Augmented Index and Quantum Streaming Algorithms for DYCK(2)

ASHWIN NAYAK, AND DAVE TOUCHETTE

University of Waterloo, Perimeter Institute

CCC 2017, Riga, Latvia

8 July 2017
Communication Complexity

- Communication Complexity setting:

\[ C_1 = f_1(X, R_A) \]
\[ C_2 = f_2(Y, R_B, C_1) \]
\[ \ldots \]
\[ C_M = f_M(Y, R_B, C_{<M}) \]

Output: \( f(x, y) \)

- How much **communication** to compute \( f \) on \((x, y)\)
- Take information-theoretic view: Information Complexity
  - How much **information** to compute \( f \) on \((x, y) \sim \mu\)
  - Information content of interactive protocols?
  - Classical vs. Quantum?
Communication Complexity

- Communication Complexity setting:

- How much communication to compute $f$ on $(x, y)$

- Take information-theoretic view: Information Complexity
  - How much information to compute $f$ on $(x, y) \sim \mu$
  - Information content of interactive protocols?
  - Classical vs. Quantum?

Output: $f(x, y)$
Communication Complexity

- Communication Complexity setting:
  - How much communication to compute $f$ on $(x, y)$
  - Take information-theoretic view: Information Complexity
    - How much information to compute $f$ on $(x, y) \sim \mu$
    - Information content of interactive protocols?
    - Classical vs. Quantum?
Communication Complexity

- Communication Complexity setting:
  - How much communication to compute \( f \) on \( x, y \)
  - Take information-theoretic view: Information Complexity
    - How much information to compute \( f \) on \( (x, y) \sim \mu \)
    - Information content of interactive protocols?
    - Classical vs. Quantum?
Quantum Communication Complexity

Protocol \( \Pi: \)

\[
\begin{array}{c}
\mu |\psi\rangle \\
A_0 U_1 X A_1 \downarrow C_1 \downarrow C_2 \\
B_0 U_2 Y B_2 \\
A_0 U_3 X A_2 \downarrow C_3 \\
\vdots \downarrow \vdots \\
A_{M-1} U_{M-1} X A_{M-1} \downarrow C_{M-1} \\
\vdots \downarrow \vdots \\
B_{M-1} U_M Y B_{M-1} \\
\vdots \downarrow \vdots \\
B_f U_f X A_f \\
\end{array}
\]

Output: \( f(X,Y) \)
Th.1: Streaming Algorithms for DYCK(2)

- Streaming algorithms: Attractive model for early Quantum Computers
- Some exponential advantages possible for specially crafted problems [LeG06, GKKRdW07]
- \( \text{DYCK}(2) = \epsilon + [\text{DYCK}(2)] + (\text{DYCK}(2)) + \text{DYCK}(2) \cdot \text{DYCK}(2) \)
- Classical bound: \( s(N) \in \Omega\left(\frac{\sqrt{N}}{T}\right) \) [MMN10, JN10, CCKM10]
- Two-way classical algorithm: \( s(N) \in O(\text{polylog}(N)) \)

Diagram:

\[ |0^s(N)\rangle \]
\[ \text{Pre} \rightarrow O_{x_1} \rightarrow O_{x_2} \rightarrow \ldots \rightarrow O_{x_N} \rightarrow \text{Post} \]

Repeat T times
Th.1: Streaming Algorithms for DYCK(2)

Th. 1: Any T-pass 1-way qu. streaming algo. for DYCK(2) needs space $s(N) \in \Omega(\frac{\sqrt{N}}{T^3})$ on length N inputs
- Even holds for non-unitary streaming operations $O$
- Reduction from multi-party QCC to streaming algorithm to DYCK(2) [MMN10]
  - Multi-party problem consists of OR of multiple instances of two-party problem
  - Space $s(N)$ in algorithm corresponds to communication between parties
  - Consider T-pass, one-way quantum streaming algorithms
- Direct sum argument allows to reduce from a two-party problem, Augmented Index
  - Multi-party QCC lower bounds requires two-party QIC lower bound on “easy distribution”
  - Subtlety for non-unitary streaming operations $O$
**Th.2: Augmented Index**

