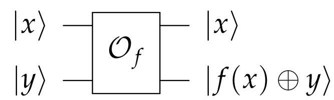
CS 410/510 Introduction to Quantum Computing
Lecture 5

Portland State U, Spring 2017 — *April 18, 2017*
Lecturer: Fang Song — *Scribe: Nate Launchbury*

VERSION: MAY 31, 2017

1 Simon's Problem

Input: $f : \{0,1\}^n \to \{0,1\}^n$ as an oracle circuit,



Promise: $\exists s \in \{0,1\}^n$ such that $\forall x, y \in \{0,1\}^n$, $f(x) = f(y)$ iff $x \oplus y = s$

Goal: Find s (using as few oracles queries as possible).

Notice that the promise in Simon's problem says that there is some shift, s, so that the function f returns the same value only on inputs x and $x \oplus s$, for all inputs x. So, intuitively, if we ever observe two inputs that map to the same output value, we can recover s, which is our goal. This gives rise to our classical algorithms for solving Simon's problem.

Deterministic algorithm (idea): query $\mathcal{O}_f$ until you observe two distinct inputs with the same output value. Since f maps to $2^n/2$ unique outputs, the pigeon-hole principle tell us that we will need $2^n/2 + 1$ oracle queries in the worst case.

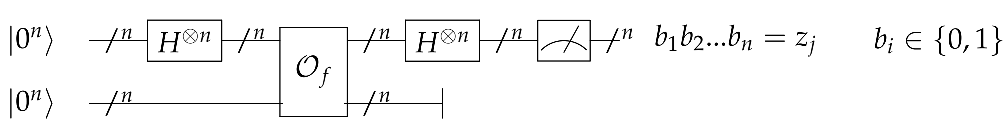
Randomized algorithm:

1. pick $x_1, ..., x_k \in \{0,1\}^n$ at random
2. compute $y_1 = f(x_1), ..., y_k = f(x_k)$
3. check if $\exists x_i, x_j$ such that $y_i = y_j$ (call this event E) and return $x_i \oplus x_j$ if so

How large must k be so that $Pr[E] \geq 0.99$? We find a collision with probability $k^2/2^n$ (by Birthday bound) so we need $k \approx \sqrt{2^n}$ oracle queries to have a high chance of finding s.

Quantum algorithm:

Repeat the following quantum circuit, Q, m times,



Post-processing on $z_1, z_2, ..., z_m$ gives s (each z_j is the string made by the first n output bits of the j-th repetition of the above circuit).

Results:

Deterministic	Randomized	Quantum
$2^n/2+1$	$\Omega(2^n/2)$	$O(n^2)$

This is the first quantum algorithm we've seen to give exponential speedup!

1.1 Analysis of quantum circuit Q

$$
\begin{aligned}
|0^n\rangle \otimes |0^n\rangle &\xrightarrow{H^{\otimes n} \otimes I} \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle \otimes |0^n\rangle \\
&\xrightarrow{\mathcal{O}_f} \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle \otimes |f(x) \oplus 0^n\rangle \\
&= \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} \Big(\frac{1}{\sqrt{2^n}} \sum_{y \in \{0,1\}^n} (-1)^{x \cdot y} |y\rangle\ \Big) \otimes |f(x)\rangle \qquad \text{by previous lemma} \\
&= \sum_{y \in \{0,1\}^n} \Big(\sum_{x \in \{0,1\}^n} \frac{1}{2^n} (-1)^{x \cdot y} |f(x)\rangle\ \Big) \otimes |y\rangle \\
&= |\psi_y\rangle \otimes |y\rangle \qquad \text{where } |\psi_y\rangle = \sum_{x \in \{0,1\}^n} \frac{1}{2^n} (-1)^{x \cdot y} |f(x)\rangle \\
&\xrightarrow{\text{measure}} \ ?
\end{aligned}
$$

We consider the possibilities after measuring $|\psi_y\rangle$.
Let $|\psi\rangle = \sum_{y \in \{0,1\}^n} |\psi_y\rangle \otimes |y\rangle$
Define $A = range(f)$, then $|A| = 2^{n-1}$
Notice if $f(x) = z$, there are two possible xs: x_z and $x_{z \oplus s}$
So

$$
\begin{aligned}
\sum_x (-1)^{x \cdot y} |f(x)\rangle &= \sum_{z \in A} ((-1)^{x_z \cdot y} + (-1)^{x_{z \oplus s} \cdot y}) |z\rangle \\
&= \sum_{z \in A} (-1)^{x_z \cdot y} (1 + (-1)^{y \cdot s}) |z\rangle
\end{aligned}
$$

Observation:

- if $y \cdot s = 1$, then $1 + (-1)^{y \cdot s} = 0$
- if $y \cdot s = 0$, then $1 + (-1)^{y \cdot s} = 2 \neq 0$
- in addition, there are 2^{n-1} strings y such that $y \cdot s = 0$.

