Lecture 12: Revealing XOR patterns II

(This is perhaps the most important lecture for the practice of Q.C. We'll see how Q.C. lets you)

find patterns in implicitly-represented data

today: XOR

(common story in data processing...)

Data vector length N — Fourier transform based on N "pattern vectors" $|\chi_0\rangle, |\chi_1\rangle, \ldots, |\chi_{N-1}\rangle$ → Length-N vector, s^{th} entry is "strength of $|\chi_s\rangle$ pattern in the data"

$|g\rangle \in \mathbb{C}^N$

Classically: · N is of "physical size" (e.g. 1000)

· vectors explicitly rep'd

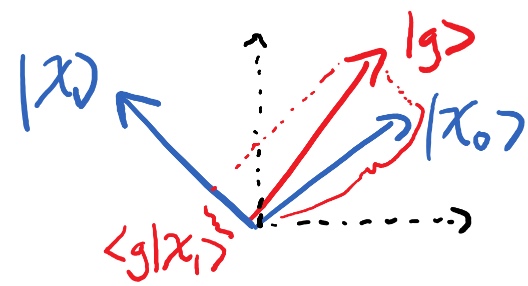
Quantum: · $N = 2^n$, n of "physical size" (e.g. N is 2^{1000})

· vecs. implicitly rep'd by n-qubit state.

Pattern vecs $|\chi_0\rangle, \ldots, |\chi_{N-1}\rangle$ can be <u>any</u> orthonormal basis for $\mathbb{C}^N$.

"Strength of patterns in $|g\rangle$":
<u>coeffs</u> when $|g\rangle$ rep'd in $|\chi_s\rangle$ basis.

"strength" of $|\chi_s\rangle$:
$\langle \chi_s | g \rangle$



(aka $\hat{g}(s)$) (← but won't dwell on this notation much)

Let $U \in \mathbb{C}^{N \times N}$ be matrix w/ cols. $|\chi_0\rangle, \ldots, |\chi_{N-1}\rangle$.
U is <u>unitary</u> (like a "rotation") since ↗ orthonormal

U : standard basis ↓ basis of $|\chi_s\rangle$

U^{-1} : $|\chi_s\rangle$ basis ⟶ std basis
$\parallel$
$U^\dagger$ (← often same as U, or nearly same)

$$|g\rangle = \begin{bmatrix} d \\ a \\ t \\ a \end{bmatrix} \xmapsto{U^\dagger,\ \text{Fourier transf.}} \begin{bmatrix} \hat{g}(0) \\ \hat{g}(1) \\ \vdots \\ \hat{g}(N-1) \end{bmatrix},$$

$\hat{g}(s) =$ "strength of $|\chi_s\rangle$ pattern"

(This is a very general setup, but we'll be focusing on just a couple of particular cases.)

Particular cases for patterns $|\chi_0\rangle, \ldots, |\chi_{N-1}\rangle$:

Want: ① "Interesting/useful"

② Associated change of basis $U \in \mathbb{C}^{N \times N}$ easy to compute by quantum gates.

Today: ① "XOR patterns"

② $U = H^{\otimes n}$: just Hadamard on each qubit

Later (Shor): ① discrete sines/cosines

② U: classic DFT mtx; a little bit harder to quantumly compute.

XOR Functions?

"N" will be 2^n (the beauty of quantum)

Crucial mental perspective:

$$\begin{bmatrix} \sim \\ \sim \\ \sim \\ \vdots \\ \vdots \\ \sim \end{bmatrix} \equiv \begin{array}{c|c} x & f(x) \\ \hline 00\ldots0 & \sim \\ 00\ldots1 & \sim \\ \vdots & \vdots \\ 11\ldots1 & \sim \end{array} \equiv \begin{array}{l} n\text{-qubit} \\ \text{quantum state} \\ \sim|00\cdots0\rangle + \\ \quad \sim|00\cdots1\rangle + \\ \qquad \cdots \\ \qquad + \sim|11\cdots1\rangle \end{array}$$

vector in $\mathbb{C}^N$, $N = 2^n$

truth-table of function $f : \{0,1\}^n \to \mathbb{C}$

(There's a notational hassle here, regarding normalization)

Unit vec. (Need to be a unit vec. Not so if Boolean-valued.) Unit vec.

