

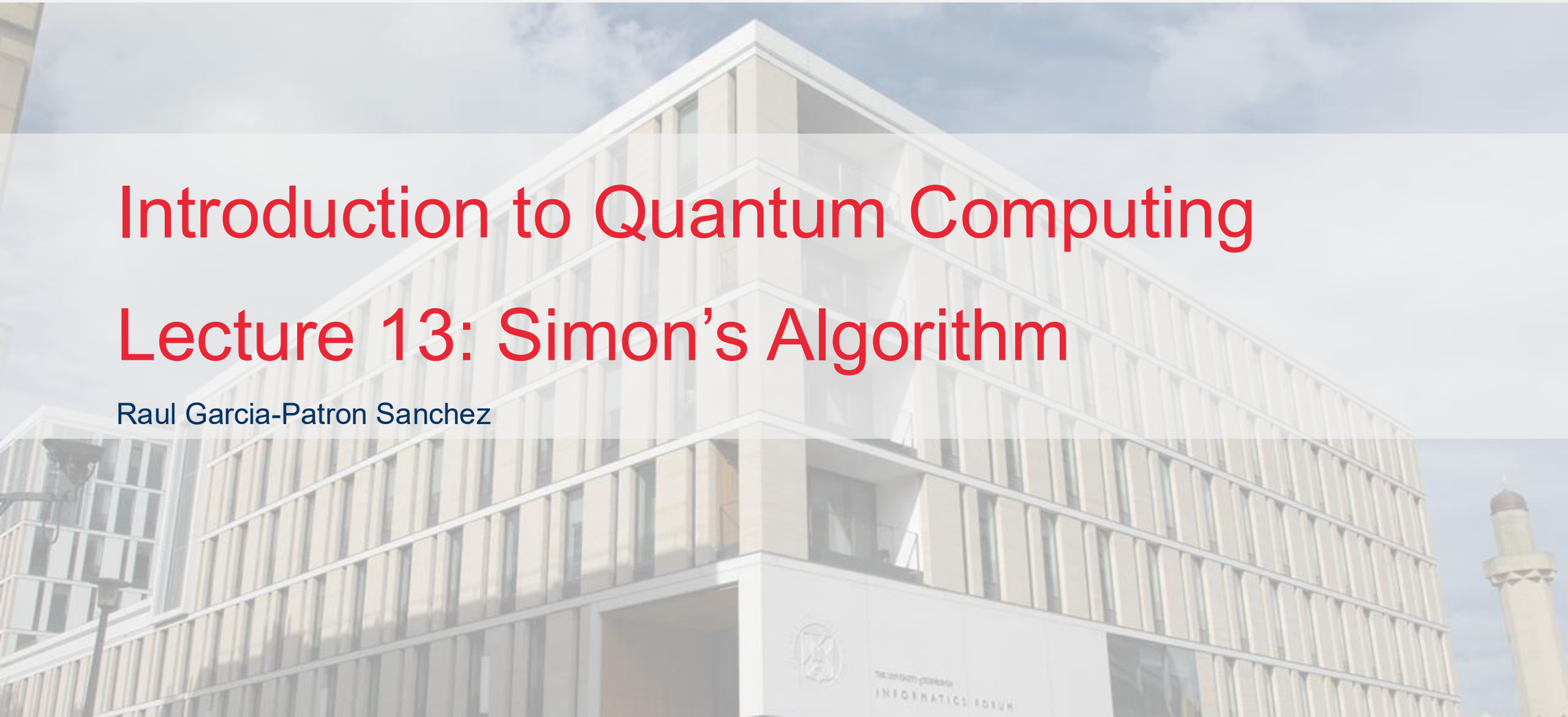


THE UNIVERSITY of EDINBURGH
informatics

Introduction to Quantum Computing

Lecture 13: Simon's Algorithm

Raul Garcia-Patron Sanchez



Find the period

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

Promise: f is a 2-to-1 and periodic on $\{0, 1\}^n$

$$f(x) = f(x') \Leftrightarrow x = x' \text{ or } x = x' \oplus a$$

Problem: Find a

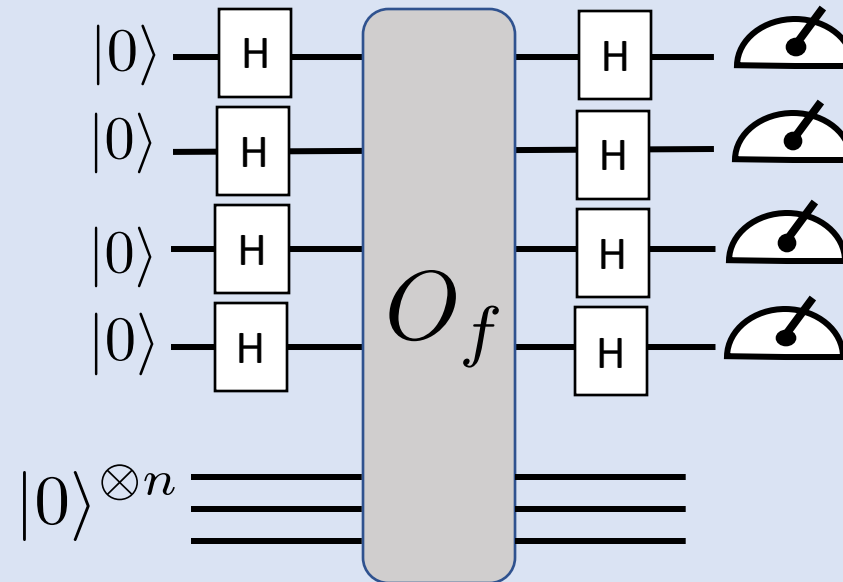
Exponential
separation



- Inspired Shor Algorithm
- Can be used to break some cryptographic primitives (see references)

