Partition Bound and Information Complexity are quadratically tight for product distributions

Prahladh Harsha
tifr

Rahul Jain
CQT | Centre for Quantum Technologies

Jaikumar Radhakrishnan
tifr

ICALP 2016

July 12, 2016

This work:
Understand the power of different lower bound methods in communication complexity

2-party communication complexity

$$f : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$$

$x \in \mathcal{X}$

$\vdots$

M

$f(x, y)$

$y \in \mathcal{Y}$

2-party communication complexity

$x \in \mathcal{X}$

$f : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$

$\longrightarrow$

$\longleftarrow$

$\vdots$

M

$\longleftarrow$

$f(x, y)$

$y \in \mathcal{Y}$

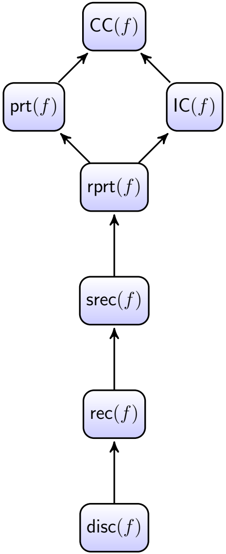
randomized communication complexity:

$$\mathsf{CC}_\epsilon(f) = \min_{\Pi} \max_{(x,y)} (\text{number of bits communicated})\,.$$

Known Lower Bounds

f – function	$\mathrm{CC}_{1/4}(f)$	Lower Bound Method
Inner Product	$\Omega(n)$	Discrepancy [CG '85]
Disjointness	$\Omega(n)$	Corruption/Rectangle Bound [KS '92, Raz '92] Information Complexity [BJKS '02]
Tribes	$\Omega(n)$	Information Complexity [JKS '03] Smooth Rectangle Bound [HJ '13]
Gap-Hamming	$\Omega(n)$	Smooth Rectangle Bound [CR '12]

Comparison of Lower Bounds



Motivating Question:

How tight (or weak) are these lower bound methods?

Motivating Question:

How tight (or weak) are these lower bound methods?

Equivalently, can $\mathrm{CC}(f)$ be upper bounded as some (possibly polynomial) function of these lower bounds?

Motivating Question:

How tight (or weak) are these lower bound methods?

Equivalently, can $\mathsf{CC}(f)$ be upper bounded as some (possibly polynomial) function of these lower bounds?

For instance, is $\mathsf{CC}_{1/4}(f) = \text{poly}(\mathsf{IC}_{1/4}(f), \log n)$?

Distributional Communication Complexity

$$(X, Y) \leftarrow \mu$$

X

$$\xrightarrow{\hspace{6em}}$$

$$\xleftarrow{\hspace{6em}}$$

$$\vdots$$

$$M$$

$$\xleftarrow{\hspace{6em}}$$

$$f(X, Y)$$

Y

distributional communication complexity:

$$\mathsf{CC}^{\mu}_{\epsilon}(f) = \min_{\Pi} \max_{(x,y)} (\text{number of bits communicated})\,.$$

Distributional Communication Complexity

$$(X, Y) \leftarrow \mu$$

X

$\longrightarrow$

$\longleftarrow$

$\vdots$

M

$\longleftarrow$

$f(X, Y)$

Y

distributional communication complexity:

$$\mathsf{CC}_\epsilon^\mu(f) = \min_\Pi \max_{(x,y)} (\text{number of bits communicated})\,.$$

Yao's minmax principle: $\mathsf{CC}_\epsilon(f) = \max_\mu \mathsf{CC}_\epsilon^\mu(f)$.

Information Complexity

X

$(X, Y) \leftarrow \mu$

$\vdots$

M

$f(X, Y)$

Y

$$\mathsf{IC}^{\mu}(\Pi) = I[X : M|Y] + I[Y : M|X]$$

$$\mathsf{IC}^{\mu}_{\epsilon}(f) = \min_{\Pi} \mathsf{IC}^{\mu}(\Pi)$$

$$\mathsf{IC}_{\epsilon}(f) = \max_{\mu} \mathsf{IC}^{\mu}_{\epsilon}(f)$$

Easy to check that, $\mathsf{CC}_{\epsilon}(f) = \max_{\mu} \mathsf{CC}^{\mu}_{\epsilon}(f) \geq \max_{\mu} \mathsf{IC}^{\mu}_{\epsilon}(f) = \mathsf{IC}_{\epsilon}(f)$.

Question: $\mathsf{CC}(f)$ vs. $\mathsf{IC}(f)$?

How tight (or weak) a lower bound is $\mathsf{IC}(f)$?

Question: $\mathsf{CC}(f)$ vs. $\mathsf{IC}(f)$?

