Title: Applications of Information Theory in Direct Sum and Direct Product Problems

Date: Feb 12, 2014 04:00 PM

URL: http://pirsa.org/14020142

Abstract: A fundamental question in complexity theory is how much resource is needed to solve k independent instances of a problem compared to the resource required to solve one instance. Suppose solving one instance of a problem with probability of correctness p, we require c units of some resource in a given model of computation. A direct sum theorem states that in order to compute k independent instances of a problem, it requires k times units of the resource needed to compute one instance. A strong direct product theorem states that, with o(k â€¢ c) units of the resource, one can only compute all the k instances correctly with probability exponentially small in k. In this talk, I am going to present some of recent progress on direct sum and direct product theorems in the model of communication complexity and two-prover one-round games with information-theoretic approach. The talk is based on parts of my doctoral work.

Applications of Information Theory in Direct Sum and Direct Product Problems

Penghui Yao

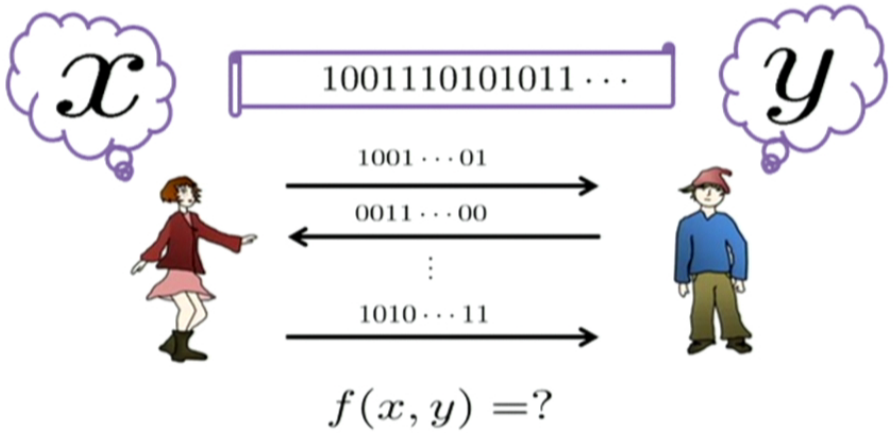
Centre for Quantum Technologies
National University of Singapore

Outline

- Communication complexity
  - Models and problems
  - Information costs and compression protocols
  - Direct sum and direct product in communication complexity
- Interactive proof systems
- Further problems

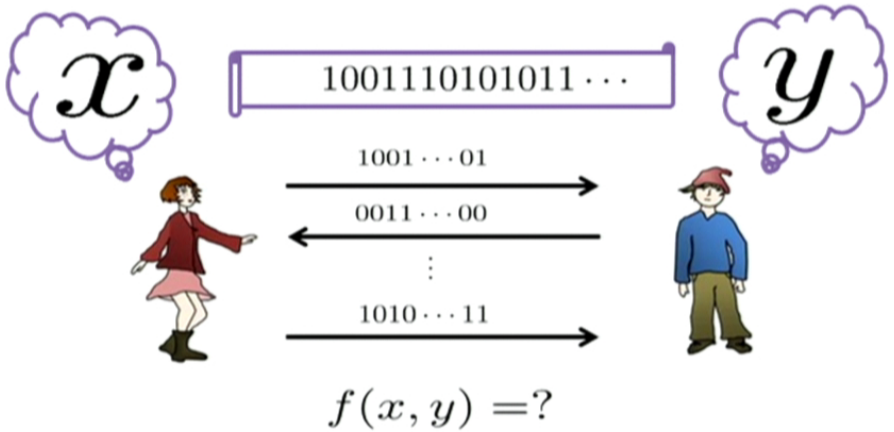
Communication complexity

Model



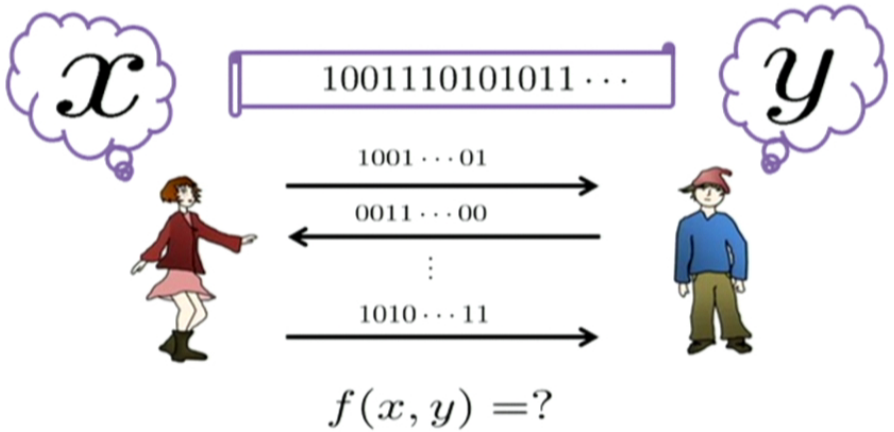
- A relation $f \subseteq \mathcal{X} \times \mathcal{Y} \times \mathcal{Z}$ is given.
- Alice is given $x \in \mathcal{X}$, and Bob is given $y \in \mathcal{Y}$.
- They shared randomness (independent of the input), communicate between each other, and at the end they output $z \in \mathcal{Z}$.
- They succeed if $(x, y, z) \in f$.

Model



- $\mathrm{R}_{\varepsilon}^{(t),\mathrm{pub}}(f)$ represents two-party t-**message** public-coin communication complexity of f with worst case error ε.
- $\mathrm{R}_{\varepsilon}^{\mathrm{pub}}(f)$ represents the two-party **unbounded-round** public-coin communication complexity of f with worst case error ε.

