Query-to-Communication Lifting

Mika Göös

Harvard & Simons Institute
Query vs. Communication

\[ f(z) \]

\[ F(x,y) \]

\[ z_1? \]

\[ z_5? \]

\[ z_7? \]

\[ z_2? \]

\[ a_1(x)? \]

\[ b_1(y)? \]

\[ b_2(y)? \]

\[ a_2(x)? \]

Decision trees

Communication protocols
Composed functions $f \circ g^n$

**Examples:**
- Set-disjointness: \( \text{OR} \circ \text{AND}^n \)
- Inner-product: \( \text{XOR} \circ \text{AND}^n \)
- Equality: \( \text{AND} \circ \neg \text{XOR}^n \)
Composed functions $f \circ g^n$

In general: $g : \{0,1\}^m \times \{0,1\}^m \rightarrow \{0,1\}$ is a small gadget

- **Alice** holds $x \in (\{0,1\}^m)^n$
- **Bob** holds $y \in (\{0,1\}^m)^n$
Composed functions $f \circ g^n$

Lifting Theorem Template

$$M^{cc}(f \circ g^n) \approx M^{dt}(f)$$
Composed functions $f \circ g^n$
Composed functions $f \circ g^n$

<table>
<thead>
<tr>
<th>$M$</th>
<th>Query</th>
<th>Communication</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>$P$</td>
<td>deterministic</td>
<td>deterministic</td>
<td>[RM99, GPW15, dRNV16, HHL16, WYY17, CKLM17]</td>
</tr>
<tr>
<td>NP</td>
<td>nondeterministic</td>
<td>nondeterministic</td>
<td>[GLM+15, G15]</td>
</tr>
<tr>
<td>many</td>
<td>poly degree</td>
<td>rank</td>
<td>[SZ09, She11, RS10, RPRC16]</td>
</tr>
<tr>
<td>many</td>
<td>conical junta</td>
<td>nonnegative rank</td>
<td>[GLM+15, KMR17]</td>
</tr>
<tr>
<td></td>
<td>degree</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sherali–Adams</td>
<td>LP complexity</td>
<td>[CLRS16, KMR17]</td>
</tr>
<tr>
<td></td>
<td>sum-of-squares</td>
<td>SDP complexity</td>
<td>[LRS15]</td>
</tr>
<tr>
<td>BPP</td>
<td>randomised</td>
<td>randomised</td>
<td>new, [AGJKM17]</td>
</tr>
<tr>
<td>$P^{NP}$</td>
<td>decision list</td>
<td>rectangle overlay</td>
<td>new</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Lifting Theorem Template**

$$M^{cc}(f \circ g^n) \approx M^{dt}(f)$$
Lifting for BPP

with Toniann Pitassi & Thomas Watson
Lifting theorem for BPP

**Index gadget** \( g: [m] \times \{0, 1\}^m \rightarrow \{0, 1\} \)

\[
g(x, y) = yx
\]

**Our result**

For \( m = n^{100} \) and every function \( f: \{0, 1\}^n \rightarrow \{0, 1\} \),

\[
\text{BPP}^{cc}(f \circ g^n) = \text{BPP}^{dt}(f) \cdot \Theta(\log n)
\]

also [AGJKM17]

**Definitions**

- \( \text{BPP}^{dt}(f) \): randomised query complexity of \( f \)
- \( \text{BPP}^{cc}(F) \): randomised communication complexity of \( F \)
New applications

\[ \text{BPP}^\text{dt}(f) \gg \text{M}^\text{dt}(f) \]

\[ \downarrow \]

\[ \text{BPP}^\text{cc}(f \circ g^n) \gg \text{M}^\text{cc}(f \circ g^n) \]
New applications

\[ \text{BPP}^{dt}(f) \gg \text{M}^{dt}(f) \]

\[ \Downarrow \]

\[ \text{BPP}^{cc}(f \circ g^n) \gg \text{M}^{cc}(f \circ g^n) \]
New applications