- Index($x_1 \ldots x_i \ldots x_n, i$) = $x_i$
- Augmented Index: $AI_n(x_1 \ldots x_n, (i, x_1 \ldots x_{<i}, b)) = x_i \oplus b$

\[
\begin{align*}
  x_1 & \quad x_2 & \quad \ldots & \quad x_{i-1} & \quad x_i & \quad \ldots & \quad x_{n-1} & \quad x_n \\
  x_1 & \quad x_2 & \quad \ldots & \quad x_{i-1} & \quad x_i & \quad \ldots & \quad x_{n-1} & \quad x_n \\
  \vdots & \quad \vdots & \quad \ddots & \quad \vdots & \quad \vdots & \quad \ddots & \quad \vdots & \quad \vdots \\
\end{align*}
\]
Th. 2.2: Augmented Index

- Th. 2.2: For any r-round protocol $\Pi$ for $AI_n$, either
  - $QC_{A\rightarrow B}(\Pi, \mu_0) \in \Omega\left(\frac{n}{r^2}\right)$ or
  - $QC_{B\rightarrow A}(\Pi, \mu_0) \in \Omega\left(\frac{1}{r^2}\right)$ with
  - $\mu_0$ the uniform distribution on zeros of $AI_n$ ("easy distribution")

- Classical bounds:
  - $IC_{A\rightarrow B}(\Pi, \mu_0) \in \Omega\left(\frac{n}{2m}\right)$ or
  - $IC_{B\rightarrow A}(\Pi, \mu_0) \in \Omega(m)$
  - [MMN10, JN10, CCKM10, CK11]

- We Build on direct sum approach of [JN10]
- General approach uses two main Tools (Sup.-Average Encoding Th., Qu. Cut-and-Paste)
- More specialized approach uses one more Tool (Information Flow Lemma)
Warm-up: Disjointness

\[ \text{Disj}_n(x,y) = \neg \lor_{i \in [n]}(x_i \land y_i) \]

\[ \text{CC}(\text{Disj}_n) \in \Omega(n) \]
Warm-up: Disjointness

\[ CC(\text{Disj}_n) \geq IC_0(\text{Disj}_n) = n IC_0(\text{AND}) \] [BJKS02]

\[ IC \leq CC, IC \text{ satisfies direct sum property (needs private and public randomness)} \]

\[ IC_0(\text{AND}) = \frac{2}{3} I(X: M|Y = 0) + \frac{2}{3} I(Y: M|X = 0) \]

Comparing message transcript \( M \) on 01, 00, 10 inputs: ?
Tool: Average Encoding Theorem

- Average encoding theorem [KNTZ01]: $E_X[h^2(M^X, M^*)] \leq I(X: M)$
  - $M^* = E_X[M^X]$, average message
  - $h^2(M_1, M_2)$, Heilinger distance
  - Follows from Pinsker’s inequality
  - Low information messages are close to average message
- For AND, $Y = 0$: $\frac{1}{2} h^2(M^{00}, M^{*0}) + \frac{1}{2} h^2(M^{10}, M^{*0}) \leq I(X: M|Y = 0)$
  - Using Jensen and triangle inequality: $\frac{1}{4} h^2(M^{00}, M^{10}) \leq I(X: M|Y = 0)$
  - Similarly, for $X=0$: $\frac{1}{4} h^2(M^{00}, M^{01}) \leq I(Y: M|X = 0)$
  - Comparing 01, 10 inputs: $\frac{1}{8} h^2(M^{10}, M^{01}) \leq I(X: M|Y = 0) + I(Y: M|X = 0) = \frac{3}{2} I_C(AND)$
Warm-up: Disjointness

\[ CC(\text{Disj}_n) \geq IC_0(\text{Disj}_n) = n IC_0(\text{AND}) \] [BJKS02]

\[ IC \leq CC, IC \text{ satisfies direct sum property, needs private and public randomness} \]

\[ IC_0(\text{AND}) = \frac{2}{3} I(X: M|Y = 0) + \frac{2}{3} I(Y: M|X = 0) \]

Comparing message transcript \( M \) on 01, 00, 10 inputs:

\[ \frac{1}{12} h^2(M^{10}, M^{01}) \leq IC_0(\text{AND}) \]
Warm-up: Disjointness

\[ CC(\text{Dis}j_n) \geq IC_0(\text{Dis}j_n) = n IC_0(\text{AND}) \] [BJKS02]

\[ IC \leq CC, IC \text{ satisfies direct sum property, needs private and public randomness} \]

\[ IC_0(\text{AND}) = \frac{2}{3} I(X: M|Y = 0) + \frac{2}{3} I(Y: M|X = 0) \]

