Introduction to Quantum Information Processing
QIC 710 / CS 768 / PH 767 / CO 681 / AM 871

Lecture 22-23 (2016)

Richard Cleve
QNC 3129
cleve@uwaterloo.ca
Communication complexity
Classical communication complexity

[Yao, 1979]

\[ x_1 x_2 \ldots x_n \quad y_1 y_2 \ldots y_n \]

E.g. equality function: \( f(x,y) = 1 \) if \( x = y \), and 0 if \( x \neq y \)

Question: can the communication be less than \( n \) bits?
Deterministic cost is \( n \) bits (I)

Table of all values of \( f(x,y) \):

<table>
<thead>
<tr>
<th></th>
<th>000</th>
<th>001</th>
<th>010</th>
<th>011</th>
<th>100</th>
<th>101</th>
<th>110</th>
<th>111</th>
</tr>
</thead>
<tbody>
<tr>
<td>000</td>
<td>1 0 0 0 0 0 0 0</td>
<td>0 1 0 0 0 0 0 0</td>
<td>0 0 1 0 0 0 0 0</td>
<td>0 0 0 1 0 0 0 0</td>
<td>0 0 0 0 1 0 0 0</td>
<td>0 0 0 0 0 1 0 0</td>
<td>0 0 0 0 0 0 1 0</td>
<td>0 0 0 0 0 0 0 1</td>
</tr>
</tbody>
</table>

Suppose the communication complexity of \( f \) is \( k \)

Each input in the domain of \( f \) fixes a conversation \( C \in \{0,1\}^{k+1} \)

Several inputs may lead to the same conversation ...

A rectangle is \( R \subseteq \{0,1\}^n \times \{0,1\}^n \)

of the form \( R = R_A \times R_B \)
**Deterministic cost is** \( n \) **bits (II)**

Table of all values of \( f(x,y) \):

<table>
<thead>
<tr>
<th></th>
<th>000</th>
<th>001</th>
<th>010</th>
<th>011</th>
<th>100</th>
<th>101</th>
<th>110</th>
<th>111</th>
</tr>
</thead>
<tbody>
<tr>
<td>000</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>001</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>010</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>011</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>100</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>101</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>110</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>111</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

In fact, the inputs leading to \( C \) must constitute a rectangle: if \((x,y), (x',y')\) both lead to \( C \) then so do \((x',y)\) and \((x,y')\)

Since each conversation has a unique output, \( f \) is constant on each of these rectangles

Need at least \( 2^{n+1} \) rectangles to \( \{0,1\} \)-partition this table

Since this implies \( \geq 2^{n+1} \) distinct conversations, \( k \geq n \)

Therefore, the deterministic communication complexity is \( n \)
Probabilistic cost is $O(\log n)$ bits

Start with a “good” classical error-correcting code, which is a function $e : \{0,1\}^n \rightarrow \{0,1\}^{cn}$ such that, for all $x \neq y$,

$$\Delta(e(x), e(y)) \geq \delta cn$$

($\Delta$ means Hamming distance), where $c, \delta$ are constants

randomly choose

$r \in \{1,2,\ldots, cn\}$

$(r, e(x)_r)$

output

$$\begin{cases} 1 \text{ if } e(y)_r = e(x)_r \\ 0 \text{ if } e(y)_r \neq e(x)_r \end{cases}$$

Can repeat to reduce error

$e(x) = 101111101011100111001$

$e(y) = 0110100100110011001010$
Quantum communication complexity

Qubit communication

Prior entanglement

Question: can quantum beat classical in this context?
Appointment scheduling
(also known as the \textit{Disjointness Problem})

\[
x = \begin{array}{cccccc}
1 & 2 & 3 & 4 & 5 & \ldots & n \\
0 & 1 & 1 & 0 & 1 & \ldots & 0
\end{array}
\quad i \quad \begin{array}{cccccc}
1 & 2 & 3 & 4 & 5 & \ldots & n \\
1 & 0 & 0 & 1 & 1 & \ldots & 1
\end{array}
\]

Classically, $\Omega(n)$ \textbf{bits} necessary to succeed with prob. $\geq 3/4$

For all $\varepsilon > 0$, $O(n^{1/2} \log n)$ \textbf{qubits} sufficient for error prob. $< \varepsilon$

[KS ‘87] [BCW ‘98]
Search problem

Given: \( x = 0 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0 \ \ldots \ 1 \) accessible via queries

\[
\log n \left\{ \begin{array}{c}
| i \rangle \\
1
\end{array} \right\} \xrightarrow{X} | i \rangle
\]

\[
1 \left\{ | b \rangle \right\} \xrightarrow{\oplus} | b \oplus x_i \rangle
\]

