The key to developing q. algs that exceed classical capabilities:

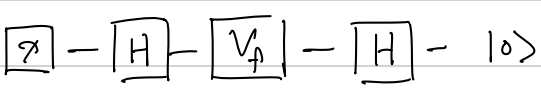
Exploit interference.

We've somewhat seen this before in the Deutsch-Jozsa alg for deciding if $f(0) \stackrel{?}{=} f(1)$.

Constructive interference $|x\rangle + |x\rangle = 2|x\rangle$

Destructive interference $|x\rangle - |x\rangle = 0$.

Deutsch-Jozsa: $V_f : |x\rangle \mapsto (-1)^{f(x)} |x\rangle$




$$|0\rangle \mapsto \frac{1}{\sqrt{2}} \left( |0\rangle + |1\rangle \right)$$

$$\mapsto \frac{1}{\sqrt{2}} \left( (-1)^{f(0)} |0\rangle + (-1)^{f(1)} |1\rangle \right)$$

$$\mapsto \frac{1}{2} \left( (-1)^{f(0)} |0\rangle + (-1)^{f(0)} |1\rangle + (-1)^{f(1)} |0\rangle - (-1)^{f(1)} |1\rangle \right)$$

$$= \frac{(-1)^{f(0)} + (-1)^{f(1)}}{2} |0\rangle + \frac{(-1)^{f(0)} - (-1)^{f(1)}}{2} |1\rangle$$

Depending on if $f(0) \stackrel{?}{=} f(1)$ one is constructive and the other is destructive

Allude to wave ripples

---

Generating interference: Fourier transform

Let $N \in \mathbb{Z}$. Then $\mathbb{Z}_N = \{0, \dots, N-1\}$ with $(+)$ mod $N$ to make a group.

Let $\omega = \omega_N = \exp\left(\frac{2\pi i}{N}\right)$.

Then $\omega, \omega^2, \dots, \omega^N$ are the solutions to $z^N - 1 = 0$.

Fact: $\sum_{j=1}^{N} \omega^j = 0$. great way to build interference patterns.

& $\sum_{j} \omega^{jz} = N \cdot \mathbb{1}\{z = 0\}$.

Intuition: Want to generate phases that are roots of unity.

Consider the Hilbert space $\mathbb{C}^N$ with basis $\{|x\rangle\}_{x \in \mathbb{Z}_N}$.

Define $X = \sum_{x \in \mathbb{Z}_N} |x+1\rangle\langle x|$ — shift operator.

generalization of $X$ on qubits.

When does $X|\psi\rangle = \lambda|\psi\rangle$ ? $\quad |\psi\rangle = \sum \alpha_x |x\rangle$

$$X|\psi\rangle = \sum \alpha_x |x+1\rangle = \sum \alpha_{x-1}|x\rangle = \lambda|\psi\rangle = \sum \lambda\alpha_x |x\rangle.$$

So, $\alpha_{x-1} = \lambda\alpha_x \Rightarrow \alpha_{x+1} = \lambda^{-1}\alpha_x \Rightarrow \alpha_0 = \alpha_N = \lambda^{-N}\alpha_0.$

Each $\alpha_x$ is non-zero for vector to have unit length.

So $\lambda^{-N} = 1 \Rightarrow \lambda^N - 1 = 0.$ $\lambda$ is a root of unity.

$|\alpha_0| = |\alpha_1| = \ldots = |\alpha_{N-1}| \Rightarrow |\alpha_0| = 1/\sqrt{N}.$

So, eigenvector is $\frac{1}{\sqrt{N}} \sum_x \lambda^{-x} |x\rangle$. When $\lambda = \omega^{-k}$, ...

Simplify notation.

For $k \in \mathbb{Z}_N$, define $|\hat{k}\rangle := \frac{1}{\sqrt{N}} \sum_x \omega^{kx} |x\rangle$.

eigenbasis of $X$ so orthonormal basis. Fourier basis.

$$X|\hat{k}\rangle = \omega^{-k}|\hat{k}\rangle.$$

What is the transform $|k\rangle \mapsto |\hat{k}\rangle$ ?

$$F_N := \sum_{k \in \mathbb{Z}_N} \left( \frac{1}{\sqrt{N}} \sum_{x \in \mathbb{Z}_N} \omega^{kx} |x\rangle\langle k| \right)$$

$$:= \frac{1}{\sqrt{N}} \sum_{x,y \in \mathbb{Z}_N} \omega^{xy} |y\rangle\langle x|.$$

conjugate transpose.