Classical vs. Quantum

- 2.5-th power total function gap [ABK16,ABB+16]
- Conjecture: 2.5 improves to 3 [AA15]
- Exponential partial function gap [Raz99,KR11]

BPP vs. Partition numbers

- 1-sided (= Clique vs. Independent Set) [GJPW15]
- 2-sided [AKK16,ABB+16]

Approximate Nash equilibria [BR17]
BPP^{cc}(f \circ g^n) \geq BPP^{dt}(f) \cdot \Omega(\log n)

...how to begin?
What we actually prove

**Input domain** partitioned into slices

\[
\begin{align*}
[m]^n \times ([0,1]^m)^n &= \bigcup_{z \in \{0,1\}^n} (g^n)^{-1}(z)
\end{align*}
\]
What we actually prove

**Simulation**

∀ deterministic protocol Π
∃ randomised decision tree of height |Π| outputting a random transcript of Π such that \[1 \approx 2\]

1. output of randomised decision tree on input \(z\)
2. transcript generated by Π on input \((x, y) \sim (g^n)^{-1}(z)\)

\([m]^n\) \((\{0,1\}^m)^n\)
What we actually prove

Simulation

∀ deterministic protocol Π
∃ randomised decision tree of height |Π| outputting a random transcript of Π such that 1 ≈ 2

1 output of randomised decision tree on input z
2 transcript generated by Π on input \((x, y) \sim (g^n)^{-1}(z)\)

Main theorem: 1. pick Π ∼ Π
2. simulate Π via query access to z
3. output value of leaf

\[
\mathbb{E}_{(x,y) \sim (g^n)^{-1}(z)} \Pr_{\Pi}[\Pi(x, y) \text{ correct}] > \frac{2}{3}
\]

\[
\mathbb{E}_{\Pi \sim \Pi} \Pr_{(x,y) \sim (g^n)^{-1}(z)}[\Pi(x, y) \text{ correct}]
\]
Goal in pictures

Goal: $1 \approx 2$

1. output of randomised decision tree on input $z$
2. transcript generated by $\Pi$ on input $(x, y) \sim (g^n)^{-1}(z)$
Goal: \(1 \approx 2\)

1. Output of randomised decision tree on input \(z\)
2. Transcript generated by \(\Pi\) on input \((x, y) \sim (g^n)^{-1}(z)\)
Goal: $1 \approx 2$

1. output of randomised decision tree on input $z$
2. transcript generated by $\Pi$ on input $(x, y) \sim (g^n)^{-1}(z)$
Goal in pictures

Goal: $1 \approx 2$

1. output of randomised decision tree on input $z$
2. transcript generated by $\Pi$ on input $(x, y) \sim (g^n)^{-1}(z)$
Goal: \(1 \approx 2\)

1. Output of randomised decision tree on input \(z\)
2. Transcript generated by \(\Pi\) on input \((x, y) \sim (g^n)^{-1}(z)\)
Goal: \( 1 \approx 2 \)

1. output of randomised decision tree on input \( z \)
2. transcript generated by \( \Pi \) on input \( (x, y) \sim (g^n)^{-1}(z) \)
Goal in pictures

Goal: 1 \approx 2

1. output of randomised decision tree on input $z$
2. transcript generated by $\Pi$ on input $(x, y) \sim (g^n)^{-1}(z)$
Goal: $1 \approx 2$

1. output of randomised decision tree on input $z$
2. transcript generated by $\Pi$ on input $(x, y) \sim (g^n)^{-1}(z)$

Idea:

Pretend marginals are uniform!
Pseudorandomness

**Uniform Marginals Lemma:**

Suppose \( X \subseteq [m]^n \) is dense
\( Y \subseteq ([0,1]^m)^n \) is “large”

Then \( \forall z \in \{0, 1\}^n \) the uniform distribution on \( (g^n)^{-1}(z) \cap X \times Y \)
has both marginal distributions close to uniform on \( X \) and \( Y \)

\[
\text{Dense: } H_\infty(X_I) \geq 0.9 \cdot |I| \log m \text{ for all } I \subseteq [n]
\]

[GLMWZ15]
Simulation

When **density** is lost, restore it!

