CS181A 10: Quantum Blackbox Algorithms

Blackbox oracles

Consider an unknown Boolean function $f : \{0,1\} \to \{0,1\}$. We would like to determine whether f satisfies a certain property or not. The only way we can gather information about the unknown function f is through a blackbox (oracle) O_f. The oracle accepts an input x (also called the query) to f and returns as output $f(x)$ (also called the answer).

The quantum blackbox oracle is normally given by the following unitary operator Q_f:

$$Q_f|x,b\rangle = |x, b \oplus f(x)\rangle.$$

It is possible to arrange for another type of quantum blackbox oracle which does not require the ancilla qubit $|b\rangle$ but returns the answer $f(x)$ as a phase factor:

$$\tilde{Q}_f|x\rangle = (-1)^{f(x)}|x\rangle.$$

The phase oracle $\tilde{Q}_f$ can be constructed from the oracle Q_f using the so-called **eigenvalue kickback** method.

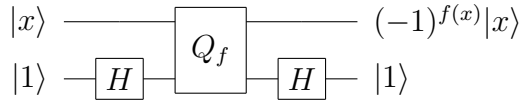

Figure 1: The eigenvalue kickback method.

We consider the trace of the quantum circuit given in Figure 1.

$$\begin{aligned}
|x\rangle|1\rangle &\xrightarrow{I\otimes H} |x\rangle\frac{|0\rangle - |1\rangle}{\sqrt{2}} \\
&\xrightarrow{Q_f} |x\rangle\frac{|f(x)\rangle - |1-f(x)\rangle}{\sqrt{2}} = (-1)^{f(x)}|x\rangle\frac{|0\rangle - |1\rangle}{\sqrt{2}} \\
&\xrightarrow{I\otimes H} (-1)^{f(x)}|x\rangle|1\rangle
\end{aligned}$$

So, we may assume if needed that we have a phase oracle instead:

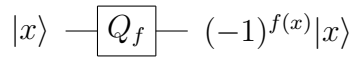

Figure 2: The phase blackbox oracle.

Deutsch-Josza problem

Suppose $f : \{0,1\} \to \{0,1\}$ is a Boolean function represented by a blackbox oracle. We want to determine if f is constant or not. It is clear that we require exactly *two* queries to determine if f is constant or not. We describe a quantum solution due to Deutsch and Josza which requires only *one* query.

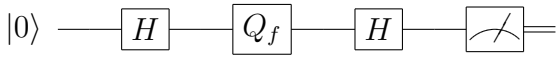

Figure 3: The Deutsch-Josza algorithm.

Consider the Deutsch-Josza algorithm given in Figure 3. The correctness of this algorithm is given by the following derivation:

$$\begin{aligned}
|0\rangle &\xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\
&\xrightarrow{\tilde{Q}_f} \frac{1}{\sqrt{2}}((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle) = \frac{(-1)^{f(0)}}{\sqrt{2}}(|0\rangle + (-1)^{f(0)\oplus f(1)}|1\rangle) \\
&\xrightarrow{H} \begin{cases} |0\rangle & \text{if } f(0) = f(1) \\ |1\rangle & \text{if } f(0) \neq f(1) \end{cases}
\end{aligned}$$

Bernstein-Vazirani problem

Suppose $f : \{0,1\}^n \to \{0,1\}$ is a Boolean function that represents a parity function $\bigoplus_{i\in A} x_i$, for some subset A of $\{1,2,\ldots,n\}$. Given a blackbox oracle for f, a classical algorithm requires n queries to discover A. We show a quantum algorithm due to Bernstein and Vazirani (1993) that requires only *one* query.

For each Boolean function $f : \{0,1\}^n \to \{0,1\}$, we may consider its equivalent $\{-1,+1\}$ version $F(x) = (-1)^{f(x)}$. The $\{-1,+1\}$ version of the parity function $f_A(x) = \bigoplus_{i\in A} x_i$ is given by $\chi_A(x) = \prod_{i\in A}(-1)^{x_i}$.

We state some useful properties of $\chi_A(x)$ in the following.

