Simple quantum algorithms

5.1 Deutsch Algorithm

Let $f : \{0,1\} \to \{0,1\}$. We want to decide whether $f(0) = f(1)$ or $f(0) \neq f(1)$ using one U_f evaluation.

Step 1 $|\psi_0\rangle = (H \otimes H)|01\rangle = (1/2)(|00\rangle - |01\rangle + |10\rangle - |11\rangle)$.

Stpe 2 Let $U_f : |x, y\rangle \mapsto |x, y \oplus f(x)\rangle$. Then

$$\begin{aligned}
|\psi_1\rangle &= U_f|\psi_0\rangle \\
&= (1/2)(|0, f(0)\rangle - |0, 1 \oplus f(0)\rangle + |1, f(1)\rangle - |1, 1 \oplus f(1)\rangle) \\
&= (1/2)(|0, f(0)\rangle - |0, \neg f(0)\rangle + |1, f(1)\rangle - |1, \neg f(1)\rangle).
\end{aligned}$$

Step 3 $|\psi_2\rangle = (H \otimes I_2)|\psi_1\rangle = \gamma[(|0\rangle + |1\rangle)(|f(0)\rangle - |\neg f(0)\rangle) + (|0\rangle - |1\rangle)(|f(1)\rangle - |\neg f(1)\rangle)]$.

Step 4 Measure the first qubit of $|\psi_2\rangle$:

Case 1. If $f(0) = f(1)$, then $|\psi_2\rangle = |0\rangle(|f(0)\rangle - |\neg f(0)\rangle)$ and we get the measurement ....

Case 2. If $f(0) \neq f(1)$, then $|\psi_2\rangle = |1\rangle(|f(0)\rangle - |\neg f(0)\rangle)$ and we get the measurement ....

φ

5.2 Deutsch-Jozsa Algorithm and Bernstein-Vazirani Algorithm

Let $S_n = \{0, 1, \ldots, 2^n - 1\}$ and $f : S_n \to \{0, 1\}$. We want to decide whether f is constant or balanced.

Step 0 $|\psi_0\rangle = |0\rangle^{\otimes n}|1\rangle$

Step 1 $|\psi_1\rangle = \boxed{W_{n+1}}|\psi_0\rangle = \gamma(\sum_x |x\rangle)(|0\rangle - |1\rangle)$.

Step 2 Let $U_f : |x\rangle|c\rangle \mapsto |x\rangle|c + f(x)\rangle$ and set

$$|\psi_2\rangle = U_f|\psi_1\rangle = \gamma \sum_x |x\rangle(|f(x)\rangle - |\neg f(x)\rangle) = \gamma \sum_x (-1)^{f(x)}|x\rangle(|0\rangle - |1\rangle).$$

$\frac{4}{2^{n+1}}$

The first equality follows from the fact that $f(|x\rangle + (|0\rangle - |1\rangle))$ always equals $|f(x)\rangle - |\neg f(x)\rangle$.

For the second inequality, if $f(|x\rangle) = |0\rangle$ then $|x\rangle(f(|x\rangle) - |\neg f(x)\rangle) = |x\rangle(|0\rangle - |1\rangle) = (-1)^{f(x)}|x\rangle(|0\rangle - |1\rangle)$, and if $f(|x\rangle) = |1\rangle$ then $|x\rangle(f(|x\rangle) - |\neg f(x)\rangle) = |x\rangle(|0\rangle - |1\rangle) = (-1)^{f(x)}|f(x)\rangle(|0\rangle - |1\rangle)$.

Step 3 $|\psi_3\rangle = (W_n \otimes I_2)|\psi_2\rangle = \gamma\left(\sum_{x,y}(-1)^{f(x)}(-1)^{x\cdot y}|y\rangle\right)(|0\rangle - |1\rangle)$.