1. Compute partition $X = \bigcup_i X^i$ where each $X^i$ is fixed on some $I \subseteq [n]$ and **dense** on $\bar{I}$
2. Update $X \leftarrow X^i$ with probability $|X^i|/|X|$
3. Query $z_I \in \{0, 1\}^I$
4. Restrict $Y$ so that $g^I(X_I, Y_I) = z_I$
5. Update $Y \leftarrow Y_I$ and $X \leftarrow X_I$ (which is **dense**)

\[X_1 \rightarrow \begin{array}{cccccccccccc}
* & * & * & * & * & * & * & * & * \\
\end{array} = Y_1\]

\[X_2 \rightarrow \begin{array}{cccccccccccc}
* & * & * & * & * & * & * & * & * \\
\end{array} = Y_2\]

\[X_3 \rightarrow \begin{array}{cccccccccccc}
* & * & * & * & * & * & * & * & * \\
\end{array} = Y_3\]

\[X_4 \rightarrow \begin{array}{cccccccccccc}
* & * & * & * & * & * & * & * & * \\
\end{array} = Y_4\]
Simulation

When **density** is lost, restore it!

1. Compute partition \( X = \bigcup_i X^i \) where each \( X^i \) is fixed on some \( I \subseteq [n] \) and **dense** on \( \bar{I} \) [GLMWZ15]
2. Update \( X \leftarrow X^i \) with probability \( \frac{|X^i|}{|X|} \)
3. Query \( z_I \in \{0, 1\}^I \)
4. Restrict \( Y \) so that \( g^I(X_I, Y_I) = z_I \)
5. Update \( Y \leftarrow Y_I \) and \( X \leftarrow X_I \) (which is **dense**)

\[
\begin{align*}
X_1 & \quad = Y_1 \\
X_2 & \quad = Y_2 \\
X_3 & \quad = Y_3 \\
X_4 & \quad = Y_4
\end{align*}
\]
When **density** is lost, restore it!

### Density-restoring partition  

**While** $X$ **is nonempty:**

1. Let $I \subseteq [n]$ be **maximal** such that for some $\alpha$
   \[
   \Pr[ X_I = \alpha ] > 2^{-0.9|I| \log m}
   \]
2. Output part $X' = \{ x \in X : x_I = \alpha \}$
3. Update $X \leftarrow X \setminus X'$

\[X \xrightarrow{x_{I_1} \neq \alpha_1} x_{I_2} \neq \alpha_2 \xrightarrow{x_{I_3} \neq \alpha_3} x_{I_4} \neq \alpha_4 \rightarrow \emptyset\]
Simulation

When **density** is lost, restore it!

1. Compute partition \( X = \bigcup_i X^i \) where each \( X^i \) is fixed on some \( I \subseteq [n] \) and **dense** on \( \overline{I} \)

2. Update \( X \leftarrow X^i \) with probability \( |X^i|/|X| \)

3. Query \( z_I \in \{0, 1\}^I \)

4. Restrict \( Y \) so that \( g^I(X_I, Y_I) = z_I \)

5. Update \( Y \leftarrow Y_I \) and \( X \leftarrow X_I \) (which is **dense**)

\[
\begin{align*}
X_1 & \quad \star \star \star \star \star \star \star \star \star \star \star = Y_1 \\
X_2 & \quad \star \star \star \star \star \star \star \star \star \star \star = Y_2 \\
X_3 & \quad \star \star \star \star \star \star \star \star \star \star \star = Y_3 \\
X_4 & \quad \star \star \star \star \star \star \star \star \star \star \star = Y_4
\end{align*}
\]
Simulation

When density is lost, restore it!

