# Simon's algorithm

RECALL:

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

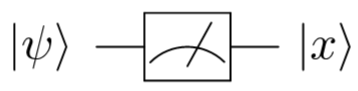
$|x\rangle_n$: n-qubit state

$x = x_{n-1}x_{n-2}\cdots x_0$

say $100\ldots1\ldots0$

## Back to quantum measurement: What happens when we measure only 1 out of n+1 qubits?

- We talked about the "Born rule" for projective measurements:




$p(x) = |\langle x|\psi\rangle|^2 \quad x = 0,1$

EXAMPLE:

$|\psi\rangle_3 = \frac{1}{\sqrt{3}}(|000\rangle + |011\rangle + |111\rangle)$

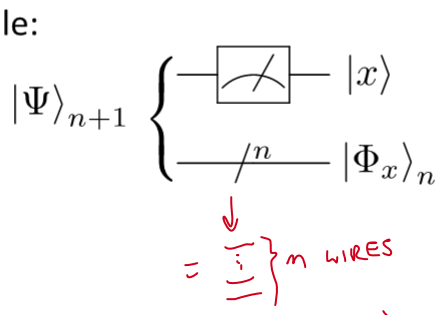
$= \frac{1}{\sqrt{3}}(|000\rangle + |011\rangle) + \frac{1}{\sqrt{3}}|111\rangle$

$= \frac{\sqrt{2}}{\sqrt{3}}|0\rangle\frac{(|00\rangle + |11\rangle)}{\sqrt{2}} + \frac{1}{\sqrt{3}}|1\rangle|11\rangle$

$= \alpha_0|0\rangle|\Phi_0\rangle + \alpha_1|1\rangle|\Phi_1\rangle$

$\alpha_0 = \sqrt{\frac{2}{3}}, \ \alpha_1 = \frac{1}{\sqrt{3}}$

- Generalized Born rule:




$p(x) = ? \quad (\Phi_x)_m = ?$

ANS.: WRITE

$|\psi\rangle_{m+1} = \alpha_0|0\rangle|\Phi_0\rangle_m + \alpha_1|1\rangle|\Phi_1\rangle_m$

WITH $|\alpha_0|^2 + |\alpha_1|^2 = 1$ AND $\langle\Phi_x|\Phi_x\rangle = 1$ BUT $\langle\Phi_0|\Phi_1\rangle$ NEED NOT BE 0!

$\Rightarrow p(x) = |\alpha_x|^2$ AND STATE "COLLAPSES" TO $|x\rangle|\Phi_x\rangle$.

## Simon's problem

$001 \oplus 101 = 100$

- Consider $f:\{0,1\}^n \to \{0,1\}^{n-1}$, with $f(x)=f(y)$ *if and only if* $x = y \oplus a$, or equivalently $x \oplus y = a$, where $\oplus$ denotes bitwise modulo-2 addition ($a=0\ldots0$ excluded). Again the n-bit string "a" is unknown. You can think of this as a period-finding problem:

$$f(x \oplus a) = f(x)$$

- The problem is to find the period "a" of f(x). Example:

$f:\{0,1\}^2 \to \{0,1\}^1 \ (n=2)$

SAY $a=10$

| x | f(x) |
|---|---|
| 00 | 0 |
| 01 | 1 |
| 10 | 1 |
| 11 | 0 |

(TWO CHOICES!)

$f:\{0,1\}^3 \to \{0,1\}^2$

$a=101$

| x | |
|---|---|
| 000 | 10 |
| 001 | 11 |
| 010 | 11 |
| 011 | 10 |
| 100 | 00 |
| 101 | 01 |
| 110 | 00 |
| 111 | 01 |

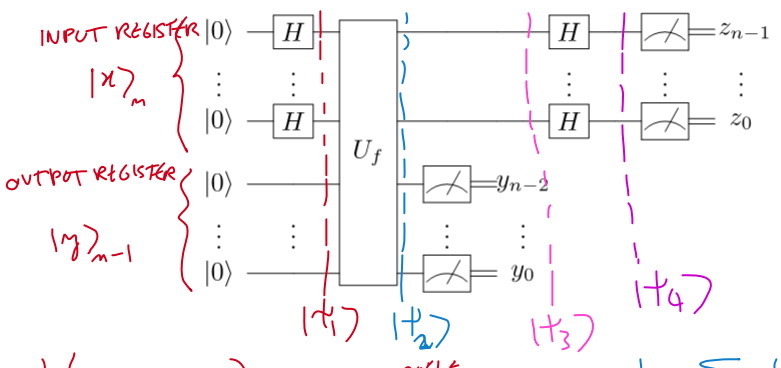
OR 4! POSSIBILITIES

- Classical computational cost? Need to input different $x_1, x_2, x_3, \ldots$ and compare the $f(x_i)$. Once you stumble upon $f(x_i)=f(x_j)$ you know that $a = x_j \oplus x_i$.
- Suppose you tried *m* different values $x_k, x_l, \ldots$ with no success. All you know is that $a \neq x_k \oplus x_l$ for $\binom{m}{2} = \frac{1}{2}m(m-1)$ values of "a". But there are $2^n-1$ values of "a". Hence your chance of success is only appreciable when

$$m \sim 2^{\frac{n}{2}}$$

## Simon's algorithm

- Quantum computer can determine "a" with high probability after running this algorithm not much more than *n* times:




$|\psi_1\rangle = \frac{1}{\sqrt{2^n}}\left(\sum_{x\in\{0,1\}^n}|x\rangle_n\right)\otimes|0\rangle_{n-1} \xrightarrow{\text{ORACLE}} |\psi_2\rangle = \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle_n|f(x)\rangle_{n-1}$

MEASURE $y_0 = f(x_0)$:

$|\psi_3\rangle = \frac{1}{\sqrt{2}}(|x_0\rangle_n + |x_0\oplus a\rangle_n)|y_0\rangle_{n-1} \xrightarrow{H^{\otimes n}} \frac{1}{\sqrt{2}}\frac{1}{\sqrt{2^n}}\sum_{z\in\{0,1\}^n}\left[(-1)^{x_0\cdot z} + (-1)^{(x_0\oplus a)\cdot z}\right]|z\rangle_n|y_0\rangle_{n-1}$

$= (-1)^{x_0\cdot z}\left[1 + (-1)^{a\cdot z}\right] = \begin{cases} 2(-1)^{x_0\cdot z} & \text{IF } a\cdot z = 0 \\ 0 & \text{IF } a\cdot z = 1 \end{cases}$

$\Rightarrow |\psi_4\rangle = \frac{2}{\sqrt{2}\sqrt{2^n}}\sum_{a\cdot z=0}(-1)^{x_0\cdot z}|z\rangle = \frac{1}{\sqrt{2^{n-1}}}\sum_{a\cdot z=0}(-1)^{x_0\cdot z}|z\rangle$

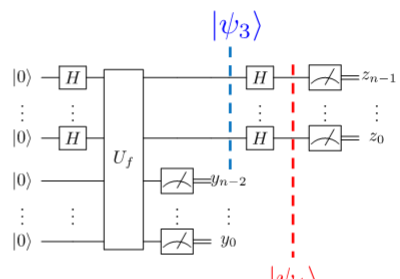
READ-OUT z, GET z SUCH THAT $a\cdot z = 0$

$\Rightarrow$ IF $z \neq 0$, $a\cdot z = 0$ REDUCES THE SPACE OF POSSIBLE a's BY 50%!

## Let's work a particular case

- For n=3, choose your favourite "a" and "f(x)". Work through Simon's.

1) Choose "a" ($a = 110$)
2) Write down the table for f(x)
3) Assume a particular "y" outcome, Calculate $|\psi_3\rangle$ and $|\psi_4\rangle$
4) Assume a particular "z" outcome, reduce "a"
5) Repeat until you find "a"




| x | f(x) |
|---|---|
| 000 | 00 |
| 001 | 01 |
| 010 | 10 |
| 011 | 10 |
| 100 | 00 |
| 101 | 01 |
| 110 | 00 |
| 111 | 01 |

1ST RUN: ASSUME $y_0 = 11$ OUTCOME:

$|\psi_3\rangle = \frac{1}{\sqrt{2}}(|011\rangle + |101\rangle)|11\rangle$

$|\psi_4\rangle = \frac{1}{\sqrt{2^2}}\sum_{a\cdot z=0}(-1)^{x_0\cdot z}|z\rangle|11\rangle$ $\quad a = 110$

$= \frac{1}{\sqrt{4}}\left(|000\rangle + (-1)^1|001\rangle + (-1)^1|110\rangle + (-1)^0|111\rangle\right)|11\rangle$

$p = \frac{3}{4}$ TO GET $z \neq 0$: SAY YOU GOT $z = 110$

$\Rightarrow$ YOU FOUND THAT $a\cdot 110 = 0 \Rightarrow a_2 \oplus a_1 = 0 \Rightarrow a_2 = a_1 \Rightarrow \boxed{a = x11}$

2ND RUN: SAY YOU GET $y_0 = 00$:

$|\psi_3\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |110\rangle)|00\rangle$ ($x_0$, $x_0\oplus a$)

$|\psi_4\rangle = \frac{1}{\sqrt{4}}(|000\rangle + |001\rangle + |110\rangle + |111\rangle)$

MEASURE z, GET $z = 111$:

$\Rightarrow a\cdot 111 = 0 \Rightarrow x11\cdot 111 = 0 \Rightarrow x\oplus x\oplus y = 0 \Rightarrow \boxed{y = 0}$

$\Rightarrow a = x10 = 110$!

(000 EXCLUDED...)

NOTE $p(\text{FIND ANS. IN 2 RUNS}) = \frac{3}{4}\times\frac{1}{2} = \frac{3}{8}$!

COMPARE TO CLASSICAL:

$p(\text{FIND ANS. IN 2 RUNS}) = \frac{1}{7}$!

## Summary

- Simon's algorithm: For $f:\{0,1\}^n \to \{0,1\}^{n-1}$, find the period "a"

$$f(x \oplus a) = f(x)$$

- Classically, you are searching a disordered database with $2^n$ entries. The search is stochastic, takes ~ $2^{n/2}$ runs *on average*.
- Quantum Simon's algorithm is also stochastic: Each time you run, you get a "z" satisfying z.a=0. There is a good chance that the "z" you got allows you reduce the number of candidates for "a" by ½. However, there is a small chance you get nothing (e.g. z=0…0 or z= previous z). On average, you need n runs to determine "a".
Exponential speed-up !!!