Model



- $\mathrm{R}_{\varepsilon}^{(t),\mathrm{pub}}(f)$ represents two-party t-**message** public-coin communication complexity of f with worst case error ε.
- $\mathrm{R}_{\varepsilon}^{\mathrm{pub}}(f)$ represents the two-party **unbounded-round** public-coin communication complexity of f with worst case error ε.

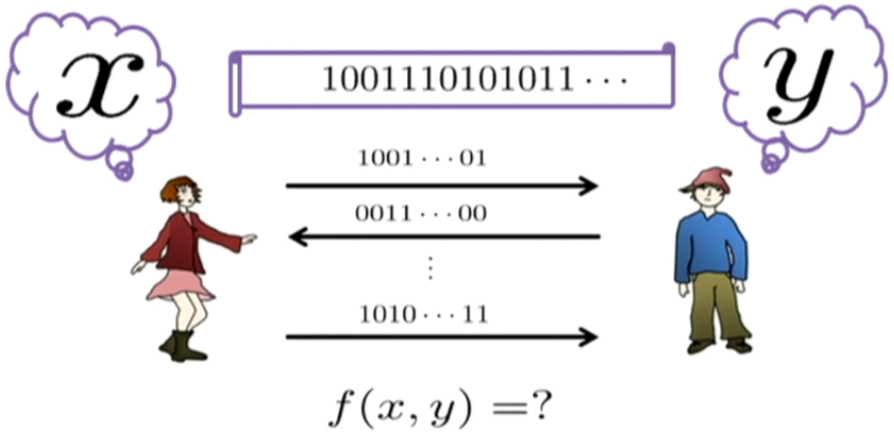
Minmax Principle

$$\mathrm{R}_{\varepsilon}^{\mathrm{pub}}(f) = \max_{\mu} \mathrm{D}_{\varepsilon}^{\mu}(f).$$

Minmax Principle

$$\mathrm{R}_{\varepsilon}^{\mathrm{pub}}(f) = \max_{\mu} \mathrm{D}_{\varepsilon}^{\mu}(f).$$

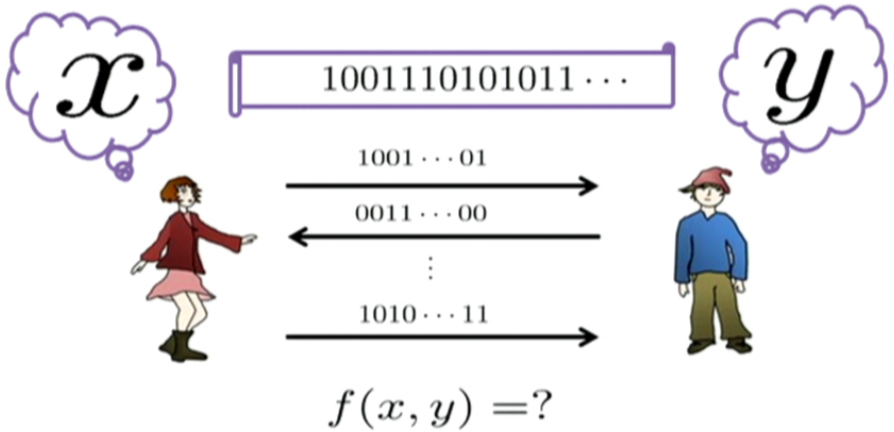
Information costs



Π: the transcript of the protocol, including the public coins and the messages communicated between Alice and Bob.

- **Exernal information cost**. $\mathrm{IC}^{\mathrm{ext}}(\Pi) = \mathrm{I}(XY;\Pi)$
- **Internal information cost**. $\mathrm{IC}(\Pi) = \mathrm{I}(X;\Pi|Y) + \mathrm{IC}(Y;\Pi|X)$

