Simon's Problem:

Input: $f: \{0,1\}^n \to \{0,1\}^n$

Assumption: $\exists s \in \{0,1\}^n$:

$\forall x, y : [f(x) = f(y)]$ iff $(x+y) \in \{0^n, s\}$

If $s = 0^n$, then f is 1-1.

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

010 +
100

$$\begin{array}{r} 010 \\ \oplus\ 100 \\ \hline 110 \end{array}$$

$S = 110$ //

REPEAT

$$\left\{ f \xrightarrow{\text{quantum}} \text{equations} \xrightarrow{\text{classical}} s \right\}$$

until success or "give up"

So, we have a probability of success //

What are the equations like?

→ We need a set of equations

$$\left\{ \begin{array}{l} y_1 \cdot s = 0 \\ y_2 \cdot s = 0 \\ \vdots \\ y_{n-1} \cdot s = 0 \end{array} \right\}$$

where $y_1, y_2, \ldots, y_{n-1} \in \{0,1\}^n$

$y \rightarrow$ ORTHOGONAL TO s

$(n-1)$ equations with n unknowns (namely the bits of s).

$(y_1, y_2 \cdots y_{n-1}) \rightarrow$ LINEARLY INDEPENDENT

THEN we can solve for s.

$P(y_1, y_2, \cdots y_{n-1}$ are linearly independent$) > 1/4$

$P($failing to find s after 1 iteration$) < 1 - 1/4$

$P(\text{failing to find } s \text{ after } 4m \text{ iterations}) < (1 - 1/4)^{4m}$

$< e^{-m}$

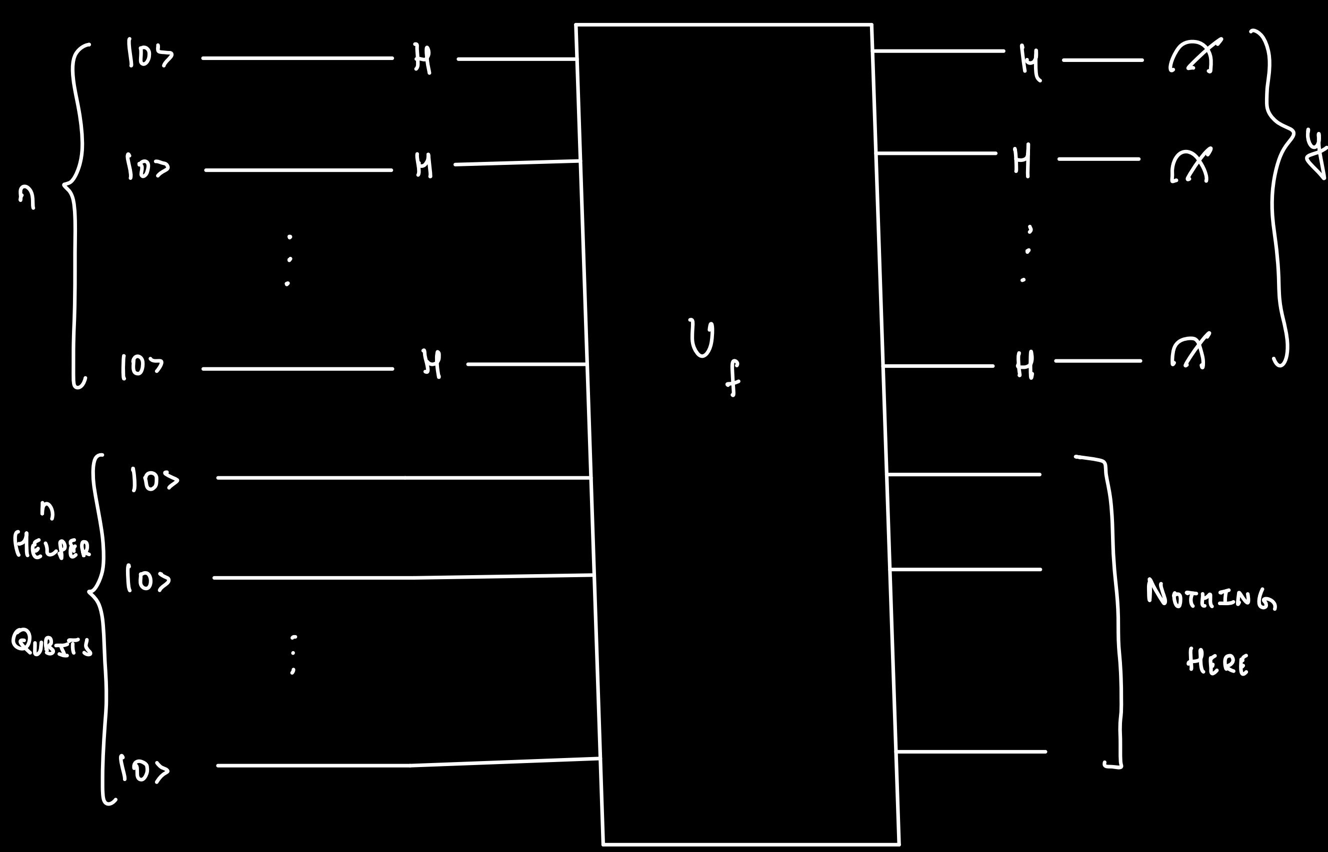
$\forall \, \varepsilon > 0 \quad \exists m : \; e^{-m} < \varepsilon$

eg: 0.01, $m = 5$, such that $e^{-m} < \varepsilon$

↳ Run $4 \times 5 = 20$ iterations.

