Lookup functions and separations in communication complexity

Ankit Garg
Microsoft Research New England

Based on:

1. [Anshu; Belovs; Ben-David; Göös; Jain; Kothari; Lee; Santha 16]
2. [Anshu; Ben-David; G.; Jain; Kothari; Lee 16]

Overview

- All the separations for total Boolean functions.
- Input size n. Complexity measures $n^{\Omega(1)}$.

- [ABBGJKLS 16]: Power 2.5 separation between randomized and quantum communication.
- Quadratic separation between randomized communication and partition number.

- [ABGJKL 16]: Quadratic separation between quantum communication complexity and log of approximate rank.
- [ABGJKL 16] + [Bun, Thaler 17]: Quadratic separation between QCC and log rank.

Notation and prelims

- $CC(F,\varepsilon)$: min communication cost of a classical protocol that outputs $F(x,y)$ w.p. $\geq 1-\varepsilon$ for $all\ x,y$.
- $CC(F) = CC(F,1/3)$.
- $QCC(F,\varepsilon)$: min communication cost of a quantum protocol that outputs $F(x,y)$ w.p. $\geq 1-\varepsilon$ for $all\ x,y$.
- $QCC(F) = QCC(F,1/3)$.

- $\mathrm{rk}(F)$ = rank of the communication matrix.
- $\mathrm{rk}_\epsilon(F) = \min\{\mathrm{rank}(M): |M - M_F|_\infty \leq \epsilon\}$.
- $\widetilde{\mathrm{rk}}(F) = \mathrm{rk}_{1/3}(F)$.
- [Yao 93; Kremer 95, Buhrman-de Wolf 01; Lee-Shraibman 08]: $QCC(F) \geq \Omega\left(\log\left(\widetilde{\mathrm{rk}}(F)\right) - O(\log(n))\right)$

Randomized vs quantum communication

- [Raz 99; Bar-Yossef, Jayram, Kerenidis 04; Kempe, Kerenidis, Raz, de Wolf, Gavinsky 08; Klartag, Regev 10; Gavinsky 16]: Exponential separations for partial functions.
- Total functions: quadratic for disjointness [Grover 96; Buhrman, Cleve, Wigderson 98; Aaronson, Ambianis 03; Razborov 02; Sherstov 07].

- [ABBGJKLS 16]: There is a total Boolean function F s.t.

$$CC(F) \geq \widetilde{\Omega}(QCC(F, 1/3)^{2.5})$$

Approximate rank

- Approximate rank is one of the *strongest known* lower bound methods for QCC.
- No super-linear separation was known between $\log\left(\widetilde{\mathrm{rk}}(F)\right)$ and $QCC(F)$.

- [ABGJKL 16]: There is a total Boolean function F s.t.
$$QCC(F) \geq \Omega(\log^{2-o(1)}(\widetilde{\mathrm{rk}}(F)))$$
- [ABGJKL 16] + [Bun, Thaler 17]:
$$QCC(F) \geq \Omega(\log^{2-o(1)}(\mathrm{rk}(F)))$$

Lookup functions

- Follow a line of works showing separations in various models of query and communication complexity.
- [Göös, Pitassi, Watson 15; Ambainis, Balodis, Belovs, Lee, Santha, Smotrovs 16; Aaronson, Ben-David, Kothari 16]
- Variants also called pointer functions or cheat sheet functions.

Address function

- Alice's input: $x \in \{0,1\}^c$ and $u \in \{0,1\}^{2^c}$.
- Bob's input: $y \in \{0,1\}^c$ and $v \in \{0,1\}^{2^c}$.

$$\ell = \boxed{\ell_1\ \ell_2\ \ell_3}$$

$$x = \boxed{x_1\ x_2\ x_3} \qquad \boxed{u_0\ u_1\ u_2\ u_3\ u_4\ u_5\ u_6\ u_7}$$

$$\oplus \qquad \oplus$$

$$y = \boxed{y_1\ y_2\ y_3} \qquad \boxed{v_0\ v_1\ v_2\ v_3\ v_4\ v_5\ v_6\ v_7}$$

Answer: $u_3 \oplus v_3$

Lookup functions

- Alice's input: $x \in \{0,1\}^{n \times c}$ and $u \in \{0,1\}^{m \times 2^c}$.
- Bob's input: $y \in \{0,1\}^{n \times c}$ and $v \in \{0,1\}^{m \times 2^c}$.
- $F: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ and family $G = (G_0, \dots, G_{2^c - 1})$,
  $G_\ell: \{0,1\}^{nc} \times \{0,1\}^m \times \{0,1\}^{nc} \times \{0,1\}^m \to \{0,1\}$.

F_G

$\ell = \boxed{\ell_1\ \ell_2\ \ell_3}$

$x = \boxed{x_1\ x_2\ x_3}$ $\quad \boxed{u_0\ u_1\ u_2\ u_3\ u_4\ u_5\ u_6\ u_7}$

F $\quad G_3$

$y = \boxed{y_1\ y_2\ y_3}$ $\quad \boxed{v_0\ v_1\ v_2\ v_3\ v_4\ v_5\ v_6\ v_7}$

Answer: $G_3(x, u_3, y, v_3)$.