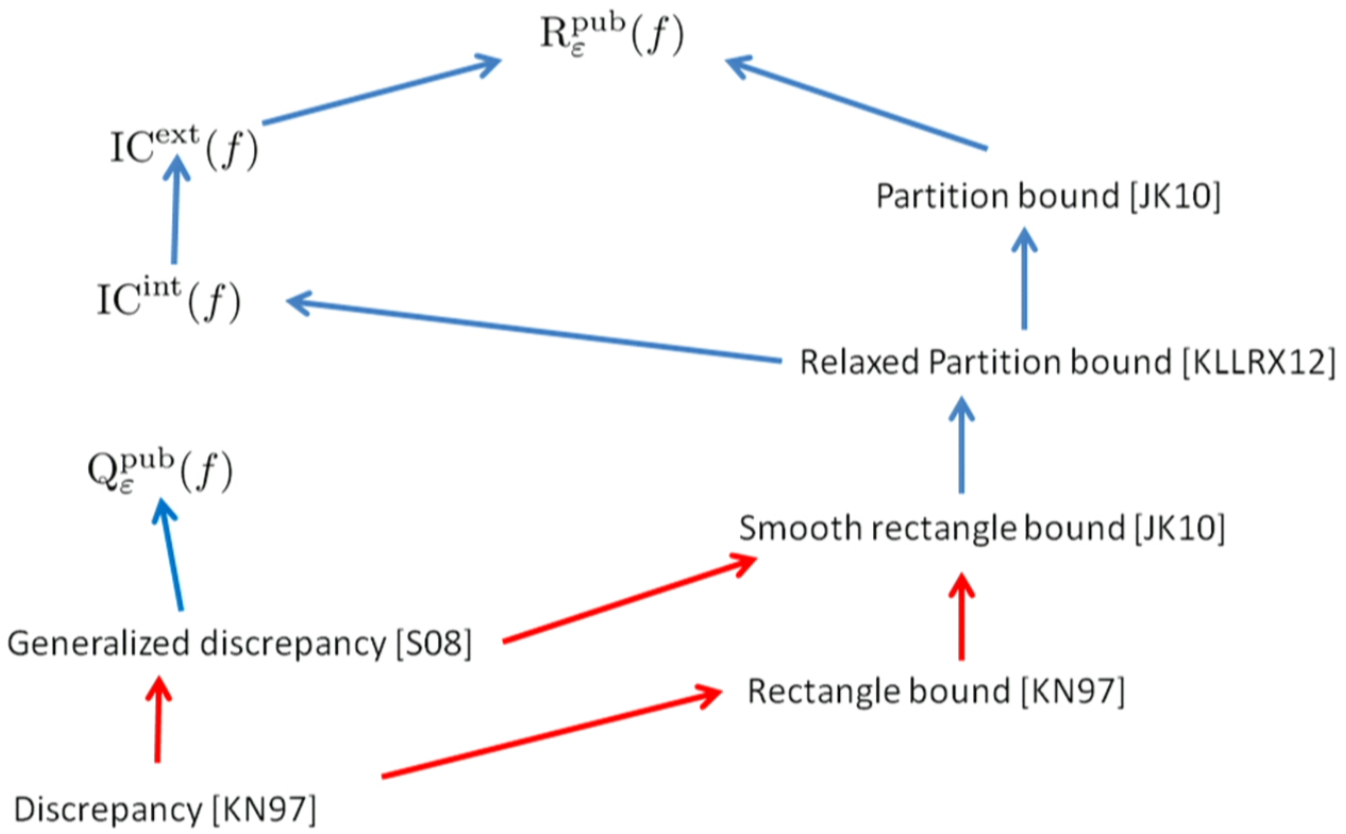
Information costs



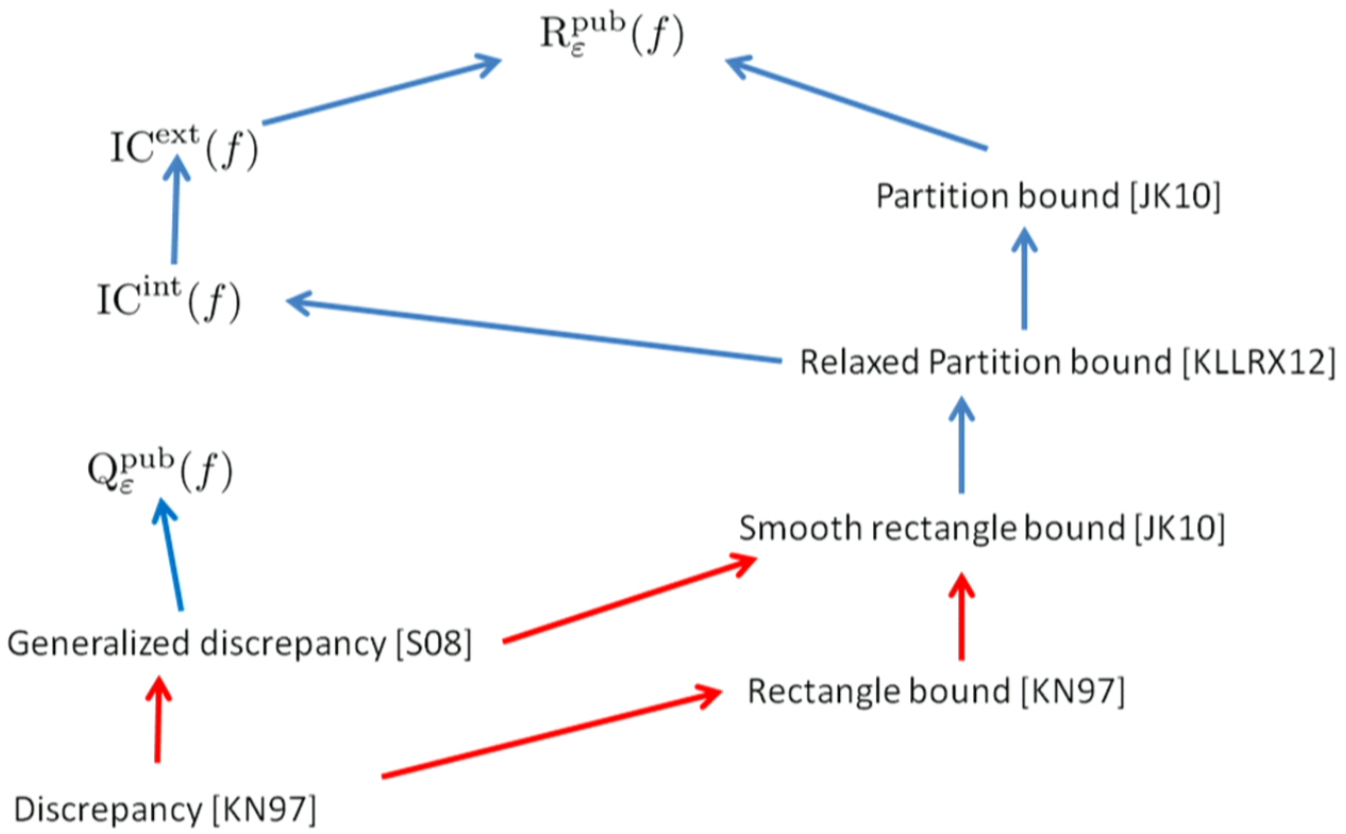
Π: the transcript of the protocol, including the public coins and the messages communicated between Alice and Bob.