Claim 1. *For $A, B \in \{0,1\}^n$, we have*

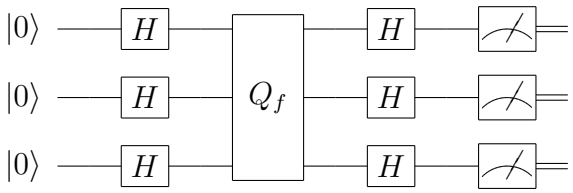

Figure 4: The Bernstein-Vazirani algorithm for $n = 3$.

- $\chi_A(x)\chi_B(x) = \chi_{A\oplus B}(x)$*, for each* $x \in \{0,1\}^n$.
- $\mathbb{E}_x[\chi_A(x)] = 1$ *if* $A = 0_n$*, otherwise the average is* 0.

We will also require the following property of the Hadamard transformation $H^{\otimes n}$ operating on n-bit inputs $x \in \{0,1\}^n$.

Claim 2. *For any* $x \in \{0,1\}^n$*, we have*

$$H^{\otimes n}|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y\in\{0,1\}^n} \chi_y(x)|y\rangle,$$

where $\chi_y(x) = (-1)^{x\cdot y} = \prod_{i=1}^n (-1)^{x_i y_i}$.

Assume that $F(x) = (-1)^{f(x)} = \chi_A(x)$. The correctness of the Bernstein-Vazirani algorithm is given in the following derivation.

$$\begin{aligned}
|0_n\rangle &\xrightarrow{H^{\otimes n}} \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle \\
&\xrightarrow{Q_f} \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)}|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} \chi_A(x)|x\rangle \\
&\xrightarrow{H^{\otimes n}} \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} \chi_A(x) \left[\frac{1}{\sqrt{2^n}} \sum_{y\in\{0,1\}^n} \chi_y(x)|y\rangle\right] \\
&= \sum_{y\in\{0,1\}^n} \left[\frac{1}{2^n} \sum_{x\in\{0,1\}^n} \chi_{A\oplus y}(x)\right] |y\rangle = |A\rangle
\end{aligned}$$

where the last equality follows from $\mathbb{E}_x[\chi_{A\oplus y}] = 0$ unless $A = y$.

Simon's problem

Consider a function $f : \{0,1\}^n \to \{0,1\}^n$ which is promised to be either one-to-one or two-to-one. If f is two-to-one then there is a period $s \neq 0_n$ where $f(x \oplus s) = f(x)$ for all $x \in \{0,1\}^n$. Given a blackbox oracle for f, a classical algorithm requires $2^{n-1} + 1$ queries to determine if f is one-to-one or not. We describe a quantum algorithm due to Simon which requires only *one* query to a blackbox oracle. Here, we have to switch back to the standard blackbox oracle $Q_f(|x\rangle|b\rangle) = |x\rangle|b \oplus f(x)\rangle$ since f outputs an n-bit string as output.

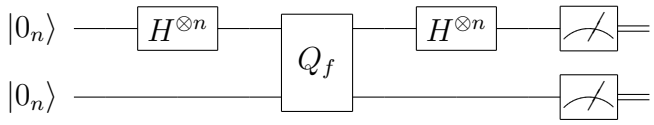

Figure 5: The Simon algorithm.

$$
\begin{aligned}
|0_n\rangle|0_n\rangle \quad &\xrightarrow{H^{\otimes n}\otimes I} \quad \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle|0_n\rangle \\
&\xrightarrow{Q_f} \quad \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle|f(x)\rangle = \frac{1}{\sqrt{2^n}} \sum_{x} (|x\rangle + |x \oplus s\rangle)|f(x)\rangle \\
&\xrightarrow{H^{\otimes n}\otimes I} \quad \frac{1}{2^n} \sum_{x} \sum_{y} \chi_y(x)(1 + \chi_y(s))|y\rangle|f(x)\rangle = \frac{1}{2^{n-1}} \sum_{x} \sum_{s\cdot y=0} \chi_y(x)|y\rangle|f(x)\rangle.
\end{aligned}
$$

So, measuring the first register yields a random $y \in \{0,1\}^n$ which satisfies $s \cdot y = 0$; that is, y is *orthogonal* to s. This gives us a randomized algorithm for selecting *vectors* from the subspace orthogonal to s.

Shor's algorithm

The FACTORING problem is reducible to the following problem.

> ORDER FINDING:
> Given an integer N and an element $a \in \mathbb{Z}_N^\star$, find the *order of* a *modulo* N which is the smallest $r > 0$ so $a^r \equiv 1 \pmod{N}$.

