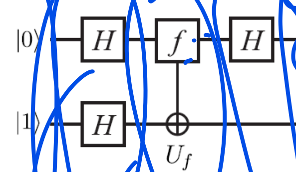
In this chapter, we introduce some simple algorithms. This demonstrate how one can use the quantum properties to solve certain problems efficiently. It should be emphasized that formulating the "right" questions to use quantum properties are important.

Simple quantum algorithms

5.1 Deutsch Algorithm

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



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

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

$|\psi_1\rangle = U_f|\psi_0\rangle$

$= (1/2)(|0, f(0)\rangle - |0, 1 \oplus f(0)\rangle + |1, f(1)\rangle - |1, 1 \oplus f(1)\rangle)$

$= (1/2)(|0, f(0)\rangle - |0, \neg f(0)\rangle + |1, f(1)\rangle - |1, \neg f(1)\rangle)$.

$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ $\quad H\begin{bmatrix}1\\0\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix}$ $\quad \begin{bmatrix}1\\-1\end{bmatrix}$

Step 3 $|\psi_2\rangle = (H \otimes I_2)|\psi_1\rangle$

$= \gamma[(|0\rangle + |1\rangle)(|f(0)\rangle - |\neg f(0)\rangle) + (|0\rangle - |1\rangle)(|f(1)\rangle - |\neg f(1)\rangle)]$

$-\gamma\left[(|0\rangle + |1\rangle) - (|0\rangle - |1\rangle)\right]|c\rangle$

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

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 ....

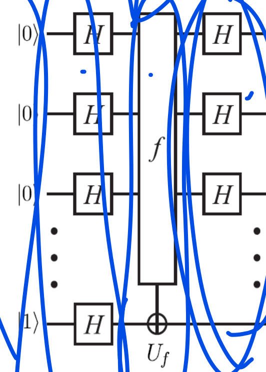
Case 2. If $f(0) \neq f(1)$, then $|\psi_2\rangle = |1\rangle(|f(0)\rangle - |\neg f(0)\rangle)$ and we get the measurement ....

$= |c\rangle$

5.2.1 Deutsch-Jozsa 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 $U_f : |x\rangle|c\rangle \mapsto |x\rangle|c \oplus f(x)\rangle$ and set

$$|\psi_2\rangle = U_f|\psi_1\rangle$$

$$= \gamma \sum_x (|x\rangle(|0\rangle - |1\rangle) \oplus f(x)\rangle)$$

$$= \gamma \sum_x |x\rangle(-1)^{f(x)}(|0\rangle - |1\rangle)$$

(as $|c\rangle = |0\rangle - |1\rangle$ changes to $\pm|c\rangle$ depending on $f(x) = |0\rangle$ or $|1\rangle$)

$$= \gamma \sum_x (-1)^{f(x)}|x\rangle(|0\rangle - |1\rangle)$$

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

Note that $W_1|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $W_1|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

so that $\gamma W_1(|0\rangle + |1\rangle) = \sum_{x,y\in\{0,1\}}(-1)^{xy}|y\rangle$. Then

$W_2(\sum_{x_1x_2}|x_1x_2\rangle)$

$= (\sum_{x_1,y_1}(-1)^{x_1y_1}|y_1\rangle)(\sum_{x_2,y_2}(-1)^{x_2y_2}|y_2\rangle)$

$= \sum_{(x_1,x_2),(y_1,y_2)}(-1)^{(x_1,x_2)\cdot(y_1,y_2)}|y_1y_2\rangle$

$= \sum_{x,y}(-1)^{x\cdot y}|y\rangle$.

Here we are summing up the entries in each row.

Step 4 Measure the first n qubits.

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

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.