Comparing message transcript \( M \) on 01, 00, 10 inputs:

\[ \frac{1}{12} h^2(M^{10}, M^{01}) \leq IC_0(\text{AND}) \]

Comparing \( M \) on 00, 11 inputs: ?
Tool: Cut-and-Paste Lemma

- Consider input subset \( \{x_1, x_2\} \times \{y_1, y_2\} \)

\[
\begin{array}{cc}
  x_1 & y_1 \\
  x_2 & y_2 \\
\end{array}
\]

- Triangle inequality implies for \( M \) on \( (x_1, y_2) \) and \( (x_2, y_1) \):
  - \( h(M^{x_1y_2}, M^{x_2y_1}) \leq h(M^{x_1y_1}, M^{x_1y_2}) + h(M^{x_1y_1}, M^{x_2y_1}) \)

\[
\begin{array}{cc}
  x_1 & y_1 \\
  x_2 & y_2 \\
\end{array}
\quad + \quad
\begin{array}{cc}
  x_1 & y_1 \\
  x_2 & y_2 \\
\end{array}
\quad \Rightarrow \quad
\begin{array}{cc}
  x_1 & y_1 \\
  x_2 & y_2 \\
\end{array}
\]

- What about \( M \) on \( (x_1, y_1) \) and \( (x_2, y_2) \)?
  - Cut-and-paste Lemma [BJKS02]: \( h(M^{x_1y_1}, M^{x_2y_2}) = h(M^{x_1y_2}, M^{x_2y_1}) \)

\[
\begin{array}{cc}
  x_1 & y_1 \\
  x_2 & y_2 \\
\end{array}
\quad \Rightarrow \quad
\begin{array}{cc}
  x_1 & y_1 \\
  x_2 & y_2 \\
\end{array}
\]
Warm-up: Disjointness

\[ CC(Disj_n) \geq IC_0(Disj_n) = n IC_0(AND) \] [BJKS02]

\[ IC \leq CC, IC \text{ satisfies direct sum property, needs private and public randomness} \]

\[ IC_0(AND) = \frac{2}{3} I(X: M|Y = 0) + \frac{2}{3} I(Y: M|X = 0) \]

Comparing message transcript \( M \) on 01, 00, 10 inputs: \( \frac{1}{12} h^2(M^{10}, M^{01}) \leq IC_0(AND) \)

Comparing \( M \) on 00, 11 inputs: \( \frac{1}{12} h^2(M^{00}, M^{11}) = \frac{1}{12} h^2(M^{10}, M^{01}) \leq IC_0(AND) \)
Warm-up: Disjointness

\[ CC(\text{Disj}_n) \geq IC_0(\text{Disj}_n) = n IC_0(\text{AND}) \] [BJKS02]

\[ IC \leq CC, IC \text{ satisfies direct sum property, needs private and public randomness} \]

\[ IC_0(\text{AND}) = \frac{2}{3} I(X: M|Y = 0) + \frac{2}{3} I(Y: M|X = 0) \]

Comparing message transcript \( M \) on 01, 00, 10 inputs: \( \frac{1}{12} h^2(M^{10}, M^{01}) \leq IC_0(\text{AND}) \)

Comparing \( M \) on 00, 11 inputs: \( \frac{1}{12} h^2(M^{00}, M^{11}) = \frac{1}{12} h^2(M^{10}, M^{01}) \leq IC_0(\text{AND}) \)

Statistical interpretation: \( h(M_1, M_2) \geq \frac{1}{4} ||M_1 - M_2||_{TV} \)

\( ||M^{00} - M^{11}||_{TV} \in \Omega(1) \) since for AND, \( M^{00} \rightarrow 0, M^{11} \rightarrow 1 \)

\[ CC(\text{Disj}_n) \in \Omega(n) \]

Quantum?
Warm-up: Disjointness

\[ QCC(\text{Disj}_n) \in \Theta(\sqrt{n}) \]
\[ QCC^r(\text{Disj}_n) \in O(\frac{n}{r}), \text{ } r \text{ round protocols} \]
\[ QCC^r(\text{Disj}_n) \geq \frac{1}{r} \overline{QTC}_0^r(\text{Disj}_n) = \frac{1}{r} n \overline{QTC}_0^r(\text{AND}) \] [JRS03]
\[ \overline{QTC} \leq r QCC, \text{ } \overline{QTC} \text{ satisfies direct sum property, requires private and public “randomness”} \]