Lookup functions

- We will work with *non-trivial XOR* lookup functions.

1. Non-triviality: For $\ell = (F(x_1, y_1), \ldots, F(x_c, y_c))$, $G_\ell(x, y, \cdot\,, \cdot\,)$ is *non-constant*.

2. XOR: $G_\ell(x, y, u_\ell\,, v_\ell)$ depends only on $x, y, u_\ell \oplus v_\ell$.

- c will be typically $\Theta(\log(n))$.

Lookup functions

- Want to separate two measures M and N.
- Find a total Boolean function F s.t. $M(F) \gg N(F)$.

1. If $M(F) \gg N(F)$ known for partial functions, then lookup functions can be used to get a separation for total functions.
2. M remains the same but N drops. $M(F_G) \geq M(F)$ but $N(F_G) \ll N(F)$.

- For CC vs QCC, use 1.
- For QCC vs rank methods, use 2.

Cheat sheet theorems

- Classical CC, IC, quantum CC remain the same in the lookup function construction.
- [ABBGJKLS 16]: Let G be a *non-trivial XOR* function family, then

$$CC(F_G) \geq \widetilde{\Omega}(CC(F))$$
$$IC(F_G) \geq \widetilde{\Omega}(IC(F))$$

- [ABGJKL 16]: $QCC(F_G) \geq \widetilde{\Omega}(QCC(F, 1/2 - 1/n^2))$.
- Open for *QIC*.

Separation

- [Bun, Thaler 17]: Boolean function f with quadratic separation between certificate complexity and approximate degree.
- Using [Sherstov 07] + error amplification [Sherstov 12]: get a two party function F with quadratic separation between $QCC(F, 1/2 - 1/n^2)$ and non-deterministic communication $N(F)$.
- Convert F into an *appropriate* lookup function F_G.
- Cheat sheet theorem: $QCC(F_G) \geq \tilde{\Omega}(QCC(F, 1/2 - 1/n^2))$.
- $\log(\mathrm{rk}(F_G)) \leq \tilde{O}(N(F))$.

Upper bound

- [Theorem]: For any F, there exists a *non-trivial XOR* function family G s.t.
$$\log\left(\mathrm{rk}(F_G)\right) \leq \tilde{O}(c \cdot N(F))$$
- Suppose $\ell = (F(x_1, y_1), \dots, F(x_c, y_c))$.
- $u_\ell \oplus v_\ell$ supposed to provide proofs that $\ell = (F(x_1, y_1), \dots, F(x_c, y_c))$.
- Formally, $G_\ell(x, u_\ell, y, v_\ell) = 1$ iff $\ell = (F(x_1, y_1), \dots, F(x_c, y_c))$ and $u_\ell \oplus v_\ell$ provides proofs that $\ell = (F(x_1, y_1), \dots, F(x_c, y_c))$.

Upper bound

- Extend G_ℓ to the whole domain by ignoring inputs.
  $G_\ell(x, u, y, v) = G_\ell(x, u_\ell, y, v_\ell)$.
  $F_G(x, u, y, v) = 1$ iff *exactly one* of $G_\ell(x, u, y, v) = 1$.
  $\implies F_G = \sum_{\ell=0}^{2^c-1} G_\ell$
  $\implies \mathrm{rk}(F_G) \leq \sum_{\ell=0}^{2^c-1} \mathrm{rk}(G_\ell) \leq \sum_{\ell=0}^{2^c-1} 2^{D(G_\ell)}$
- $D(G_\ell) \leq O(c \cdot N(F))$.

High level overview: cheat sheet theorem

- To prove: $CC(F_G) \geq \tilde{\Omega}(CC(F))$
- Proof overview: Assume on the contrary. Π is a protocol for F_G with communication $q \ll CC(F)$.

1. Alice and Bob don't have much idea about $\ell = (F(x_1, y_1), \ldots, F(x_c, y_c))$.
2. Alice and Bob have talked about a few of the cells (u_i, v_i). Since number of cells $2^c \gg n \geq q$.

- Show that this implies Alice doesn't know much about v_ℓ and Bob doesn't know much about u_ℓ.

High level overview

- Alice doesn't know much about v_ℓ and Bob doesn't know much about u_ℓ.
- This already seems a contradiction: can't predict $G_\ell(x, u_\ell, y, v_\ell)$.
- However only know that G_ℓ is *non-trivial*. No control over its *bias*.
- *Cut-and-paste* property comes to the rescue.

- Extend to the quantum case via quantum information theoretic arguments.
- High level idea same but differ in details.
- Get a weaker statement $QCC(F_G) \geq \widetilde{\Omega}(QCC(F, 1/2 - 1/n^2))$.
- Quantum information proofs go round by round.

Open problems

- Lifting theorem for quantum communication complexity.
- Other applications of cheat sheet theorems.
- Information and communication complexity?

Thank You