A closed look for a 2-qubit example

$f(0,0)=0, f(0,1)=1, f(1,0)=1, f(1,1)=0.$

$$U_f(W_2|00\rangle|1\rangle) = \gamma U_f \left\{ \begin{pmatrix}1\\0\\0\\0\end{pmatrix} + \begin{pmatrix}0\\1\\0\\0\end{pmatrix} + \begin{pmatrix}0\\0\\1\\0\end{pmatrix} + \begin{pmatrix}0\\0\\0\\1\end{pmatrix} \right\} \left(\begin{pmatrix}1\\0\end{pmatrix} - \begin{pmatrix}0\\1\end{pmatrix} \right)$$

$$= \gamma \left\{ \begin{pmatrix}1\\0\\0\\0\end{pmatrix} - \begin{pmatrix}0\\1\\0\\0\end{pmatrix} - \begin{pmatrix}0\\0\\1\\0\end{pmatrix} + \begin{pmatrix}0\\0\\0\\1\end{pmatrix} \right\} \left(\begin{pmatrix}1\\0\end{pmatrix} - \begin{pmatrix}0\\1\end{pmatrix} \right).$$

Applying $H \otimes H \otimes I_2$ to the vector, we can only get $|00\rangle$ when all $(-1)^{f(x)}$ are equal for all $|x\rangle$. Else, it has the form $\sum_y c_y|y\rangle$, where $c_y = \sum_x (-1)^{f(x)}(-1)^{x\cdot y}$.

Here note that:

$$W_2(\textstyle\sum_{x_1x_2}|x_1x_2\rangle) = (\sum_{x_1,y_1}(-1)^{x_1y_1}|y_1\rangle)(\sum_{x_2,y_2}(-1)^{x_2y_2}|y_2\rangle) = \sum_{(x_1,x_2),(y_1,y_2)}(-1)^{(x_1,x_2)\cdot(y_1,y_2)}|y_1y_2\rangle.$$

5.2.2 Bernstein-Vazirani algorithm

In the above example, $f(x_1,x_2) = (1,1)\cdot(x_1,x_2)$.

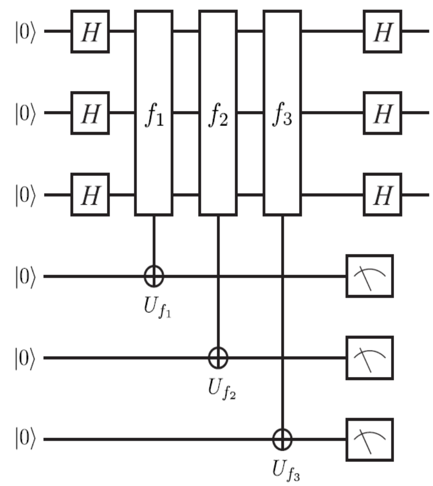
Then the resulting measurement of the first two qubits of $|\psi_3\rangle$ yields $|11\rangle$.

In general, let $f(x) = c\cdot x = (c_{n-1},\ldots,c_0)\cdot(x_{n-1},\ldots,x_0)$. Apply the Deutsch-Jozsa algorithm to get:

$$|\psi_3\rangle = \gamma \left(\sum_{x,y} (-1)^{c\cdot x}(-1)^{x\cdot y}|y\rangle \right) (|0\rangle - |1\rangle) = \gamma|c\rangle(|0\rangle - |1\rangle).$$

Measuring the first n-qubits will give $c = (c_{n-1},\ldots,c_0)$.

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 $N = 2^n$.

   Use the Walsh-Hadamard transformation W_n to get

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

   where $\eta = \frac{1}{\sqrt{N}} = \frac{1}{\sqrt{2^n}}$.

2. Use U_f and n controlled-NOT gates with control

   qubits $f_1(x), \ldots, f_k(x)$ 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

   $|\psi_4\rangle = \eta \sum_y (-1)^{x_0 \cdot y}[1 + (-1)^{p \cdot y}]|y\rangle|f(x_0)\rangle$

   $= \eta\sqrt{2} \sum_{p \cdot y = 0} (-1)^{x_0 \cdot y}|y\rangle|f(x_0)\rangle$.

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.