Comparing \( M \) on 01, 00, 10 inputs: ?
Tool: Quantum Average Encoding Theorem

- Average encoding theorem [KNTZ01, JRS03]: $E_X [h^2 (\rho_B^X, \rho_B)] \leq I(X:B)_\rho$
  - $\rho_{XB} = \sum_x p_X(x) |x\rangle \langle x| \otimes \rho_B^x$
  - $\rho_B = E_X [\rho_B^X]$, average state
  - $h^2 (\sigma, \theta) = 1 - F(\sigma, \theta)$, Bures distance, with $F(\sigma, \theta) = || \sqrt{\sigma} \sqrt{\theta} ||_1$
  - Follows from Pinsker’s inequality
- For AND: $\frac{1}{4} h^2 (\rho_{B_iC_i}^{00}, \rho_{B_iC_i}^{10}) \leq I(X: B_iC_i | Y = 0)_{\rho_i} = \overrightarrow{QC_i}$, odd $i$
  - Similarly, for $X=0$: $\frac{1}{4} h^2 (\rho_{A_iC_i}^{00}, \rho_{A_iC_i}^{01}) \leq I(Y: A_iC_i | X = 0)_{\rho_i} = \overrightarrow{QC_i}$, even $i$
Warm-up: Disjointness

\[ QCC(\text{Disj}_n) \in \Theta(\sqrt{n}) \]

\[ QCC^r(\text{Disj}_n) \in O\left(\frac{n}{r}\right), \ r \text{ round protocols} \]

\[ QCC^r(\text{Disj}_n) \geq \frac{1}{r} \widetilde{QIC}^r_0(\text{Disj}_n) = \frac{1}{r} n \widetilde{QIC}^r_0(\text{AND}) \quad [\text{JRS03}] \]

\[ \widetilde{QIC} \leq r \ QCC, \ \widetilde{QIC} \text{ satisfies direct sum property, requires private and public “randomness”} \]

Comparing \( M \) on 01, 00, 10 inputs:
- \[ \frac{1}{4} h^2(\rho_{B_iC_i}, \rho_{B_iC_i}^{10}) \leq \widetilde{QIC}_i \text{, odd } i \]
- \[ \frac{1}{4} h^2(\rho_{A_iC_i}, \rho_{A_iC_i}^{01}) \leq \widetilde{QIC}_i \text{, even } i \]
- \( \widetilde{QIC}^r_0(\text{AND}) = \sum_i \widetilde{QIC}_i \)
Warm-up: Disjointness

\[
QCC(Disj_n) \in \Theta(\sqrt{n})
\]

\[
QCC^r(Disj_n) \in O\left(\frac{n}{r}\right), \text{ } r \text{ round protocols}
\]

\[
QCC^r(Disj_n) \geq \frac{1}{r} \widetilde{QIC}^r_0(Disj_n) = \frac{1}{r} n \widetilde{QIC}^r_0(AND) \text{ [JRS03]}
\]

\[
\widetilde{QIC} \leq r \text{ } QCC, \text{ } \widetilde{QIC} \text{ satisfies direct sum property, requires private and public “randomness”}
\]

Comparing \(M\) on 01, 00, 10 inputs:

- \(\frac{1}{4} h^2(\rho_{B_iC_i}^{00}, \rho_{B_iC_i}^{10}) \leq \widetilde{QIC}_i, \text{ odd } i\)
- \(\frac{1}{4} h^2(\rho_{A_iC_i}^{00}, \rho_{A_iC_i}^{01}) \leq \widetilde{QIC}_i, \text{ even } i\)
- \(\widetilde{QIC}^r_0(AND) = \sum_i \widetilde{QIC}_i\)

Comparing \(M\) on 00, 11 inputs: ?
Tool: Quantum Cut-and-Paste Lemma

- Variant of a tool developed in [JRS03, JN10]
- Consider input subset \( \{x_1, x_2\} \times \{y_1, y_2\} \)
- Lemma: If for odd \( i \) and for even \( i \), then
  \[
  h \left( V_{A_t}^{x_1 \rightarrow x_2} V_{B_t}^{y_1 \rightarrow y_2} (\rho_{A_tB_tC_t}^{x_1y_1}), \rho_{A_tB_tC_t}^{x_2y_2} \right) \leq 2 \sum_{j=t} \delta_j
  \]

\[
\rho_{A_iC_j}^{i}, \rho_{A_iC_j}^{i} = \delta_i
\]
Tool: Quantum Cut-and-Paste Lemma

