Overview of Lecture 7

• The one-out-of-four search problem
• The constant vs. balanced problem
• $H \otimes H \otimes \ldots \otimes H$
• Fourier sampling
• Preview of where black-box results are headed: period-finding
• Simulating black boxes
Query algorithms

**Last time:** quantum algorithm for computing $f(0) \oplus f(1)$ making just 1 query to $f$, whereas any classical algorithm requires 2 queries

**This time:** other, stronger quantum vs. classical separations, plus discussion about their relevance to algorithm design
one-out-of-four search
One-out-of-four search

Let $f : \{0,1\}^2 \rightarrow \{0,1\}$ have the property that there is exactly one $x \in \{0,1\}^2$ for which $f(x) = 1$

Four possibilities:

<table>
<thead>
<tr>
<th>$x$</th>
<th>$f_{00}(x)$</th>
<th>$x$</th>
<th>$f_{01}(x)$</th>
<th>$x$</th>
<th>$f_{10}(x)$</th>
<th>$x$</th>
<th>$f_{11}(x)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>1</td>
<td>00</td>
<td>0</td>
<td>00</td>
<td>0</td>
<td>00</td>
<td>0</td>
</tr>
<tr>
<td>01</td>
<td>0</td>
<td>01</td>
<td>1</td>
<td>01</td>
<td>0</td>
<td>01</td>
<td>0</td>
</tr>
<tr>
<td>10</td>
<td>0</td>
<td>10</td>
<td>0</td>
<td>10</td>
<td>1</td>
<td>10</td>
<td>0</td>
</tr>
<tr>
<td>11</td>
<td>0</td>
<td>11</td>
<td>0</td>
<td>11</td>
<td>0</td>
<td>11</td>
<td>1</td>
</tr>
</tbody>
</table>

Goal: find $x \in \{0,1\}^2$ for which $f(x) = 1$

Classically: 3 queries are necessary and sufficient

Quantumly: 1 query suffices!
Quantum algorithm

Black box for 1-4 search:

Input state to query:

Output state:

\[(|00\rangle + |01\rangle + |10\rangle + |11\rangle)(|0\rangle - |1\rangle)\]
Quantum algorithm

Output state of the first two qubits in the four cases:

\[ |\psi_{00}\rangle = -|00\rangle + |01\rangle + |10\rangle + |11\rangle \]
\[ |\psi_{01}\rangle = +|00\rangle - |01\rangle + |10\rangle + |11\rangle \]
\[ |\psi_{10}\rangle = +|00\rangle + |01\rangle - |10\rangle + |11\rangle \]
\[ |\psi_{11}\rangle = +|00\rangle + |01\rangle + |10\rangle - |11\rangle \]

Note that these states are orthogonal!

Challenge Exercise: simulate the above \( U \) in terms of \( H \), Toffoli, and NOT gates
one-out-of-$N$ search?

**Natural question:** what about search problems in spaces larger than *four* (and without uniqueness conditions)?

For spaces of size *eight* (say), the previous method breaks down—the state vectors will not be orthogonal.

Later on, we’ll see how to search a space of size $N$ with $O(\sqrt{N})$ queries ...
constant vs. balanced
Constant vs. balanced

Let \( f : \{0,1\}^n \rightarrow \{0,1\} \) be either constant or balanced, where

**constant** means \( f(x) = 0 \) for all \( x \), or \( f(x) = 1 \) for all \( x \)

**balanced** means \( \sum_x f(x) = 2^{n-1} \)

**Goal**: determine whether \( f \) is constant or balanced

**Classically**: \( \frac{1}{2} 2^n + 1 \) queries are needed

**Example**: if \( f(0000) = f(0001) = f(0010) = \ldots = f(0111) = 0 \) then could be either

**Quantumly**: just 1 query suffices!

[Deutsch & Jozsa, 1992]
Quantum algorithm

Constant case: $|\psi\rangle = \pm \sum |x\rangle$ (why?)

Balanced case: $|\psi\rangle$ is orthogonal to $\pm \sum |x\rangle$ (why?)

How to distinguish between the cases? What is $H^\otimes n |\psi\rangle$?

Constant case: $H^\otimes n |\psi\rangle = \pm |00...0\rangle$

Balanced case: $H^\otimes n |\psi\rangle$ is orthogonal to $|0...00\rangle$

Last step of the algorithm: if the measured result is 000 then output “constant”, otherwise output “balanced”
Probabilistic classical algorithm solving constant vs balanced

But here’s a classical procedure that makes only 2 queries and has one-sided error probability $\frac{1}{2}$:

1. pick $x_1, x_2 \in \{0, 1\}^n$ randomly
2. if $f(x_1) \neq f(x_2)$ then output balanced else output constant

If $f$ is constant the algorithm always succeeds
If $f$ is balanced the algorithm succeeds with probability $\frac{1}{2}$

By repeating the above procedure $k$ times: $2k$ queries and one-sided error probability $(\frac{1}{2})^k$

Therefore, for large $n$, $<< 2^n$ queries are likely sufficient
About $H \otimes H \otimes \ldots \otimes H = H^\otimes n$

**Theorem:** for $x \in \{0,1\}^n$, $H^\otimes n |x\rangle = \frac{1}{2^{n/2}} \sum_{y \in \{0,1\}^n} (-1)^{x \cdot y} |y\rangle$

where $x \cdot y = x_1y_1 \oplus \ldots \oplus x_ny_n$

**Example:** $H \otimes H = \frac{1}{2} \begin{bmatrix} +1 & +1 & +1 & +1 \\ +1 & -1 & +1 & -1 \\ +1 & +1 & -1 & -1 \\ +1 & -1 & -1 & +1 \end{bmatrix}$

**Pf:** For all $x \in \{0,1\}^n$, $H |x\rangle = |0\rangle + (-1)^{x} |1\rangle = \sum_y (-1)^{x \cdot y} |y\rangle$

Thus, $H^\otimes n |x_1 \ldots x_n\rangle = (\sum_{y_1} (-1)^{x_1y_1} |y_1\rangle) \ldots (\sum_{y_n} (-1)^{x_ny_n} |y_n\rangle)$

$= \sum_y (-1)^{x_1y_1 \oplus \ldots \oplus x_ny_n} |y_1 \ldots y_n\rangle$