To see the equality, we need to show that $W_n \sum_x |x\rangle = \sum_{x,y}(-1)^{x\cdot y}|y\rangle$. Note that the rows of W_n are $|y_0\rangle, \ldots, |y_N\rangle$ with $|y_r\rangle = |r\rangle$. We can label the entries of $|v\rangle = W_n(\sum_x |x\rangle)$ using $|r\rangle$. Then, the first entry of $|v\rangle$ is the sum of the first entries of $W_n|0\rangle, W_n|1\rangle, \ldots, W_n|N\rangle$ and equals $\sum_x(-1)^{x\cdot 0}$; the second entry of $|v\rangle$ is the sum of the second entries of $W_n|0\rangle, \ldots, W_n|N\rangle$ and equals $\sum_x(-1)^{x\cdot 1}$, so that the rth entry of $|v\rangle$ is the sum of the rth entries of $W_n|0\rangle, W_n|1\rangle, \ldots, W_n|N\rangle$ and equals $\sum_x(-1)^{x\cdot r}$. Renaming r as y, we see the equality. For example, if $n = 2$, $(-1)^1$

$$W_2 \sum_x |x\rangle = \sum_x \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} |x\rangle = \begin{bmatrix} \sum_x(-1)^{y_0\cdot x} \\ \sum_x(-1)^{y_1\cdot x} \\ \sum_x(-1)^{y_2\cdot x} \\ \sum_x(-1)^{y_3\cdot x} \end{bmatrix} = \sum_{x,y}(-1)^{x\cdot y}|y\rangle.$$

$\begin{bmatrix}1\\0\\0\\0\end{bmatrix} = |00\rangle$, $\begin{bmatrix}0\\1\\0\\0\end{bmatrix} = |01\rangle$, $\begin{bmatrix}0\\0\\1\\0\end{bmatrix} = |10\rangle$, $\begin{bmatrix}0\\0\\0\\1\end{bmatrix} = |11\rangle$

Step 4 Measure the first n qubits.

Case 1. If f is constant, then $|\psi_3\rangle = \gamma|0\rangle^{\otimes n}(|0\rangle - |1\rangle)$.

Case 2. If f is balanced, then the probability of the measurement of the first n-qubits equal $|y\rangle = |0\cdots 0\rangle$ is proportional to $\sum_x(-1)^{f(x)}(-1)^{x\cdot 0} = \sum_x(-1)^{f(x)} = 0$ because half of the $f(x)$ values are 0 and the rest are 1.

Bernstein-Vazirani algorithm

Suppose $f(x) = c \cdot x$. Then the above algorithm will give c in the last step.

5.3 Simon Algorithm

$\in \mathbb{Z}_2^n$

Let $f : \{0,1\}^n \to \{0,1\}^n$. Determine the nonzero $p \in \{0,1\}^n$ if $f(x \oplus p) = f(x)$.

1. Set $|\psi_0\rangle = \underbrace{|0\rangle}_{=2^n}\underbrace{|0\rangle}_{=2^n}$ in $\mathbf{C}^N \otimes \mathbf{C}^N$ with $N = 2^n$. Then use the Walsh-Hadamard transformation W_n to get

$$|\psi_1\rangle = (W_n \otimes I)|\psi_0\rangle = \eta \sum_{x=0}^{2^n-1} |x\rangle|0\rangle, \quad \eta = \frac{1}{\sqrt{N}} = \frac{1}{\sqrt{2^n}}.$$

2. Use U_f and n controlled-NOT gates with control qubits $f_k(x)$ to get

$$|\psi_2\rangle = \eta \boxed{\sum_x |x\rangle} |f(x)\rangle.$$

2^n

3. Apply measurement $f(x_0)$ to the second state to get

$$|\psi_3\rangle = \frac{1}{\sqrt{2}}(|x_0\rangle + |x_0 + p\rangle)|f(x_0)\rangle.$$

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

4. Apply $W_n \otimes I$ again to get

$$\begin{aligned} |\psi_4\rangle &= \eta \sum_x (-1)^{x_0 \cdot y} |y\rangle|f(x_0)\rangle \\ &= \eta \sum_y (-1)^{x_0 \cdot y}[1 + (-1)^{p \cdot y}]|y\rangle|f(x_0)\rangle \\ &= \eta\sqrt{2} \sum_{p \cdot y = 0} (-1)^{x_0 \cdot y}|y\rangle|f(x_0)\rangle. \end{aligned}$$

5. Measure the first state to get $|y\rangle$ such that $p \cdot y = 0$.

   The only states $|y\rangle$ with positive probability in the sum are those satisfying $p \cdot y = 0$. Thus, a measurement will always yield such a vector $y_1 = (y_{11} \cdots y_{1n})$.

   Repeat this to get linearly independent $y_1, \ldots, y_n$ such that $p \cdot y_j = 0$ for all j, i.e., we have a linear system

$$(y_{ij})(p_0, \ldots, p_{n-1})^t = (0, \ldots, 0)^t.$$

   We need to do it in $O(n)$ attempts with a good probability. Then solve for p.