- Consider input subset \( \{x_1, x_2\} \times \{y_1, y_2\} \)

- Hybrid argument (up to correction unitaries \( V_{A_t}^{x_1 \rightarrow x_2}, V_{B_t}^{y_1 \rightarrow y_2} \), with previous round dependence)
Warm-up: Disjointness

\( QCC(\text{Disj}_n) \in \Theta(\sqrt{n}) \)

\( QCC^r(\text{Disj}_n) \in O\left(\frac{n}{r}\right) \), \( r \) round protocols

\( QCC^r(\text{Disj}_n) \geq \frac{1}{r} \widehat{QIC}_0^r(\text{Disj}_n) = \frac{1}{r} n \widehat{QIC}_0^r(\text{AND}) \) [JRS03]

\( \widehat{QIC} \leq r QCC \), \( \widehat{QIC} \) satisfies direct sum property, requires private and public “randomness”

Comparing \( M \) on 01, 00, 10 inputs:
- \( \frac{1}{4} h^2(\rho_{B_{iC_i}}^{00}, \rho_{B_{iC_i}}^{10}) \leq \widehat{QIC}_i \), odd \( i \)
- \( \frac{1}{4} h^2(\rho_{A_{iC_i}}^{00}, \rho_{A_{iC_i}}^{01}) \leq \widehat{QIC}_i \), even \( i \)
- \( \widehat{QIC}_0^r(\text{AND}) = \sum_i \widehat{QIC}_i \)

Comparing \( M \) on 00, 11 inputs: \( \frac{1}{4} h^2(\rho_{C_i}^{00}, \rho_{C_i}^{11}) \leq 4 r \sum_i \widehat{QIC}_i = 4 r \widehat{QIC}_0^r(\text{AND}) \)
Warm-up: Disjointness

\[ \text{QCC}(\text{Disj}_n) \in \Theta(\sqrt{n}) \]
\[ \text{QCC}^r(\text{Disj}_n) \in O\left(\frac{n}{r}\right), \text{ } r \text{ round protocols} \]
\[ \text{QCC}^r(\text{Disj}_n) \geq \frac{1}{r} \overline{QTC}_0^r(\text{Disj}_n) = \frac{1}{r} n \overline{QTC}_0^r(\text{AND}) \text{ [JRS03]} \]
\[ \overline{QTC} \leq r \text{ QCC}, \overline{QTC} \text{ satisfies direct sum property, requires private and public “randomness”} \]

Comparing \( M \) on 01, 00, 10 inputs:
\[ \frac{1}{4} h^2(\rho_{BiCi}^{00}, \rho_{BiCi}^{10}) \leq \overline{QTC}_i, \text{ odd } i \]
\[ \frac{1}{4} h^2(\rho_{AiCi}^{00}, \rho_{AiCi}^{01}) \leq \overline{QTC}_i, \text{ even } i \]
\[ \overline{QTC}_0^r(\text{AND}) = \sum_i \overline{QTC}_i \]

Comparing \( M \) on 00, 11 inputs:
\[ \frac{1}{4} h^2(\rho_{Ci}^{00}, \rho_{Ci}^{11}) \leq 4 r \sum_i \overline{QTC}_i = 4 r \overline{QTC}_0(\text{AND}) \]

Gives \( \overline{QTC}_0^r(\text{AND}) \in \Omega\left(\frac{1}{r}\right), \text{ QCC}^r(\text{Disj}_n) \in \Omega\left(\frac{n}{r^2} + r\right) \text{ [JRS03]} \]
Augmented Index

\[ AI_n(x_1 \ldots x_n, (i, x_1 \ldots x_{i-1}, b)) = x_i \oplus b \]

\( \mu_0 \): uniform distribution on \( x_i \oplus b = 0 \)

Either \( IC_{B \rightarrow A}(\Pi, \mu_0) \in \Omega(1) \)
Augmented Index

\[ AI_n(x_1 \ldots x_n, (i, x_1 \ldots x_{i-1}, b)) = x_i \oplus b \]