For $F:\{0,1\}^n \to \{0,1\}$,

$$\underset{F}{\begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \\ \vdots \end{bmatrix}} \to \underset{f = (-1)^F}{\begin{bmatrix} +1 \\ -1 \\ -1 \\ +1 \\ \vdots \end{bmatrix}} \rightsquigarrow \underset{\text{unit! :)}}{\frac{1}{\sqrt{N}}\begin{bmatrix} +1 \\ -1 \\ -1 \\ +1 \\ \vdots \end{bmatrix}}$$

def: (Non-standard.) If $g:\{0,1\}^n \to \mathbb{C}$,

$|g\rangle$ denotes $\displaystyle\frac{1}{\sqrt{N}} \sum_{x\in\{0,1\}^n} g(x)\,|x\rangle.$

rem: A quantum state/unit vec. iff

$$\underbrace{\frac{1}{N}\sum_x |g(x)|^2}_{\text{avg}_x\{|g(x)|^2\}} = 1$$

E.g., if $g(x)\in\{\pm 1\}$.

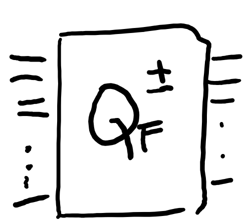
E.g. if $g = f = (-1)^F$

for some $F:\{0,1\}^n \to \{0,1\}$.

recall:

(we'll recall later)

unif. superpos



$|f\rangle$

"Pattern vectors" $|\chi_s\rangle$ also thought of as functions $\{0,1\}^n \to \mathbb{C}$.

Today: $|\chi_s\rangle$ given by "XOR function"

$$\chi_s : \{0,1\}^n \to \{-1,+1\}$$
$$x \longmapsto (-1)^{XOR_s(x)},$$

where $s \in \{0,1\}^n$, $XOR_s(x) = \sum_{i:\, s_i = 1} x_i \mod 2$.

(We'll remember why these are "orthonormal" later.)

Unusual/special property: these pattern vectors are Boolean-valued!

(This is the beauty & simplicity of the Hadamard / Boolean Fourier transform. Typically not like this.)

cf: "usual DFT" (for Shor): $\chi_s(x) = e^{\frac{2\pi i}{N} sx}$,

$$s, x \in \{0,1,2,3,\ldots,N-1\}.$$

"Strength" of pattern $|\chi_s\rangle$ in $|g\rangle$?

(Recall, it's just the coefficient of $|g\rangle$ on $|\chi_s\rangle$ in the χ-basis....) "$\hat{g}(s)$" $= \langle \chi_s | g \rangle$

U^{-1} transform maps $|g\rangle \longmapsto \underset{\substack{\text{pattern} \\ \text{indices} \\ s \in \{0,1\}^n}}{\sum} \hat{g}(s) |s\rangle.$

$\hat{g}(s)$ ← "strengths"

In function notation:

$$\hat{g}(s) = \langle \chi_s | g \rangle = \frac{1}{\sqrt{N}} \overbrace{\left[\chi_s(00\ldots0)^* \;\cdots\cdots\; \chi_s(11\ldots1)^* \right]}^{\langle \chi_s |} \cdot \frac{1}{\sqrt{N}} \overbrace{\begin{bmatrix} g(00\cdots0) \\ \vdots \\ \vdots \\ g(11\cdots1) \end{bmatrix}}^{|g\rangle}$$

$$= \frac{1}{N} \sum_{x \in \{0,1\}^n} \chi_s(x)^* g(x)$$

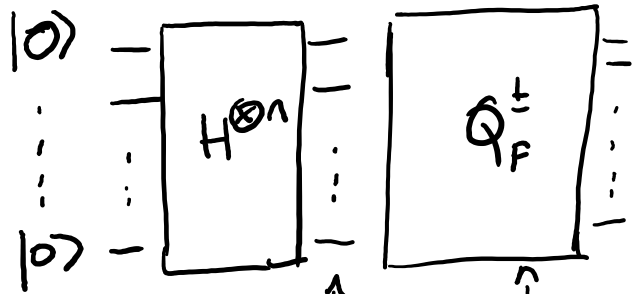
$$= \underset{x \in \{0,1\}^n}{\text{avg}} \left\{ \chi_s(x)^* g(x) \right\} = \text{"correlation of } \chi_s \text{ and } g\text{"}$$

If $g : \{0,1\}^n \to \{\pm 1\}$, and $\chi_s : \{0,1\}^n \to \{\pm 1\}$ (as in XOR patterns)

it's $\underset{x}{\text{avg}} \begin{cases} +1 & \text{if } g(x) = \chi_s(x) \\ -1 & \text{if } g(x) \neq \chi_s(x) \end{cases}$

$$= \Pr_{x \in \{0,1\}^n} \left[g(x) = \chi_s(x) \right] - \Pr_{x} \left[g(x) \neq \chi_s(x) \right], \text{ in } [-1, +1]$$

(Let's redraw the picture.)



