Communication Complexity and its application to lower bound

Fiorini, Samuel, et al. “Exponential lower bounds for polytopes in combinatorial optimization.”

Presented by Binghui Peng

Outline of this talk

- An introduction to communication complexity
- A central problem ---- Set Disjointness
- Application to prove lower bound

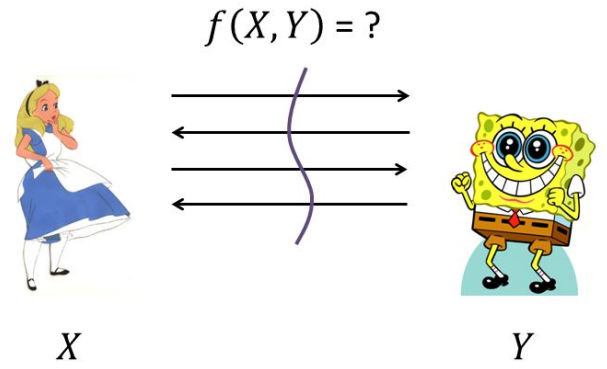
Communication complexity

- Started by Andrew Yao
- Some complexity questions related to distributive computing STOC(1979)
- Goal:
  - A simple, clean model for deriving lower bound.
  - Capture computational bottlenecks in certain problem and provide useful tool for resolving complexity issue
  - Derive Unconditional lower bound

Basic model

- Two party, Alice and Bob, get x, y separately, unknown to each other
- Goal: compute f(x, y): $\{0,1\}^m \times \{0,1\}^n \rightarrow \{0,1\}$
- Only concerned about communication issue

Motivation: Communication Complexity



Yao '79, **"Some complexity questions related to distributive computing"**

Case study

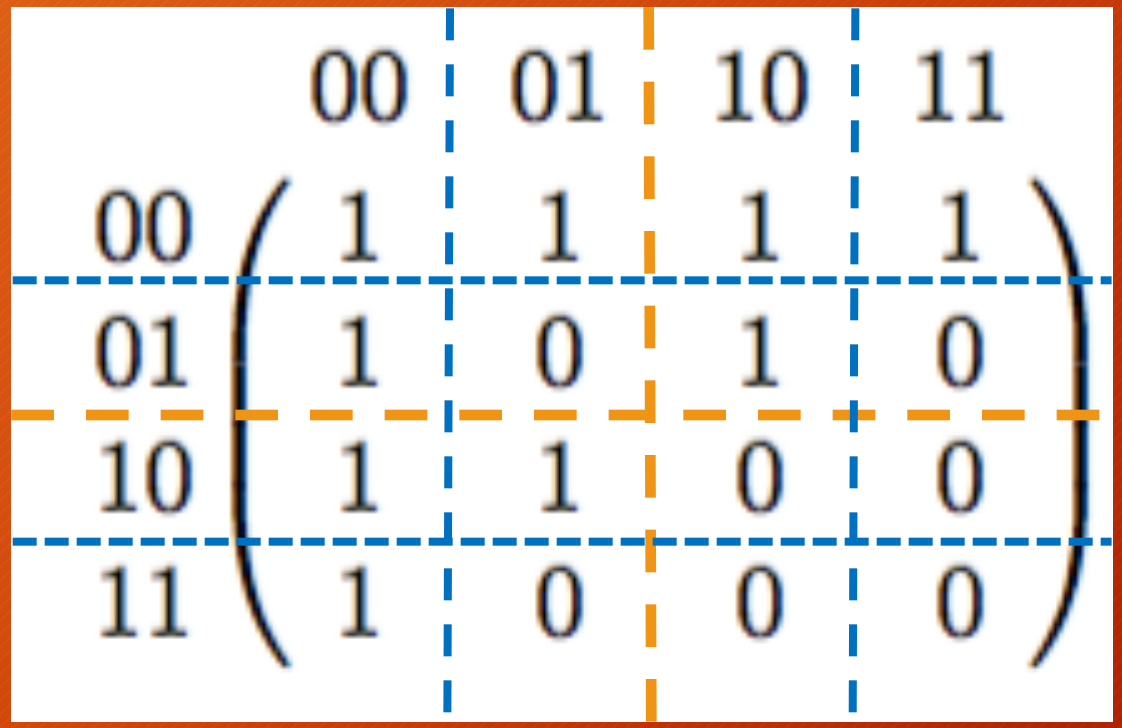
- EQUALITY: f(x, y) = 1 if and only if x = y
- One way protocol:
  - Alice send some bits to Bob only once
  - Bob output answer
- Trivial solution: send O(n) bits
- Lower bound? $\Omega(n)$
- Pigeonhole principle