\( \mu_0 \): uniform distribution on \( x_i \oplus b = 0 \)

Either \( IC_{B \rightarrow A} (\Pi, \mu_0) \in \Omega(1) \) or \( IC_{A \rightarrow B} (\Pi, \mu_0) \in \Omega(n) \)

\[ x \]
\[ x_1 \]
\[ x_2 \]
\[ \ldots \]
\[ x_{i-1} \]
\[ x_i \]
\[ \ldots \]
\[ x_{n-1} \]
\[ x_n \]

\[ y \]
\[ x_1 \]
\[ x_2 \]
\[ \ldots \]
\[ x_{i-1} \]
\[ x_i \]
\[ \ldots \]
\[ x_{n-1} \]
\[ x_n \]

\[ i \in [n] \]

\[ b \in \{0, 1\} \]

\[ x_i \oplus b \]
Augmented Index

Direct sum approach [JN10]

Avoid switching Bob’s prefix: $x_l$ for $l \in \left[\frac{n}{2} + 1, n\right]$

\[
x = \begin{cases}
    x_1 & \\
    \vdots & \\
    x_{n/2} & \\
    x_{n/2+1} & \\
    x_l & \\
    \vdots & \\
    x_n & \\
\end{cases}
\]

\[
y = \begin{cases}
    x_1 & \\
    x_2 & \\
    \vdots & \\
    x_{i-1} & \\
\end{cases}
\]

$k \in [1, \frac{n}{2}]$

$l \in [\frac{n}{2} + 1, n]$

\[
\mathcal{A} \leftarrow \{0, 1\}
\]

\[
x_l \oplus \mathcal{A}
\]
Augmented Index

Direct sum approach [JN10]

Avoid switching Bob’s prefix: $x_l$ for $l \in \left[\frac{n}{2} + 1, n\right]$

Bob’s one bit input: $c$
- $c = 0 \leftrightarrow i = k$, $b = x_k$
- $c = 1 \leftrightarrow i = l$, $b = \tilde{x}_l$

Alice’s one bit input: $a$
- $x_i = \tilde{x}_l \oplus a$

Output $x_i \oplus b = 1 \leftrightarrow (a, c) = (1, 1)$
Augmented Index

Classical: Uses Average Encoding Theorem and Cut-and-Paste Lemma

Quantum?

$k \in [1, \frac{n}{2}]$

$l \in [\frac{n}{2} + 1, n]$

$x_k$

$x_{n/2}$

$x_{n/2+1}$

$x_l$

$x_{i-1}$

$x_{i+1}$

$x_n$

Bob’s one bit input: $c$

- $c = 0 \leftrightarrow i = k, \ b = x_k$
- $c = 1 \leftrightarrow i = l, \ b = \tilde{x}_l$

Alice’s one bit input: $a$

- $x_i = \tilde{x}_l \oplus a$

Output $x_i \oplus b = 1 \leftrightarrow (a, c) = (1, 1)$

$b \in \{0, 1\}$

$x_i \oplus b$
Augmented Index

- $\widetilde{QIC}_{A \rightarrow B}$ and $\widetilde{QIC}_{B \rightarrow A}$ allows for reduction between DYCK(2) and Augmented Index [JN10]
  - But Quantum Average Encoding Theorem + Cut-and-Paste approach breaks down
- $\widetilde{QIC}_{A \rightarrow B}$ and $\widetilde{QIC}_{B \rightarrow A}$ allows for Quantum Average Encoding Theorem + Cut-and-Paste [JN10]
  - But reduction between DYCK(2) and Augmented Index breaks down
  - $\widetilde{QIC}_{B \rightarrow A}$ does not satisfy direct sum, $\widetilde{QIC}_{B \rightarrow A} \leq QCC$
- Looking for alternative QIC that trades-off between these
- Subtle issues about dealing with distributions vs. dealing with superpositions, private randomness
Superposition vs. Distribution

- Input distribution: $\rho_{X,Y}^{\mu} = \sum_{x,y} \mu(x,y) |xy\rangle \langle xy|_{X,Y}$
- Superposition: $|\rho^{\mu}\rangle_{X,Y,R_X R_Y} = \sum_{x,y} \sqrt{\mu(x,y)} |xyxy\rangle_{X,Y,R_X R_Y}$
- $Tr_{R_X R_Y} [\rho_{X,Y,R_X R_Y}^{\mu}] = \rho_{X,Y}^{\mu}$
- Superposition can leak information
Superposition vs. Distribution