- **Exernal information cost.** $\mathrm{IC}^{\mathrm{ext}}(\Pi) = \mathrm{I}(XY; \Pi)$
- **Internal information cost.** $\mathrm{IC}(\Pi) = \mathrm{I}(X; \Pi|Y) + \mathrm{IC}(Y; \Pi|X)$

Why information costs



Why information costs



Compression protocols

Open question:

$$\mathrm{R}_{\varepsilon}^{\mathrm{pub}}(f) = \mathcal{O}(\max_{\mu} \mathrm{IC}_{\mu}^{\mathrm{ext}}(f)), \quad \mathrm{R}_{\varepsilon}^{\mathrm{pub}}(f) = \mathcal{O}(\max_{\mu} \mathrm{IC}_{\mu}^{\mathrm{int}}(f))$$

Compression protocols

Open question:

$$\mathrm{R}_{\varepsilon}^{\mathrm{pub}}(f) = \mathcal{O}(\max_{\mu} \mathrm{IC}_{\mu}^{\mathrm{ext}}(f)), \quad \mathrm{R}_{\varepsilon}^{\mathrm{pub}}(f) = \mathcal{O}(\max_{\mu} \mathrm{IC}_{\mu}^{\mathrm{int}}(f))$$

Given a protocol π,

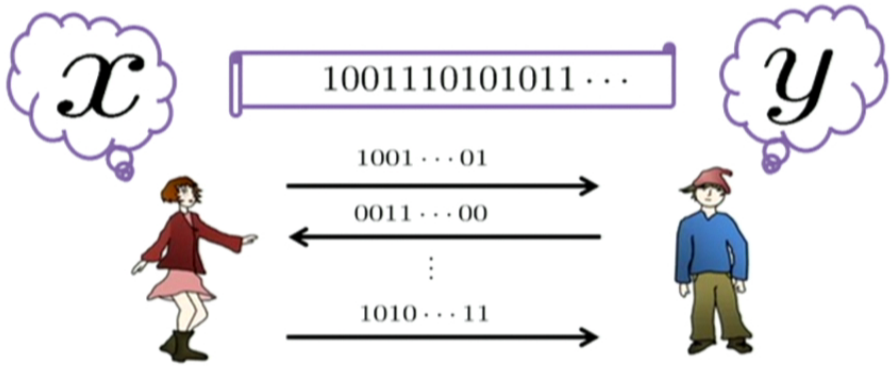
- [BRWY13] there exists a protocol λ simulating π such that

$$\mathrm{CC}(\lambda) = \mathcal{O}(\mathrm{IC}^{\mathrm{ext}}(\pi) \cdot \log \mathrm{CC}(\pi)).$$

- [BBCR10] there exists a protocol λ simulating π such that

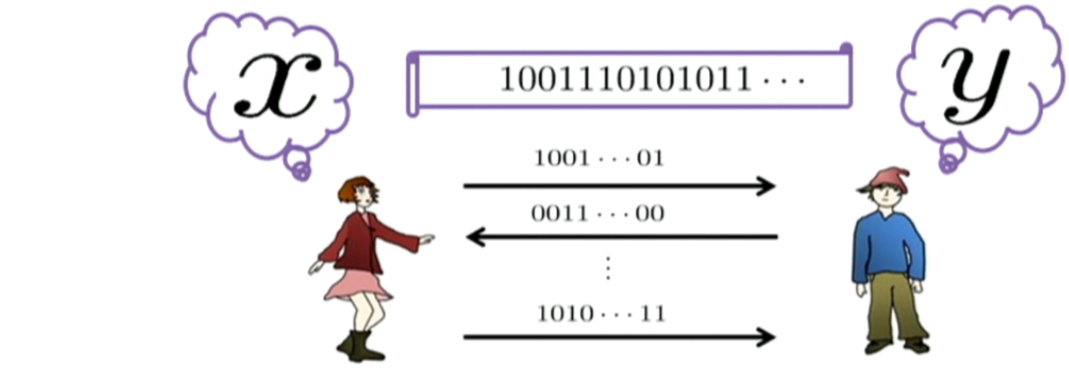
$$\mathrm{CC}(\lambda) = \mathcal{O}(\sqrt{\mathrm{CC}(\pi) \cdot \mathrm{IC}^{\mathrm{int}}(\pi)}).$$