Goal: find \( i \in \{1, 2, \ldots, n\} \) such that \( x_i = 1 \)

Classically: \( \Omega(n) \) queries are necessary

Quantum mechanically: \( O(n^{1/2}) \) queries are sufficient

[Grover, 1996]
Alice \quad x = \begin{array}{ccccccc}
1 & 2 & 3 & 4 & 5 & 6 & \ldots & n \\
0 & 1 & 1 & 0 & 1 & 0 & \ldots & 0
\end{array}

Bob \quad y = \begin{array}{ccccccc}
1 & 0 & 0 & 1 & 1 & 0 & \ldots & 1
\end{array}

x \land y = \begin{array}{ccccccc}
0 & 0 & 0 & 0 & 1 & 0 & \ldots & 0
\end{array} \quad \text{(bitwise AND of } x \text{ and } y \text{)}

Communication per $x \land y$-query: $2(\log n + 3) = O(\log n)$
Appointment scheduling: epilogue

Bit communication:
Cost: $\theta(n)$

Qubit communication:
Cost: $\theta(n^{1/2})$ (with refinements)

Bit communication & prior entanglement:
Cost: $\theta(n^{1/2})$

Qubit communication & prior entanglement:
Cost: $\theta(n^{1/2})$

[R ‘02] [AA ‘03]
Quantum fingerprinting
Equality revisited
in simultaneous message model

$x_1 x_2 \ldots x_n$  $y_1 y_2 \ldots y_n$

Equality function:
$$f(x,y) = \begin{cases} 1 & \text{if } x = y \\ 0 & \text{if } x \neq y \end{cases}$$

Exact protocols: require $2n$ bits communication
Equality revisited
in simultaneous message model

\[ x_1 x_2 \ldots x_n \]

\[ y_1 y_2 \ldots y_n \]

classically correlated

\[ f(x, y) \]

\[ \Pr[00] = \Pr[11] = \frac{1}{2} \]

Bounded-error protocols with a shared random key:
require only \( O(1) \) bits communication

Error-correcting code:
\[
\begin{align*}
e(x) &= 1 0 1 1 1 1 1 0 1 1 0 1 1 0 0 1 1 0 0 1 \\
e(y) &= 0 1 1 0 1 0 0 1 0 0 1 1 0 0 1 1 0 0 1 0 1 0
\end{align*}
\]

random \( k \)
Equality revisited in simultaneous message model

\[ x_1 x_2 \ldots x_n \quad y_1 y_2 \ldots y_n \]

\[ \sqrt{n \times n} \quad \sqrt{n \times n} \]

\[ e(x) = \begin{array}{cccccc}
1 & 0 & 1 & 1 & 1 & 1 \\
0 & 1 & 0 & 1 & 1 & 0 \\
0 & 1 & 1 & 0 & 1 & 1
\end{array} \]

\[ e(y) = \begin{array}{cccccc}
1 & 1 & 0 & 0 & 0 & 1 & 0 \\
1 & 1 & 1 & 1 & 0 & 0 \\
0 & 1 & 0 & 0 & 1 & 1 \\
0 & 0 & 1 & 1 & 1 & 0 \\
1 & 1 & 0 & 1 & 0 & 1 \\
1 & 0 & 1 & 1 & 0 & 1 \\
\end{array} \]

Bounded-error protocols \textit{without} a shared key:

\textbf{Classical:} \( \theta(n^{1/2}) \)

\textbf{Quantum:} \( \theta(\log n) \) using “quantum fingerprints”

[A ‘96] [NS ‘96] [BCWW ‘01]
Quantum fingerprints

Question 1: how many orthogonal states in \( m \) qubits?

Answer: \( 2^m \)

Let \( \varepsilon \) be an arbitrarily small positive constant

Question 2: how many almost orthogonal\(^*\) states in \( m \) qubits?

\(^*\) where \( |\langle \psi_x | \psi_y \rangle| \leq \varepsilon \)

Answer: \( 2^{2am} \), for some constant \( 0 < a < 1 \)

Construction of almost orthogonal states: start with a special classical error-correcting code, which is a function

\[ e : \{0,1\}^n \rightarrow \{0,1\}^{cn} \]

such that, for all \( x \neq y \),

\[ \delta cn \leq \Delta(e(x), e(y)) \leq (1-\delta)cn \]

\( (c, \delta \) are constants)
Construction of almost orthogonal states

Set \( |\psi_x\rangle = \frac{1}{\sqrt{cn}} \sum_{k=1}^{cn} (-1)^{e(x)_k} |k\rangle \) for each \( x \in \{0,1\}^n \) (log\(cn\) qubits)