$$|x\rangle |0\rangle^n \xrightarrow{O_f} |x\rangle |f(x)\rangle$$

Quantum subroutine



Simon Algorithm

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

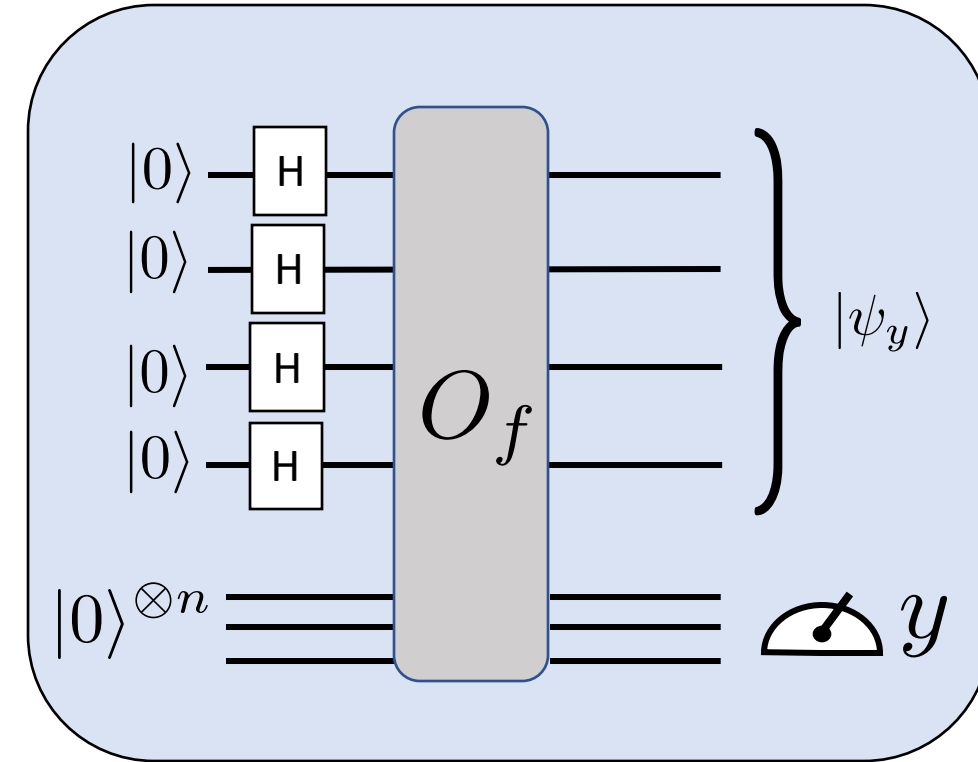
$$f(x) = f(x') \Leftrightarrow x = x' \text{ or } x = x' \oplus a$$

- $$|0\rangle^n \otimes |0\rangle^n \xrightarrow{H^{\otimes n}} \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle \otimes |0\rangle^{\otimes n}$$

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

$$= \frac{1}{\sqrt{2^n}} \sum_{\text{Image}} \left(\sum_{\text{Preimage of } f(x)} |x\rangle \right) |f(x)\rangle$$

- Measurement outcome y : $|\psi_y\rangle = \frac{1}{\sqrt{2}} [|x_y\rangle + |x_y \oplus a\rangle]$





THE UNIVERSITY of EDINBURGH
informatics

Projective and partial measurements



Projective measurement

A projective measurement consist of a set of projectors P_i

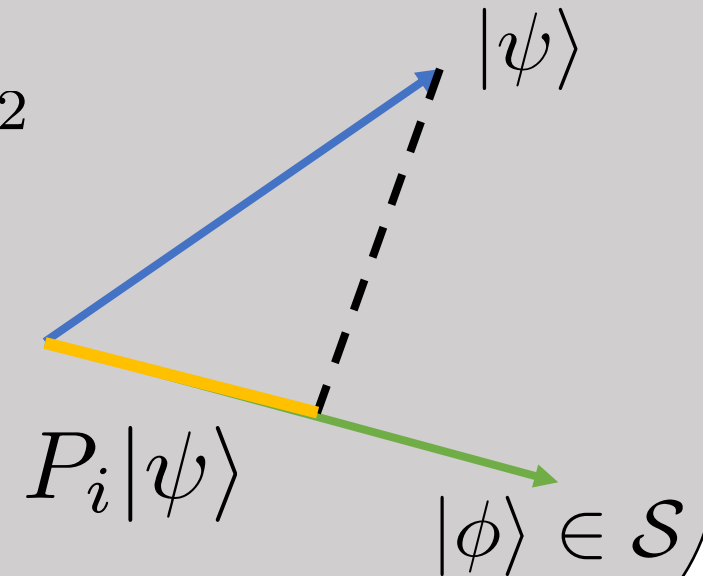
Satisfying a completeness relation: $\sum_{i=0}^l P_i = I_d$

Satisfy orthogonal relation: $P_m P_n = \delta_{n,m} P_m$

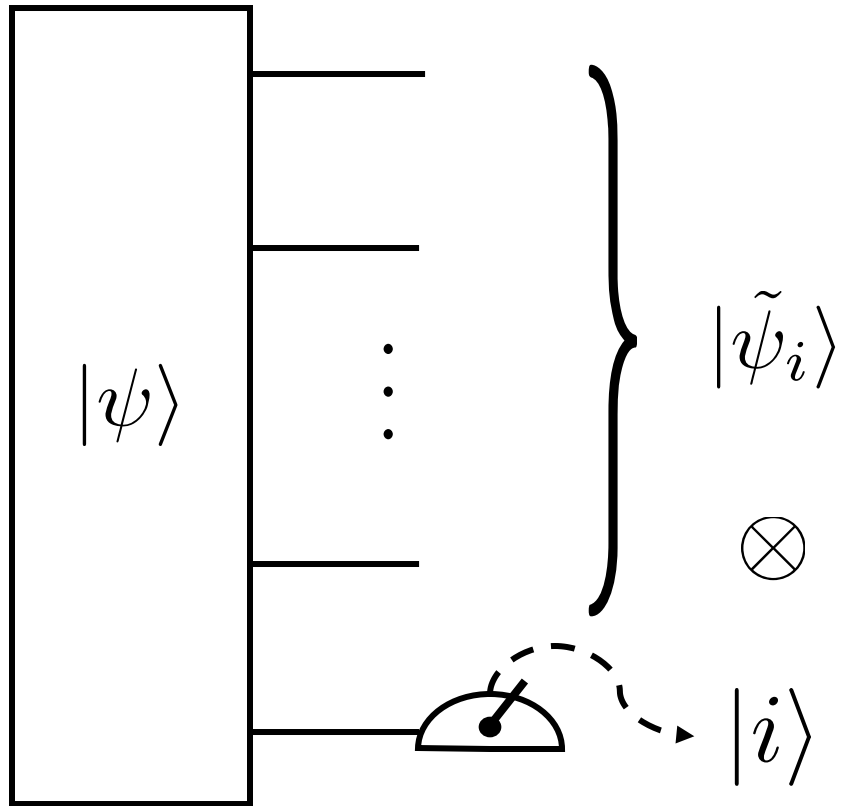
Probability of outcome i reads: $P(i) = ||P_i|\psi\rangle||^2$

