

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

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

Approximate rank

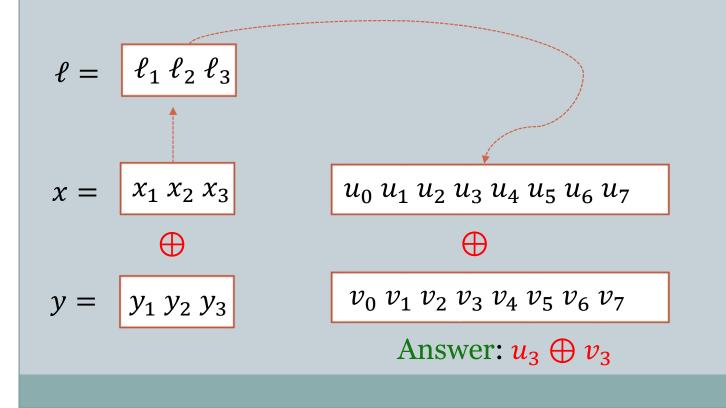
- Approximate rank is one of the *strongest known* lower bound methods for *QCC*.
- No super-linear separation was known between $log(\tilde{rk}(F))$ and QCC(F).
- [ABGJKL 16]: There is a total Boolean function F s.t. $QCC(F) \ge \Omega(\log^{2-o(1)}(\tilde{rk}(F)))$
- [ABGJKL 16] + [Bun, Thaler 17]: $QCC(F) \ge \Omega(\log^{2-o(1)}(\operatorname{rk}(F)))$

- 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]

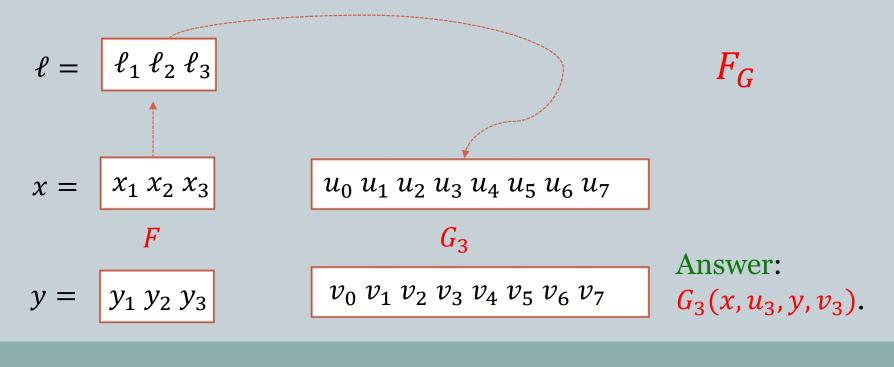
• Variants also called pointer functions or cheat sheet functions.

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 $v \in \{0,1\}^{2^c}$.



- 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 $G = (G_0, \dots, G_{2^c-1}), G_\ell: \{0,1\}^{nc} \times \{0,1\}^m \times \{0,1\}^{nc} \times \{0,1\}^m \to \{0,1\}.$



- We will work with *non-trivial XOR* lookup functions.
- 1. Non-triviality: For $\ell = (F(x_1, y_1), \dots, F(x_c, y_c)),$ $G_{\ell}(x, y, \cdot, \cdot)$ 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 $\Theta(\log(n))$.

- 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. $M(F_G) \ge M(F)$ 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

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

• [ABGJKL 16]: $QCC(F_G) \ge \widetilde{\Omega}(QCC(F, 1/2 - 1/n^2))$.

• 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/n²) and non-deterministic communication N(F).
- Convert F into an *appropriate* lookup function F_G .
- Cheat sheet theorem: $QCC(F_G) \ge \widetilde{\Omega}(QCC(F, 1/2 1/n^2))$.
- $\log(\operatorname{rk}(F_G)) \leq \tilde{O}(N(F)).$

Upper bound

- [Theorem]: For any *F*, there exists a *non-trivial XOR* function family *G* s.t. $\log(\operatorname{rk}(F_G)) \leq \tilde{O}(c \cdot N(F))$
- Suppose $\ell = (F(x_1, y_1), \dots, F(x_c, y_c)).$
- $u_{\ell} \bigoplus v_{\ell}$ 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 $u_{\ell} \bigoplus v_{\ell}$ 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_ℓ(x, u, y, v) = G_ℓ(x, u_ℓ, y, v_ℓ). F_G(x, u, y, v) = 1 iff exactly one of G_ℓ(x, u, y, v) = 1.
⇒ F_G = ∑^{2^c-1}_{ℓ=0} G_ℓ ⇒ rk(F_G) ≤ ∑^{2^c-1}_{ℓ=0} rk(G_ℓ) ≤ ∑^{2^c-1}_{ℓ=0} 2^{D(G_ℓ)}
D(G_ℓ) ≤ O(c · N(F)).

High level overview: cheat sheet theorem

- To prove: $CC(F_G) \ge \widetilde{\Omega}(CC(F))$
- 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 $\ell = (F(x_1, y_1), \dots, F(x_c, y_c)).$
- 2. Alice and Bob have talked about a few of the cells (u_i, v_i) . Since number of cells $2^c \gg n \ge q$.
- 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 $QCC(F_G) \ge \widetilde{\Omega}(QCC(F, 1/2 1/n^2))$.
- 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?