1. Compute partition $X = \bigcup_i X_i$ where each $X_i$ is fixed on some $I \subseteq [n]$ and dense on $\bar{I}$ [GLMWZ15]
2. Update $X \leftarrow X^i$ with probability $|X^i|/|X|
3. Query $z_I \in \{0, 1\}^I$
4. Restrict $Y$ so that $g^I(X_I, Y_I) = z_I$
5. Update $Y \leftarrow Y_I$ and $X \leftarrow X_I$ (which is dense)
Simulation

When \textbf{density} is lost, restore it!

1. Compute partition $X = \bigcup_i X^i$ where each $X^i$ is fixed on some $I \subseteq [n]$ and dense on $\overline{I}$ \cite{GLMWZ15}
2. Update $X \leftarrow X^i$ with probability $|X^i|/|X|$
3. Query $z_I \in \{0, 1\}^I$
4. Restrict $Y$ so that $g^I(X_I, Y_I) = z_I$
5. Update $Y \leftarrow Y_I$ and $X \leftarrow X_I$ (which is dense)

---

When \textbf{density} is lost, restore it!

1. Compute partition $X = \bigcup_i X^i$ where each $X^i$ is fixed on some $I \subseteq [n]$ and dense on $\overline{I}$ \cite{GLMWZ15}
2. Update $X \leftarrow X^i$ with probability $|X^i|/|X|$
3. Query $z_I \in \{0, 1\}^I$
4. Restrict $Y$ so that $g^I(X_I, Y_I) = z_I$
5. Update $Y \leftarrow Y_I$ and $X \leftarrow X_I$ (which is dense)

---

When \textbf{density} is lost, restore it!

1. Compute partition $X = \bigcup_i X^i$ where each $X^i$ is fixed on some $I \subseteq [n]$ and dense on $\overline{I}$ \cite{GLMWZ15}
2. Update $X \leftarrow X^i$ with probability $|X^i|/|X|$
3. Query $z_I \in \{0, 1\}^I$
4. Restrict $Y$ so that $g^I(X_I, Y_I) = z_I$
5. Update $Y \leftarrow Y_I$ and $X \leftarrow X_I$ (which is dense)
Simulation

When **density** is lost, restore it!

1. Compute partition $X = \bigcup_i X^i$ where each $X^i$ is fixed on some $I \subseteq [n]$ and **dense** on $\overline{I}$ [GLMWZ15]
2. Update $X \leftarrow X^i$ with probability $|X^i|/|X|$
3. Query $z_I \in \{0, 1\}^I$
4. Restrict $Y$ so that $g^I(X_I, Y_I) = z_I$
5. Update $Y \leftarrow Y_I$ and $X \leftarrow X_{\overline{I}}$ (which is **dense**)

### Correctness

1. $\#\text{queries} \leq |\Pi|$ (whp)
2. Resulting transcript is close to that generated by random input from $(g^n)^{-1}(z)$
Application (via $P^{NP}$ lifting)

with Pritish Kamath, Toniann Pitassi & Thomas Watson
Monochromatic rectangles

\[
\text{mon}(F) := \min_{R \text{ mono}} \log \frac{1}{\mu(R)}
\]

\[
\begin{array}{cccccc}
1 & 0 & 0 & 1 & 1 & 1 \\
0 & 1 & 0 & 1 & 1 & 1 \\
0 & 0 & 1 & 1 & 1 & 1 \\
0 & 1 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 1 & 1 \\
1 & 0 & 1 & 1 & 0 & 1 \\
\end{array}
\]
Monochromatic rectangles

\[ \text{mon}(F) := \max_{\mu \text{ product}} \min_{R \text{ mono}} \log \frac{1}{\mu(R)} \]

\[
\begin{array}{cccccc}
1 & 0 & 0 & 1 & 1 & 1 \\
0 & 1 & 0 & 1 & 1 & 1 \\
0 & 0 & 1 & 1 & 1 & 1 \\
0 & 1 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 1 & 1 \\
1 & 0 & 1 & 1 & 0 & 1 \\
\end{array}
\]
Monochromatic rectangles

\[ \text{mon}(F) := \max_{\mu \text{ product}} \min_{R \text{ mono}} \log \frac{1}{\mu(R)} \]

