Query-to-Communication Lifting Theorems for Adversary Bounds

Srijita Kundu

Joint work with Anurag Anshu & Shalev Ben-David

February 4, 2021

arXiv: 2012.03415

Query complexity

- $\mathrm{D^{dt}}(f)$ = deterministic queries

$$\mathrm{D^{dt}}(\mathrm{OR}_n) = n$$

- $\mathrm{R^{dt}}(f)$ = randomized queries, 1/3 error on all inputs

$$\mathrm{R^{dt}}(\mathrm{OR}_n) = \Theta(n)$$

- $\mathrm{Q^{dt}}(f)$ = quantum queries, 1/3 error on all inputs

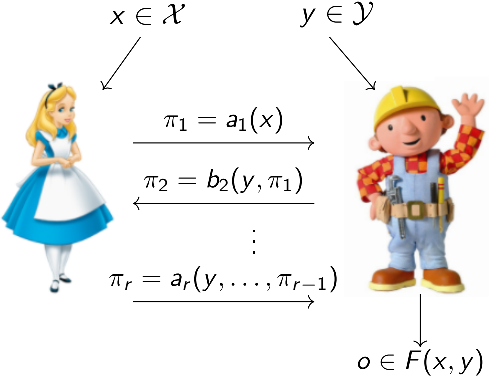
$$|i\rangle \xrightarrow{O_z} (-1)^{z_i} |i\rangle$$

$$\mathrm{Q^{dt}}(\mathrm{OR}_n) = \Theta(\sqrt{n}) \quad \text{(Grover search)}$$

- These are easy to prove!

Communication complexity

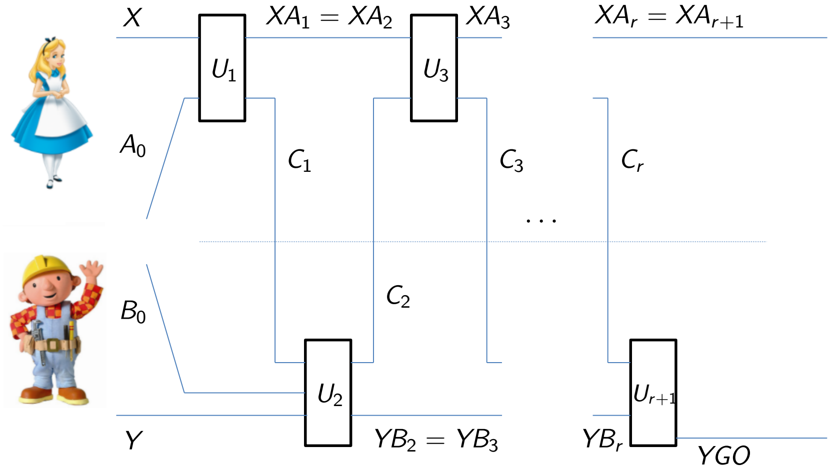
Known two-party relation $F : \mathcal{X} \times \mathcal{Y} \times \mathcal{O}$



In randomized protocols, Alice and Bob share random bits and π_i-s depend on them.

Communication complexity

Quantum communication protocol



Communication complexity

How many bits/qubits of communication is needed between Alice and Bob, to compute F for the worst case inputs?

- $\mathrm{D}^{\mathrm{cc}}(F) =$ deterministic communication
- $\mathrm{R}^{\mathrm{cc}}(F) =$ randomized communication, $1/3$ error on all inputs
- $\mathrm{Q}^{\mathrm{cc}}(F) =$ quantum communication, $1/3$ error on all inputs

Communication is more powerful than querying:

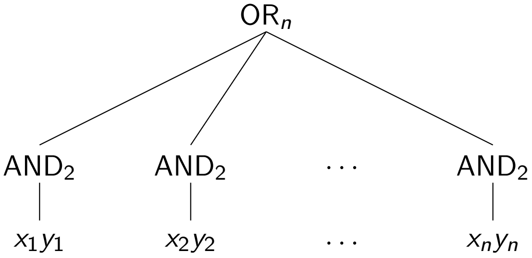
$$\mathrm{D}^{\mathrm{cc}}(\mathrm{OR}_n) = \mathrm{R}^{\mathrm{cc}}(\mathrm{OR}_n) = \mathrm{Q}^{\mathrm{cc}}(\mathrm{OR}_n) = 1$$

Also much harder to prove lower bounds!