The quantum state is updated to

$$\frac{P_i|\psi\rangle}{||P_i|\psi\rangle||}$$



Subsystem measurement

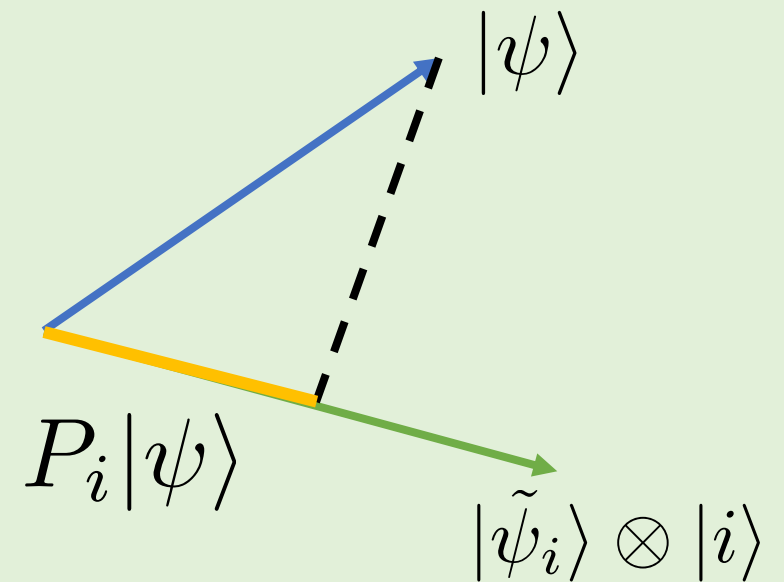


$$\tilde{P}_0 = I \otimes I \otimes \dots \otimes |0\rangle\langle 0|$$

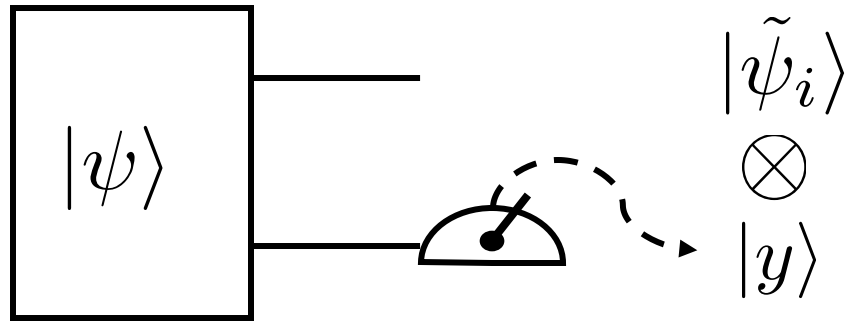
$$\tilde{P}_1 = I \otimes I \otimes \dots \otimes |1\rangle\langle 1|$$

$$\tilde{P}_0 + \tilde{P}_1 = I_{\mathcal{H} \otimes n}$$

$$\sum_i c_i (A_i \otimes C) = \left(\sum_i c_i A_i \right) \otimes C$$



Two qubit example



$$\begin{aligned}\tilde{P}_0 &= I \otimes |0\rangle\langle 0| \\ \tilde{P}_1 &= I \otimes |1\rangle\langle 1| \\ \tilde{P}_0 + \tilde{P}_1 &= I\end{aligned}$$

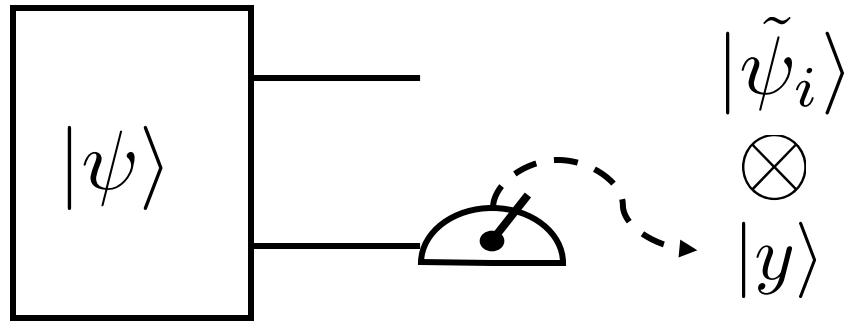
$$|\psi\rangle = \psi_{00}|0\rangle \otimes |0\rangle + \psi_{01}|0\rangle \otimes |1\rangle + \psi_{10}|1\rangle \otimes |0\rangle + \psi_{11}|1\rangle \otimes |1\rangle$$

$$\tilde{P}_0|i\rangle \otimes |0\rangle = (I \otimes |0\rangle\langle 0|)(|i\rangle \otimes |0\rangle) = I|i\rangle \otimes |0\rangle \underbrace{\langle 0|0\rangle}_{=1} = |i\rangle \otimes |0\rangle$$

$$\tilde{P}_0|i\rangle \otimes |1\rangle = (I \otimes |0\rangle\langle 0|)(|i\rangle \otimes |1\rangle) = I|i\rangle \otimes |0\rangle \underbrace{\langle 0|1\rangle}_{=0} = 0$$

$$\tilde{P}_0|\psi\rangle = \psi_{00}|0\rangle \otimes |0\rangle + \psi_{10}|1\rangle \otimes |0\rangle = (\psi_{00}|0\rangle + \psi_{10}|1\rangle) \otimes |0\rangle$$

Two qubit example



$$\begin{aligned}\tilde{P}_0 &= I \otimes |0\rangle\langle 0| \\ \tilde{P}_1 &= I \otimes |1\rangle\langle 1| \\ \tilde{P}_0 + \tilde{P}_1 &= I\end{aligned}$$

$$|\psi\rangle = \psi_{00}|0\rangle \otimes |0\rangle + \psi_{01}|0\rangle \otimes |1\rangle + \psi_{10}|1\rangle \otimes |0\rangle + \psi_{11}|1\rangle \otimes |1\rangle$$