- Extension of Input distribution: $\bar{\rho}_{XYE}^{\mu} = \sum_{xye} \bar{\mu}(x, y, e) |xye\rangle\langle xye|_{XE}$ s.t. $Tr_E[\bar{\rho}_{XYE}^{\mu}] = \rho_{XY}^{\mu}$

- Alternative Superposition: $|\tilde{\rho}^{\mu}\rangle_{XYRXRYR_{E_1}R_{E_2}} = \sum_{xye} \sqrt{\tilde{\mu}(x, y, e)} |xyxyee\rangle_{XYRXRYR_{E_1}R_{E_2}}$

- $Tr_{R_XR_YR_{E_2}}[\tilde{\rho}_{XYRXRYR_{E_1}R_{E_2}}^{\mu}] = I_{E\rightarrow R_{E_1}}[\tilde{\rho}_{XYE}^{\mu}]$

- Isometry $V_{RXRYR_{E_1}R_{E_2}}$ maps $\rho^{\mu}$ to $\tilde{\rho}^{\mu}$
Superposition for Augmented Index

- Augmented Index: \( x = x_1 \ldots x_n, y = (i, x_1 \ldots x_{i-1}, b), b = x_i \) under \( \mu_0 \)
- Extension: \( K \in R \left[ \frac{1}{2}, \frac{n}{2} \right], L \in R \left[ \frac{n}{2} + 1, n \right], C \in R \{0,1\}, Z \in R \{0,1\}^L, W \in R \{0,1\}^{n-L} \)
  - \( X = ZW, I \in \{K, L\} \) according to \( C \)
  - \( Z = Z' Z'' \) with \( |Z'| = K \)
  - \( E = KLZWC \)
- \( |\tilde{\phi}^{\mu_0}\rangle_{R_{E_1}R_{E_2}R_XR_YX_Y} = \sum_{klzw} \sqrt{\ldots} |kl_{xzww}\rangle (|00\rangle|zw\rangle|jz'|zw\rangle^X|jz'|^Y + |11\rangle|zw\rangle|lz\rangle|zw\rangle^X|lz\rangle^Y) \)
- How to deal with such superposition?
Quantum Information Complexity (QIC)

\[ \text{QIC}(\Pi, \mu) = \sum_{i \text{ odd}} I(R_X R_Y: C_i | YB_i) + \sum_{i \text{ even}} I(R_X R_Y: C_i | XA_i) \]

- Motivated by quantum state redistribution, with \( R_X R_Y \) purifying the \( XY \) input registers:
  \[ \rho_{\mu_{RXRY}} = \sigma_x x, y \]
- Invariant under choice of purifying register. Works also with \( \tilde{\rho}_{\mu_{XYRXRYR_{E1}R_{E2}}} \)

Referee

|ψ\rangle_{ABCR} -> B
Quantum Information Complexity (QIC)

\[ \text{QIC}(\Pi, \mu) = \sum_{i \text{ odd}} I(R_X R_Y: C_i | Y B_i) + \sum_{i \text{ even}} I(R_X R_Y: C_i | X A_i) \]

- Motivated by quantum state redistribution, with \( R_X R_Y \) purifying the \( XY \) input registers:
  \[ |\rho_{\mu} \rangle_{R_X X R_Y Y} = \sum_{x,y} \sqrt{\mu(x,y)} |x y y \rangle_{R_X X R_Y Y} \]
- Invariant under choice of purifying register. Works also with \( |\tilde{\rho}_{\mu} \rangle_{X Y R_X R_Y R_E_1 R_E_2} \)

Properties [T15]:
- Additivity
- \( \text{QIC} \leq \text{QCC} \)

- QIC allows for reduction between DYCK(2) and Augmented Index
- What about Quantum Average Encoding Theorem + Cut-and-Paste approach?
  - Not directly. Superposition-Average Encoding Theorem!
Recoverability

- Recoverability [FR15]
  - There exists a recovery map $T_{B \rightarrow BC}$ such that
  - $h^2 (\rho_{RBC}, T_{B \rightarrow BC} (\rho_{RB})) \leq I(R: C|B)_{\rho}$

---

Diagram:

- Referee
- $\rho_{RBC}$
- $C$
- $B$
- $|\psi\rangle_{ABCR}$
- $R$
- $A$
- $C$
- $B$
- $T$
- $C$
- $B$
Tool: Superposition-Average Encoding Th.