How tight (or weak) a lower bound is $\mathsf{IC}(f)$?

$$\mathsf{CC}_\epsilon(f) = \mathsf{poly}(\mathsf{IC}_\epsilon(f), \log n) \qquad ?$$

Protocol Compression Results [BBCR '10]

Product Distributions: μ – product distribution

$\exists$ protocol Π that computes f with $\mathrm{IC}^{\mu}(\Pi) = I$ and $\mathrm{CC}^{\mu}(\Pi) = C$

Protocol Compression Results [BBCR '10]

Product Distributions: μ – product distribution

$$\exists \text{ protocol } \Pi \text{ that computes } f \text{ with } \mathsf{IC}^{\mu}(\Pi) = I \text{ and } \mathsf{CC}^{\mu}(\Pi) = C$$

$$\Downarrow$$

$$\exists \text{ protocol } \Pi' \text{ that computes } f \text{ with } \mathsf{CC}^{\mu}(\Pi') = O(I \cdot \text{polylog } C).$$

Protocol Compression Results [BBCR '10]

Product Distributions: μ – product distribution

$$\exists \text{ protocol } \Pi \text{ that computes } f \text{ with } \mathrm{IC}^{\mu}(\Pi) = I \text{ and } \mathrm{CC}^{\mu}(\Pi) = C$$

$$\Downarrow$$

$$\exists \text{ protocol } \Pi' \text{ that computes } f \text{ with } \mathrm{CC}^{\mu}(\Pi') = O(I \cdot \text{polylog } C).$$

General Distributions: μ – arbitrary distribution

$$\exists \text{ protocol } \Pi \text{ that computes } f \text{ with } \mathrm{IC}^{\mu}(\Pi) = I \text{ and } \mathrm{CC}^{\mu}(\Pi) = C$$

$$\Downarrow$$

$$\exists \text{ protocol } \Pi' \text{ that computes } f \text{ with } \mathrm{CC}^{\mu}(\Pi') = O(\sqrt{I \cdot C}).$$

Counterexample to Protocol Compression [GKR '14-15]

For every $k \in \mathbb{N}$, there exists a function f and a (non-product) distribution μ such that

Counterexample to Protocol Compression [GKR '14-15]

For every $k \in \mathbb{N}$, there exists a function f and a (non-product) distribution μ such that

- $\exists$ a protocol Π that computes f s.t. $\mathsf{IC}^{\mu}(f) = O(k)$

Counterexample to Protocol Compression [GKR '14-15]

For every $k \in \mathbb{N}$, there exists a function f and a (non-product) distribution μ such that

- $\exists$ a protocol Π that computes f s.t. $\mathsf{IC}^{\mu}(f) = O(k)$
- Any protocol Π' that computes f satisfies $\mathsf{CC}^{\mu}(\Pi') = 2^{\Omega(k)}$.

Counterexample to Protocol Compression [GKR '14-15]

For every $k \in \mathbb{N}$, there exists a function f and a (non-product) distribution μ such that

- $\exists$ a protocol Π that computes f s.t. $\mathsf{IC}^{\mu}(f) = O(k)$ & $\mathsf{CC}^{\mu}(f) = 2^{2^{\Theta(k)}}$
- Any protocol Π' that computes f satisfies $\mathsf{CC}^{\mu}(\Pi') = 2^{\Omega(k)}$.

Note:
Does not rule out a BBCR-style compression result for general distributions?

Better compression for product distributions?

- Can the protocol compression result for product distributions be improved? (i.e., can the dependence on $\log C$ be removed?)

Better compression for product distributions?

- Can the protocol compression result for product distributions be improved? (i.e., can the dependence on $\log C$ be removed?)

– OR —

- Can a GKR-type counterexample be obtained for product distributions?

Better compression for product distributions?

- Can the protocol compression result for product distributions be improved? (i.e., can the dependence on $\log C$ be removed?)

“YES”

– OR —

- Can a GKR-type counterexample be obtained for product distributions?

Result: “Better” compression for product distributions

For any product distribution μ,

Result: “Better” compression for product distributions

For any product distribution μ,

Result 1: [Information Complexity]

$$\mathsf{CC}^{\mu}_{1/4}(f) = O\left((\mathsf{IC}(f))^2 \cdot \text{polylog } \mathsf{IC}(f)\right).$$

Result: "Better" compression for product distributions

For any product distribution μ,

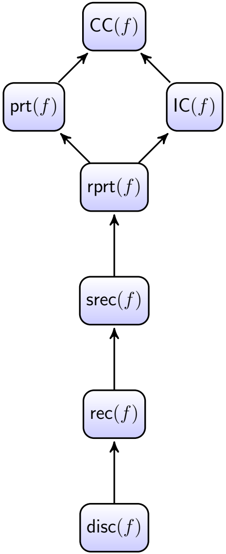
Result 1: [Information Complexity]

$$\mathsf{CC}^{\mu}_{1/4}(f) = O\left((\mathsf{IC}(f))^2 \cdot \text{polylog}\, \mathsf{IC}(f)\right).$$

Result 2: [Partition Bound]

$$\mathsf{CC}^{\mu}_{1/4}(f) = O\left((\mathsf{prt}(f))^2 \cdot \text{polylog}\, \mathsf{prt}(f)\right).$$