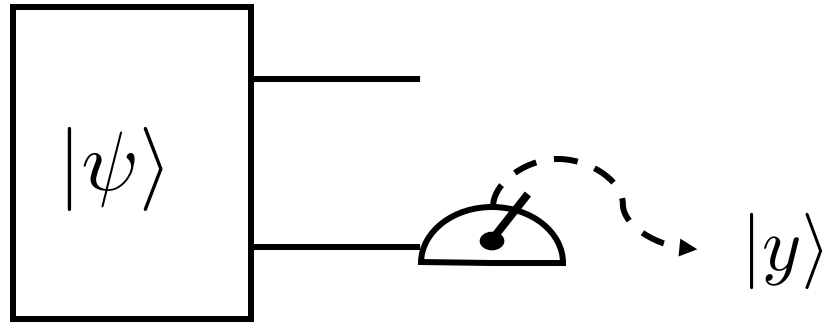
$$\tilde{P}_0|\psi\rangle = \psi_{00}|0\rangle \otimes |0\rangle + \psi_{10}|1\rangle \otimes |0\rangle = (\psi_{00}|0\rangle + \psi_{10}|1\rangle) \otimes |0\rangle$$

$$||\tilde{P}_0|\psi\rangle||^2 = \langle\psi|\tilde{P}_0\tilde{P}_0|\psi\rangle = \langle\psi|\tilde{P}_0|\psi\rangle = |\psi_{0,0}|^2 + |\psi_{1,0}|^2$$

$$\frac{\tilde{P}_0|\psi\rangle}{||\tilde{P}_0|\psi\rangle||} = \frac{1}{\sqrt{|\psi_{00}|^2 + |\psi_{01}|^2}} (\psi_{00}|0\rangle + \psi_{10}|1\rangle) \otimes |0\rangle = |\tilde{\psi}_0\rangle \otimes |0\rangle$$

Two registers example

Two register of n and m qubits respectively :



$$\tilde{P}_y = I \otimes |y\rangle\langle y|$$
$$\sum_{y \in \{0,1\}^n} P_y = I_{\mathcal{H}^{\otimes n}}$$

$$|\psi\rangle = \sum_{x,w} \psi_{x,w} |x\rangle \otimes |w\rangle$$

$$\tilde{P}_y |\psi\rangle = \left(\sum_x \psi_{x,y} |x\rangle \right) \otimes |y\rangle$$

$$||\tilde{P}_y |\psi\rangle||^2 = \langle \psi | \tilde{P}_y | \psi \rangle = \sum_x |\psi_{x,y}|^2$$

$$\frac{\tilde{P}_y |\psi\rangle}{||\tilde{P}_y |\psi\rangle||} = \frac{1}{\sqrt{\sum_x \psi_{x,y}}} \left(\sum_x \psi_{x,y} |x\rangle \right) \otimes |y\rangle = |\tilde{\psi}_y\rangle \otimes |y\rangle$$



THE UNIVERSITY of EDINBURGH
informatics

Simon's Algorithm

Raul Garcia-Patron Sanchez



Simon Algorithm

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

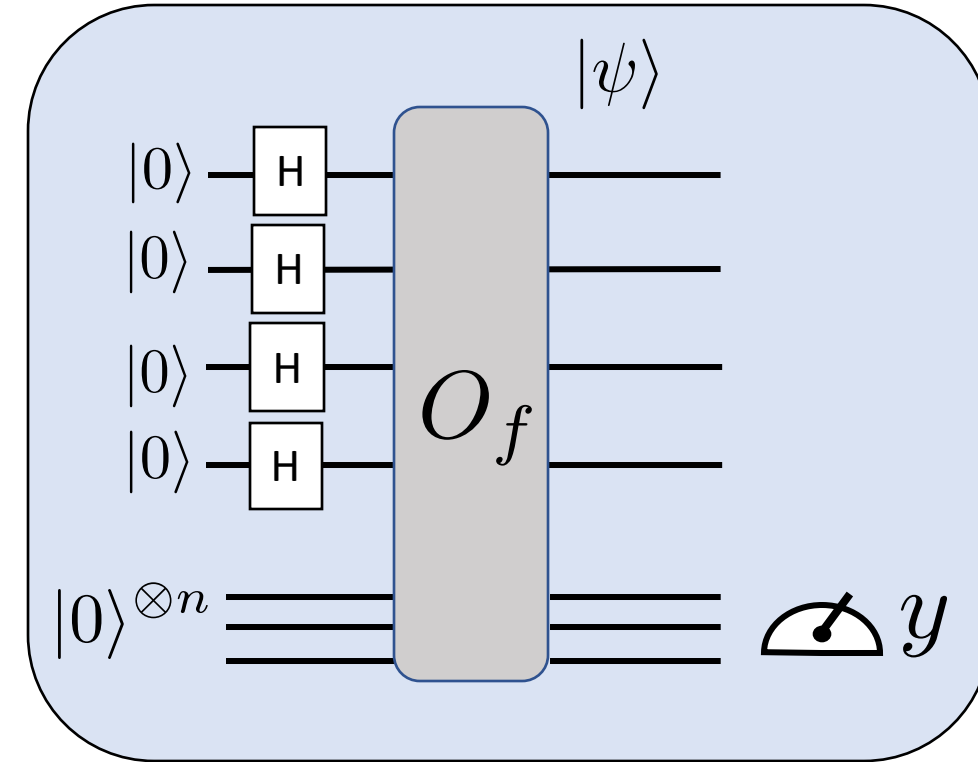
$$f(x) = f(x') \Leftrightarrow x = x' \text{ or } x = x' \oplus a$$

$$\bullet \quad |0\rangle^n \otimes |0\rangle^n \xrightarrow{H^{\otimes n}} \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle \otimes |0\rangle^{\otimes n}$$

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

$$|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{w \in f[\{0,1\}^n]} \left(\sum_{x: x=f^{-1}(w)} |x\rangle \right) \otimes |w\rangle$$