Query vs communication

Sometimes, communication is no more powerful than query:

$F = \mathrm{Disj}_n = \mathrm{OR}_n \circ \mathrm{AND}_2^n$



$\mathrm{D}^{\mathrm{cc}}(\mathrm{Disj}_n) = n \qquad \mathrm{R}^{\mathrm{cc}}(\mathrm{Disj}_n) = \Theta(n) \qquad \mathrm{Q}^{\mathrm{cc}}(\mathrm{Disj}_n) = \Theta(\sqrt{n})$

Composition with gadgets

Can $f \circ G^n$ be as hard for communication as a general f is for query?

- $f = \text{OR}_n, G = \text{AND}_2$ ✓
- $f = \text{AND}_n, G = \text{AND}_2$ ✗
- $f = \text{AND}_n, G = \text{OR}_2$ ✓
- $f = \text{OR}_n, G = \text{OR}_2$ ✗

G needs to contain both AND_2 and OR_2.

Eg - 1. $\text{VER} : \{0,1,2,3\} \times \{0,1,2,3\} \to \{0,1\}$

b \ a	0	1	2	3
0	0	0	1	1
1	0	1	1	0
2	1	1	0	0
3	1	0	0	1

2. Inner product, $\text{IP}_m(a,b) = a_1 b_1 + \ldots + a_m b_m \mod 2$

Lifting theorems

With an appropriate gadget,

$$\mathcal{C}^{\text{cc}}(f \circ G^n) = \Omega(\mathcal{C}^{\text{dt}}(f)).$$

Lifting theorems via simulation:

- $\text{D}^{\text{cc}}(f \circ \text{Ind}_m^n) = \Omega(\text{D}^{\text{dt}}(f) \cdot \log m)$, with $m = n^{O(1)}$ [RM99, GPW15]
- $\text{D}^{\text{cc}}(f \circ \text{IP}_m^n) = \Omega(\text{D}^{\text{dt}}(f) \cdot \log m)$, with $m = O(\log n)$ [WYY17]
- $\text{R}^{\text{cc}}(f \circ \text{Ind}_m^n) = \Omega(\text{R}^{\text{dt}}(f) \cdot \log m)$, with $m = n^{O(1)}$ [GPW17]
- $\text{R}^{\text{cc}}(f \circ \text{IP}_m^n) = \Omega(\text{R}^{\text{dt}}(f) \cdot \log m)$, with $m = O(\log n)$ [CFKMP19]

Constant-sized gadget lifting theorems:

- $\log \widetilde{\text{rank}}(f \circ G^n) = \Omega(\widetilde{\deg}(f))$ [She09]
  - $\widetilde{\text{rank}}$ ↓ lower bound on $\text{Q}^{\text{cc}}(f \circ G^n)$
  - $\widetilde{\deg}$ ↓ lower bound on $\text{Q}^{\text{dt}}(f)$
- $\text{R}^{\text{cc}}(f \circ \text{VER}^n) = \Omega(\text{cbs}(f))$ [GP13]
  - cbs ↓ lower bound on $\text{R}^{\text{dt}}(f)$

Lifting theorems

Our results:

- $\mathrm{R}^{\mathrm{cc}}(f \circ \mathrm{VER}^n) = \Omega(\mathrm{CAdv}(f))$

  ↓ stronger lower bound on $\mathrm{R}^{\mathrm{dt}}(f)$

- $\mathrm{Q}_r^{\mathrm{cc}}(f \circ \mathrm{VER}^n) = \Omega\left(\frac{\mathrm{CAdv}(f)}{r^2}\right)$
- $\mathrm{Q}^{\mathrm{cc}}(f \circ G^n) = \Omega(\mathrm{Adv}_1(f) \cdot \mathrm{QICZ}(G))$