Case study

- EQUALITY: $f(x, y) = 1$ if and only if $x = y$
- Deterministic protocol
  - Message can be sent in multiple round
  - The message sent only depend on current transcript and own input

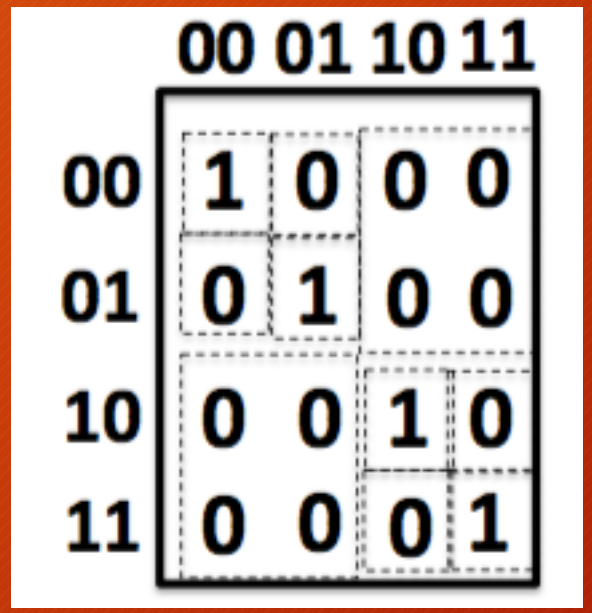
Case study

- Deterministic protocol
- Lemma 1 (Rectangles) For every transcript z of a deterministic protocol P, the set of inputs (x, y) that generate z are a rectangle, of the form $A \times B$ for $A \subseteq X$ and $B \subseteq Y$.
- Lemma 4.2 If a deterministic protocol P computes a function f, then every rectangle induced by P is monochromatic in the matrix M(f).


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

Case study

- Theorem 1. Let f be a function such that every covering of M(f) into monochromatic rectangles requires at least t rectangles. Then the deterministic communication complexity of f is at least $\log_2 t$
- Corollary: The deterministic communication complexity of Equality is at least n



More on deterministic protocol

- Fooling set method
- Rectangle size bound
- Rank bound
- Discrepancy

Case study

- EQUALITY: f(x, y) = 1 if and only if x = y
- Randomized protocol
  - Message can be sent in multiple round
  - The message sent only depend on current transcript and own input, as well as public coin
- Public coin: random coin can be seen by both party
- Two side error, constant error rate

Case study

- Protocol: O(1)
- Alice just calculate $a_1 x_1 + \cdots + a_n x_n \pmod 2$ and send it to Bob, where $a_1, \cdots, a_n \in \{0,1\}$ are output by random coin
- Bob calculate $a_1 y_1 + \cdots + a_n y_n \pmod 2$ and compare the bit received, output 0 if not equal
- Repeat the process for constant times
- Bob output 1

