Simon's Periodicity Algorithm

Finding patterns in a function, a combination of quantum on classical algorithms.

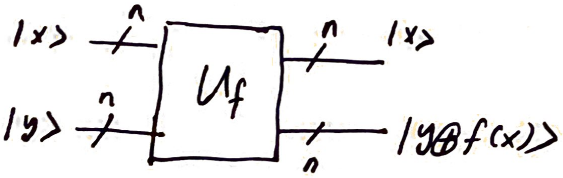
Assum we are given $f: \{0,1\}^n \rightarrow \{0,1\}^n$ that we can evaluate but given as a black box. We are also told there is a hidden binary string $\underbrace{c = c_0 c_1 \ldots c_{n-1}}$ such that for all strings $x, y \in \{0,1\}^n$ we have → period of $f(x)$

$$f(x) = f(y) \quad \text{iff} \quad x = y \oplus c$$

bitwise XOR.

if $c = 0^{\otimes n}$ then $f(x)$ is one to one otherwise two to one.

example on 1.5



setting $|y\rangle = |0\rangle^{\otimes n}$ evaluates $f(x)$

Classical solution: evaluate the function using different input strings if an output has been already found, we can be sure $(f(x_1) = f(x_2))$ that $x_1 = x_2 \oplus c$ and $\oplus x_2$ from right (both sides of the equality)

$$x_1 \oplus x_2 = x_2 \oplus c \oplus x_2 = c \quad \text{(we find } c\text{)},$$

if the function two to one we will not have to evaluate more than half of the inputs before we find a match, if the function is one to one $(c = 0^{\otimes n})$. we evaluate one more than half of the inputs with no match. in the worst case $\rightarrow \frac{2^n}{2} + 1 = 2^{n-1} + 1$ function evaluations are required.

example: (assume $c = 011$)

x	y	$f(x) = f(y)$
000	011	111
001	010	000
010	001	000
011	000	111
100	111	101
101	110	001
110	101	001
111	100	101

Classical algorithm

evaluate $f(000) = 111$

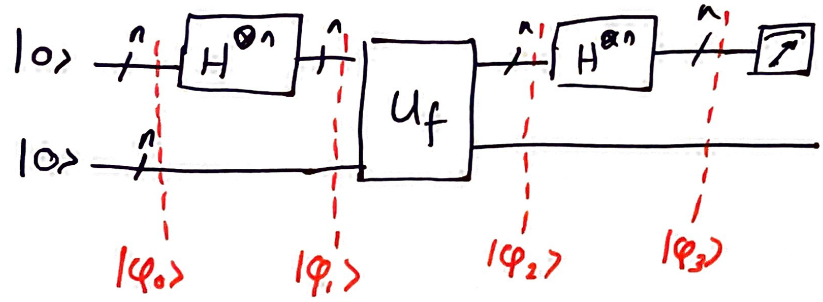
evaluate $f(001) = 000$

evalute $f(010) = 000$

evaluat $f(011) = 111$

match → $000 \oplus 011 = 011 = c$

Quantum Algorithm: Applying the following several times



$$|\varphi_3\rangle = (H^{\otimes n} \otimes I)\, U_f\, (H^{\otimes n} \otimes I)\, |0^{\otimes n} 0^{\otimes n}\rangle$$

$$|\varphi_0\rangle = |0^{\otimes n} 0^{\otimes n}\rangle$$

$$|\varphi_1\rangle = \frac{\sum_{x \in \{0,1\}^n} |x, 0^{\otimes n}\rangle}{\sqrt{2^n}}$$

$$|\varphi_2\rangle = \frac{\sum_{x \in \{0,1\}^n} |x, f(x)\rangle}{\sqrt{2^n}}$$

$$|\varphi_3\rangle = \frac{\sum_{x \in \{0,1\}^n} \sum_{z \in \{0,1\}^n} (-1)^{\langle z, x\rangle} |z, f(x)\rangle}{2^n}$$

since we know that $|z, f(x)\rangle = |z, f(x \oplus c)\rangle$ then we can say:

$$(-1)^{\langle z,x\rangle} = \frac{(-1)^{\langle z,x\rangle} + (-1)^{\langle z, x \oplus c\rangle}}{2}$$

