Introduction to Quantum Information Processing

Lecture 18

Richard Cleve
Overview of Lecture 18

• Continuation of fingerprinting
• Hidden matching problem
• Restricted-equality nonlocality
• Universal sets of gates
quantum fingerprints
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

\[ x_1 x_2 \ldots x_n \quad \text{classical} \]

\[ y_1 y_2 \ldots y_n \quad \text{classical} \]

\[ f(x, y) \]

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

Error-correcting code:  
\[ e(x) = 1 0 1 1 1 1 1 0 0 1 \]
\[ e(y) = 1 1 0 1 0 1 0 1 0 1 0 1 0 1 0 \]

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

$\mathbf{x}_1 \mathbf{x}_2 \ldots \mathbf{x}_n$

$\mathbf{y}_1 \mathbf{y}_2 \ldots \mathbf{y}_n$

Bounded-error protocols "without" a shared key:

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

Quantum: $\theta(\log n)$

[A '96] [NS '96] [BCWW '01]
Quantum 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 \textit{almost orthogonal}\(^*\) states in \( m \) qubits?
(* where \( |\langle \psi_x | \psi_y \rangle| \leq \varepsilon \) )

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

To be continued during next lecture ...
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 \( a > 0 \)

The states can be constructed via a suitable (classical) error-correcting code, which is a function \( e: \{0,1\}^n \rightarrow \{0,1\}^{cn} \) where, for all \( x \neq y \), \( dcn \leq \Delta(e(x),e(y)) \leq (1-d)cn \) (\( c \), \( d \) 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 $dcn \leq \Delta(e(x),e(y)) \leq (1-d)cn$, we have $|\langle \psi_x | \psi_y \rangle| \leq 1-2d$

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: $(1-2d)^r \leq \epsilon$

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

Let $|\psi_{000}\rangle, |\psi_{001}\rangle, \ldots, |\psi_{111}\rangle$ be $2^n$ states on $O(\log n)$ qubits such that $|\langle \psi_x | \psi_y \rangle| \leq \varepsilon$ 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: $|0\rangle|\psi_x\rangle|\psi_y\rangle + |1\rangle|\psi_y\rangle|\psi_x\rangle$

if $x = y$, $\Pr[\text{output} = 0] = 1$
if $x \neq y$, $\Pr[\text{output} = 0] = \frac{(1 + \varepsilon^2)}{2}$

Note: error probability can be reduced to $((1 + \varepsilon^2)/2)^{\ell}$
Equality revisited
in simultaneous message model

$x_1 x_2 \ldots x_n$

\[ f(x, y) \]

$y_1 y_2 \ldots y_n$

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

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

\textbf{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 ...
...hidden matching problem
Hidden matching problem

For this problem, a quantum protocol is exponentially more efficient than any classical protocol—even with a shared key.

Inputs: \( x \in \{0,1\}^n \)

Output: \( (i,j, x_i \oplus x_j) \), such that \( (i,j) \in M \)

Only **one-way** communication (Alice to Bob) is permitted

[Bar-Yossef, Jayram, Kerenidis, 2004]
The hidden matching problem

Inputs: \( x \in \{0,1\}^n \)

Output: \((i, j, x_i \oplus x_j), \ (i, j) \in M\)

Classically, one-way communication is \(\Omega(\sqrt{n})\), even with a shared classical key (the proof is omitted here)

**Rough intuition:** Alice doesn’t know which edges are in \( M \), so she would have to send \(\Omega(\sqrt{n})\) bits of the form \(x_i \oplus x_j\) …
The hidden matching problem

Inputs: \( x \in \{0,1\}^n \)

Output: \((i, j, x_i \oplus x_j), (i, j) \in M\)

Quantum protocol: Alice sends \( \frac{1}{\sqrt{n}} \sum_{k=1}^{n} (-1)^{x_k} |k\rangle \) (log n qubits)