Case study

- What about private coin? i.e. the message can depend random coin can not be seen by other party
- We compute $x_1 + x_2 z + \cdots + x_n z^{n-1}$ (mod p) for some pre-determined prime number p, 2n < p < 4n, z < n is the random number generate by private coin
- Send z as well as $x_1 + x_2 z + \cdots + x_n z^{n-1}$ O(log(n))
- If $x_1 \cdots x_n \neq y_1 \cdots y_n$, Bob still have at least 50% chance to figure out inequality in one round. Why?
- The number of root to $(x_1 - y_1) + (x_2 - y_2)z + \cdots + (x_n - y_n)z^{n-1}$ is at most n/p < ½

- Actually, we have...
- Theorem(Newman 1991) If there is a public-coin protocol for a function f with n-bit inputs that has two-sided error 1/3 and communication cost c, then there is a private-coin protocol for the problem that has two-sided error 1/3 and communication cost $O(c + \log n)$.

Case study

- Lower bound for private coin is $\Omega(\log_2 n)$
- Generally, proving lower bound for randomize protocol would be hard
- Yao's minmax principle
- In order to derive a lower bound for randomize protocol, we can construct a hard distribution and consider all deterministic protocol.

Outline of this talk

- An introduction to communication complexity
- A central problem ---- Disjointness
- Application to prove lower bound

Central problem---DISJOINTNESS

- Definition: DISJ(x,y) = 0 if there is an index $i \in \{1, 2, \cdots, n\}$, with $x_i = y_i = 1$, and DISJ(x, y) = 1 otherwise.
- Tim Roughgarden says “If you only remember one problem that is hard for communication protocols, it should be the disjointness problem.”
- Various technique has been develop for Disjointness problem.

Results on Disjointness

Determinitic	$\Omega(n)$
Randomize	$\Omega(\sqrt{n})$(Babai et al. 1986) $\Omega(n)$ (Razborov (1992)
Nondeterministic	$\Omega(n)$
Multiparty(deterministic&randomize)	$\Omega\left(\frac{n}{k}\right)$ (Radhakrishnan 2002) (Gronemeier, 2009)

Outline of this talk

- An introduction to communication complexity
- A central problem ---- Disjointness
- Application to prove lower bound

Application to lower bound

- Streaming algorithm
- Data structure
- Property testing
- Algorithmic game theory
- Extension Complexity