Basic questions

- Log-rank conjecture?  \iff \ \forall F: \ \text{mon}(F) \leq \log^{O(1)} \text{rk}(F)
- Protocols from mon?  \iff \ \forall F: \ \text{PSPACE}_{cc}^{cc}(F) \leq \text{mon}(F)^{O(1)}
Monochromatic rectangles

\[ \text{mon}(F) := \max_{\mu \text{ product}} \min_{R \text{ mono}} \log \frac{1}{\mu(R)} \]

Basic questions

- Log-rank conjecture? \iff \forall F: \text{mon}(F) \leq \log^{O(1)} \text{rk}(F)
- Protocols from mon? \iff \forall F: \text{PSPACE}^{cc}(F) \leq \text{mon}(F)^{O(1)}

Known

- \forall F: \text{non-product-mon}(F) = P^{cc}(F)^{\Theta(1)} \quad [AUY83,KKN95]
- \forall F: \text{mon}(F) \leq P^{NP^{cc}}(F) \quad [IW10,PSS14]
- \exists F: P^{NP^{cc}}(F) \leq \log n \ll n^{\Omega(1)} \leq PP^{cc}(F) \quad [BVdW07]
Monochromatic rectangles

\[
\text{mon}(F) := \max \mu \text{ product} \quad \min \mu \text{ mono} \log \frac{1}{\mu(R)}
\]

Lifting application:

\[
\exists F: \quad \text{mon}(F) \leq \log^{O(1)} n \ll n^{\Omega(1)} \leq P^{NPcc}(F)
\]

Known

- \( \forall F: \) \text{non-product-mon}(F) = P^{cc}(F)^{\Theta(1)} \quad [AUY83,KKN95]
- \( \forall F: \) \text{mon}(F) \leq P^{NPcc}(F) \quad [IW10,PSS14]
- \( \exists F: \) P^{NPcc}(F) \leq \log n \ll n^{\Omega(1)} \leq PP^{cc}(F) \quad [BVdW07]
$p^{NP}$ decision trees / protocols

Oracle query cost:

$NP^{dt} = \text{DNF width}$ \quad \text{vs.} \quad $NP^{cc} = \log \#\text{rectangles}$
Decision lists: $DL^{dt}$ and $DL^{cc}$

**Equivalent (up to quadratic factors):**

$z_3 \bar{z}_4 \bar{z}_6 ? \quad 1 \quad 0$

$z_3 \bar{z}_1 ? \quad 1 \quad 1$

$\bar{z}_2 \bar{z}_3 ? \quad 1 \quad 0$

$\top \quad 1 \quad 1$

$(x, y) \in R_1 ? \quad 1 \quad 0$

$(x, y) \in R_2 ? \quad 1 \quad 1$

$(x, y) \in R_3 ? \quad 1 \quad 0$

$\top \quad 1 \quad 1$

**Conjunction width vs.** $\log \#$rectangles

[Riv87, PSS14]
Lifting theorems

**Lifting for \( P^{NP} \)**

For poly-size index gadget \( g \) and every \( f : \{0,1\}^n \rightarrow \{0,1\} \),

\[
P^{NPcc}(f \circ g^n) \geq \sqrt{P^{NPdt}(f) \cdot \Omega(\log n)}
\]

**Lifting for decision lists**

For poly-size index gadget \( g \) and every \( f : \{0,1\}^n \rightarrow \{0,1\} \),