Direct sum and direct product problems

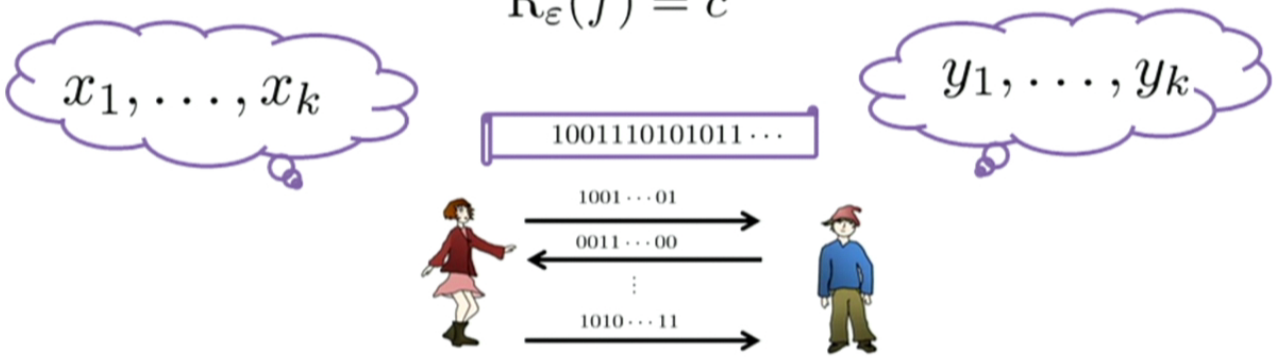


$$\mathrm{R}_{\varepsilon}(f) = c$$

Direct sum and direct product problems



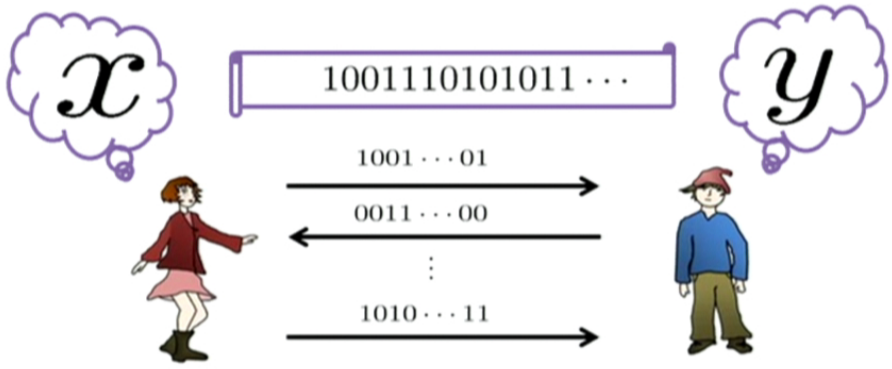
$$\mathrm{R}_{\varepsilon}(f) = c$$



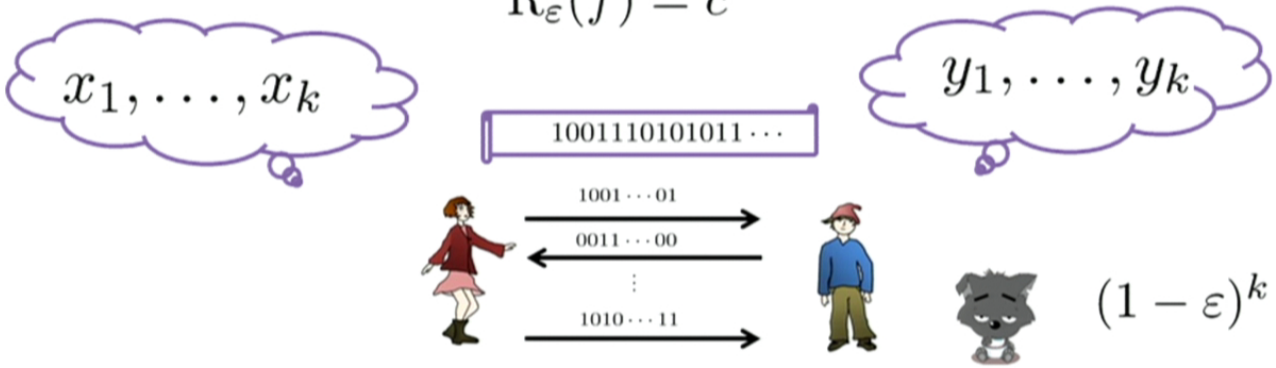
kc bits

$$f(x_1, y_1) =? \cdots f(x_k, y_k) =?$$

Direct sum and direct product problems



$$\mathrm{R}_\varepsilon(f) = c$$



kc bits

$$f(x_1, y_1) =? \cdots f(x_k, y_k) =?$$

Conjectures

Direct sum

$$\mathrm{R}_{\varepsilon}(f^k) = \Omega(k \cdot \mathrm{R}_{\varepsilon}(f))$$

Direct product

$$\mathrm{R}_{1-2^{-\Omega(k)}}(f^k) = \Omega(k \cdot \mathrm{R}_{\varepsilon}(f))$$

Conjectures

Direct sum

$$\mathrm{R}_{\varepsilon}(f^k) = \Omega(k \cdot \mathrm{R}_{\varepsilon}(f))$$

Direct product

$$\mathrm{R}_{1-2^{-\Omega(k)}}(f^k) = \Omega(k \cdot \mathrm{R}_{\varepsilon}(f))$$

Examples

Direct product theorems

- Lee et.al.'s theorem for discrepancy bound [LSS08].
- Sherstov's theorem for generalized discrepancy [She11].
- Jain's theorem for randomized one-way communication complexity [Jai11].
- Braverman et.al.'s theorem for two-way public-coin communication complexity [BRWY13].
- Raz's parallel repetition theorem for two-prover games [Raz95].
- .....

Direct sum theorems

- Jain et.al.'s theorem for classical and quantum one-way communication complexity [JRS05].
- Braverman et. al.'s theorem for bounded-round communicaiton complexity [BR10].
- .....

[JPY12]

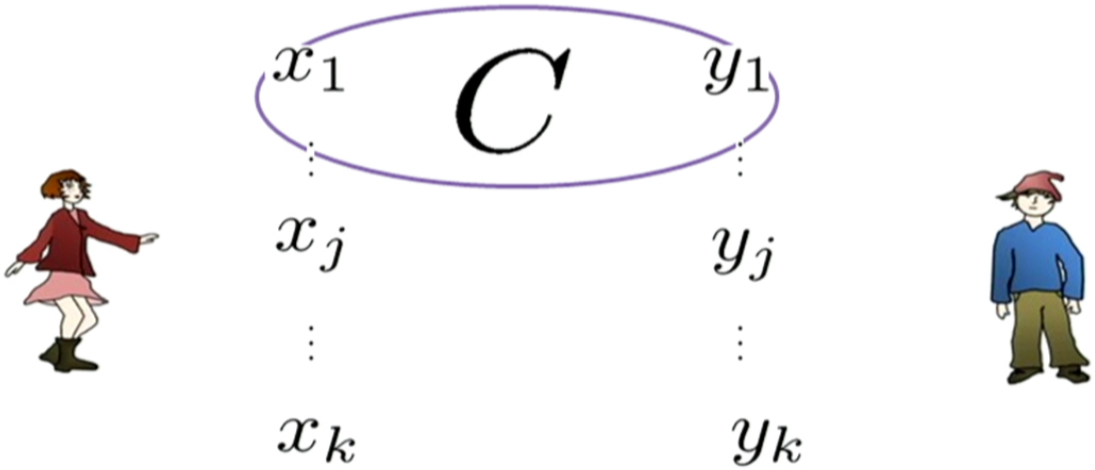
$$\mathrm{R}^{(t),\mathrm{pub}}_{1-2^{-\Omega(k/t^2)}}(f^k) = \Omega(\tfrac{k}{t} \cdot (\mathrm{R}^{(t),\mathrm{pub}}_{\varepsilon}(f) - kt^2)).$$

