Quantum algorithms

Question 1. Show, step by step, that the Deutsch-Jozsa algorithm works for the case of f, where $f(0) = f(1) = 1$.

Question 2. For the case of $n = 3$ and a function f where

$$\begin{array}{rclcl} f(000) & = & f(010) & = & 110 \\ f(001) & = & f(011) & = & 101 \end{array} \qquad \begin{array}{rclcl} f(100) & = & f(110) & = & 011 \\ f(111) & = & f(101) & = & 111 \end{array}$$

give two different examples of equations that the first step of Simon's algorithm may produce. Explain what those equations mean.

Question 3. Show, step-by-step, that Grover's algorithm works for the case of 2 qubits and a function f where $f(01) = 1$ and $f(00) = f(10) = f(11) = 0$.

Question 1. Show, step by step, that the Deutsch-Jozsa algorithm works for the case of f, where $f(0) = f(1) = 1$.

Initial state: $|00\rangle$

After the first X gate, the state of the two qubits is $|01\rangle$

After the two uses of H, followed by the use of U_f, followed by the single use of H, the state of the two qubits is:

$$(H \otimes I)\, U_f\, (H \otimes H)\, |01\rangle$$

$$= (H \otimes I)\, U_f\, (H|0\rangle \otimes H|1\rangle) = (H \otimes I)\, U_f\, (|+\rangle \otimes |-\rangle)$$

$$= (H \otimes I)\, U_f\, \left(\tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |-\rangle\right)$$

$$= \tfrac{1}{\sqrt{2}} (H \otimes I)\, U_f \left(\sum_{x \in \{0,1\}} |x\rangle \otimes |-\rangle\right)$$

Lemma 2: $U_f |x\rangle|-\rangle = (-1)^{f(x)} |x\rangle|-\rangle$

$$= \tfrac{1}{\sqrt{2}} (H \otimes I) \sum_{x \in \{0,1\}} (-1)^{f(x)} |x\rangle \otimes |-\rangle$$

$$= \tfrac{1}{\sqrt{2}} (H \otimes I) \sum_{x \in \{0,1\}} (-1)^{1} |x\rangle \otimes |-\rangle \qquad f(0) = f(1) = 1$$

$$= \tfrac{-1}{\sqrt{2}} (H \otimes I) \sum_{x \in \{0,1\}} |x\rangle \otimes |-\rangle$$

Lemma 3: $H|x\rangle = \frac{1}{\sqrt{2}} \sum_{y \in \{0,1\}} (-1)^{x \cdot y} |y\rangle$

$$= \tfrac{-1}{\sqrt{2}} \sum_{x \in \{0,1\}} \tfrac{1}{\sqrt{2}} \sum_{y \in \{0,1\}} (-1)^{x \cdot y} |y\rangle \otimes |-\rangle$$

$$= -\tfrac{1}{2} \sum_{y \in \{0,1\}} \left((-1)^{0 \cdot y} |y\rangle + (-1)^{1 \cdot y} |y\rangle \right) \otimes |-\rangle$$

$$= -\tfrac{1}{2} \left((-1)^{0 \cdot 0} |0\rangle + (-1)^{0 \cdot 1} |1\rangle + (-1)^{1 \cdot 0} |0\rangle + (-1)^{1 \cdot 1} |1\rangle \right) \otimes |-\rangle$$

$$= -\tfrac{1}{2} \left(|0\rangle + |1\rangle + |0\rangle - |1\rangle \right) \otimes |-\rangle$$

$$= -|0\rangle \otimes |-\rangle$$

If we measure the first qubit, we will get 0 with probability $|-1|^2 = 1$. Hence, f is constant and the Deutsh-Joza algorithm works for f.

Question 2. For the case of $n = 3$ and a function f where

$$
\begin{aligned}
f(000) &= f(010) = 110 \qquad & f(100) &= f(110) = 011 \\
f(001) &= f(011) = 101 \qquad & f(111) &= f(101) = 111
\end{aligned}
$$

give two different examples of equations that the first step of Simon's algorithm may produce. Explain what those equations mean.