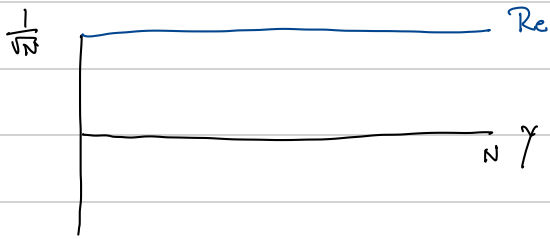
We've seen $F_2$ before! $F_2 = H$.

$$F_N^\dagger = \frac{1}{\sqrt{N}} \sum_{x,y \in \mathbb{Z}_N} \omega^{-xy} |y\rangle\langle x|.$$

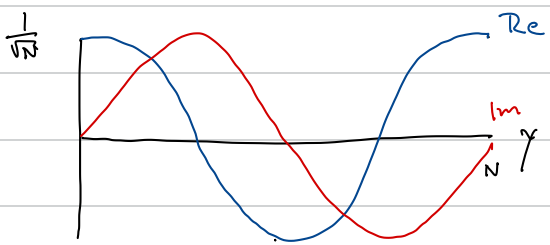
Visualizing $F_N$ (for large $N$):

$$(F_N)_{xy} = \frac{1}{\sqrt{N}}\,\omega^{xy}.$$

$x = 0$

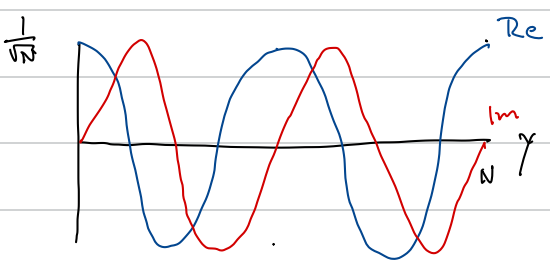



$x = 1$




Curves are discrete approximation of sine & cosine.

$x = 2$




⋮

Ok, let's see this idea in action. (Bernstein-Vazirani)

Consider a fn $f: \mathbb{Z}_N^n \to \mathbb{Z}_N$.

Suppose we are promised that $f$ is a linear fn meaning,

$$f(x_1, \dots, x_N) = \sum_{j \in \mathbb{Z}_N} s_j x_j \quad \text{for some } (s_0, \dots, s_N).$$

$$= s \cdot x.$$

We have query access to $O_f: |x_1, \dots, x_N, y\rangle \mapsto |x_1, \dots x_N, y + \sum s_j x_j\rangle$.

How many classical & quantum queries does it take to learn $s$?

Classically, querying at $x$ for answer $y$ reveals eq. $y = x \cdot s$.
Need $n$ equations to solve for $s$.

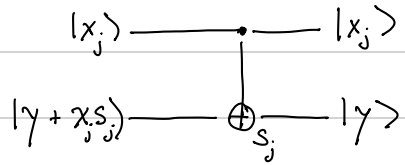
Ex. query at $x = e_j = (0 \dots 1 \dots 0)$ and get out $s_j$.

↑ $j^{th}$ location

Q. alg will use just 1 query.

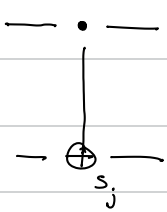
What is the structure of $\mathcal{O}_f$ ?

Define




Then




$$= \sum_{x_j \in \mathbb{Z}_N} |x_j\rangle\langle x_j| \otimes X^{x_j s_j}$$

This is just the controlled shift operator.

We're going to switch to basis where shift is diagonal to generate interference.

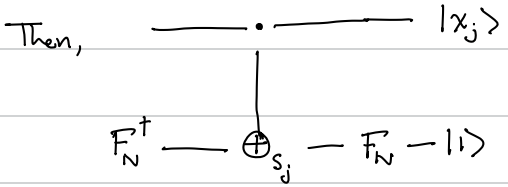
$$X|\hat{\gamma}\rangle = \omega^{-\gamma}|\hat{\gamma}\rangle \qquad \text{so}$$

$$F_N^\dagger X F_N |\gamma\rangle = F_N^\dagger X |\hat{\gamma}\rangle = F_N^\dagger \omega^{-k}|\hat{\gamma}\rangle = \omega^{-\gamma}|\gamma\rangle$$

$$\text{so} \qquad Z := F_N^\dagger X F_N = \sum_{\gamma \in \mathbb{Z}_N} \omega^{-\gamma} |\gamma\rangle\langle\gamma|.$$

$$\text{then} \qquad F_N^\dagger X^{x_j s_j} F_N = Z^{x_j s_j} = \sum_{\gamma \in \mathbb{Z}_N} \omega^{-x_j s_j \gamma} |\gamma\rangle\langle\gamma|.$$

