Separating quantum communication and approximate rank

Anurag Anshu[a], Shalev Ben-David[b], Ankit Garg[c], Rahul Jain[a,d,e], Robin Kothari[b], Troy Lee[a,e,f]

[a] CQT, National University of Singapore
[b] Massachusetts Institute of Technology
[c] Microsoft Research, New England
[d] Dept. of CS, National University of Singapore
[e] MajuLab, UMI 3654, Singapore
[f] SPMS, Nanyang Technological University

July 8, 2017

Roadmap

1. Some background
2. Separating quantum communication and approximate rank

Models of query complexity

- For a function F, Randomized (two-sided error of ε) query complexity $\mathrm{R}_{\varepsilon}^{dt}(F)$, Quantum (two sided error of ε) query complexity $\mathrm{Q}_{\varepsilon}^{dt}(F)$.
- Quadratic separation: using Grover's search algorithm [Grov95] and its variant proved in [BBHT96].
- OR: $\{0,1\}^n \rightarrow \{0,1\}$ outputs 1 if the input contains at least one 1.

	$\mathrm{Q}_{1/3}^{dt}$
$\mathrm{R}_{1/3}^{dt}$	2 [BBHT96]

Lower bounds on quantum query complexity

- For a function F, approximate polynomial degree $\mathrm{deg}_\varepsilon(F)$ is the minimum among the degrees of all polynomials $p(x)$ satisfying $|p(x) - F(x)| \leq \varepsilon$, for all x.
- It lower bounds quantum query complexity [Beals, Buhrman, Cleve, Mosca, de Wolf 1998]: $\mathrm{Q}^{dt}_\varepsilon(F) \geq \frac{1}{2}\mathrm{deg}_\varepsilon(F)$.
- Example: $\mathrm{deg}_{1/3}(OR) = \Theta(\sqrt{n})$.
- Other well known bounds: Adversary bound [Ambainis 2000], Negative weights adversary bound [Hoyer, Lee, Spalek 2005].

Degree not a tight lower bound

- It is known that $\mathrm{Q}^{dt}_{1/3}(F) = O(\deg_{1/3}(F))^6$.
- Moreover, there exists a function F, such that $\mathrm{Q}^{dt}_{1/3}(F) = \Theta(\deg_{1/3}(F))^{1.3219}$ [Ambainis 2003].
- Is this the best possible separation?

Cheat sheets

- Aaronson, Ben-David and Kothari [2016] introduced the technique of cheat sheet.
- Follow up to the works Göös, Pitassi and Watson [2015] and Ambainis, Balodis, Belovs, Lee, Santha and Smotrovs [2015].
- A transformation from $F \to F_{cs}$.

	$\mathrm{Q}^{dt}_{1/3}$
$\mathrm{R}^{dt}_{1/3}$	2.5 [ABK16]

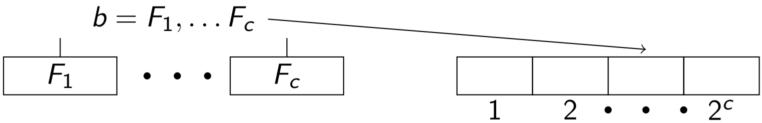
Cheat sheets

- Aaronson, Ben-David and Kothari [2015] introduced the technique of cheat sheet.
- Follow up to the works Göös, Pitassi and Watson [2015] and Ambainis, Balodis, Belovs, Lee, Santha and Smotrovs [2015].
- A transformation from $F \to F_{cs}$.

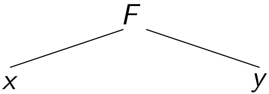
	$\deg_{1/3}$
$Q^{dt}_{1/3}$	4 [ABK16]

Cheat sheet review

- F_{cs} has two components: 'c' copies of a parent function F and a cheat sheet cs.
- Compute based on inputs to functions and content at '$\mathrm{decimal}(b)$'.



Communication complexity



- Randomized communication complexity $\mathrm{R}_{1/3}(F)$: number of bits communicated in a randomized protocol.
- Quantum communication complexity $\mathrm{Q}_{1/3}(F)$: number of qubits communicated in an entanglement assisted quantum protocol.

Lower bound on quantum communication complexity

- Approximate rank for F,
  $\mathrm{rk}_\varepsilon(F) = \min_{F'}\{\mathrm{rk}(F') : |F'(x,y) - F(x,y)| \leq \varepsilon\}$.
- Lower bound on quantum communication complexity [Buhrman and de Wolf 2001, Lee and Shraibman 2008]: For $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$,

$$\mathrm{Q}_{1/3}(F) \geq \Omega(\log \mathrm{rk}_{1/3}(F) - \log n).$$

- Quantum log-rank conjecture: are $\mathrm{Q}_{1/3}(F)$ and $\log \mathrm{rk}_{1/3}(M_F)$ polynomially related?