$f[\{0, 1\}^n]$: image of $f(x)$



Simon Algorithm

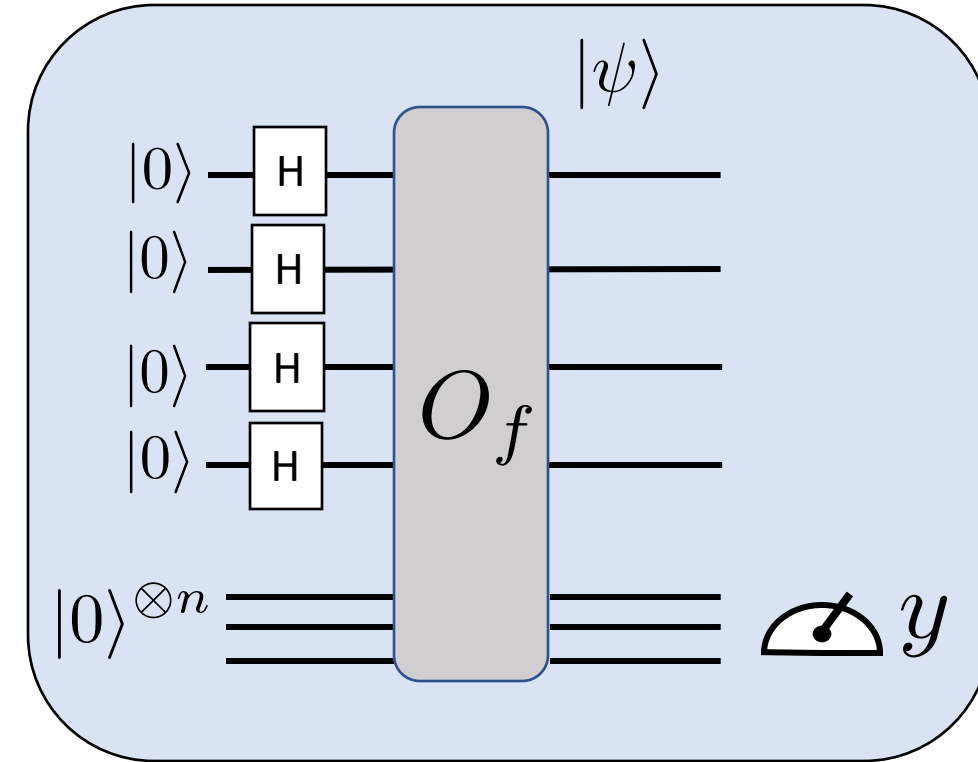
$$f : \{0, 1\}^n \rightarrow \{0, 1\}^n$$

$$f(x) = f(x') \Leftrightarrow x = x' \text{ or } x = x' \oplus a$$

- $|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{w \in \{0,1\}^n} \left(\sum_{x: x=f^{-1}(w)} |x\rangle \right) \otimes |w\rangle$

$$P_y |\psi\rangle = \frac{1}{\sqrt{2^n}} \left(\sum_{x: x=f^{-1}(y)} |x\rangle \right) \otimes |y\rangle$$

$$||P_y |\psi\rangle||^2 = \frac{|\{x : f^{-1}(y)\}|}{2^n}$$



$$P_y = I \otimes |y\rangle\langle y|$$

Simon Algorithm

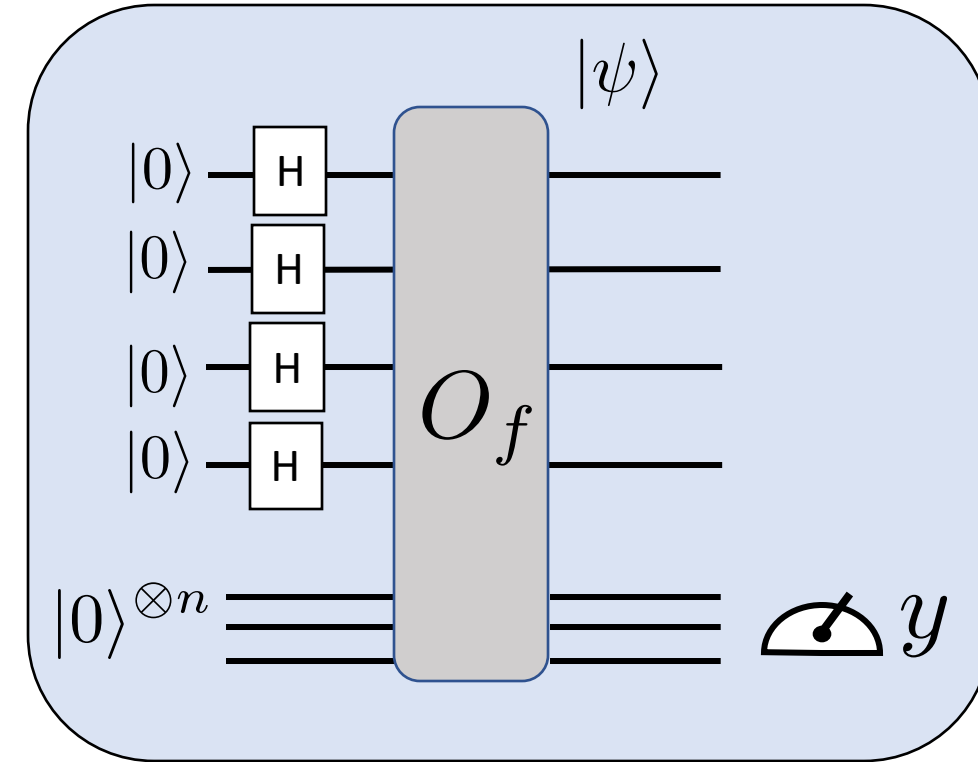
$$f : \{0, 1\}^n \rightarrow \{0, 1\}^n$$

$$f(x) = f(x') \Leftrightarrow x = x' \text{ or } x = x' \oplus a$$

$$\bullet \quad |\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{w \in \{0,1\}^n} \left(\sum_{x: x=f^{-1}(w)} |x\rangle \right) \otimes |w\rangle$$

$$P_y |\psi\rangle = \frac{1}{\sqrt{2^n}} \left(\sum_{x: x=f^{-1}(y)} |x\rangle \right) \otimes |y\rangle$$

$$\|P_y |\psi\rangle\|^2 = \frac{|\{x : f^{-1}(y)\}|}{2^n}$$



$$P_y = I \otimes |y\rangle\langle y|$$

$$\frac{P_y |\psi\rangle}{\|P_y |\psi\rangle\|} = \left(\frac{1}{\sqrt{|\{x : f^{-1}(y)\}|}} \sum_{x: x=f^{-1}(y)} |x\rangle \right) \otimes |y\rangle$$