[JPY12]

$$\mathrm{R}^{(t),\mathrm{pub}}_{1-2^{-\Omega(k/t^2)}}(f^k) = \Omega(\tfrac{k}{t} \cdot (\mathrm{R}^{(t),\mathrm{pub}}_{\varepsilon}(f) - kt^2)).$$

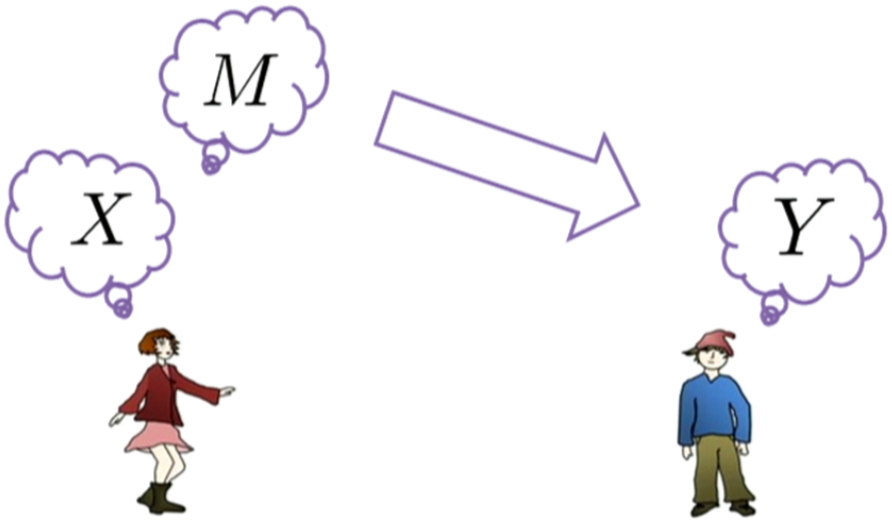
It implies **a strong direct product theorem** for the two-party constant-message public-coin randomized communication complexity of all relations.

Embedding



Given a protocol for f^k with communication $\mathcal{O}(ck)$, if the probablilty of overall success in coordinates in C is not small, then there exists a coordinate $j \notin C$, such that we can embed a fresh input into this coordinate, and simulate the protocol with communication less than c.

Compression protocol



$$\mathrm{I}(X : M|Y) = c \text{ and } \mathrm{I}(Y : M|X) = \varepsilon$$

- Braverman and Rao [BR10] showed that $\mathcal{O}(c)$ bits are enough when $\varepsilon = 0$.
- Jain [Jai11] showed that only $\mathcal{O}(\frac{c}{\varepsilon})$ bits are enough.

[JY12]

$$\mathrm{R}^{\mathrm{pub}}_{1-2^{-\Omega(k)}}(f^k) = \Omega(k \cdot \mathrm{srec}_\delta(f)).$$

[JY12]

$$\mathrm{R}^{\mathrm{pub}}_{1-2^{-\Omega(k)}}(f^k) = \Omega(k \cdot \mathrm{srec}_\delta(f)).$$

Our result implies a strong direct product theorem for all relations for which an (asymptotically) optimal lower bound can be provided using the smooth rectangle bound.

[JY12]

$$\mathrm{R}^{\mathrm{pub}}_{1-2^{-\Omega(k)}}(f^k) = \Omega(k \cdot \mathrm{srec}_\delta(f)).$$

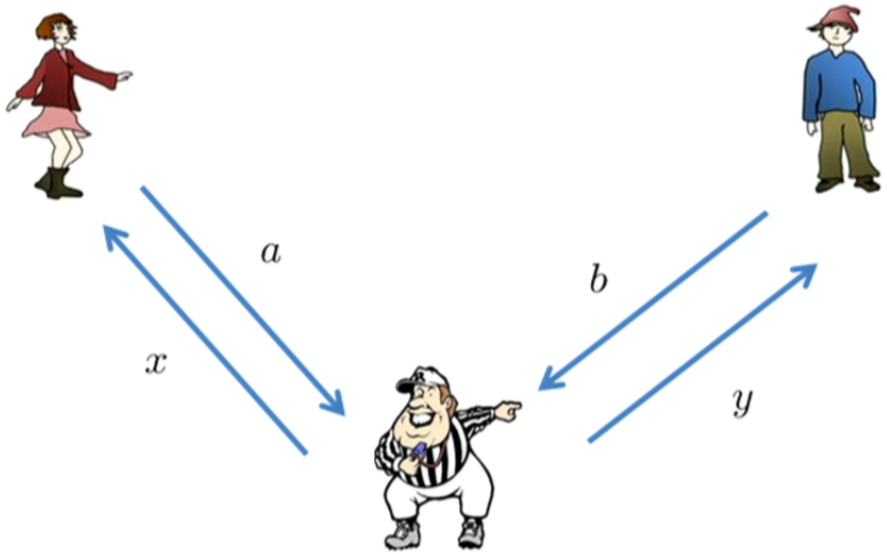
Our result implies a strong direct product theorem for all relations for which an (asymptotically) optimal lower bound can be provided using the smooth rectangle bound.