- Average encoding theorem [KNTZ01]: \( E_X[h^2(\rho_B^X, \rho_B)] \leq I(X: B)_\rho \)
- What about superposition over (part of) \( X \)?
- Recall [FR15]'s recoverability theorem
  - There exists a recovery map \( T_{B \rightarrow BC} \) such that \( h^2(\rho_{RBC}, T_{B \rightarrow BC}(\rho_{RB})) \leq I(R: C|B)_\rho \)
- Theorem: If for odd \( i \) then \( h^2(\rho_{RXY_{i}Y_{B_i}}^f, \sigma_{RXY_{i}Y_{B_i}}^f) \leq M \sum_{i=t}^{\varepsilon_i} \)

\[ I(R_X R_Y : C_i | Y B_i ) = \varepsilon_i \]
Quantum Information Complexity (QIC)

- \( \text{QIC}(\Pi, \mu) = \sum_{i \text{ odd}} I( R_X R_Y : C_i | Y B_i ) + \sum_{i \text{ even}} I( R_X R_Y : C_i | X A_i ) \)
  - Motivated by quantum state redistribution, with \( R_X R_Y \) purifying the \( XY \) input registers:
    \[ |\rho(\mu)_{R_X R_Y} \rangle = \sum_{x,y} \sqrt{\mu(x,y)} |xxyy\rangle_{R_X R_Y} \]
  - Invariant under choice of purifying register. Works also with \( |\bar{\rho}(\mu)_{X Y R X R_Y R_E_1 R_E_2} \rangle \)

- Properties [T15]:
  - Additivity
  - \( \text{QIC} \leq \text{QCC} \)

- QIC allows for reduction between DYCK(2) and Augmented Index

- What about Quantum Average Encoding Theorem + Cut-and-Paste approach?
  - Superposition average encoding theorem allows to deal with such superpositions
  - How else?
Tool: Information Flow Lemma

- Lemma [LT17]: $I(R_E:XA_f|R_F) - I(R_E:X|R_F) = \sum_{i \text{ even}} I(R_E:C_i|XA_iR_F) - \sum_{i \text{ odd}} I(R_E:C_i|XA_iR_F)$
- $R_E, R_F$ arbitrary quantum extension to inputs $XY$
- $\tilde{QIC_i'} = I(R_1R_{K_1}R_{C_1}:R_{W_1}R_{W_2}WA_iC_i|R_{L_1}Z)_{\tilde{\rho_i}} = I(R_1R_{K_1}R_{C_1}:WZA_iC_i|R_{W_1}R_{W_2}R_{L_1}R_{Z_1})_{\tilde{\rho_i}} \leq QIC$
- Handles superposition such that it does not leak information about preparation
- Allows for Average Encoding Theorem

Diagram: Information Flow in a quantum system with controlled operations $U_i$ and measurements $C_i$.
Outlook

- Information-Theoretic Tools for Interactive Quantum Protocols
  - Superposition-average encoding theorem
  - Quantum Cut-and-Paste Lemma
  - Information Flow Lemma to handle superpositions

- Applications
  - Space lower bound on quantum streaming algorithms for DYCK(2)
    - Streaming with non-unitary operations
  - Quantum information trade-off for Augmented Index
    - Superposition vs. Distributions

- Open Questions
  - Remove dependence on number of round in Augmented Index trade-off
  - Obtain better quantum round elimination
  - Obtain stronger trade-off, $m$ vs. $\frac{n}{2^m}$
  - Obtain trade-off for $\mathcal{C}^{B\rightarrow A}$ (i.e. only limit how much information about index $i$ flows to Alice)
  - Find Further applications of tools...
References

[LeG06] - Le Gall. SPAA'06.
[GKKRdW06] - Gavinsky, Kempe, Kerenidis, Raz and de Wolf. STOC'07.
[BJKS02] - Bar-Yossef, Jayram, Kumar, and Sivakumar. FOCS'02.
[KNTZ01] - Klauck, Nayak, Ta-Shma and Zuckerman. STOC'01.
[JRS03] - Jain, Radhakrishnan and Sen. FOCS'03.