Separations in communication complexity using cheat sheet and information complexity

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

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

January 16, 2017
Roadmap

1. Some background

2. New separations in communication complexity
For a function $F$, Randomized (make an error of $1/3$) query complexity $R^{dt}(F)$, Quantum (make error of $1/3$) query complexity $Q^{dt}(F)$.

Quadratic separation: using Grover’s search algorithm [Grov95] and its variant proved in [BBHT96].

$$\text{OR: } \{0, 1\}^n \rightarrow \{0, 1\} \text{ outputs 1 if the input contains at least one 1.}$$

<table>
<thead>
<tr>
<th>$R^{dt}$</th>
<th>$Q^{dt}$</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2 [BBHT96]</td>
</tr>
</tbody>
</table>
Randomized communication complexity $R(F)$: number of bits communicated in a randomized protocol.

Quantum communication complexity $Q(F)$: 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.
A quantum query algorithm for a function gives rise to a quantum communication protocol for a related function [BCW98].

Disjointness function \( \text{DISJ} \) inputs two subsets \( x, y \) of the set \( \{1, 2, \ldots, n\} \) and outputs 0 if the subsets are disjoint.

\[
\text{DISJ}(x, y) = \text{OR}(x_1 \text{ AND } y_1, x_2 \text{ AND } y_2, \ldots, x_n \text{ AND } y_n)
\]

\[
\begin{array}{c|c}
\text{R} & \text{Q} \\
2 [\text{BCW98}] & \text{[KS87],[Raz91]}
\end{array}
\]
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 ‘decimal($b$)’.

\[ b = F_1, \ldots F_c \]

\[ \begin{array}{ccc}
F_1 & \cdots & F_c \\
\end{array} \]

\[ \begin{array}{cccc}
1 & 2 & \cdots & 2^c \\
\end{array} \]

\[ \begin{array}{|cc|}
Q^{dt} & \\
R^{dt} & 2.5 \ [ABK16] \\
\end{array} \]
Separating exact quantum and randomized

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

<table>
<thead>
<tr>
<th></th>
<th>$Q$</th>
<th>$Q_{E}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$R$</td>
<td>$2.5$</td>
<td>$1.15$</td>
</tr>
<tr>
<td></td>
<td>[ABK16]</td>
<td>[Amb12]</td>
</tr>
<tr>
<td>$dt$</td>
<td>$2$</td>
<td>$1.15$</td>
</tr>
<tr>
<td>$com$</td>
<td>$dt$</td>
<td>$com$</td>
</tr>
<tr>
<td></td>
<td>[Amb12]</td>
<td>[Amb12]</td>
</tr>
</tbody>
</table>
Exact quantum query complexity of $F$, denoted $Q_{E dt}^d(F)$, is number of quantum queries needed to compute $F$ with zero error.

Similarly we define $Q_E(F)$ for communication complexity.

<table>
<thead>
<tr>
<th>$R$</th>
<th>$Q_{dt}$</th>
<th>$Q_{com}$</th>
<th>$Q_{E dt}$</th>
<th>$Q_{E com}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>[ABK16]</td>
<td>2.5</td>
<td>2</td>
<td>1.5</td>
<td>1.15</td>
</tr>
<tr>
<td>$dt$</td>
<td>$com$</td>
<td>$dt$</td>
<td>$com$</td>
<td></td>
</tr>
</tbody>
</table>
Unambiguous certificate complexity $\text{UN}^{dt}$ is a lower bound on deterministic query complexity. Analogously Partition number $\text{UN}$ in communication complexity.

Goos, Pitassi, Watson [2015] presented first super linear separation between $\text{UN}^{dt}$ and deterministic query complexity. Similar result in communication complexity.

<table>
<thead>
<tr>
<th></th>
<th>$Q$</th>
<th>$Q_E$</th>
<th>$\text{UN}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$R$</td>
<td>2.5</td>
<td>1.5</td>
<td>1.5</td>
</tr>
<tr>
<td></td>
<td>[ABK16]</td>
<td>[Amb12]</td>
<td>[GJPW]</td>
</tr>
<tr>
<td>$dt$</td>
<td>$com$</td>
<td>$dt$</td>
<td>$com$</td>
</tr>
<tr>
<td>$com$</td>
<td>$dt$</td>
<td>$com$</td>
<td>$com$</td>
</tr>
</tbody>
</table>
Unambiguous certificate complexity $\text{UN}^{dt}$ is a lower bound on deterministic query complexity. Analogously Partition number $\text{UN}$ in communication complexity.

