $x + y$ is divisible by 2016.
Can we have a communication protocol that uses less that $n + 1$ bits?
Think for a moment.......
$C(f) \leq \log(2016) + 1$.

ExM:1

Given two integers(in binary) x and y of lenth n
$f(x, y)$ decides whether $x + y$ is the binary representation of an EVEN integer.
Can we have a communication protocol that uses less that $n + 1$ bits?
Think for a moment.......
Indeed, $C(f) \leq 2$

ExM:2

Given two integers(in binary) x and y of lenth n, $f(x, y)$ decides whether $x + y$ is divisible by 2016.
Can we have a communication protocol that uses less that $n + 1$ bits?
Think for a moment.......
$C(f) \leq \log(2016) + 1$.
Round one: Alice divids x by 2016 and sends the remainder r to Bob!
Round two: Bob checks divisibility of $(y + r)$ by 2016 and sends it back to Alice!
Hence, $C(f) \in O(1)$!

Fix n.
Let $x,y \in \{0,1\}^n$.

$$H(x,y) = \begin{cases} 1 & \text{if } x = 1^n \text{ and } y \text{ is a Turing machine that halts on the input } x \\ 0 & \text{otherwise} \end{cases}$$

The Halting Problem

Fix n.
Let x,$y \in \{0,1\}^n$.

$$H(x,y) = \begin{cases} 1 & \text{if } x = 1^n \text{ and } y \text{ is a Turing machine that halts on the input } x \\ 0 & \text{otherwise} \end{cases}$$

$C(f) \leq 2$

Round one: Alice confirms whether x is of the form 1^n.
Round two: Bob determines whether the Turing machine halts on x.
Remember: Alice and Bob have unbounded computational power, including the ability to decide the Halting Problem.

Lower Bound

EQ

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

Lower Bound

EQ

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

$C(EQ) \geq n$

Yao proved it.

Lower Bound Methods

Fooling Set

We say that a function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ has a size M fooling set if there is an M-sized subset $S \subset \{0,1\}^n \times \{0,1\}^n$ and a value $b \in \{0,1\}$ such that

Fooling Set

We say that a function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ has a size M fooling set if there is an M-sized subset $S \subset \{0,1\}^n \times \{0,1\}^n$ and a value $b \in \{0,1\}$ such that
(1) for every $< x, y > \in S, f(x,y) = b$ and

Fooling Set

We say that a function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ has a size M fooling set if there is an M-sized subset $S \subset \{0,1\}^n \times \{0,1\}^n$ and a value $b \in \{0,1\}$ such that
(1) for every $< x, y > \in S, f(x,y) = b$ and
(2) for every distinct $< x, y >, < x', y' > \in S$, either $f(x,x') \neq b$ or $f(x',y) \neq b$.

Fooling Set

We say that a function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ has a size M fooling set if there is an M-sized subset $S \subset \{0,1\}^n \times \{0,1\}^n$ and a value $b \in \{0,1\}$ such that
(1) for every $< x, y > \in S, f(x,y) = b$ and
(2) for every distinct $< x, y >, < x', y' > \in S$, either $f(x,x') \neq b$ or $f(x',y) \neq b$.

Disjointness

Input strings x, y can be interpreted as characteristic vectors of subsets of $\{1, 2, ..., n\}$.

$$DISJ(x,y) = \begin{cases} 1 & \text{if these two subsets are disjoint} \\ 0 & \text{otherwise} \end{cases}$$

Fooling Set

We say that a function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ has a size M fooling set if there is an M-sized subset $S \subset \{0,1\}^n \times \{0,1\}^n$ and a value $b \in \{0,1\}$ such that
(1) for every $< x, y >\in S, f(x,y) = b$ and
(2) for every distinct $< x, y >, < x', y' >\in S$, either $f(x,x') \neq b$ or $f(x',y) \neq b$.