$W_n \sum_x |x\rangle = W_n \begin{bmatrix} \vdots \end{bmatrix}$

Math 410 Quantum Computing C.K. Li Notes on Chapter 6

This is a generalizations of the use of Hadamard gate to compute $W_n \sum_x |x\rangle$ and $W_n \sum_x |f(x)\rangle$.

6.1 Quantum Integral Transform

Replace W_n by $K = K(i,j)$

Let $S_n = \{0, \ldots, N-1\}$ with $N = 2^n$ and let K be an $N \times N$ complex matrix with entries $K(i,j)$ with $i, j \in S_n$. Then K is a QIT transform converting $f = (f(0), \ldots, f(N-1))^t$ to $\boxed{\tilde{f} = (\tilde{f}(0), \ldots, \tilde{f}(N-1))^t}$ by $\boxed{\tilde{f} = Kf.}$

$K^{-1}\hat{f} = f$

$= \begin{pmatrix} f(0) \\ \vdots \\ f(N-1) \end{pmatrix}$

If K is unitary (invertible) then

$$f = K^\dagger \tilde{f} \quad \text{(respectively, } f = K^{-1}\tilde{f}\text{).}$$

Proposition If $U|x\rangle = K|y\rangle$, then

$$U\left[\sum_{x=0}^{2^n-1} f(x)|x\rangle\right] = \sum_{y=0}^{2^n-1} \tilde{f}(y)|y\rangle.$$

$$U \begin{bmatrix} f(0) \\ f(1) \\ \vdots \\ f(N-1) \end{bmatrix} = \begin{bmatrix} \hat{f}(0) \\ \vdots \\ \hat{f}(N-1) \end{bmatrix}$$

$$0 \cdots N = 2^n - 1$$

$$= \frac{1}{\sqrt{N}}\begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & & & & \\ & & w^{ij} & & \\ & & & & \end{pmatrix} \longrightarrow \left(w^{ij}\right)$$

$$0 \le i < N,\quad 0 \le j < N \qquad \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & w^{-1} & w^{-2} & \cdots & w^{-N} \\ 1 & w^{-2} & w^{-4} & \cdots & w^{-2(N-1)} \\ \vdots & & & & \end{pmatrix}$$

6.2 Quantum Fourier Transform

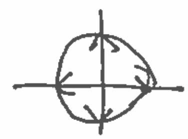
Suppose $N = 2^n$, $w_n = e^{2\pi i/N}/\sqrt{N}$ and $K = K(x, y)$ with $K(x, y) = (w_n^{-xy})$.
Then $\tilde{f} = Kf$ is a commonly used QFT.

Example When $n = 1, 2$.

$n = 1,\ N = 2 \qquad w_n = -1$

$$K(x,y) = \begin{array}{c|c} & x \\ \begin{pmatrix} (-1)^{0\cdot 0} & (-1)^{0\cdot 1} \\ (-1)^{1\cdot 0} & (-1)^{1\cdot 1} \end{pmatrix} & \begin{matrix} 0 \\ 1 \end{matrix} \\ y = \ 0 \quad 1 & \end{array} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$n = 2,\ N = 4,\quad w_n = i$



$$K(x,y) = \begin{array}{cc} \begin{bmatrix} (i)^{0\cdot 0} & (i)^{0\cdot 1} & & \\ (i)^{1\cdot 0} & & & \\ & & & \\ & & & \end{bmatrix} & \begin{matrix} 0 \\ 1 \\ 2 \\ 3 \end{matrix} \\ 0 \quad 1 \quad 2 \quad 3 & \end{array}$$

$$= \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & +i \end{bmatrix}$$

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & w & w^2 & w^3 & w^4 & w^5 \\ 1 & w^2 & w^4 & w^6 & w^8 & w^{10} \\ 1 & w^3 & w^6 & w & & \\ 1 & w^4 & \cdots & & & \end{bmatrix}$$

$i^{2\cdot 0} \quad i^{2\cdot 1} \quad i^{2\cdot 2} \quad i^{2\cdot 3}$

$i^{3\cdot 0} \quad i^{3\cdot 1} \quad i \quad i^{3\cdot 3}$

6.3 Application of QFT to period finding

This is an essential component in the Shor's algorithm.