Goos, Pitassi, Watson [2015] presented first super linear separation between $\text{UN}^{dt}$ and deterministic query complexity. Similar result in communication complexity.

<table>
<thead>
<tr>
<th></th>
<th>$Q$</th>
<th>$Q_E$</th>
<th>$\text{UN}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$R$</td>
<td>2.5</td>
<td>1.5</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>$\text{com}$</td>
<td>$\text{com}$</td>
<td>$\text{com}$</td>
</tr>
<tr>
<td>$[\text{ABK16}]$</td>
<td>$[\text{ABK16}]$</td>
<td>$[\text{Amb12}]$</td>
<td>$[\text{AKK16}]$</td>
</tr>
<tr>
<td>$dt$</td>
<td>$dt$</td>
<td>$dt$</td>
<td>$dt$</td>
</tr>
<tr>
<td>$[\text{GJPW}]$</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Can we somehow lift these query results to communication? What gadgets should be used?

AND is not a good: $\text{AND}(x_1 \text{ AND } y_1, \ldots, x_n \text{ AND } y_n)$ is easy.

Inner Product lifts a lower bound (junta degree) on $R^{dt}(F)$ to a lower bound on communication complexity $R(F)$ (smooth rectangle bound) [GLMWZ, 2015].

But we have no idea what is junta degree for cheat sheet function.
Look-up function $F_G$

$F : \mathcal{X} \otimes \mathcal{Y} \rightarrow \{0, 1\}$

$F_1, F_2 \ldots F_c \equiv F$

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

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

$u_0, v_0, u_1, v_1 \ldots u_{2c}, v_{2c} \in \mathcal{W}$
Look-up function $F_g$

Compute $b = (F_1, F_2, \ldots, F_c)$
Look-up function $F_g$

$F_{1}$

$F_{c}$

$u_0 \rightarrow v_0$

$u_1 \rightarrow v_1$

$u_{2c} \rightarrow v_{2c}$

goto block number

decimal($b$)

Anurag Anshu, Aleksandrs Belovs, Shalev Ben-David, Mika Göös, Rahul Jain, Robin Kothari, Troy Lee, Miklos Santha (CQT)
Look-up function $F_G$

\[ F_G = 1 \quad \text{iff} \quad G(u_b \oplus v_b, x_1, y_1 \ldots x_c, y_c) = 1 \]
Lower bound on communication complexity of look-up function

- For reasonably non-trivial function $G$, we show the following.

**Theorem**

\[ R(F_G) = \Omega\left(\frac{R(F)}{c^2}\right) \text{ and } IC(F_G) = \Omega\left(\frac{IC(F)}{c^3}\right). \]
An idea of the proof: pointer function

\[ F : \mathcal{X} \otimes \mathcal{Y} \rightarrow \{0, 1\} \]

\[ F_1, F_2 \ldots F_c \equiv F \]
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

\[ F : \mathcal{X} \otimes \mathcal{Y} \to \{0, 1\} \]

\[ F_1, F_2 \ldots F_c \equiv F \]

Output \( u_b \oplus v_b \)
An idea of the proof: pointer function

\[ F : X \otimes Y \to \{0, 1\} \]

\[ F_1, F_2 \ldots F_c \equiv F \]

Hard distribution for F: \( \mu \)

Distribution for pointer:

\[ \mu \otimes^c \otimes \text{uniform}_{UV} \]
An idea of the proof: pointer function

\[ F : \mathcal{X} \otimes \mathcal{Y} \rightarrow \{0, 1\} \]

\[ F_1, F_2 \ldots F_c \equiv F \]

transcript \( \Pi \)

\[ I(\Pi : b | UVY) \text{ small} \]

\[ I(\Pi U : b | VY) \text{ small} \]
An idea of the proof: pointer function

\[ F : \mathcal{X} \otimes \mathcal{Y} \rightarrow \{0, 1\} \]

\[ F_1, F_2 \ldots F_c \equiv F \]

transcript \( \Pi \)

\[ \left( \prod U \right)_{b,v,y} \approx \left( \prod U \right)_{v,y} \]

averaged over \( b, v, y \)