Examples. Inner Product, Set-Disjointness, Gap-Hamming Distance, Greater-Than, Vector in Subspace, Hidden Matching, Tribes, etc.

As far as we know, no function (or relation) is known for which its smooth rectangle bound is (asymptotically) strictly smaller than its two-way public-coin communication complexity.

Parallel repetition theorem

Model

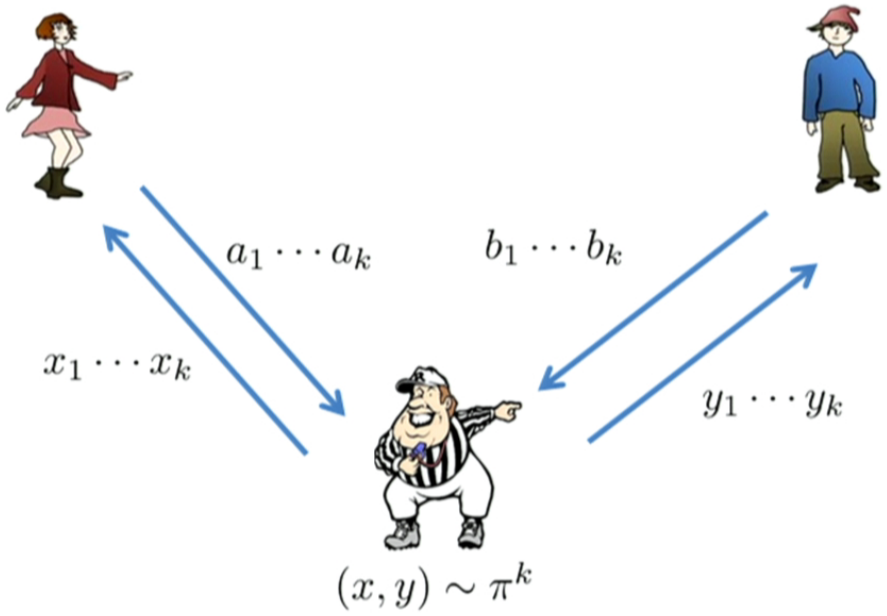


$G = (\pi, V, \mathcal{X}, \mathcal{Y}, \mathcal{A}, \mathcal{B})$

π is a distribution over $\mathcal{X} \times \mathcal{Y}$, and $V : \mathcal{X} \times \mathcal{Y} \times \mathcal{A} \times \mathcal{B} \to \{0, 1\}$

$\omega(G) = \max_{A:\mathcal{X}\to\mathcal{A}, B:\mathcal{Y}\to\mathcal{B}} \sum_{xy} \pi(x, y) V(x, y, A(x), B(y))$

Parallel repetition



$G^k = (\pi^k, V^k, \mathcal{X}^k, \mathcal{Y}^k, \mathcal{A}^k, \mathcal{B}^k)$

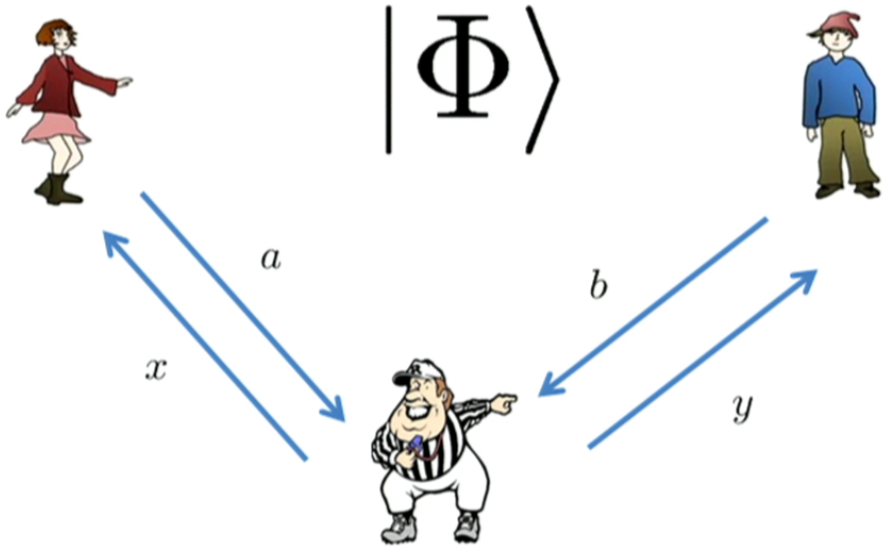
$V^k(x, y, a, b) = 1$ iff $V(x_i, y_i, a_i, b_i) = 1$ for all i.

Parallel repetition theorem

[Raz 95, Hol 08]

$$\omega(G^k) \leq (1-(1-\omega(G))^3)^{\Omega(\frac{k}{\log(|\mathcal{A}|\cdot|\mathcal{B}|)})}$$

Quantum games



$$\omega^*(G) = \lim_{N\to\infty} \max_{\Phi\in\mathbb{C}^N} \max_{\{A_a^x\}_{xa},\{B_b^y\}_{yb}} \sum_{xy} \pi(x,y) V(x,y,a,b) \langle\Phi| A_a^x \otimes B_b^y |\Phi\rangle$$

Parallel repetition theorems for quantum games

[CSSU08] If G is a XOR game, then $\omega^*(G^k) = \omega^*(G)^k$.

