Simon's Problem

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

such that $\exists s \in \{0,1\}^n$, $\forall x,y \in \{0,1\}^n$

$f(x)=f(y) \iff x=y\oplus s$ (equiv's: $x\oplus s=y$, $x\oplus y=s$)

$s=0$: f is 1-1; $s\neq 0$: f is 2-1 with $f(x)=f(x\oplus s)$

s is uniquely determined by f.

Quantum circuit using U_f gate once

Circuit for Simon:

Running circuit:

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

$\xrightarrow{U_f} \frac{1}{2^{n/2}}\sum_x |x,0^m\oplus f(x)\rangle$

$= \frac{1}{2^{n/2}}\sum_x |x,f(x)\rangle$

$\xrightarrow{H^{\otimes n}} \frac{1}{2^{n/2}}\sum_x H^{\otimes n}|x,f(x)\rangle$

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

$= |\psi_{out}\rangle$

Measure $|\psi_{out}\rangle$ on 1st n qubits, get some $y\in\{0,1\}^n$ with some probability.

$|\psi_{out}\rangle = \frac{1}{2}(|\psi_{out}\rangle + |\psi_{out}\rangle)$

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

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

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

$= \frac{1}{2^n}\sum_x\left(\sum_{\substack{y\\ s\cdot y=0}}|y,f(x)\rangle\right)$

Measure 1st n qubits, get some y such that $s\cdot y \equiv 0 \pmod 2$ with uniform probability.

Run the circuit above repeatedly getting $y_1, y_2, y_3, \dots$ get

$\mod 2\left(\begin{array}{l} y_1\cdot s=0\\ y_2\cdot s=0\\ \vdots\\ y_n\cdot s=0\end{array}\right) \iff \begin{bmatrix} -y_1^T-\\ -y_2^T-\\ \vdots\\ -y_n^T-\end{bmatrix}\begin{bmatrix}|\\ s\\ |\end{bmatrix} = \begin{bmatrix}0\\ 0\\ \vdots\\ 0\end{bmatrix}$

Repeat until $\operatorname{rank}\begin{bmatrix} -y_1^T-\\ \vdots\\ -y_n^T-\end{bmatrix} = n-1$

Then $\begin{bmatrix} -y_1^T-\\ \vdots\\ -y_n^T-\end{bmatrix}\begin{bmatrix}|\\ s\\ |\end{bmatrix} = 0$ has only 2 solutions: 0 and $s'\neq 0$.

Run query $f(s')$ using one run of U_f; query $f(0)$ using one use.

IF $f(0)=f(s')$ then return s' ($s=s'$)

else return 0 ($s=0$).

Quantum Fourier Transform (QFT)

Discrete Fourier Transform (DFT) on dimension d:

$DFT_d : \mathbb{C}^d \to \mathbb{C}^d$, linear with matrix $\frac{1}{\sqrt{d}}\begin{bmatrix}1 & 1 & 1 & \cdots & 1\\ 1 & \omega & \omega^2 & \cdots & \omega^{d-1}\\ 1 & \omega^2 & \omega^4 & \cdots & \omega^{2(d-1)}\\ \vdots & & & & \\ 1 & \omega^{d-1} & \omega^{2(d-1)} & \cdots & \omega^{(d-1)^2}\end{bmatrix}$

where $\omega = e^{2\pi i/d}$ is the principal d'th root of 1 ($\omega^d = 1$)

Generally $\forall i,j \in \{0,\dots,d-1\} = \mathbb{Z}_d$,

$[DFT_d]_{i,j} = \frac{\omega^{ij}}{\sqrt{d}}$

$x = \begin{bmatrix}x_0\\ \vdots\\ x_{d-1}\end{bmatrix}$, $\left(DFT_d\right)x)_j = \frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}\omega^{jk}x_k$

Claim that DFT_d is unitary

$DFT_d^* = \begin{bmatrix}1 & 1 & 1 & \cdots & 1\\ 1 & \omega^{-1} & \omega^{-2} & \cdots & \omega^{-(d-1)}\\ \vdots & & & & \\ 1 & \omega^{-(d-1)} & \omega^{-2(d-1)} & \cdots & \omega^{-(d-1)^2}\end{bmatrix}$ $\omega^{-1} = \omega^{d-1}$

$[DFT_d^*]_{j,k} = \frac{1}{\sqrt{d}}\omega^{-jk}$

$\left[(DFT_d)(DFT_d^*)\right]_{j,k} = \delta_{j,k}$ (WTS)

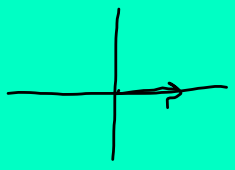
$\left[(DFT_d)(DFT_d^*)\right]_{jk} = \sum_{\ell=0}^{d-1}[DFT_d]_{j\ell}[DFT_d^*]_{\ell k}$

$$\left[(DFT_d)(DFT_d^*)\right]_{jk}$$

$$= \sum_{\ell=0}^{d-1} \left[DFT_d\right]_{j\ell} \left[DFT_d^*\right]_{\ell k}$$

$$= \frac{1}{d} \sum_{\ell} \omega^{j\ell} \omega^{-\ell k}$$

$$= \frac{1}{d} \sum_{\ell} \omega^{\ell(j-k)}$$



$j=k$: get 1

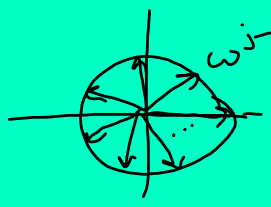
$j \neq k$: since $j,k \in \mathbb{Z}_d$, we have $\omega^{j-k} \neq 1$ because $j-k$ do not differ by a multiple of d.

Then $\sum_{\ell} \omega^{\ell(j-k)} = \sum_{\ell} (\underbrace{\omega^{j-k}}_{\neq 1})^{\ell}$

proper geometric series (finite)

$$= \frac{1-(\omega^{j-k})^d}{1-\omega^{j-k}} = \frac{1-1}{1-\omega^{j-k}} = 0$$

$\therefore$ DFT_d is unitary.



arrows cancel, sum to 0.