$(-1)^{F(x)}$

$$\frac{1}{\sqrt{n}} \sum_x f(x)|x\rangle = \text{"}|f\rangle\text{"}$$

uniform superpos

$$\frac{1}{\sqrt{N}} \sum_x |x\rangle$$

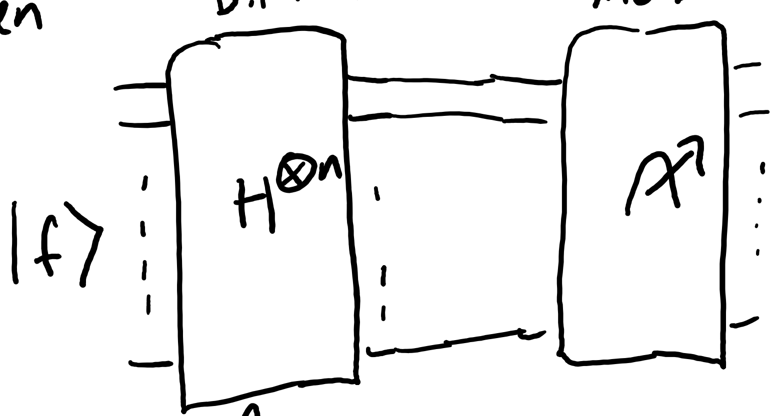
sign-implementation of a classical circuit computing $F : \{0,1\}^n \to \{0,1\}$

"LOADING THE DATA"

(Sort of a coincidence that we get unif. superpos via $\boxed{H^{\otimes n}}$. Just a convenient way to do it. Tho. it *is* $|\chi_{00\ldots0}\rangle$; i.e., |constantly +1 function⟩.)

(There are other ways to do it; particularly for $F : \{0,1\}^n \to \{0,1\}^m$. We'll discuss later.)

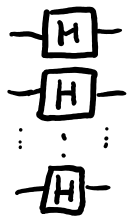
Then D.F.T. measure (usually) "Fourier sampling" paradigm



some $s \in \{0,1\}^n$

$H \otimes H \otimes \cdots \otimes H$, Hadamard/Boolean Fourier transform

$$H^{\otimes n} = H \otimes H \otimes \cdots \otimes H$$



$n=2$ e.g.

$$\frac{1}{\sqrt{2}}\begin{bmatrix} +1 & +1 \\ +1 & -1 \end{bmatrix} \otimes \frac{1}{\sqrt{2}}\begin{bmatrix} +1 & +1 \\ +1 & -1 \end{bmatrix}$$

$N \times N$ unitary,

$N = 2^n$

$$= \frac{1}{\sqrt{4}} \begin{array}{c|cccc} |x\rangle \backslash |s\rangle & |00\rangle & |01\rangle & |10\rangle & |11\rangle \\ \hline |00\rangle & +1 & +1 & +1 & +1 \\ |01\rangle & +1 & -1 & +1 & -1 \\ |10\rangle & +1 & +1 & -1 & -1 \\ |11\rangle & +1 & -1 & -1 & +1 \end{array}$$

From last time:

$$H^{\otimes n}|s\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^{s_1}|1\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^{s_2}|1\rangle\right) \otimes \cdots$$

$$= \frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} (-1)^{XOR_s(x)} |x\rangle$$

$$= |\chi_s\rangle, \quad \text{where } \chi_s : \{0,1\}^n \to \{-1,+1\}$$

$$\chi_s(x) = (-1)^{XOR_s(x)}$$

$$XOR_s(x) = \sum_{i : s_i = 1} x_i \pmod 2 = \sum_{i=1}^{n} s_i x_i \pmod 2$$

$$= s \cdot x \quad (\text{in } \mathbb{F}_2^n)$$

(symmetric in s, x: $(H^{\otimes n})^T = H^{\otimes n}$.)