Smooth Rectangle (srec)



Smooth Rectangle (srec)

For $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$,

$$\mathsf{srec}_{\epsilon,\delta}(f) := \max\{\mathsf{srec}^{z}_{\epsilon,\delta}(f) : z \in \mathcal{Z}\},$$

where $\mathsf{srec}^{z}_{\epsilon,\delta}(f)$ is defined as

$$\begin{aligned}
\mathsf{srec}^{z}_{\varepsilon,\delta}(f) = \quad & \min \sum_{R} w_R \\
& \sum_{R:(x,y)\in R} w_R \geq 1-\epsilon, && \forall (x,y) \in f^{-1}(z) \\
& \sum_{R:(x,y)\in R} w_R \leq \delta, && \forall (x,y) \notin f^{-1}(z) \\
& \sum_{R:(x,y)\in R} w_R \leq 1, && \forall (x,y) \\
& w_R \geq 0, && \forall R\ .
\end{aligned}$$

Result in terms of Smooth Rectangle

For any product distribution μ,

$$\text{Suppose there exists } k \text{ s.t. } \mathrm{srec}^{\mu}_{\epsilon}(f) \leq k \text{ for } \epsilon = \frac{1}{k^5}$$

$$\Downarrow$$

$$\mathrm{CC}^{\mu}_{1/4}(f) = O(k^2).$$

Result in terms of Smooth Rectangle

For any product distribution μ,

$$\text{Suppose there exists } k \text{ s.t. } \mathsf{srec}^{\mu}_{\epsilon}(f) \leq k \text{ for } \epsilon = \frac{1}{k^5}$$

$$\Downarrow$$

$$\mathsf{CC}^{\mu}_{1/4}(f) = O(k^2).$$

Comments:

- Above result requires srec with low-error. However, error-reduction for srec not known

Result in terms of Smooth Rectangle

For any product distribution μ,

$$\text{Suppose there exists } k \text{ s.t. } \mathsf{srec}_{\epsilon}^{\mu}(f) \leq k \text{ for } \epsilon = \frac{1}{k^5}$$
$$\Downarrow$$
$$\mathsf{CC}_{1/4}^{\mu}(f) = O(k^2).$$

Comments:

- Above result requires srec with low-error. However, error-reduction for srec not known
- Using the fact that error for IC and prt can be reduced and srec $\leq$ prt and srec $\leq$ IC, we obtain results in previous slide.

Related & Subsequent Work

For product distributions μ,

Related & Subsequent Work

For product distributions μ,

- Kol [Kol '16] independently and in parallel proved the following related result

$$\mathsf{CC}^{\mu}(f) = O\left((\mathsf{IC}^{\mu}(f))^2 \cdot \mathsf{polylog}\ \mathsf{IC}^{\mu}(f)\right).$$

Related & Subsequent Work

For product distributions μ,

- Kol [Kol '16] independently and in parallel proved the following related result

$$\mathsf{CC}^{\mu}(f) = O\left((\mathsf{IC}^{\mu}(f))^2 \cdot \text{polylog}\ \mathsf{IC}^{\mu}(f)\right).$$

- Two weeks ago, Sherstov [She '16] improved the above to

$$\mathsf{CC}^{\mu}(f) = O\left(\mathsf{IC}^{\mu}(f) \cdot \text{polylog}\ \mathsf{IC}^{\mu}(f)\right).$$

Open Questions

Open Questions

- Error-reduction for srec? This would imply, for product μ

$$\mathsf{CC}^{\mu}(f) = O\left(\mathsf{srec}^{\mu}(f) \cdot \log \mathsf{srec}^{\mu}(f)\right)^{2} \ ?$$

Open Questions

- Error-reduction for srec? This would imply, for product μ

$$\mathsf{CC}^{\mu}(f) = O\left(\mathsf{srec}^{\mu}(f) \cdot \log \mathsf{srec}^{\mu}(f)\right)^2 \ ?$$

- A la Sherstov for srec? I.e., for product μ,

$$\mathsf{CC}^{\mu}(f) = O\left(\mathsf{srec}^{\mu}(f) \cdot \text{polylog}\, \mathsf{srec}^{\mu}(f)\right)?$$

Open Questions

- Error-reduction for srec? This would imply, for product μ

$$\mathsf{CC}^{\mu}(f) = O\left(\mathsf{srec}^{\mu}(f) \cdot \log \mathsf{srec}^{\mu}(f)\right)^2 \ ?$$

- A la Sherstov for srec? I.e., for product μ,

$$\mathsf{CC}^{\mu}(f) = O\left(\mathsf{srec}^{\mu}(f) \cdot \mathsf{polylog}\, \mathsf{srec}^{\mu}(f)\right)?$$

- For general distributions μ,

$$\mathsf{CC}^{\mu}(f) = \mathsf{poly}(\mathsf{IC}(f), \log n)?$$

Thank You