$= \{(0\cdots0), \cdots, (1,\cdots,1)\}$

$= \{|0\cdots0\rangle, \cdots, |1,\cdots1\rangle\}$

For a periodic function, $f : S_n \to S_n$, where $S_n = \mathbb{Z}_2^n$, we want to detect $P \in S_n$ such that

$= (P_1 \cdots P_n)$

$$f(x) = f(x + P) \quad \text{for all } x \in S_n.$$

Example Let $n = 3$, $P = 2$; $f(0) = f(2) = f(4) = f(6) = a$, $f(1) = f(3) = f(5) = f(7) = b$.

$|0\rangle|0\rangle|0\rangle$

Step 1. Prepare $|\Psi_0\rangle = |0\rangle|0\rangle \in S_3 \otimes S_3$.

Step 2. Apply $W_3 \otimes I_8$ to $|\Psi_0\rangle$ and the oracle U_f to get $|\Psi\rangle = \gamma \sum_x |x\rangle|f(x)\rangle$.

Step 3. Apply $F = [e^{-2\pi i x y/8}] \otimes I_n$ to $|\Psi\rangle$ to get

$$
\begin{aligned}
|\Psi'\rangle &= \boxed{\gamma \sum_{x,y} e^{-2\pi i x y/8} |y, f(x)\rangle} \\
&= \gamma|0\rangle[|f(0)\rangle + |f(1)\rangle + \cdots + f(7)\rangle] \qquad (y = 0) \\
&\quad + \gamma|1\rangle[|f(0)\rangle + e^{-2\pi i/8}|f(1)\rangle + \cdots + e^{-2\pi i 7/8} f(7)\rangle] \qquad (y = 1) \\
&\quad + \qquad \cdots \quad \cdots \\
&\quad + \gamma|7\rangle[|f(0)\rangle + e^{-14\pi i/8}|f(1)\rangle + \cdots + e^{-14\pi i 7/8} f(7)\rangle] \qquad (y = 7) \\
&= \frac{1}{2}(|0, a\rangle + |0, b\rangle + |4, a\rangle + e^{-i\pi}|4, b\rangle).
\end{aligned}
$$

Step 4. Measurement of the first register gives 0, 4. So the period is 2.

Remark In general, the observed value of the first register is one of

$$\frac{1}{P} k \cdot 2^n, \qquad k = 0, 1, \ldots, P - 1.$$

Remark: After getting $\sum_x |x\rangle|f(x)\rangle$, we want to get a vector so that one of some of the entries can tell us the answer we want.

6.4 Implementation of QFT

We need the controlled B_{jk} gate corresponds to $U_{jk}|x,y\rangle = e^{-i\theta_{jk}xy}|x,y\rangle$ for $|x,y\rangle \in S_2$, and the Swap gate.

Proposition QFT can be implemented using $O(n^2)$ elementary gates.

6.5 Walsh-Hadamard Transform

The kernel $W_n = ((-1)^{x \cdot y})$ defines the discrete integral transform

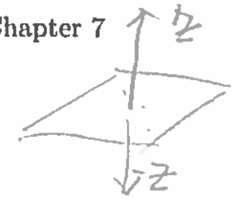
$$\tilde{f}(y) = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} (-1)^{x \cdot y} f(x).$$

6.6 Selective Phase Rotation Transform

The kernel diag $(\theta_0, \ldots, \theta_{N-1})$ defines the transform

$$\tilde{f}(y) = \sum e^{i\theta_x} \delta_{xy} f(x) = e^{i\theta_y} f(y).$$

Please study the textbook.



$|00\rangle, |01\rangle, |10\rangle, |11\rangle$

$z = |01\rangle$

$|z\rangle\langle z| = \begin{bmatrix} 0 & & & \\ & 1 & & \\ & & 0 & \\ & & & 0 \end{bmatrix}$, $I_4 - 2|z\rangle\langle z| = \begin{bmatrix} 1 & & & \\ & -1 & & \\ & & 1 & \\ & & & 1 \end{bmatrix}$

§7.1 Search for a single file

Let $f : S_n \to \{0, 1\}$ be defined by

$$f(x) = \begin{cases} 1 & \text{if } x = z, \\ 0, & \text{if } x \neq z. \end{cases}$$

$I - 2[\ ][\ ]$

Step 1 Define the reflection R_f such that $R_f = I - 2|z\rangle\langle z|$. We have

$$R_f f = \sum_x f(x) R_f |x\rangle = \sum_x (-1)^{f(x)} |x\rangle.$$

$\to (I - 2|z\rangle\langle z|)\,\gamma \begin{bmatrix} 1 \\ \vdots \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ -1 \\ \vdots \\ 1 \end{bmatrix} \leftarrow z$