[KRT10] If G is a unique game, then $\omega^*(G^k) = (1-(1-\omega^*(G))^2)^{\Omega(k)}$.

[DSV13] If G is projective, then $\omega^*(G^k) = (1-(1-\omega^*(G))^c)^{\Omega(k)}$.

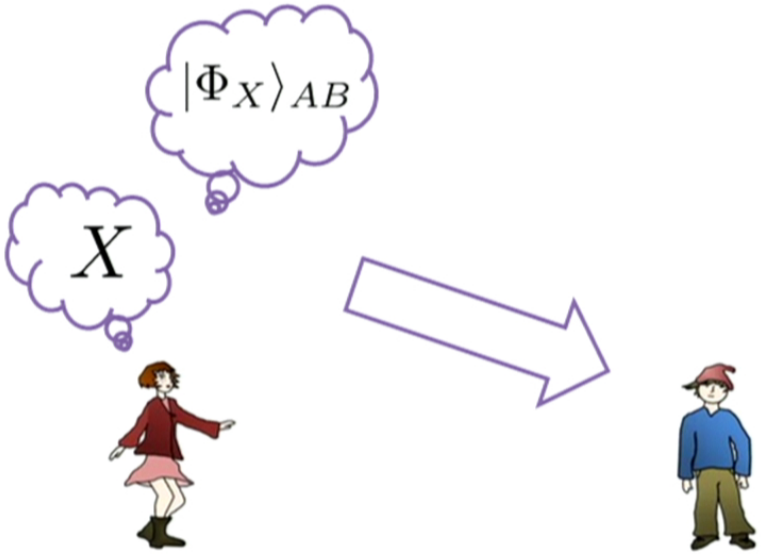
[CS13] If μ is uniform, then $\omega^*(G^k) = (1-(1-\omega^*(G))^2)^{\Omega(\frac{k}{\log(|\mathcal{X}||\mathcal{Y}||\mathcal{A}||\mathcal{B}|)})}$.

[JPY13]

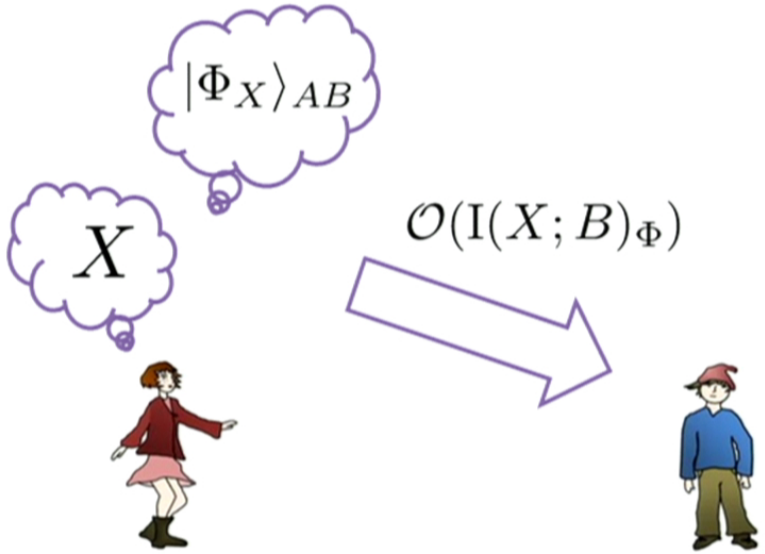
If μ is a product distribution over $\mathcal{X} \times \mathcal{Y}$, then

$$\omega^*(G^k) \leq (1 - (1 - \omega^*(G))^3)^{\frac{k}{\log |\mathcal{A}||\mathcal{B}|}}.$$

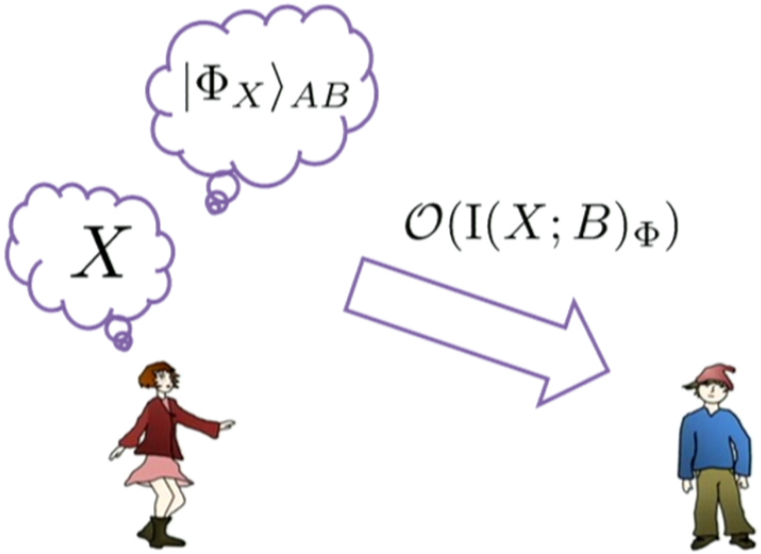
Compression protocol



Compression protocol



Compression protocol



Using the same compression protocol, we can show a strong direct product theorem for shared-entanglement quantum one-way communication complexity under product distribution.

Open problems

Open problems

- Information costs and strong direct product problems
  - Information theory in quantum communication complexity.
  - Direct sum and direct product problems in quantum communication complexity.

Open problems

- Information costs and strong direct product problems
  - Information theory in quantum communication complexity.
  - Direct sum and direct product problems in quantum communication complexity.

- Parallel repetition theorems
  - Parallel repetition theorems for general quantum games.
  - Parallel repetition theorems for multi-party games.

Thank you