  ↓ lower bound on $\mathrm{Q}^{\mathrm{dt}}(f)$

  $\mathrm{QICZ}(G)$: (informally) related to secure 2-party computation

Comparison with previous results:

- $\mathrm{CAdv}(f) = \Omega(\mathrm{cbs}(f))$ for all partial functions

  $\mathrm{CAdv}(f) = \Omega(\mathrm{cbs}(f)^{3/2})$ for a family of total functions
- $\mathrm{Adv}_1(f) = O(\widetilde{\deg}(f))$ for all partial functions [ABK+20]

  ...but techniques may generalize!

Adversary bounds (dual formulation)

$$\mathrm{CAdv}(f) = \min_{\{q(z,i)\}} \max_{z} \sum_{i=1}^{n} q(z,i)$$

$$\text{s.t.} \sum_{i: z_i \neq w_i} \min\{q(z,i), q(w,i)\} \geq 1 \, \forall z, w \text{ s.t. } f(z) \cap f(w) = \emptyset$$

$$\mathrm{Adv}(f) = \min_{\{q(z,i)\}} \max_{z} \sum_{i=1}^{n} q(z,i)$$

$$\text{s.t.} \sum_{i: z_i \neq w_i} \sqrt{q(z,i)q(w,i)} \geq 1 \, \forall z, w \text{ s.t. } f(z) \cap f(w) = \emptyset$$

$$\mathrm{Adv}_1(f) = \min_{\{q(z,i)\}} \max_{z} \sum_{i=1}^{n} q(z,i)$$

$$\text{s.t.} \sqrt{q(z,i)q(w,i)} \geq 1 \, \forall z, w, i \text{ s.t. } f(z) \cap f(w) = \emptyset,$$

z and w differ only on i

Showing an adversary lower bound

Given an algorithm/protocol

$$q(z,i) \sim \text{how much it learns } z_i$$

In query complexity, $q(z,i) =$ probability algorithm queries i on z (scaled)

1. $\sum_{i=1}^{n} q(z,i) \leq$ number of queries by $\mathcal{A}$ $\forall z$
2. CAdv(f): $\sum_{i:z_i \neq w_i} \min\{q(z,i), q(w,i)\} \geq 1 \; \forall z, w$ s.t. $f(z) \cap f(w) = \emptyset$

2'. Adv(f): $\sum_{i:z_i \neq w_i} \sqrt{q(z,i)q(w,i)} \geq 1 \; \forall z, w$ s.t. $f(z) \cap f(w) = \emptyset$

Information complexity of communication protocols

Distribution μ on inputs X, Y of a classical communication protocol with shared randomness R

$\Rightarrow$ Induced distribution on the transcript Π.

$$\mathsf{IC}(\Pi, \mu) = I(X : \Pi | YR)_\mu + I(Y : \Pi | XR)_\mu$$

- $\mathsf{CC}(\Pi) \geq \mathsf{IC}(\Pi, \mu)\ \forall \mu$
- Chain rule for $X_1 \dots X_n$:

$$I(X : \Pi | YR) = \sum_{i=1}^{n} I(X_i : \Pi | X_{<i} YR)$$

QIC: quantum analogue (defined round-by-round) [Tou15]

Information complexity lower bounds

μ_0: uniform distribution on 0-inputs of AND_2
μ_1: uniform distribution on 1-inputs of OR_2

[BJKS04]: For any classical protocol Π for AND_2, $\text{IC}(\Pi, \mu_0) = \Omega(1)$.

Similarly, for any classical protocol Π' for OR_2, $\text{IC}(\Pi', \mu_1) = \Omega(1)$.

[BGK+18]: For any r-round quantum protocol Π^r, $\text{QIC}(\Pi^r, \mu_0) = \tilde{\Omega}(\frac{1}{r})$.

For any r-round quantum protocol Π'^r, $\text{QIC}(\Pi'^r, \mu_1) = \tilde{\Omega}(\frac{1}{r})$.