Simon Algorithm

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

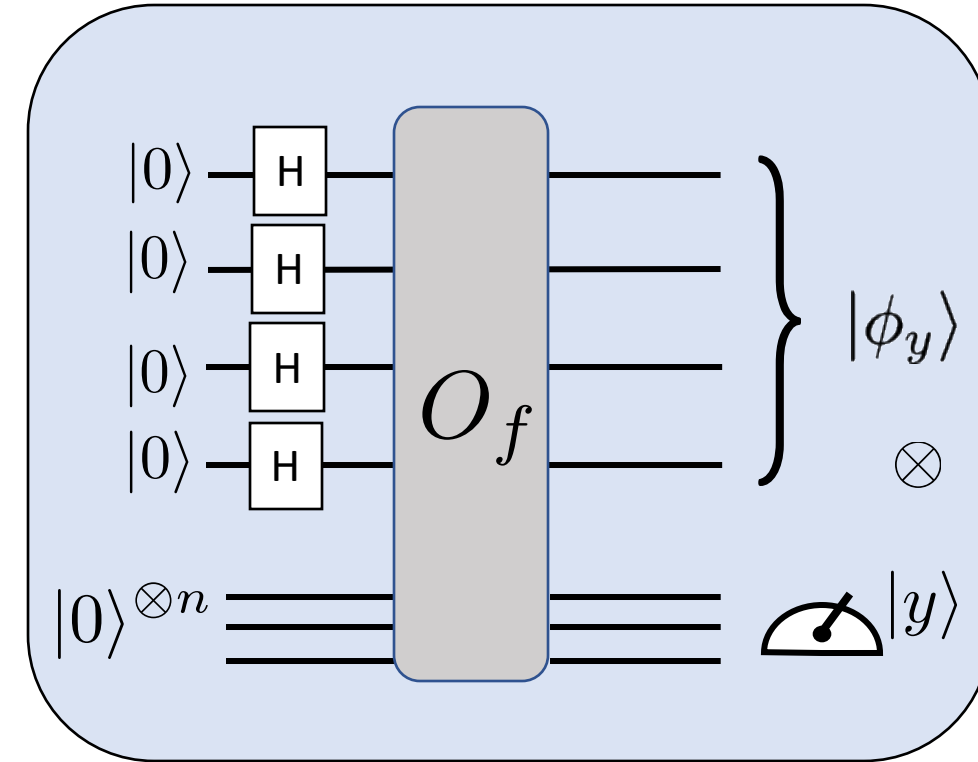
$$f(x) = f(x') \Leftrightarrow x = x' \text{ or } x = x' \oplus a$$

$$\frac{P_y |\psi\rangle}{\|P_y |\psi\rangle\|} = \left(\frac{1}{\sqrt{|\{x : f^{-1}(y)\}|}} \sum_{x: x=f^{-1}(y)} |x\rangle \right) \otimes |y\rangle$$

$$|\psi_y\rangle = |\phi_y\rangle \otimes |y\rangle = \left(\frac{1}{\sqrt{|\{x : f^{-1}(y)\}|}} \sum_{x: x=f^{-1}(y)} |x\rangle \right) \otimes |y\rangle$$

- $f(x)$ being 2-1 function:

$$|\phi_y\rangle = \frac{1}{\sqrt{2}} [|x_y\rangle + |x_y \oplus a\rangle]$$



$$P_y = I \otimes |y\rangle\langle y|$$

What if we measure after the oracle?

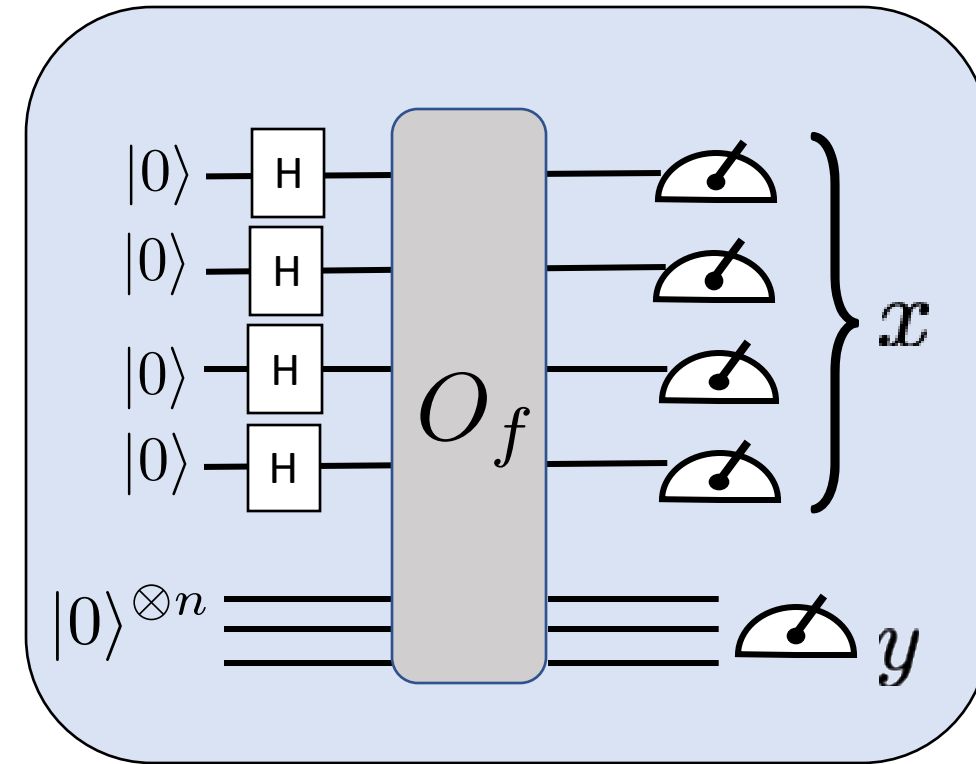
$$f : \{0, 1\}^n \rightarrow \{0, 1\}^n$$

$$f(x) = f(x') \Leftrightarrow x = x' \text{ or } x = x' \oplus a$$

- $f(x)$ being 2-1 function:

$$|\phi_y\rangle = \frac{1}{\sqrt{2}} [|x_y\rangle + |x_y \oplus a\rangle]$$

?



$$P_y = I \otimes |y\rangle\langle y|$$

What if we measure after the oracle?