CIRCUIT FOR SIMON'S ALGORITHM:

$2n$ qubits



Properties of y:

$\longrightarrow$ Orthogonal to s $\quad y_i \cdot s = 0$

$\longrightarrow$ Probabilities of y should be uniform to ensure they are linearly independent.

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

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

$$U_f\, |x\rangle\, |b\rangle = |x\rangle\, |b \oplus f(x)\rangle$$

$$= (H^{\otimes n} \otimes I^{\otimes n})\, \frac{1}{\sqrt{2^n}} \sum_{x} |x\rangle\, |f(x)\rangle \longrightarrow 0^n \oplus f(x)$$

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

$$= \sum_{y} |y\rangle \left(\frac{1}{2^n} \sum_{x} (-1)^{x \cdot y}\, |f(x)\rangle \right)$$

$\longrightarrow$ MEASURE!

$$\sum_y |y\rangle \left(\frac{1}{2^n} \sum_x (-1)^{x \cdot y} |f(x)\rangle \right)$$

CASE 1:

if $s = 0^n$, f is 1-1

$$\left\| \frac{1}{2^n} \sum_x (-1)^{x \cdot y} |f(x)\rangle \right\|^2$$

$$= \frac{1}{2^{2n}} \left\| \sum_x (-1)^{x \cdot y} |f(x)\rangle \right\|^2$$

↳ all possible x's will be an $f(x)$

Orthonormal vectors

$$\sum_x |f(x)\rangle = \sum_x |x\rangle = \underbrace{\begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix}}_{2^n \text{ elements}}$$

$$\sum_x (-1)^{x \cdot y} |f(x)\rangle = \begin{bmatrix} 1 \\ -1 \\ 1 \\ -1 \\ \vdots \\ 1 \end{bmatrix}$$

→ 2^n elements with some -1, some 1.

$$\left\| \sum_x (-1)^{x \cdot y} |f(x)\rangle \right\|^2 = 1^2 + (-1)^2 \ldots + 1^2 = 2^n$$ //

$$= \frac{1}{2^{2n}} \left(\sqrt{2^n}\right)^2$$

$$= \frac{1}{2^{2n}} \cdot 2^n = 1/2^n$$

Irrespective of y, all probability is $1/2^n$

UNIFORM DISTRIBUTION

OF y //

$y \cdot s = 0$ as $s = 0^n$ //.

CASE 2:

$$\sum_y |y\rangle \left(\frac{1}{2^n} \sum_x (-1)^{x \cdot y} |f(x)\rangle \right)$$

$s \neq 0^n$. Let A denote the range of f,

For each $z \in A$, we have $x_z, x_z' \in \{0,1\}^n$

$f(x_z) = f(x_z')$ $x_z \neq x_z'$

$x_z \oplus x_z' = s \iff x_z' = x_z \oplus s$

$$\left\| \frac{1}{2^n} \sum_x (-1)^{x \cdot y} |f(x)\rangle \right\|^2$$

↳ not all possible values now.

$$= \left\| \frac{1}{2^n} \sum_{z \in A} \left((-1)^{x_2 \cdot y} + (-1)^{\overset{x_2 \oplus s}{x_2'} \cdot y} \right) |z\rangle \right\|^2$$

$$= \left\| \frac{1}{2^n} \sum_{z \in A} (-1)^{x_2 \cdot y} \left(1 + (-1)^{s \cdot y} \right) |z\rangle \right\|^2$$

note: dot product is %2, so xor can be taken as +.

$$= \begin{cases} 0, & \text{if } s \cdot y = 1 \\ 1/2^{n-1}, & \text{if } s \cdot y = 0 \end{cases}$$

$\rightarrow$ it is always $s \cdot y = 0$

$S = 110$ $\quad n = 3$

Output from the quantum computer

$y \cdot S = 0$

eg:
$$\left.\begin{matrix} 001 \\ 111 \end{matrix}\right\} 2\ y\text{'s}$$

$$\left.\begin{matrix} 001 \cdot s = 0 \\ 111 \cdot s = 0 \end{matrix}\right] \xrightarrow[\text{Solver}]{\text{Constraint}} S = 110 \ //$$

#iteration

$$\underbrace{4n(n-1)}_{\hookrightarrow \text{ small}} \ //$$