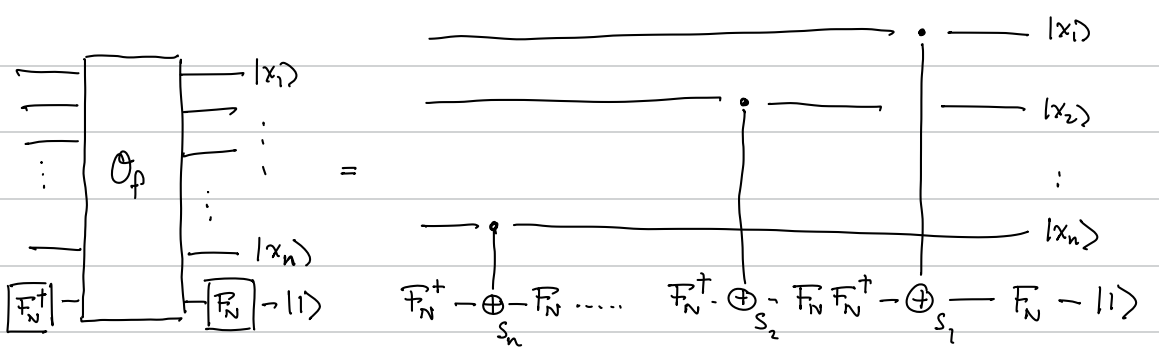
Then,




$$= \quad |x_j\rangle \otimes \omega^{-x_j s_j}|1\rangle$$

$$= \quad \omega^{-x_j s_j}|x_j\rangle$$

$$= \quad |1\rangle$$



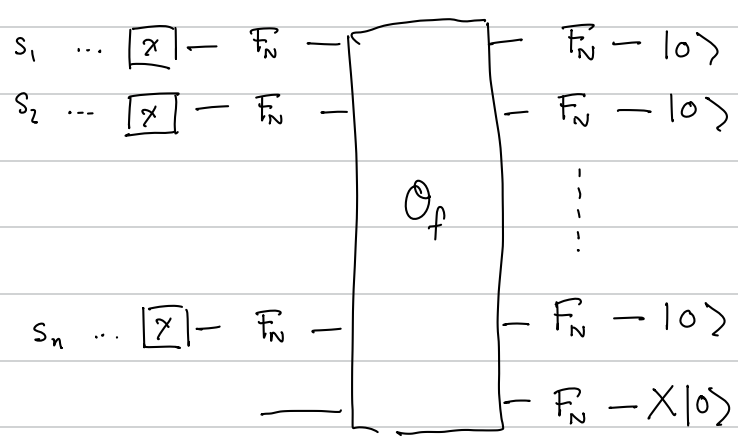
yields $\omega^{-x_1 s_1} |x_1\rangle \otimes \cdots \otimes \omega^{-x_n s_n} |x_n\rangle \otimes |1\rangle$.

Crucially, $(\mathbb{1}^{\otimes n} \otimes F_N^\dagger)\, \mathcal{O}_f\, (\mathbb{1} \otimes F_N)$ is diagonal and kicks back phases.

Now observe that $\frac{1}{\sqrt{N}} \sum_{x_j \in \mathbb{Z}_N} \omega^{-x_j s_j} |x_j\rangle = F_N^\dagger |s_j\rangle$.

And that $F_N |0\rangle = \frac{1}{\sqrt{N}} \sum_{x_j \in \mathbb{Z}_N} |x_j\rangle$.

Full ckt:



Where were the interference patterns?

After oracle, the $j^{th}$ qubit is

$\frac{1}{\sqrt{N}} \sum_{x_j} \omega^{-x_j s_j} |x_j\rangle$ - Applying $F_N$ yields

$$\frac{1}{N} \sum_{x_j} \omega^{-x_j s_j} \sum_{z} \omega^{x_j z} |z\rangle$$

$$= \frac{1}{N} \left( \sum_{z} \left( \sum_{x_j} \omega^{x_j(-s_j+z)} \right) |z\rangle \right)$$

$$N \cdot \mathbb{1}\{-s_j + z = 0\}$$

$$= |s_j\rangle .$$

Only the good amplitude survives.