---

Anurag Anshu\textsuperscript{a}, Aleksandrs Belovs\textsuperscript{b}, Shalev \textsuperscript{c}

\textsuperscript{a} CQT

January 16, 2017
An idea of the proof: pointer function

\[ F : \mathcal{X} \otimes \mathcal{Y} \rightarrow \{0, 1\} \]

\[ F_1, F_2 \ldots F_c \equiv F \]

\[ I(\Pi : U_b | VY) \text{ small} \]

\( b \) distributed correctly

\[ u_0 \rightarrow v_0 \]

\[ u_1 \rightarrow v_1 \]

\[ u_2 \rightarrow v_2 \]
An idea of the proof: pointer function

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

\[ \prod_{b, v, y} (\prod U_b)_{v, y} \approx \prod_{v, y} \otimes U_b \]

averaged over \( b, v, y \)
An idea of the proof: pointer function

$$F : \mathcal{X} \otimes \mathcal{Y} \to \{0, 1\}$$

$$F_1, F_2 \ldots F_c \equiv F$$

$$[\prod U_b]_{v,y} \approx \prod_{v,y} \otimes U_b$$

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

averaged over $$b, v, y$$
An idea of the proof: pointer function

\[ F : \mathcal{X} \otimes \mathcal{Y} \rightarrow \{0, 1\} \]

\[ F_1, F_2 \ldots F_c \equiv F \]

\[ [(\prod U_b)_{v,y} \approx \prod_{v,y} \otimes U_b] \]

\[ [(\prod U_b)_{b,v,y} \approx (\prod U_b)_{v,y}] \]

averaged over \( b, v, y \)
An idea of the proof: pointer function

\[ F : \mathcal{X} \otimes \mathcal{Y} \to \{0, 1\} \]

\[ F_1, F_2 \ldots F_c \equiv F \]

\[ (\prod U_b)_{b,v,y} \approx (\prod)_{b,v,y} \otimes U_b \]

error!!
Main results

- We choose $G$ 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 $R(F) = \tilde{\Omega}(Q(F)^{2.5})$.

<table>
<thead>
<tr>
<th></th>
<th>$Q$</th>
<th>$Q_E$</th>
<th>$UN$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$R$</td>
<td>2.5 \cite{ABK16} $dt$</td>
<td>2.5 \cite{ABK16} com</td>
<td>1.5 \cite{Amb12} $dt$</td>
</tr>
</tbody>
</table>
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 $R(F) = \tilde{\Omega}(Q_E(F)^{1.5})$. 

<table>
<thead>
<tr>
<th></th>
<th>$Q$</th>
<th>$Q_E$</th>
<th>UN</th>
</tr>
</thead>
<tbody>
<tr>
<td>$R$</td>
<td>2.5 [ABK16] $dt$</td>
<td>1.5 [AKK16] $dt$</td>
<td>2 [GJPW] $dt$</td>
</tr>
<tr>
<td></td>
<td>2.5 [ABK16] $com$</td>
<td>1.5 [AKK16] $com$</td>
<td>1.5 [GJPW] $com$</td>
</tr>
</tbody>
</table>
Main results

- Following Ambianis, Kokainis and Kothari (2016), we separate $R(F)$ 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 $R(F) > UN(F)^{2-o(1)}$.

<table>
<thead>
<tr>
<th></th>
<th>$Q$</th>
<th>$Q_E$</th>
<th>UN</th>
</tr>
</thead>
<tbody>
<tr>
<td>$R$</td>
<td>2.5</td>
<td>1.5</td>
<td>2</td>
</tr>
<tr>
<td>[ABK16]</td>
<td>$dt$</td>
<td>$dt$</td>
<td>$dt$</td>
</tr>
<tr>
<td></td>
<td>2.5</td>
<td>1.5</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>$com$</td>
<td>$com$</td>
<td>$com$</td>
</tr>
</tbody>
</table>
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?