$$= \frac{(-1)^{\langle z,x\rangle} + (-1)^{\langle z,x\rangle \oplus \langle z,c\rangle}}{2}$$

$$= \frac{(-1)^{\langle z,x\rangle} + (-1)^{\langle z,x\rangle} \cdot (-1)^{\langle z,c\rangle}}{2}$$

so if $\langle z, c\rangle = 1 \rightarrow$ the coefficient becomes 0

if $\langle z, c\rangle = 0 \longrightarrow$ " " " $\frac{\pm 2}{2} = \pm 1$

Hence, after measuring top (z) qubits will find those binary strings such that $\langle z, c\rangle = 0$ (with equal probability)

$$z_1^1 c_1 + z_2^1 c_2 + \cdots + z_n^1 c_n = 0$$
$$z_1^2 c_1 + z_2^2 c_2 + \cdots + z_n^2 c_n = 0$$
$$z_1^{n-1} c_1 + z_2^{n-1} c_2 + \cdots + z_n^{n-1} c_n = 0$$
$$z_1^n c_1 + z_2^n \cdots + z_n^n c_n = 0$$

Example:

$x \to f(x)$ $\qquad f: \{0,1\}^2 \to \{0,1\}^2$

$c = 01$

assume $f(x)$ is two to one

$00 \to 00$
$01 \to 00$
$10 \to 01$
$11 \to 01$

$$|\varphi_0\rangle = |00\rangle \otimes |00\rangle$$

$$|\varphi_1\rangle = \frac{\sum_{x \in \{0,1\}^2} |x\rangle \otimes |00\rangle}{\sqrt{4}}$$

$$|\varphi_2\rangle = \frac{\sum_{x \in \{0,1\}^2} |x, f(x)\rangle}{\sqrt{4}} = \frac{|00\rangle \otimes |00\rangle + |01\rangle \otimes |00\rangle + |10\rangle \otimes |01\rangle + |11\rangle \otimes |01\rangle}{\sqrt{4}}$$

(after the applying $H \otimes I$)

$$|\varphi_3\rangle = \frac{\sum_{x \in \{0,1\}^2} \sum_{z \in \{0,1\}} (-1)^{\langle z, x\rangle} |z\rangle \otimes |f(x)\rangle}{4}$$

$$|\varphi_3\rangle = \frac{1}{4}\Big(+|00\rangle \otimes |00\rangle + \cancel{|01\rangle \otimes |00\rangle} + |10\rangle \otimes |00\rangle + \cancel{|11\rangle \otimes |00\rangle} + |00\rangle \otimes |00\rangle$$
$$- \cancel{|01\rangle \otimes |00\rangle} + |10\rangle \otimes |00\rangle - \cancel{|11\rangle \otimes |00\rangle} + |00\rangle \otimes |01\rangle + \cancel{|01\rangle \otimes |01\rangle}$$
$$- |10\rangle \otimes |01\rangle - \cancel{|11\rangle \otimes |01\rangle} + |00\rangle \otimes |01\rangle - \cancel{|01\rangle \otimes |01\rangle} - |10\rangle \otimes |01\rangle$$
$$+ \cancel{|11\rangle \otimes |01\rangle} \Big)$$

$$|\varphi_3\rangle = \frac{1}{4}\Big(2|00\rangle \otimes |00\rangle + 2|10\rangle \otimes |00\rangle + 2|00\rangle \otimes |01\rangle - 2|10\rangle \otimes |01\rangle \Big)$$

$$|\varphi_3\rangle = \frac{1}{2}\Big(|00\rangle \otimes (|00\rangle + |01\rangle) + |10\rangle \otimes (|00\rangle - |01\rangle) \Big)$$

if we measure the top qubit we either get $|00\rangle$ or $|10\rangle$ and we know that for all of them

$\langle z, c\rangle = 0$, $c = c_1c_0$

$c_1 \cdot 0 + c_0 \cdot 0 = 0$

$c_1 \cdot 1 + c_0 \cdot 0 = 0 \to c_1 = 0$ and we know $c_1c_0 \neq 00$ $\Rightarrow c_0 = 1 \Rightarrow c_1c_0 = 01$.

(for this example we know that we never measure $|01\rangle$ or $|11\rangle$)