Simon's Algorithm

Fabio A. González

QCP 2020-2

Universidad Nacional de Colombia

1. Simon's problem

$$f : \{0,1\}^n \longrightarrow \{0,1\}^n$$

<u>one-to-one (1-1)</u> : $\forall x_1, x_2$ if $f(x_1) = f(x_2) \Longrightarrow x_1 = x_2$

<u>two-to-one (2-1)</u> : Given $b \neq 0$ $\forall x_1, x_2$ if $f(x_1) = f(x_2) \Longrightarrow x_1 \oplus x_2 = b$

$b = 1001$ $\qquad x_1 \oplus x_2 = b \qquad 0101 \oplus \underline{1100} = 1001$

$x_1 = 0101$

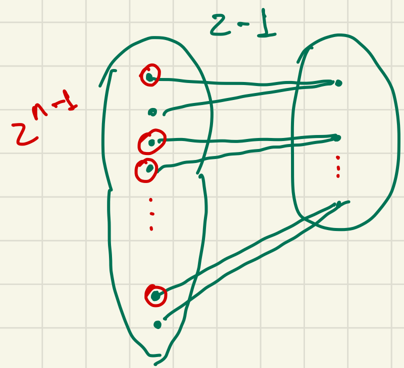
$x_2 = ?$

$b = 0 \Longrightarrow x_1 = x_2$

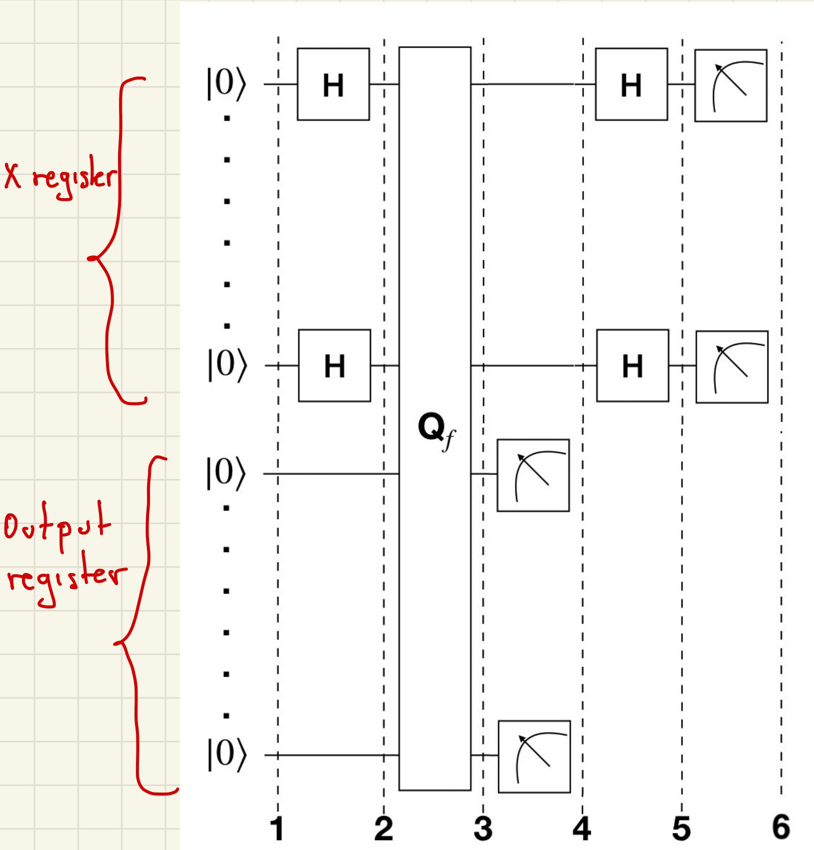
$b = 0 \Longleftrightarrow 1-1$ False

$b \neq 0 \Longleftrightarrow 2-1$ True

```
def Simon(f, n):
    out = set()
    for x in range(2^(n-1)+1):
        if f(x) in out:
            return True        # f is 2-1
        out.add(f(x))
    return False               # f is 1-1
```



2. Quantum Algorithm



$$Q_f : \{0,1\}^{2n} \longrightarrow \{0,1\}^{2n}$$

$$|x\rangle|a\rangle \longmapsto |x\rangle|a \oplus f(x)\rangle$$

$$|x\rangle|0\rangle^{\otimes n} \longmapsto |x\rangle|f(x)\rangle$$

step 1. $|\psi_1\rangle = |0\rangle^{\otimes n}|0\rangle^{\otimes n}.$

step 2. $|\psi_2\rangle = \left(H^{\otimes n} \otimes I\right)|\psi_1\rangle$

$$|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle\, |0\rangle^{\otimes n}$$

step 3. Apply Q_f oracle

$$|\psi_3\rangle = Q_f\, |\psi_2\rangle$$

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

Step 4. Measure the 2^{nd} register

$$|\psi_3\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle\, |f(x)\rangle$$

We measure $|f(x)\rangle$, two compatible inputs x and $y = x \oplus b$

$$|\psi_4\rangle = \frac{1}{\sqrt{2}} \left(|x\rangle + |y\rangle\right) |f(x)\rangle$$

$$|\psi\rangle = \alpha_1 |x_1\rangle|y_1\rangle + \alpha_2|x_2\rangle|y_2\rangle + \alpha_3 |x_3\rangle|y_1\rangle + \alpha_4|x_4\rangle|y_2\rangle)$$

Measure y subsystem $\Longrightarrow |y_2\rangle$

$$|\psi'\rangle = \frac{\alpha_2|x_2\rangle|y_2\rangle + \alpha_4|x_4\rangle|y_2\rangle}{\|\alpha_2|x_2\rangle|y_2\rangle + \alpha_4|x_4\rangle|y_2\rangle\|}$$

Step 5 Apply Hadamard to the 1^{st} register.

$$H^{\otimes n}|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{z\in\{0,1\}^n} (-1)^{x\cdot z} |z\rangle$$

$$|\psi_5\rangle = \left(H^{\otimes n} \otimes I\right) |\psi_4\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum_{z\in\{0,1\}^n} \left[(-1)^{x\cdot z} + (-1)^{y\cdot z}\right] |z\rangle\, |f(x)\rangle$$

Step 6 Measure the 1^{st} register

$x \cdot z = x_1 z_1 \oplus \dots \oplus x_n z_n$

if $|z\rangle$ is measured $\Longrightarrow (-1)^{x \cdot z} = (-1)^{y \cdot z}$

$$x \cdot z = y \cdot z$$
$$x \cdot z = (x \oplus b) \cdot z$$
$$x \cdot z = x \cdot z \oplus b \cdot z$$
$$b \cdot z = 0 \pmod 2$$

Measure $\approx n$ times $\Longrightarrow z_1, z_2 \dots z_n$

$$\left.\begin{aligned} b \cdot z_1 &= 0 \\ b \cdot z_2 &= 0 \\ &\vdots \\ b \cdot z_n &= 0 \end{aligned}\right\} \text{ solve to find } b$$