Separations in communication complexity using cheat sheet and information complexity

Anurag Anshu[a], Aleksandrs Belovs[b], Shalev Ben-David[c], Mika Göös[d], Rahul Jain[a,e,f], Robin Kothari[c], Troy Lee[a,f,g], Miklos Santha[a,h]

[a] CQT, National University of Singapore
[b] University of Latvia
[c] Massachusetts Institute of Technology
[d] SEAS, Harvard University
[e] Dept. of CS, National University of Singapore
[f] MajuLab, UMI 3654, Singapore
[g] SPMS, Nanyang Technological University
[h] IRIF, Université Paris Diderot, CNRS

January 16, 2017

Roadmap

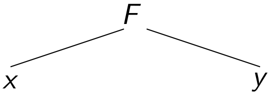
1. Some background
2. New separations in communication complexity

Separations in query complexity

- For a function F, Randomized (make an error of $1/3$) query complexity $\mathrm{R}^{dt}(F)$, Quantum (make error of $1/3$) query complexity $\mathrm{Q}^{dt}(F)$.
- Quadratic separation: using Grover's search algorithm [Grov95] and its variant proved in [BBHT96].
- OR: $\{0,1\}^n \to \{0,1\}$ outputs 1 if the input contains at least one 1.

	Q^{dt}
R^{dt}	2 [BBHT96]

Communication complexity



- Randomized communication complexity $\mathrm{R}(F)$: number of bits communicated in a randomized protocol.
- Quantum communication complexity $\mathrm{Q}(F)$: number of qubits communicated in an entanglement assisted quantum protocol.
- Information complexity $IC(F)$: amount of information about input that must be revealed (to other party) to compute the function.

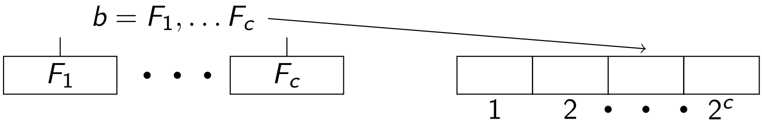
Porting query separations to communication

- A quantum query algorithm for a function gives rise to a quantum communication protocol for a related function [BCW98].
- Disjointness function DISJ inputs two subsets x, y of the set $\{1, 2, \ldots n\}$ and outputs 0 if the subsets are disjoint.
- $\mathrm{DISJ}(x, y) = \mathrm{OR}(x_1 \text{ AND } y_1, x_2 \text{ AND } y_2, \ldots, x_n \text{ AND } y_n)$!!

	Q
R	2 [BCW98] [KS87],[Raz91]

Super-Grover query separation

- Aaronson, Ben-David and Kothari [2016] introduced the technique of cheat sheet.
- 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 '$\mathrm{decimal}(b)$'.



	Q^{dt}
R^{dt}	2.5 [ABK16]

Separating exact quantum and randomized

- Exact quantum query complexity of F, denoted $\mathrm{Q}_E^{dt}(F)$, is number of quantum queries needed to compute F with zero error.
- Similarly we define $\mathrm{Q}_E(F)$ for communication complexity.

	Q		Q_E	
R	2.5 [ABK16] *dt*	2 *com*	1.15 [Amb12] *dt*	1.15 [Amb12] *com*

Separating exact quantum and randomized

- Exact quantum query complexity of F, denoted $\mathrm{Q}_E^{dt}(F)$, is number of quantum queries needed to compute F with zero error.
- Similarly we define $\mathrm{Q}_E(F)$ for communication complexity.

	Q		Q_E	
R	2.5 [ABK16] *dt*	2 *com*	1.5 [ABK16] *dt*	1.15 [Amb12] *com*

Partition and Randomized

- Unambiguous certificate complexity UN^{dt} is a lower bound on deterministic query complexity. Analogously Partition number UN in communication complexity.
- Goos, Pitassi, Watson [2015] presented first super linear separation between UN^{dt} and deterministic query complexity. Similar result in communication complexity.

	Q		Q_E		UN	
R	2.5 [ABK16] *dt*	2 *com*	1.5 [ABK16] *dt*	1.15 [Amb12] *com*	1.5 [GJPW] *dt*	1.5 [GJPW] *com*

Partition and Randomized

- Unambiguous certificate complexity UN^{dt} is a lower bound on deterministic query complexity. Analogously Partition number UN in communication complexity.
- Goos, Pitassi, Watson [2015] presented first super linear separation between UN^{dt} and deterministic query complexity. Similar result in communication complexity.

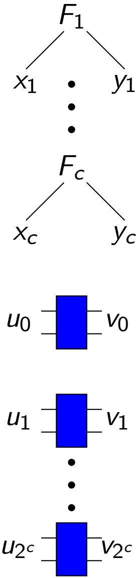
	Q		Q_E		UN	
R	2.5 [ABK16] *dt*	2 *com*	1.5 [ABK16] *dt*	1.15 [Amb12] *com*	2 [AKK16] *dt*	1.5 [GJPW] *com*

Super-Disjointness in communication world?