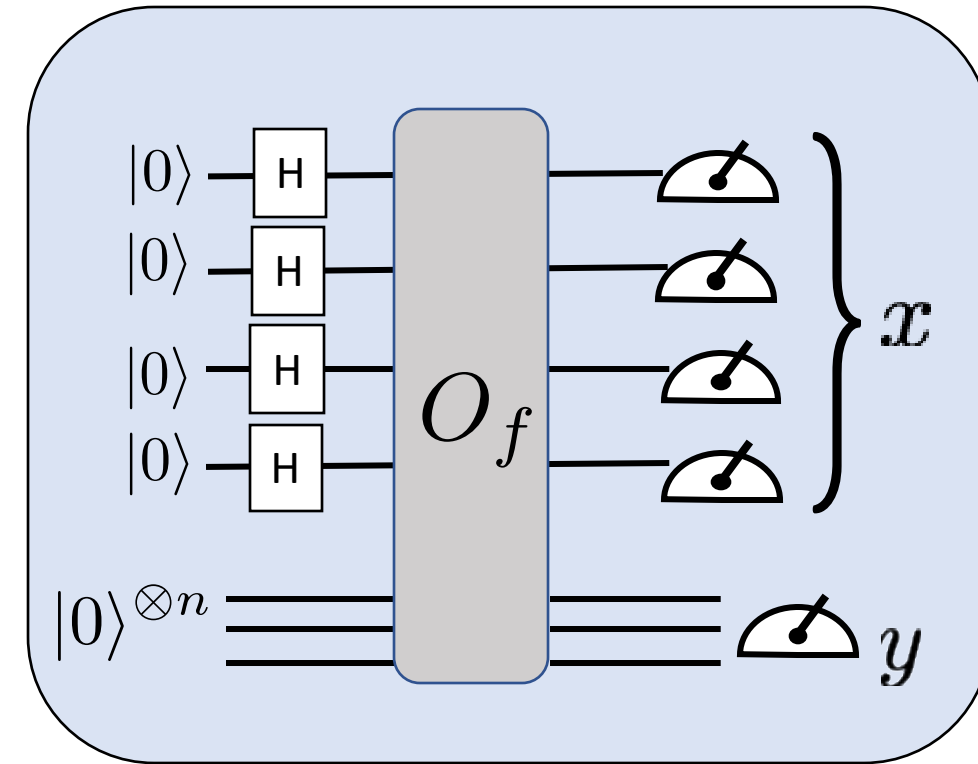
$$f : \{0, 1\}^n \rightarrow \{0, 1\}^n$$

$$f(x) = f(x') \Leftrightarrow x = x' \text{ or } x = x' \oplus a$$

- $f(x)$ being 2-1 function:

$$|\phi_y\rangle = \frac{1}{\sqrt{2}} [|x_y\rangle + |x_y \oplus a\rangle]$$

We get an input “x” associated to output “y” as $y=f(x)$. But to guess “a” we need both “x” and “x + a” and the probability to measure the same “y” again is going to be exponentially small.



$$P_y = I \otimes |y\rangle\langle y|$$

Simon Algorithm

$$f(x) = f(x') \Leftrightarrow x = x' \text{ or } x = x' \oplus a$$

- Measurement outcome y :

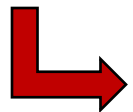
$$|\psi_y\rangle = \frac{1}{\sqrt{2}} [|x_y\rangle + |x_y \oplus a\rangle]$$

- Walsh-Hadamard:

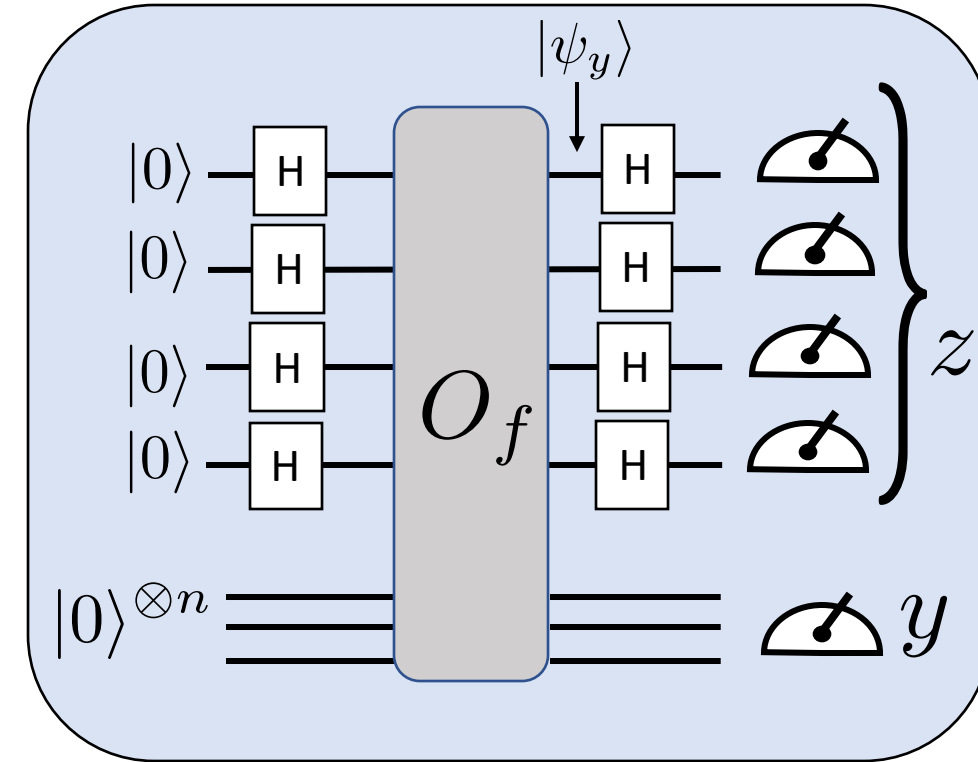
$$|\psi_y\rangle \xrightarrow{H^{\otimes n}} \frac{1}{\sqrt{2^{n+1}}} \sum_{z \in \{0,1\}^n} \left[(-1)^{x_y \cdot z} + (-1)^{(x_y \oplus a) \cdot z} \right] |z\rangle$$

$$= \frac{1}{\sqrt{2^{n+1}}} \sum_{z \in \{0,1\}^n} (-1)^{x_y \cdot z} [1 + (-1)^{a \cdot z}] |z\rangle$$

$$= \frac{1}{\sqrt{2^{n-1}}} \sum_{z: a \cdot z = 0} (-1)^{x_y \cdot z} |z\rangle$$



$$\{z \in \{0,1\}^n : a \cdot z = 0\}$$



Walsh-Hadamard transform

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

We generate samples z of n bits that satisfy: $az = 0$.

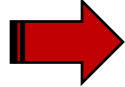
Simon Algorithm

Quantum: $O(n)$

Classical: ?

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

$$f(x) = f(x') \Leftrightarrow x = x' \text{ or } x = x' \oplus a$$

● Classical post-processing: solve system of linear eq.  a

$$\begin{cases} a_1 z_1^{(1)} + a_2 z_2^{(1)} + \dots + a_n z_n^{(1)} = 0 \pmod{2} \\ a_1 z_1^{(2)} + a_2 z_2^{(2)} + \dots + a_n z_n^{(2)} = 0 \pmod{2} \\ \vdots \\ a_1 z_1^{(n-1)} + a_2 z_2^{(n-1)} + \dots + a_n z_n^{(n-1)} = 0 \pmod{2} \end{cases}$$

1. Each outcome generates a samples z of n bits that satisfy:
 $az = 0$.
2. We generate n samples.
3. If n equations are independent we solve system of equations.