The reduction from FACTORING is as follows: given an integer N (to factor), we choose a random $a \in \mathbb{Z}_N^\star$. The probability that the order r of a modulo N is even

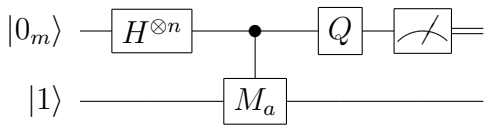

Figure 6: The Shor algorithm.

and $a^{r/2} \not\equiv -1 \pmod N$ is at least $1 - 2^{-m}$ whenever N has m distinct prime factors. If the latter event occurs, then $\gcd(a^{r/2} \pm 1, N)$ yields a non-trivial factor of N.

We now describe Shor's quantum algorithm for solving ORDER FINDING. Given an integer N and an element $a \in \mathbb{Z}_N^\star$, define the map $M_a(x) = ax \bmod N$. Consider a unitary operation U_a on two inputs defined as:

$$U_a(|k\rangle|x\rangle) = |k\rangle M_a^k(|x\rangle) = |k\rangle\big|a^k x \bmod N\big\rangle.$$

Let $\omega = \exp(2\pi i/r)$. We define the following collection of states $|\psi_j\rangle$, where $j = 0, 1, \ldots, r-1$:

$$|\psi_j\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \omega^{-jk} \big|a^k\big\rangle.$$

Claim 3. *The quantum states* $|\psi_j\rangle$ *satisfy two interesting properties:*

- *The state* $|\psi_j\rangle$ *is an eigenvector of* M_a *with eigenvalue* ω^j*:*

$$M_a|\psi_j\rangle = \omega^j|\psi_j\rangle, \quad \textit{for } j = 0, 1, \ldots, r-1.$$

- *The uniform superposition of* $|\psi_j\rangle$ *is a simple and known state:*

$$\frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} |\psi_j\rangle = |1\rangle.$$

We can now trace Shor's circuit:

$$\begin{aligned}
|0_m\rangle|1\rangle \quad &\xrightarrow{H^{\otimes m} \otimes I} \quad \frac{1}{\sqrt{2^m}} \sum_k |k\rangle|1\rangle = \frac{1}{\sqrt{2^m}} \sum_k |k\rangle \frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} |\psi_j\rangle \\
&\xrightarrow{\text{C-}M_a} \quad \frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} \frac{1}{\sqrt{2^m}} \sum_k \omega^{jk}|k\rangle|\psi_j\rangle \\
&= \quad \frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} \left[\frac{1}{\sqrt{2^m}} \sum_k \exp(2\pi i jk/r)|k\rangle \right] |\psi_j\rangle
\end{aligned}$$

We focus on the amplitude expression for $|k\rangle$ which involves $\exp(2\pi ijk/r)$. Suppose we express the rational number j/r in binary using m bits:

$$\frac{j}{r} = 0.b_1 b_2 \ldots b_m = \frac{1}{2^m}(b_1 2^{m-1} + b_2 2^{m-2} + \ldots + b_m).$$

We denote $[j]_r$ as the m-bit integer $b_1 2^{m-1} + b_2 2^{m-2} + \ldots + b_m$. Thus,

$$\frac{j}{r} = \frac{[j]_r}{2^m}. \tag{1}$$

Then, the final state obtained by Shor's circuit is

$$|\Psi\rangle = \frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} \frac{1}{\sqrt{2^m}} \sum_{k=0}^{2^m-1} \exp(2\pi i [j]_r k/2^m)|k\rangle|\psi_j\rangle.$$

Shor described a unitary transformation Q, called the *quantum Fourier transform*, whose inverse satisfies

$$Q^{-1}\left(\frac{1}{\sqrt{2^m}} \sum_{k=0}^{2^m-1} \exp(2\pi i [j]_r k/2^m)|k\rangle\right) = |[j]_r\rangle.$$

The analysis showed that the Shor circuit provides a way for generating random fractions of the form j/r given by the integer $[j]_r$ satisfying (1). If j is relatively prime to r, then we can recover r; otherwise, this procedure will return a fraction j'/r' with $r' < r$. We can check if r' is the order of a by checking $a^{r'} \equiv 1 \pmod{N}$.

References

[1] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, 2000.