Bob measures in \(|i\rangle \pm |j\rangle\) basis, \((i, j) \in M\), and uses the outcome’s relative phase to determine \(x_i \oplus x_j\)
nonlocality revisited
Restricted-equality nonlocality

inputs: \(x\) \((n\ \text{bits})\) \hspace{2cm} \(y\) \((n\ \text{bits})\)

outputs: \(a\) \((\log n\ \text{bits})\) \hspace{2cm} \(b\) \((\log n\ \text{bits})\)

Precondition: either \(x = y\) or \(\Delta(x,y) = n/2\)

Required postcondition: \(a = b\) iff \(x = y\)

With classical resources, \(\Omega(n)\ \text{bits of communication needed}\)

for an exact solution*

With \((|00\rangle + |11\rangle)^{\otimes \log n}\) prior entanglement, no communication is needed at all*

* Technical details similar to restricted equality of Lecture 17

[BCT '99]
Restricted-equality nonlocality

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

**Qubit communication:**
- Cost: $\log n$

**Bit communication & prior entanglement:**
- Cost: zero

**Qubit communication & prior entanglement:**
- Cost: zero
Nonlocality and communication complexity conclusions

• Quantum information affects communication complexity in interesting ways

• There is a rich interplay between quantum communication complexity and:
  – quantum algorithms
  – quantum information theory
  – other notions of complexity theory …
universality of two-qubit gates
A universal set of gates

**Theorem:** any unitary operation $U$ acting on $k$ qubits can be decomposed into $O(4^k)$ CNOT and one-qubit gates

(This was stated in Lecture 5 without a proof)

**Proof sketch** (for a slightly worse bound of $O(k^24^k)$):

We first show how to simulate a controlled-$U$, for any one-qubit unitary $U$

**Fact:** for any one-qubit unitary $U$, there exist $A$, $B$, $C$, and $\lambda$, such that:

- $A B C = I$
- $e^{i\lambda} A X B X C = U$, where $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
A universal set of gates

The aforementioned fact implies

\[
\begin{bmatrix}
U \\
A \\
B \\
C
\end{bmatrix}
\equiv
\begin{bmatrix}
P \\
A \\
B \\
C
\end{bmatrix}
\]

where

\[
P = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{pmatrix}
\]

Using such controlled-\(U\) gates, one can simulate controlled-controlled-\(V\) gates, for any unitary \(V\), as follows:

\[
\begin{bmatrix}
V \\
U \\
U^\dagger \\
U
\end{bmatrix}
\equiv
\begin{bmatrix}
U \\
U \\
U^\dagger \\
U
\end{bmatrix}
\]

where \(V = U^2\)
A universal set of gates

When $U = X$, this construction yields the 3-qubit Toffoli gate

From this gate, generalized Toffoli gates can be constructed:
A universal set of gates

From generalized Toffoli gates, \textit{generalized controlled-}U gates (controlled-controlled- \ldots \textit{controlled}-U) can be constructed:

\[ U |0\rangle = |0\rangle \]

\[
\begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & U_{00} & U_{01} \\
0 & 0 & 0 & 0 & 0 & 0 & U_{10} & U_{11}
\end{pmatrix}
\]
A universal set of gates

The approach essentially enables any \( k \)-qubit operation of the simple form

\[
\begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & U_{00} & 0 & 0 & U_{01} & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & U_{10} & 0 & 0 & U_{11} & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{pmatrix}
\]

to be computed with \( O(k^2) \) CNOT and one-qubit gates

Any \( 2^k \times 2^k \) unitary matrix can be decomposed into a product of \( O(4^k) \) such simple matrices
A universal set of gates

This completes the proof sketch

Thus, the set of all one-qubit gates and the CNOT gate are universal in that they can simulate any other gate set

Question: is there a finite set of gates that is universal?

Answer 1: strictly speaking, no, because this results in only countably many quantum circuits, whereas there are uncountably many unitary operations on $k$ qubits (for any $k$)
THE END