Disjointness

Input strings x, y can be interpreted as characteristic vectors of subsets of $\{1, 2, ..., n\}$.

$$DISJ(x,y) = \begin{cases} 1 & \text{if these two subsets are disjoint} \\ 0 & \text{otherwise} \end{cases}$$

$$S = \left\{ (A, \overline{A}) : A \subset \{1, 2, ..., n\} \right\}$$

is a fooling set of size 2^n.

Theorem

If f has a size-M fooling set then $C(f) \geq \log M$.

Fooling Set Method:Theorem

Theorem

If f has a size-M fooling set then $C(f) \geq \log M$.

Corollary

1) $C(DISJ) \geq n$
2) $C(EQ) \geq n$

$M(f) = 2^n \times 2^n$ matrix of f.

$M(f) = 2^n \times 2^n$ matrix of f.

Definition

An f-monochromatic tiling of $M(f)$ is a partition of $M(f)$ into disjoint monochromatic rectangles.
We denote by $\chi(f)$ the minimum number of rectangles in any monochromatic tiling of $M(f)$.

$M(f) = 2^n \times 2^n$ matrix of f.

Definition

An f-monochromatic tiling of $M(f)$ is a partition of $M(f)$ into disjoint monochromatic rectangles.
We denote by $\chi(f)$ the minimum number of rectangles in any monochromatic tiling of $M(f)$.

Theorem

If f has a fooling set with m pairs, then $\chi(f) \geq m$.

$M(f) = 2^n \times 2^n$ matrix of f.

Definition

An f-monochromatic tiling of $M(f)$ is a partition of $M(f)$ into disjoint monochromatic rectangles.
We denote by $\chi(f)$ the minimum number of rectangles in any monochromatic tiling of $M(f)$.

Theorem

If f has a fooling set with m pairs, then $\chi(f) \geq m$.
Also, we have $C(f) \geq \log \chi(f)$

$M(f) = 2^n \times 2^n$ matrix of f.

Definition

An f-monochromatic tiling of $M(f)$ is a partition of $M(f)$ into disjoint monochromatic rectangles.
We denote by $\chi(f)$ the minimum number of rectangles in any monochromatic tiling of $M(f)$.

Theorem

If f has a fooling set with m pairs, then $\chi(f) \geq m$.
Also, we have $C(f) \geq \log \chi(f)$
One can also show that
$\log \chi(f) \leq C(f) \leq (\log \chi(f))^2$

Definition

For every function f, $\chi(f) \geq rank(M(f))$.

Summary

Results

1. $$\log_2 rank(M(f)) \leq \log_2 \chi(f) \leq C(f) \leq (n+1)$$

Summary

Results

1. $$\log_2 rank(M(f)) \leq \log_2 \chi(f) \leq C(f) \leq (n+1)$$

2. Also,
$$\log_2 \chi(f) \leq C(f) \leq 16(\log_2 \chi(f))^2$$

Summary

Results

1. $$\log_2 rank(M(f)) \leq \log_2 \chi(f) \leq C(f) \leq (n+1)$$

2. Also,
$$\log_2 \chi(f) \leq C(f) \leq 16(\log_2 \chi(f))^2$$

3. There is a constant $c > 1$ such that,
$$C(f) \in O(\log_2 (rank(M(f)))^c)$$
for all f and for all input size n.
The rank is taken over the reals.

Results

1. $$\log_2 rank(M(f)) \leq \log_2 \chi(f) \leq C(f) \leq (n+1)$$

2. Also,
$$\log_2 \chi(f) \leq C(f) \leq 16(\log_2 \chi(f))^2$$

3. There is a constant $c > 1$ such that,
$$C(f) \in O(\log_2 (rank(M(f)))^c)$$
for all f and for all input size n.
The rank is taken over the reals. It's still a conjecture!

Variants

1. Multiparty games

Variants

1. Multiparty games
2. Nondeterministic communication protocols

References

a. “Communication Complexity”, Eyal Kushilevitz, Noam Nisan

b. “Computational Complexity”, Arora, Barak

c. “1979 Yao”,

Thank You!