Lower bound on quantum communication complexity

- Approximate rank for F,
  $\mathrm{rk}_\varepsilon(F) = \min_{F'}\{\mathrm{rk}(F') : |F'(x,y) - F(x,y)| \leq \varepsilon\}$.
- Lower bound on quantum communication complexity [Buhrman and de Wolf 2001, Lee and Shraibman 2008]: For $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$,

$$\mathrm{Q}_{1/3}(F) \geq \Omega(\log \mathrm{rk}_{1/3}(F) - \log n).$$

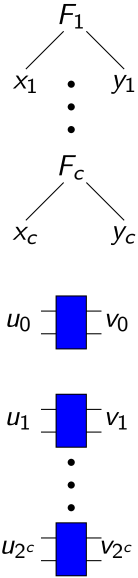
- Quantum log-rank conjecture: are $\mathrm{Q}_{1/3}(F)$ and $\log \mathrm{rk}_{1/3}(F)$ polynomially related?
- Other lower bound: quantum information complexity ([Touchette 2015]).

Cheat sheets in communication complexity

- Notion of cheat sheet extended to communication complexity in A., Belovs, Ben-David, Göös, Jain, Kothari, Lee and Santha [2016].
- A similar transformation: $F \to F_{\mathcal{G}}$, called look-up function.
- Super-quadratic separation between $R_{1/3}(F)$ and $Q_{1/3}(F)$.

Look-up function $F_{\mathcal{G}}$

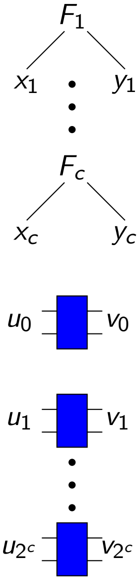
$$F : \mathcal{X} \otimes \mathcal{Y} \to \{0,1\}$$
$$F_1, F_2 \ldots F_c \equiv F$$



$$\mathcal{G} : \mathcal{X}^{\otimes c} \otimes \mathcal{Y}^{\otimes c} \otimes W \to \{0,1\}$$
W is set of strings

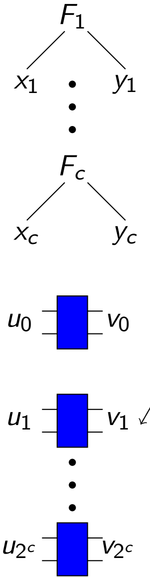
$$u_0, v_0, u_1, v_1 \ldots u_{2^c}, v_{2^c} \in W$$

Look-up function $F_{\mathcal{G}}$



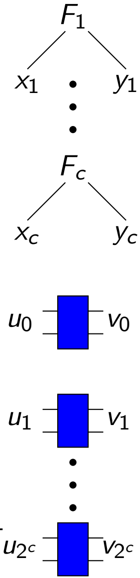
compute
$b = (F_1, F_2, \ldots F_c)$

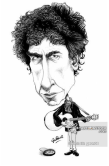
Look-up function $F_{\mathcal{G}}$



goto block number decimal(b)

Look-up function $F_{\mathcal{G}}$





$$F_{\mathcal{G}} = 1$$

Iff $\mathcal{G}(u_b \oplus v_b, x_1, y_1 \dots x_c, y_c) = 1$

Quantum communication complexity of look-up function

- For reasonably non-trivial function $\mathcal{G}$, we show the following.

Theorem

$$Q_{1/3}(F_{\mathcal{G}}) = \Omega(\log \frac{1}{\mathrm{disc}(F)}).$$

- $\mathrm{disc}(F)$ is the discrepancy of F.

An outline of proof

- We show that for any r-round protocol Π for $F_{\mathcal{G}}$ that makes an error of $\frac{1}{3}$, there exists a protocol Π' for F that makes an error of $\frac{1}{2} - \frac{1}{r^2}$ and communicates the same as in Π.
- So, $Q_{1/3}(F_{\mathcal{G}}) = \Omega(Q_{\frac{1}{2}-\frac{1}{r^2}}(F)) = \Omega(\log \frac{1}{\mathrm{disc}(F)} - \log r^2)$.

An outline of proof

- Key idea: Quantum cut and paste theorem [Jain, Radhakrishnan and Sen 2003, Nayak and Touchette 2016].
- In a protocol where each player has low information about content of the correct location of other player's 'look up part', output cannot be correct.

Choice of $\mathcal{G}$

- Recall: in cheat sheet of Aaronson, Ben-David and Kothari, correct cheat sheet location must certify the evaluation of $F_1, F_2, \ldots F_c$ on their inputs.
- Fix a circuit $\mathcal{C}$ for F, with number of gates $\mathrm{size}(F)$.
- We require that $u_b \oplus v_b$ certifies the evaluation of inputs (to $F_1, F_2, \ldots F_c$) on $\mathcal{C}$.

Choice of $\mathcal{G}$

Theorem

For $\mathcal{G}$ as defined above, $\log \mathrm{rk}_{1/3}(F_{\mathcal{G}}) = O(\sqrt{\mathrm{size}(F)})$.

- Now choose F to be inner product function $\mathrm{IP}_n(x, y) = \sum_i x_i y_i \bmod 2$. We have $\mathrm{size}(\mathrm{IP}_n) = O(n)$ and $\log \frac{1}{\mathrm{disc}(\mathrm{IP}_n)} = \Theta(n)$.

Theorem

There exists a total function F such that $\mathrm{Q}(F) = \tilde{\Omega}(\log \mathrm{rk}_{1/3}(F))^2$.

Open questions

- Can the round dependence in our main result be removed or weakened?
- Is there a general lifting theorem from quantum query complexity to quantum communication complexity?
  - Recently, a lifting theorem shown from randomized query complexity to randomized communication complexity [GPW17].
- Quantum log-rank conjecture?