Then \( \langle \psi_x | \psi_y \rangle = \frac{1}{cn} \sum_{k=1}^{cn} (-1)^{[e(x) \oplus e(y)]_k} |k\rangle = 1 - \frac{2\Delta(e(x), e(y))}{cn} \)

Since \( \delta cn \leq \Delta(e(x), e(y)) \leq (1-\delta)cn \), we have \( |\langle \psi_x | \psi_y \rangle| \leq 1 - 2\delta \)

By duplicating each state, \( |\psi_x\rangle \otimes |\psi_x\rangle \otimes \ldots \otimes |\psi_x\rangle \), the pairwise inner products can be made arbitrarily small: \( (1 - 2\delta)^r \leq \epsilon \)

Result: \( m = r \log(cn) \) qubits storing \( 2^n = 2^{(1/c)2^{m/r}} \) different states

(as opposed to \( n \) qubits!)
What are these almost orthogonal states good for?

Question 3: can they be used to somehow store $n$ bits using only $O(\log n)$ qubits?

Answer: No—recall that Holevo’s theorem forbids this.

Here’s what we can do: given two states from an almost orthogonal set, we can distinguish between these two cases:

• they’re both the same state
• they’re almost orthogonal

Question 4: How?
Quantum fingerprints

Let $|\psi_{000}\rangle$, $|\psi_{001}\rangle$, ..., $|\psi_{111}\rangle$ be $2^n$ states on $O(\log n)$ qubits such that $|\langle \psi_x|\psi_y\rangle| \leq \epsilon$ for all $x \neq y$

Given $|\psi_x\rangle|\psi_y\rangle$, one can check if $x = y$ or $x \neq y$ as follows:

Intuition: $|0\rangle|\psi_x\rangle|\psi_y\rangle + |1\rangle|\psi_y\rangle|\psi_x\rangle$

Note: error probability can be reduced to $((1+\epsilon^2)/2)^r$
Equality revisited in simultaneous message model

\[ x_1 x_2 \ldots x_n \quad y_1 y_2 \ldots y_n \]

Bounded-error protocols **without** a shared key:

**Classical:** \( \theta(n^{1/2}) \)

**Quantum:** \( \theta(\log n) \)

[A ‘96] [NS ‘96] [BCWW ‘01]
Quantum protocol for equality in simultaneous message model

Recall that, with a shared key, the problem is easy classically ...

This quantum protocol only requires $\theta(\log n)$ qubits
Inner product
Inner product function

\[ f(x, y) = x \cdot y = x_1 y_1 + x_2 y_2 + \ldots + x_n y_n \mod 2 \]
Aside: Bernstein-Vazirani problem I

Let $f(x_1, x_2, \ldots, x_n) = a_1 x_1 + a_2 x_2 + \ldots + a_n x_n \mod 2$

Given:

$$\begin{align*}
|x_1\rangle & \rightarrow |x_1\rangle \\
|x_2\rangle & \rightarrow |x_2\rangle \\
& \vdots \\
|x_n\rangle & \rightarrow |x_n\rangle \\
|b\rangle & \rightarrow |b \oplus f(x_1, x_2, \ldots, x_n)\rangle
\end{align*}$$

Goal: determine $a_1, a_2, \ldots, a_n$

Classically, $n$ queries are necessary
Aside: Bernstein-Vazirani problem II

Let $f(x_1, x_2, ..., x_n) = a_1 x_1 + a_2 x_2 + ... + a_n x_n \mod 2$

Given:

\[
\begin{align*}
|0\rangle & \quad H \quad H \quad |a_1\rangle \\
|0\rangle & \quad H \quad H \quad |a_2\rangle \\
\vdots & \quad \vdots \\
|0\rangle & \quad H \quad H \quad |a_n\rangle \\
|1\rangle & \quad H \quad H \quad |1\rangle
\end{align*}
\]

Goal: determine $a_1, a_2, ..., a_n$

Classically, $n$ queries are necessary

Quantum mechanically, 1 query is sufficient
Lower bound for inner product I

\[ x \cdot y = x_1 y_1 + x_2 y_2 + \ldots + x_n y_n \mod 2 \]

Proof:

Alice and Bob’s IP protocol

Alice and Bob’s IP protocol inverted

Proof:
Lower bound for inner product II

\[ x \cdot y = x_1 y_1 + x_2 y_2 + \ldots + x_n y_n \mod 2 \]

Proof:

Since \( n \) bits are conveyed from Alice to Bob, \( n \) qubits communication necessary (by Holevo’s Theorem)