- Optimal up to logarithmic factors.

The VER gadget

$$\mathrm{VER}(a, b) = \begin{cases} 1 & \text{if } a + b = 2 \text{ or } 3 \mod 4 \\ 0 & \text{otherwise.} \end{cases}$$

1. **Flippability:** Given (a, b) Alice and Bob can locally generate (a', b') such that $\mathrm{VER}(a', b') = 1 - \mathrm{VER}(a, b)$.
2. **Random self-reducibility:** Given (a, b) Alice and Bob can use shared randomness to uniformly sample from $\mathrm{VER}^{-1}(\mathrm{VER}(a, b))$.
3. **Non-triviality:** VER contains AND_2 and OR_2 as subfunctions.

1.+2.$\Rightarrow$ Distinguishing m inputs to VER evaluating to 0^m vs 1^m on average $\Rightarrow$ Computing VER

3.$\Rightarrow$ Protocol that computes VER has

$$\mathrm{IC}(\Pi, \mu_0), \mathrm{IC}(\Pi, \mu_1) = \Omega(1)$$

$\mathrm{R}^{\mathrm{cc}}(f \circ \mathrm{VER}^n) = \Omega(\mathrm{CAdv}(f))$

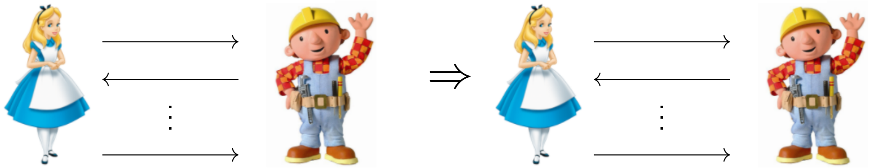
$q(z, i) = \mathrm{info}(\Pi, z, i)$ w.r.t. uniform $X_1 \dots X_n, Y_1 \dots Y_n$ evaluating to z

$\sim$ information about X_i, Y_i conditioned on other variables

Chain rule: $\sum_i \mathrm{info}(\Pi, z, i) \leq \mathrm{CC}(\Pi)$

Π for $f \circ \mathrm{VER}^n$ $\qquad\qquad$ Π' for VER

$X_1 \dots X_n$ $\qquad$ $Y_1 \dots Y_n$ $\qquad\qquad$ A $\qquad$ B



z, w differing on $\mathcal{B}$, $f(z) \cap f(w) = \emptyset$

$$\sum_{i \in \mathcal{B}} \min\{\mathrm{info}(\Pi, z, i), \mathrm{info}(\Pi, w, i)\} \quad \geq \quad \mathrm{IC}(\Pi', \mu_0) \text{ or } \mathrm{IC}(\Pi', \mu_1) = \Omega(1)$$

$Q_r^{cc}(f \circ \mathrm{VER}^n) = \Omega(\frac{\mathrm{CAdv}(f)}{r^2})$

Same proof gives $\Omega(\frac{\mathrm{CAdv}(f)}{r})$?

- Problems with chain rule ☹

Use measure HQIC rather than QIC:

$$\frac{1}{r}\mathrm{HQIC}(\Pi^r, \mu) \leq \mathrm{QIC}(\Pi^r, \mu) \leq \log|\Pi^r|$$

Corollary: $\mathrm{CC}(\Pi^r) \geq \max\{r, \mathrm{CAdv}(f)/r^2\} \geq \mathrm{CAdv}(f)^{1/3}$

- New for relations

Future directions

- Solve chain rule issue: $\Omega(\mathrm{CAdv}(f)/r)$, $\Omega(\mathrm{sAdv}(f) \cdot \mathrm{QICZ}(G))$ lower bounds for $\mathrm{Q}^{\mathrm{cc}}(f \circ G^n)$?
- Unconditionally lower bound $\mathrm{QICZ}(G)$ helpful: techniques from cryptography helpful?
- $\mathrm{Adv}^{\pm}(f)$ lower bound? For $\mathrm{R}^{\mathrm{cc}}(f \circ G^n)$?