Therefore,

$$
Pr[\text{measure } y] = \begin{cases} 0 & \text{if } y \cdot s = 1 \\ \frac{1}{2^{n-1}} & \text{if } y \cdot s = 0 \end{cases}
$$

1.2 Geometric interpretation

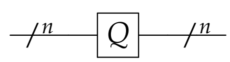
View $\{0,1\}^n$ as a vector space and pick m vectors on a hyperplane orthogonal to s We end up with:

$$
\begin{gathered}
z_1 \cdot s = 0 \\
z_2 \cdot s = 0 \\
\dots \\
z_m \cdot s = 0
\end{gathered}
$$

since every z_i is orthogonal to s. We need n linearly independent equations to uniquely determine s in this way. To get n with high probability we need $m = O(n^2)$. We can then solve for s classically using Coppersmith-Winogard in $O(n^{2.376})$

2 Phase Estimation

Consider the following quantum circuit, Q:



where Q implements a unitary transformation $U_{N\times N}$ for $N = 2^n$ and has eigenvectors, $\{|\psi_1\rangle, |\psi_2\rangle, ..., |\psi_N\rangle\}$. Since $|\psi_j\rangle$ are eigenvectors,

$$
U|\psi_j\rangle = e^{2\pi i\theta_j}|\psi_j\rangle \text{ and also } \langle\psi_j|\psi_k\rangle = \begin{cases} 1 & \text{if } j = k \\ 0 & \text{otherwise} \end{cases}
$$

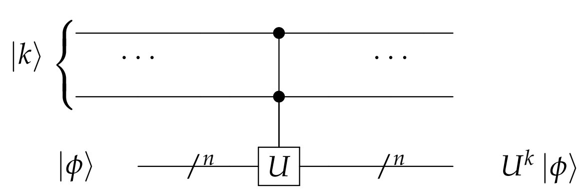
This means that the set of eigenvectors is orthonormal.

Input:

1. Q, a quantum circuit for U
2. $|\psi\rangle$, an eigenvector of U (so $U|\psi\rangle = e^{2\pi i\theta}|\psi\rangle$).

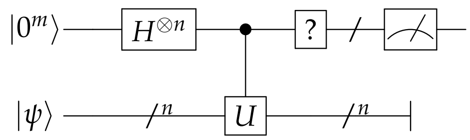
Goal: Compute θ approximately.

Notation: $\Lambda_m(U)|k\rangle|\phi\rangle = |k\rangle U^k|\phi\rangle$ is a *controlled unitary* with $k \in \{0, ..., 2^{m-1}\}$:



Fact: if $k = O(\log n)$ then we can implement $\Lambda_m(U)$ efficiently.

2.1 Algorithm



Let's track how the state changes to figure out the ? gate.

$$
\begin{aligned}
|0^m\rangle \otimes |\psi\rangle \xrightarrow{H^{\otimes n} \otimes I} & \frac{1}{\sqrt{2^m}} \sum_{x \in \{0,1\}^m} |x\rangle \otimes |\psi\rangle \\
\xrightarrow{C-U} & \frac{1}{\sqrt{2^m}} \sum_{x \in \{0,1\}^m} |x\rangle \otimes U^x |\psi\rangle \\
= & \frac{1}{\sqrt{2^m}} \sum_{x \in \{0,1\}^m} \mathrm{e}^{2\pi i \theta x} |x\rangle \otimes |\psi\rangle \qquad \text{since } U^x |\psi\rangle = \mathrm{e}^{2\pi i \theta x} |\psi\rangle
\end{aligned}
$$

So right before we apply the ? gate, we have information about θ. We just need to think of a way to extract that information so that we can recover θ after measuring (approximately and with high probability).

2.2 Special case

Consider the case where $\theta = j/2^m, \quad j \in \mathbb{Z}$. Then,

$$
\sum_{x \in \{0,1\}^m} \mathrm{e}^{2\pi i \theta x} |x\rangle = \sum_{x \in \{0,1\}^m} \mathrm{e}^{2\pi i (j/2^m) x} |x\rangle = \sum_{x \in \{0,1\}^m} \omega^{xj} |x\rangle \qquad \text{where } \omega = \mathrm{e}^{2\pi i/2^m}
$$

Define:

$$
|\phi_j\rangle := \frac{1}{\sqrt{2^m}} \sum_{x \in \{0,1\}^m} \omega^{xj} |x\rangle, \qquad j \in \{0, ..., 2^{m-1}\}
$$

Notice, $\{|\phi_j\rangle : j \in \{0, ..., 2^{m-1}\}\ \}$ has the property that $\langle \phi_j | \phi_{j'} \rangle = \begin{cases} 1 & \text{if } j = j' \\ 0 & \text{otherwise} \end{cases}$

Then these form a basis for m-qubit states $(\mathbb{C}^2)^{\otimes m}$.
Of course, we also have the normal basis: $\{\ |j\rangle : j \in \{0,1\}^m\ \}$.

Do we have a transformation F such that, $F|\phi_j\rangle = |j\rangle$? If we did, we could use F for the ? gate and then our measurement would give us $j = \theta \cdot 2^m$ and we could easily recover θ. Figuring out F and how to generalize this special case will give us a phase-estimation algorithm.