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 ....

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

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

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

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 $n = 2$,

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

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

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 $|\psi_0\rangle = |0\rangle|0\rangle$ 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

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

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

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

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 $y_1, \ldots, y_{n-1}$ 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.