- Can we somehow lift these query results to communication? What gadgets should be used?
- AND is not a good: AND(x_1 AND $y_1, \ldots, x_n$ AND y_n) is easy.
- Inner Product lifts a lower bound (junta degree) on $\mathrm{R}^{dt}(F)$ to a lower bound on communication complexity $\mathrm{R}(F)$ (smooth rectangle bound) [GLMWZ, 2015].
- But we have no idea what is junta degree for cheat sheet function.

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

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

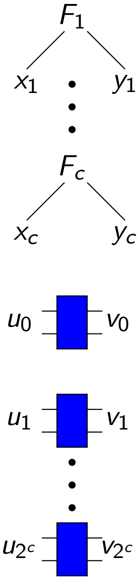


$$\mathcal{G} : \mathcal{X}^{\otimes c} \otimes \mathcal{Y}^{\otimes c} \otimes W \to \{0, 1\}$$

W is set of strings of size $\mathcal{O}(n^2)$

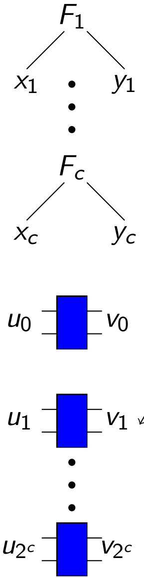
$$u_0, v_0, u_1, v_1 \dots u_{2^c}, v_{2^c} \in W$$

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



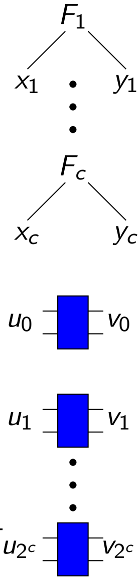
compute
$b = (F_1, F_2, \ldots F_c)$

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



goto block number decimal(b)

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



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

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

Lower bound on communication complexity of look-up function

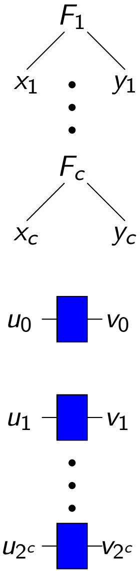
- For reasonably non-trivial function $\mathcal{G}$, we show the following.

Theorem

$\mathrm{R}(F_{\mathcal{G}}) = \Omega(\mathrm{R}(F)/c^2)$ *and* $IC(F_{\mathcal{G}}) = \Omega(IC(F)/c^3)$.

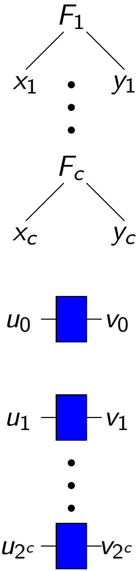
An idea of the proof: pointer function

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



An idea of the proof: pointer function

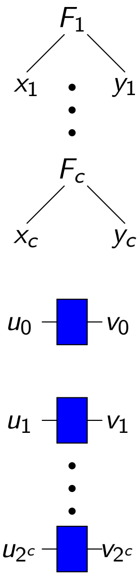
$$F : \mathcal{X} \otimes \mathcal{Y} \to \{0,1\}$$
$$F_1, F_2 \ldots F_c \equiv F$$



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

An idea of the proof: pointer function

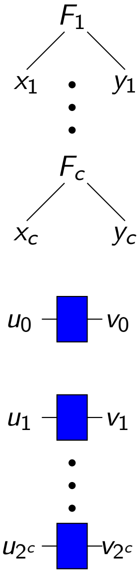
$$F : \mathcal{X} \otimes \mathcal{Y} \to \{0,1\}$$
$$F_1, F_2 \dots F_c \equiv F$$



Output $u_b \oplus v_b$

An idea of the proof: pointer function

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



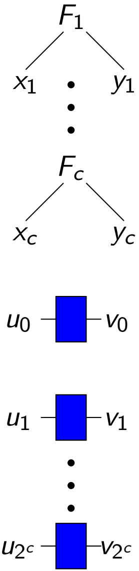
Hard distribution for F: μ

Distribution for pointer:

$$\mu^{\otimes c} \otimes \mathrm{uniform}_{UV}$$

An idea of the proof: pointer function

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



transcript Π

$\mathrm{I}(\Pi : b|UVY)$ small

$\mathrm{I}(\Pi U : b|VY)$ small

An idea of the proof: pointer function

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

F_1

x_1 y_1

$\vdots$

F_c

x_c y_c

u_0 — v_0

u_1 — v_1

$\vdots$

u_{2^c} — v_{2^c}

transcript Π

$$[(\Pi U)_{b,v,y} \approx (\Pi U)_{v,y}]$$

averaged over b, v, y

An idea of the proof: pointer function

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

F_1

x_1 y_1

$\vdots$

F_c

x_c y_c

u_0 — v_0

u_1 — v_1

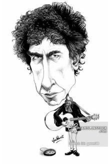
$\vdots$

u_{2^c} — v_{2^c}

$\mathrm{I}(\Pi : U_b | VY)$ small

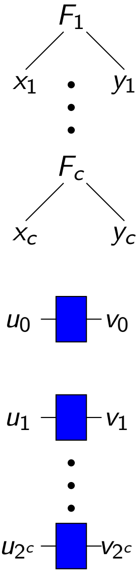
b distributed correctly

$\Big|$  $\Big\rangle$

$\Big|$  $\Big\rangle$

An idea of the proof: pointer function

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



$[(\Pi U_b)_{v,y} \approx \Pi_{v,y} \otimes U_b]$

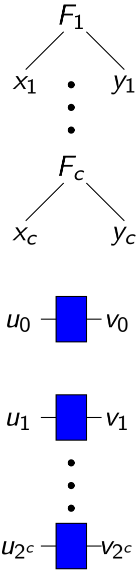
averaged over b, v, y

$\Big|$  $\Big\rangle$

$\Big|$  $\Big\rangle$

An idea of the proof: pointer function

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

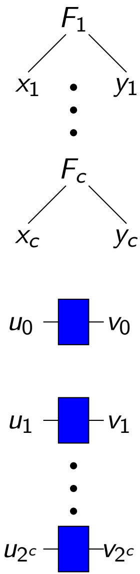


$$[(\Pi U_b)_{v,y} \approx \Pi_{v,y} \otimes U_b]$$
$$[(\Pi U)_{b,v,y} \approx (\Pi U)_{v,y}]$$
averaged over b, v, y

An idea of the proof: pointer function

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

$$[(\Pi U_b)_{v,y} \approx \Pi_{v,y} \otimes U_b]$$
$$[(\Pi U_b)_{b,v,y} \approx (\Pi U_b)_{v,y}]$$
averaged over b, v, y



$|$  $\rangle$

$|$  $\rangle$

An idea of the proof: pointer function

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

F_1

x_1 y_1

$\vdots$

F_c

x_c y_c

$$(\Pi U_b)_{b,v,y} \approx (\Pi)_{b,v,y} \otimes U_b$$

error!!

$\Big|$  $\Big\rangle$

u_0 — v_0

u_1 — v_1

$\vdots$

u_{2^c} — v_{2^c}

$\Big|$  $\Big\rangle$

Main results

- We choose $\mathcal{G}$ in similar way as in cheat sheet function.
- We choose appropriate F, lifting $SIMON \circ TRIBES$ (a la Aaronson,Ben-David,Kothari [2016]). Lifting done using Inner Product gadget ([Goos et. al., 2015]).

Theorem

There exists a total function F such that $R(F) = \tilde{\Omega}(Q(F)^{2.5})$.

Main results

Theorem

There exists a total function F such that $R(F) = \tilde{\Omega}(Q(F)^{2.5})$.

	Q		Q_E		UN	
R	2.5 [ABK16] *dt*	2.5 *com*	1.5 [ABK16] *dt*	1.15 [Amb12] *com*	2 [AKK16] *dt*	1.5 [GJPW] *com*

Main results

- Similarly for exact quantum separation, lifting the super linear separation of Aaronson, Ben-David, Kothari [2016].

Theorem

There exists a total function F such that $R(F) = \tilde{\Omega}(Q_E(F)^{1.5})$.

	Q		Q_E		UN	
R	2.5 [ABK16] *dt*	2.5 *com*	1.5 [ABK16] *dt*	1.5 *com*	2 [AKK16] *dt*	1.5 [GJPW] *com*

Main results

- Following Ambianis,Kokainis and Kothari (2016), we separate $\mathrm{R}(F)$ and $UN(F)$.
- We use the lower bound on information complexity (IC) of look-up function, since it has nice properties required for F.

Theorem (ABBG+16)

There exists a function F with the following relation between $R(F)$ and unambiguous non-deterministic communication complexity $UN(F)$: $R(F) > UN(F)^{2-o(1)}$.

Main results

Theorem (ABBG+16)

There exists a function F such that $R(F) > UN(F)^{2-o(1)}$.

	Q		Q_E		UN	
R	2.5 [ABK16] *dt*	2.5 *com*	1.5 [ABK16] *dt*	1.5 *com*	2 [AKK16] *dt*	2 *com*

Open questions

- Is there a general lifting theorem from randomized query complexity to randomized communication complexity?
- Are randomized communication complexity and quantum communication complexity of total functions polynomially related?
- Can we reduce the number of blocks in cheat sheet?