Step 2 Construct $D = -I + 2|\varphi_0\rangle\langle\varphi_0|$ with $|\varphi_0\rangle = \sum_{x=0}^{N-1} |x\rangle/\sqrt{N}$. $= \frac{2}{N}\begin{bmatrix} 1 & \cdots & 1 \\ \vdots & & \vdots \\ 1 & \cdots & 1 \end{bmatrix} - I_N$

Step 3 Construct $U_f = DR_f$ and its action on $|\varphi\rangle = \sum_x w_x |x\rangle$ with $\sum_x |w_x|^2 = 1$. Then

$$U_f^k |\varphi_0\rangle = a_k |z\rangle + b_k \sum_{x \neq z} |x\rangle$$

$$\underbrace{\left(\frac{2}{N}\begin{bmatrix} 1 & \cdots & 1 \\ \vdots & & \vdots \\ 1 & \cdots & 1 \end{bmatrix} - I_N\right)\begin{pmatrix} 1 & & & 0 \\ & -1 & & \\ & & \ddots & \\ 0 & & & 1 \end{pmatrix}}_{U_f}$$

$z \to \begin{bmatrix} b_k \\ b_k \\ a_k \\ b_k \\ b_k \end{bmatrix}$

such that $a_0 = b_0 = 1/\sqrt{N}$. For $k \geq 1$ we have

$$\begin{pmatrix} a_k \\ b_k \end{pmatrix} = \frac{1}{N} \begin{pmatrix} N-2 & 2(N-1) \\ -2 & N-2 \end{pmatrix} \begin{pmatrix} a_{k-1} \\ b_{k-1} \end{pmatrix}.$$

Here note that $U_f[b_k, \ldots, b_k, a_k, b_k, \ldots, b_k]^t = [b_{k+1}, \ldots, b_{k+1}, a_{k+1}, b_{k+1}, \ldots, b_{k+1}]^t$.

Let $c_k = \sqrt{N-1}b_k$. If $(a_0, c_0) = (1, \sqrt{N-1})/\sqrt{N} = (\sin\theta, \cos\theta)$, then

$$\begin{pmatrix} a_k \\ c_k \end{pmatrix} = \begin{pmatrix} \cos 2\theta & \sin 2\theta \\ -\sin 2\theta & \cos 2\theta \end{pmatrix} \begin{pmatrix} a_{k-1} \\ c_{k-1} \end{pmatrix} = \begin{pmatrix} \sin[(2k+1)\theta] \\ \cos[(2k+1)\theta] \end{pmatrix}.$$

Step 4 Maximize $P_{z,k}^2 = a_k^2$ by putting $(2k+1)\theta \approx \pi/2$. For large N we have $m = \lfloor \pi/4\theta \rfloor$ so that $m = O(\sqrt{N})$.

$\varphi_0 = \frac{1}{\sqrt{N}}\begin{bmatrix} 1 \\ \vdots \\ 1 \end{bmatrix} \leftarrow z \quad \therefore\ a_0 = b_0 = \frac{1}{\sqrt{N}}$

$|v_{k-1}\rangle = U_f^{k-1}|\varphi_0\rangle = \begin{bmatrix} b_{k-1} \\ b_{k-1} \\ a_{k-1} \\ b_{k-1} \\ b_{k-1} \end{bmatrix} \leftarrow z$

$z \to \begin{pmatrix} b_k \\ b_k \\ a_k \\ b_k \\ b_k \end{pmatrix}$ Then $= \left(\frac{2}{N}\begin{bmatrix} 1 & \cdots & 1 \\ \vdots & & \vdots \\ 1 & \cdots & 1 \end{bmatrix} - I_N\right)\begin{pmatrix} b_{k-1} \\ \vdots \\ b_{k-1} \\ -a_{k-1} \\ b_{k-1} \\ \vdots \\ b_{k-1} \end{pmatrix} = \frac{2}{N}\begin{pmatrix} (N-1)b_{k-1} - a_{k-1} \\ \vdots \\ (N-1)b_{k-1} - a_{k-1} \end{pmatrix} - \begin{pmatrix} b_{k-1} \\ \vdots \\ b_{k-1} \\ -a_{k-1} \\ b_{k-1} \\ \vdots \\ b_{k-1} \end{pmatrix}$