● We always have $a = 0$ as solution $\Rightarrow$ We need only $n - 1$ equations.

● Probability of linear independent set $P > \frac{1}{4}$

Classical queries

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

$$f(x) = f(x') \Leftrightarrow x = x' \text{ or } x = x' \oplus a$$

- We need to find a pair x and x' such that $f(x) = f(x')$

Solution $a = x \oplus x'$

- Success probability: $\Pr[x = x' \oplus a] = \frac{1}{2^n - 1}$

- For T queries we have at most T^2 different pairs:

- $\Pr[\text{find } a] \leq T^2 2^{-n}$

- $T \geq \sqrt{P} 2^{n/2}$

Quantum: $O(n)$

Classical: $\Omega(2^{n/2})$



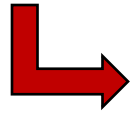
We do not need to measure lower register

- Measurement outcome y :

$$|\psi_y\rangle = \frac{1}{\sqrt{2}} [|x_y\rangle + |x_y \oplus a\rangle]$$

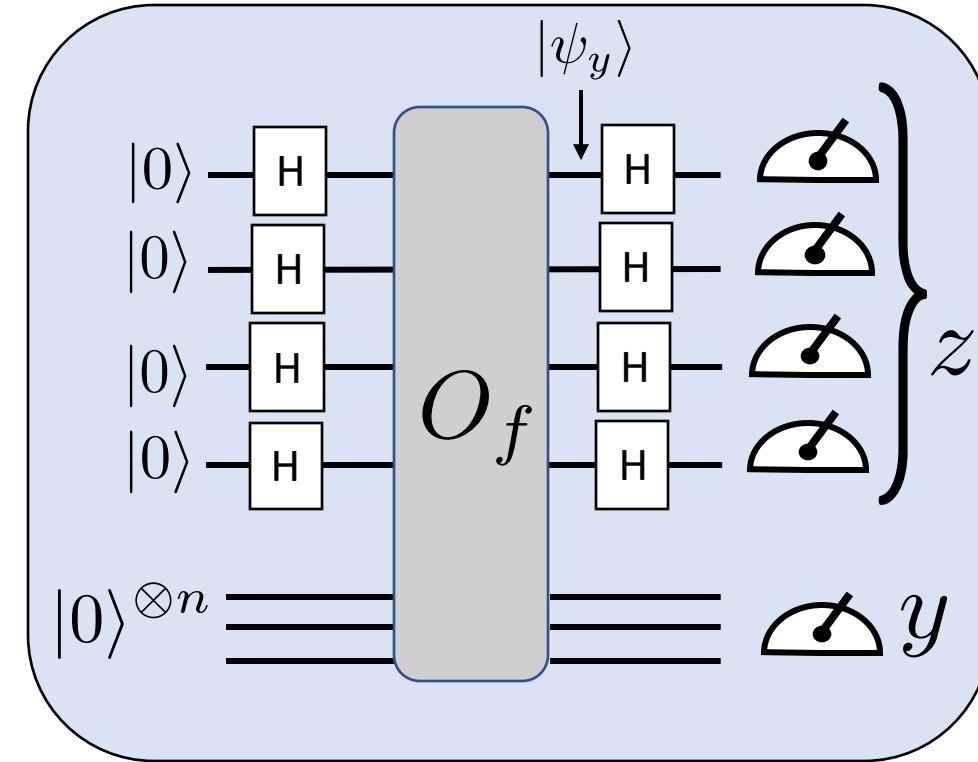
- Walsch-Hadamard:

$$|\psi_{\text{out}}\rangle = \frac{1}{\sqrt{2^{n-1}}} \sum_{z: a \cdot z = 0} (-1)^{x_y \cdot z} |z\rangle$$



$$\{z \in \{0, 1\}^n : a \cdot z = 0\}$$

Neither " x_y " nor " y " play a role in the post-processing. We could forget the value of " y " and nothing would change!



Simon Algorithm

- $\{z \in \{0, 1\}^n : a \cdot z = 0\}$ is of size $2^n/2 = 2^{n-1}$
- k lin. indep. z^i has size 2^k

● Probability of linear independent set

$$P = \prod_{k=0}^{n-2} \left(\frac{2^{n-1} - 2^k}{2^{n-1}} \right) = \prod_{j=1}^{n-1} \left(1 - \frac{1}{2^j} \right)$$

Relabeling: $j = n - k - 1$

$$= \prod_{j=1}^{n-1} \left(1 - \frac{1}{2^j} \right) \geq \prod_{j=1}^{\infty} \left(1 - \frac{1}{2^j} \right)$$

Extend the product with terms < 1

Use: $(1 - a)(1 - b) > 1 - (a + b)$

$$= \frac{1}{2} \prod_{j=2}^{\infty} \left(1 - \frac{1}{2^j} \right) > \frac{1}{2} \left[1 - \sum_{j=2}^{\infty} \frac{1}{2^j} \right]$$
$$> \frac{1}{2} \left[1 - \frac{1}{4} \sum_{j=0}^{\infty} \frac{1}{2^j} \right] > \frac{1}{4}$$

Geometric series

References

Reading references

1. Simon: NC 1.4.3 RdW 3 and G 8

NC $\equiv$ Michael Nielsen and Isaac Chuang, Quantum Computing and Quantum Information
Cambridge University Press (2010)

RdW $\equiv$ Quantum Computing Lecture Notes, Ronald de Wolf, <https://arxiv.org/abs/1907.09415>

G $\equiv$ Introduction to Quantum Computation, Sevag Gharibian, [Lectures notes](#)

Simon Algorithm breaks cryptographic primitives

1. T. Santoli and C. Schaffner, *Using Simon's algorithm to attack symmetric-key cryptographic primitives*, Quantum Information & Computation 17, 65 (2017).
2. H. Kuwakado and M. Morii, *Quantum distinguisher between the 3-round feistel cipher and the random permutation*, In 2010 IEEE International Symposium on Information Theory, pages 2682-2685, June (2010).
3. M. Kaplan, Gaetan L., A. Leverrier, and M. Naya-Plascencia, *Breaking symmetric cryptosystems using quantum period finding*, In Advances in Cryptology - CRYPTO 2016., volume 9815 of Lecture Notes in Computer Science, 2016.