\[
DL^{cc}(f \circ g^n) = DL^{dt}(f) \cdot \Theta(\log n)
\]
\( \text{mon}(F) \leq \text{DL}^{cc}(F) \)
\[
\text{mon}(F) \leq \text{DL}_{cc}^{cc}(F)
\]
\( \text{mon}(F) \leq \text{DL}^{cc}(F) \)
\[ \text{mon}(F) \leq DL^{cc}(F) \]
\[ \text{mon}(F) \leq DL^{cc}(F) \]
\( \text{mon}(F) \leq \text{DL}^{cc}(F) \)
$$\text{mon}(F) \leq \text{DL}^{cc}(F)$$
\[ \text{mon}(F) \leq \text{DL}^{cc}(F) \]
\[ \text{mon}(F) \leq DL^{cc}(F) \]
\[ \text{mon}(F) \leq \text{DL}^{cc}(F) \]
\[ \text{mon}(F) \leq DL^{cc}(F) \]
\( \text{mon}(F) \leq DL^{cc}(F) \)
\[ \text{mon}(F) \leq DL^{cc}(F) \]
**Construction**

**Lifting application:**

\[ \exists F = f \circ g^n : \text{mon}(F) \iff P^{NP_{cc}}(F) \]

\[ \forall \cdot \text{US-complete } f \]

**Input:**

\[ M \in \{0, 1\}^{\sqrt{n} \times \sqrt{n}} \]

**Output:**

- yes iff
- \( \forall \) row has unique 1

\[
\begin{array}{|c|c|c|c|}
\hline
1 & & & \\
\hline
& 1 & & \\
\hline
& & 1 & \\
\hline
& & & 1 \\
\hline
\end{array}
\]
\( \text{mon}(F) \leq \log^{O(1)} n \)
\[ \text{mon}(F) \leq \log^{O(1)} n \]

\[ F \in \forall \cdot \text{US}^{cc} \]
\[ \text{mon}(F) \leq \log^{O(1)} n \]

\[ F \in \forall \cdot \text{US}^{cc} \]

- \( \forall \text{row}: \text{unique 1} \)
- \( \exists \text{row}: \text{multiple 1s} \)
- \( \text{done!} \)

\[ [\text{IW10,PSS14}] \]
\[ \text{mon}(F) \leq \log^{O(1)} n \]
mon(F) \leq \log^{O(1)} n

∀row: unique 1

∃row: multiple 1s

∀\forall\cdot US^{cc}

\downarrow [IW10,PSS14]

F|_{\mu} \in \forall\cdot UP^{cc}
\[ \text{mon}(F) \leq \log^{O(1)} n \]

\[
\forall \text{row: unique 1} \quad \exists \text{row: multiple 1s}
\]

- \[ F \in \forall \cdot \text{US}^{cc} \]
  - \[ [\text{IW10,PSS14}] \]
- \[ F|_\mu \in \forall \cdot \text{UP}^{cc} \]
  - \[ [\text{Yan89}] \]
- \[ F|_\mu \in \forall \cdot \text{P}^{cc} \]
\[ \text{mon}(F) \leq \log^{O(1)} n \]
\[
\text{mon}(F) \leq \log^{O(1)} n
\]

\[F \in \forall \cdot \text{US}^{cc}\]

\[F|_{\mu} \in \forall \cdot \text{UP}^{cc}\]

\[F|_{\mu} \in \forall \cdot \text{P}^{cc} = \text{coNP}^{cc}\]

\[\text{done!}\]
Some problems
Problems

- Exhibit $F$ with $\text{mon}(F) \ll \text{UPP}^{cc}(F)$
- Lifting using constant-size gadgets?
- Lifting for BQP? \[\text{[ABG}^+17]\]

Challenges

- Disprove the log-rank conjecture
- Explicit lower bounds against $\text{PH}^{cc}$?
  Or even $\text{SZK}^{cc} \subseteq \text{AM}^{cc} \subseteq \Pi_2 P^{cc}$? \[\text{[BCHTV16]}\]
Problems

- Exhibit $F$ with $\text{mon}(F) \ll \text{UPP}^{cc}(F)$
- Lifting using constant-size gadgets?
- Lifting for BQP? [ABG+17]

Challenges

- Disprove the log-rank conjecture
- Explicit lower bounds against $\text{PH}^{cc}$?
  Or even $\text{SZK}^{cc} \subseteq \text{AM}^{cc} \subseteq \Pi_2^{P^{cc}}$? [BCHTV16]

Cheers!