Extension Complexity

An extended formulation (EF) of a polytope $P \subseteq R^d$ is a linear system

$$E^{=}x + F^{=}y = g^{=}, E^{\leq}x + F^{\leq}y \leq g^{\leq}$$

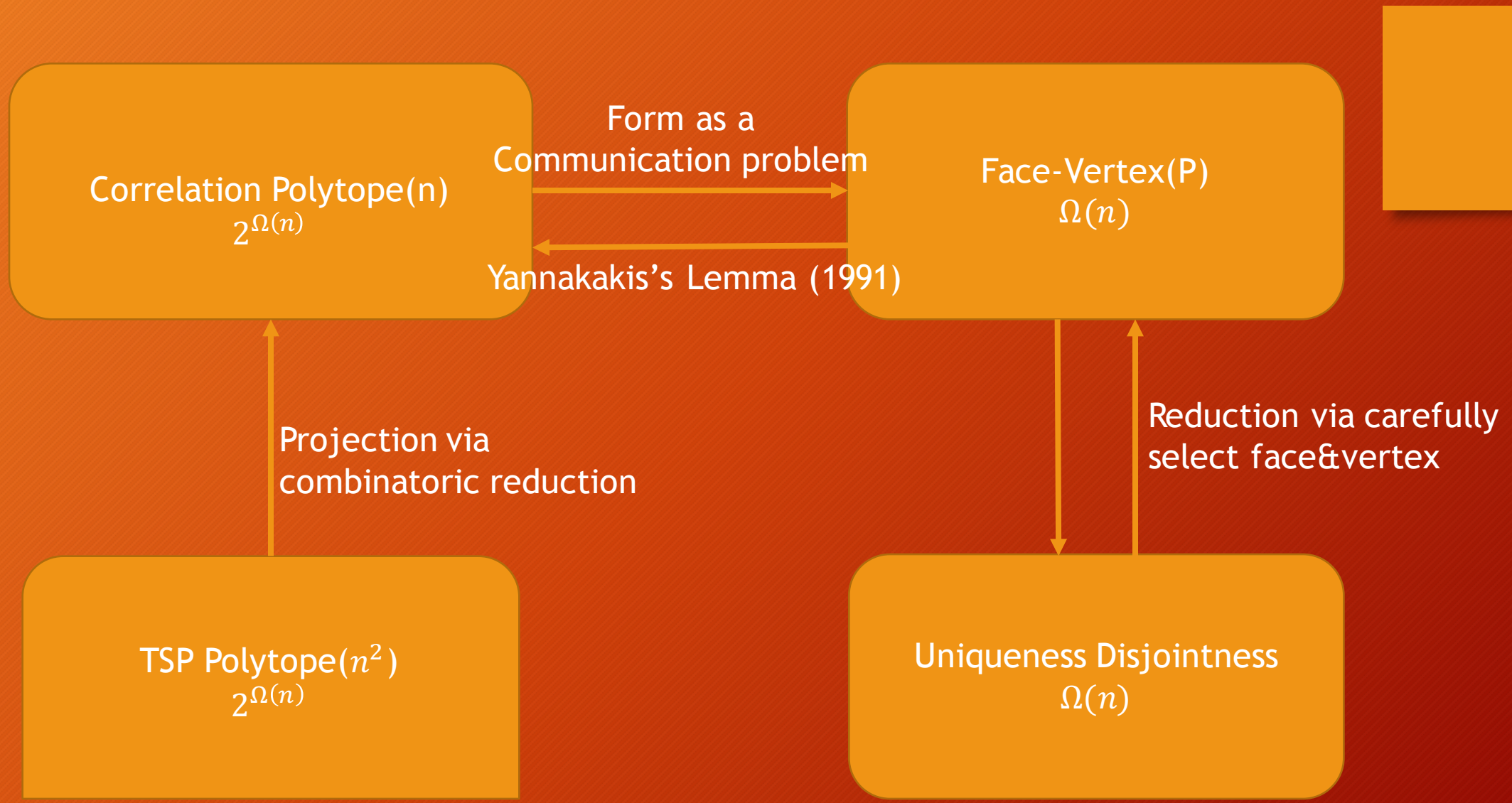
for variables $(x, y) \in R^{d+r}$, where $E^{=}, E^{\leq}, F^{\leq}, F^{=}$ are real matrices with d,k,d,k columns respectively, and $g^{=}, g^{\leq}$ are column vectors, such that $x \in P$ if and only if there exists y such the above constraints holds.

The size of an EF is defined as the number of inequalities in the system

Basically, the extension complexity capture the minimum number of linear inequality to describe convex hull of some vertex.

- We want exponential bound for extension complexity for NPC problem.
- Necessary condition for $P \neq NP$
- Actually, Rothvob(2014) proved that every extended formulation of the convex hull of the perfect matchings of the complete graph has exponential size.

- Theorem (Fiorini 2015) The extension complexity of the TSP polytope TSP(n) is $2^{\Omega(\sqrt{n})}$


Correlation Polytope(n)
$2^{\Omega(n)}$
Form as a
Communication problem
Yannakakis's Lemma (1991)
Face-Vertex(P)
$\Omega(n)$
Projection via
combinatoric reduction
Reduction via carefully
select face&vertex
TSP Polytope(n^2)
$2^{\Omega(n)}$
Uniqueness Disjointness
$\Omega(n)$

Reference

- Tim Roughgarden’s lecture note: http://theory.stanford.edu/~tim/w15/w15.html
- Fiorini, Samuel, et al. "Exponential lower bounds for polytopes in combinatorial optimization.”
- Sherstov, Alexander A. "Communication complexity theory: Thirty-five years of set disjointness.”
- Yao, Andrew Chi-Chih. "Some complexity questions related to distributive computing

“

Thanks for listening!

”