We can easily know that $S = 010$ on this function f since

For output 110, we see that pointwise addition mod 2 of the two inputs $000 \oplus 010 = 010 = S$

For output 101, $001 \oplus 011 = 010 = S$

For output 011, $100 \oplus 110 = 010 = S$

For output 111, $111 \oplus 101 = 010 = S$.

In the first step of Simon's algorithm, the measurement will produce a bit string y that satisfies $y \cdot s = 0$, and the distribution is uniform across all such bit string.

$$\Pr(\text{measuring } y) = \frac{1}{2^{2n}} \sum_{z \in A} \left\| (-1)^{x_z \cdot y} \left((1 + (-1)^{y \cdot s}) \right) |z\rangle \right\|^2 .$$

$$= \begin{cases} 2^{-(n-1)} = 2^{-(3-1)} = \frac{1}{4} & \text{if } y \cdot s = 0 \\ 0 & \text{if } y \cdot s = 1 \end{cases}$$

Suppose that the two runs produced 101 and 100

we can get the two equation:

$$101 \cdot S = 0 \quad \text{and} \quad 100 \cdot S = 0$$

These equations mean:

① They decide what bit strings y can still be existed in the equation for the probability of measuring y.

② Since 101 and 100 can be produced by the measurement, it means $101 \cdot s = 0$ and $100 \cdot s = 0$ must be true

③ By solving these equations, we can have a single solution that is different from 000, and that is S.

Question 3. Show, step-by-step, that Grover's algorithm works for the case of 2 qubits and a function f where $f(01) = 1$ and $f(00) = f(10) = f(11) = 0$.

$$H^{\otimes 2}(|00\rangle - |01\rangle + |10\rangle + |11\rangle)$$
$$= H^{\otimes 2}|00\rangle - H^{\otimes 2}|01\rangle + H^{\otimes 2}|10\rangle + H^{\otimes 2}|11\rangle$$
$$= \tfrac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) - \tfrac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle) +$$
$$\tfrac{1}{2}(|00\rangle + |01\rangle - |10\rangle - |11\rangle) + \tfrac{1}{2}(|00\rangle - |01\rangle - |10\rangle + |11\rangle)$$
$$= \tfrac{1}{2}(2|00\rangle + 2|01\rangle - 2|10\rangle + 2|11\rangle)$$
$$= |00\rangle + |01\rangle - |10\rangle + |11\rangle$$

$$H^{\otimes 2}(-|00\rangle + |01\rangle - |10\rangle + |11\rangle)$$
$$= -H^{\otimes 2}|00\rangle + H^{\otimes 2}|01\rangle - H^{\otimes 2}|10\rangle + H^{\otimes 2}|11\rangle$$
$$= -\tfrac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) + \tfrac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle))$$
$$- \tfrac{1}{2}(|00\rangle + |01\rangle - |10\rangle - |11\rangle) + \tfrac{1}{2}(|00\rangle - |01\rangle - |10\rangle + |11\rangle$$
$$= -|01\rangle$$

$$GH^{\otimes 2}|0^n\rangle = G\tfrac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$
$$= -H^{\otimes 2} Z_0 H^{\otimes 2} Z_f \tfrac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$
$$= -H^{\otimes 2} Z_0 H^{\otimes 2} \tfrac{1}{2}(|00\rangle - |01\rangle + |10\rangle + |11\rangle)$$

since $Z_f|x\rangle = (-1)^{f(x)}|x\rangle$, $f(01)=1 \Rightarrow Z_f|01\rangle = -|01\rangle$.

$$= -H^{\otimes 2} Z_0 \tfrac{1}{2}(|00\rangle + |01\rangle - |10\rangle + |11\rangle)$$
$$= -\tfrac{1}{2} H^{\otimes 2}(-|00\rangle + |01\rangle - |10\rangle + |11\rangle)$$

since $Z_0|x\rangle = \begin{cases} -|x\rangle, & \text{for } x = 0^n \\ |x\rangle, & \text{for } x \neq 0^n \end{cases}$.

$$= -\tfrac{1}{2} \cdot -|01\rangle \quad = |01\rangle$$

∴ We get 01 with probability 1 which matches $f(01)=1$.

∴ Grover's algorithm works.