(Stare at 4x4 example! — cols. of $H^{\otimes n}$ are the $|\chi_s\rangle$ vectors)

$$H^{\otimes n}|s\rangle = |\chi_s\rangle = \frac{1}{\sqrt{N}} \sum_x (-1)^{s\cdot x} |x\rangle$$

e.g.: $\cdot\ H^{\otimes n}|00\cdots0\rangle = \frac{1}{\sqrt{N}} \sum_x |x\rangle$ (unif superpos. ✓)

$\cdot\ H^{\otimes n}|11\cdots1\rangle = \frac{1}{\sqrt{N}} \sum_x (-1)^{\hat{\sum}_{i=1} x_i \bmod 2} |x\rangle$

$\cdot\ H^{\otimes n}|s\rangle = \frac{1}{\sqrt{N}} \sum_{\underbrace{x:\ s\cdot x=0}} |x\rangle - \frac{1}{\sqrt{N}} \sum_{x:\ s\cdot x=1} |x\rangle$

(a vector subspace)

Rec: "strength of pattern $|\chi_s\rangle$ for $|g\rangle$"

= coeff of $|g\rangle$ in basis of χ's

$$\langle\chi_s|g\rangle = \text{“}\hat{g}(s)\text{”} = \Pr_{x\in\{0,1\}^n}[g(x)=\chi_s(x)] - \Pr_{x\in\{0,1\}^n}[g(x)\neq\chi_s(x)]$$

$\in[-1,+1]$

$H^{\otimes n}$: std basis $\rightarrow$ χ_s basis.

$\leftarrow$ via $(H^{\otimes n})^{-1} = H^{\otimes n}$.

$\therefore$ $|g\rangle$ — $H^{\otimes n}$ — $\sum_s \hat{g}(s)|s\rangle$.

Measure: get "s" $\in\{0,1\}^n$ w.prob. $|\hat{g}(s)|^2$.

(squared "strength" of pattern)

Last lecture (Bernstein-Vazirani)

Someone gives you quantum chip Q_F implementing $F = XOR_s$ for some unknown $s \in \{0,1\}^n$. Which?

(We're imagining the "query/oracle/black-box" model, like in HW6 #4 – we'll discuss more later.)
(Can't "look inside" Q_F; want to apply it few times.)

Classical inputs only: $x \longmapsto x \cdot s \bmod 2$.

Could do $x = (1,0,0,\dots,0) \to$ get s_1

$(0,1,0,\dots,0) \to$ get s_2

$\vdots \qquad \vdots$

$(0,0,\dots,0,1) \to$ get s_n

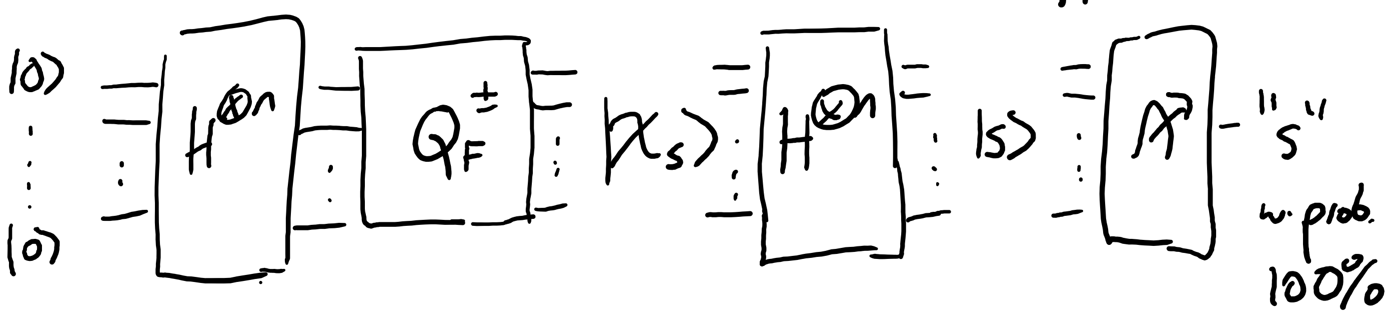
$\underline{n}$ applications. (Not bad. n is a "physically plausible amount.)

Rem: $\geq n$ necessary. Each application $Q_F(x)$ yields only 1 bit of info; need n bits to determine s.

(Indeed, each query yields one $\mathbb{F}_2$-linear equation on unknown s: $x_1 \cdot s_1 + \dots + x_n \cdot s_n = Q_F(x)$.)

(For this problem, randomness doesn't really help. Still only get 1 bit of info/query.)

Quantumly: 1 use of Q_F $\hookrightarrow Q_F^{\pm}$.



Similar speedups?

Deutsch-Jozsa '92:

- Given Q_F implementing $F: \{0,1\}^n \to \{0,1\}$.

Promise: either $F(x) = 0 \quad \forall x$

or F is "balanced": 0 for 50% of x's, 1 for 50% of x's.

- Try to decide which.

(Yes, this problem is highly contrived.)