Lecture 13 - Simon's Algorithm

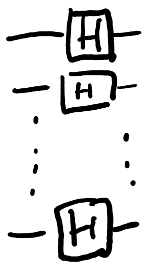
(A problem where quantum algorithms have an exponential speedup over classical ones — but in a contrived, "black-box query" scenario.)

Recap of Fourier sampling paradigm

Let $g : \{0,1\}^n \to \mathbb{C}$ have $\operatorname{avg}_x \{|g(x)|^2\} = 1$.

(E.g. $g(x) = (-1)^{F(x)}$, $F : \{0,1\}^n \to \{0,1\}$.)

Identify it with quantum state $"|g\rangle" := \frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} g(x)|x\rangle$. $(N = 2^n)$

"LOAD DATA" $|g\rangle$  $\sum_{s \in \{0,1\}^n} \hat{g}(s)|s\rangle$,

Hadamard / Bool. Fourier Transf.

$\hat{g}(s)$ = "correlation" of g and χ_s

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

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

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

$$\hat{g}(s) = \langle \chi_s | g \rangle$$

$$= \operatorname*{avg}_{x \in \{0,1\}^n} \{\chi_s(x) g(x)\}.$$

Simon's Algorithm

F is a mystery Boolean function with a secret property.
You can buy copies of Q_F, quantum circuit/gate "implementing" F.
Want to build q. circuit finding the secret ppty using as few copies of Q_F as possible.
Like the Bernstein-Vazirani problem where $F = XOR_s$ for some mystery s. We only needed 1 Q_F there.
Differences today: · we'll need >1 Q_F.
· F will be a Boolean fcn. w/ multiple output bits.

Now $F: \{0,1\}^n \to \{0,1\}^m$. $m \geq n$.

I like to think: F outputs "colors".
(I just want to emphasize that F's inputs & outputs are very different "types" of objects.)
(Strings can stand for any number of things in computing, so why not colors?)

(There are lots of colors in this world; assume each one encoded by some bit-string.)

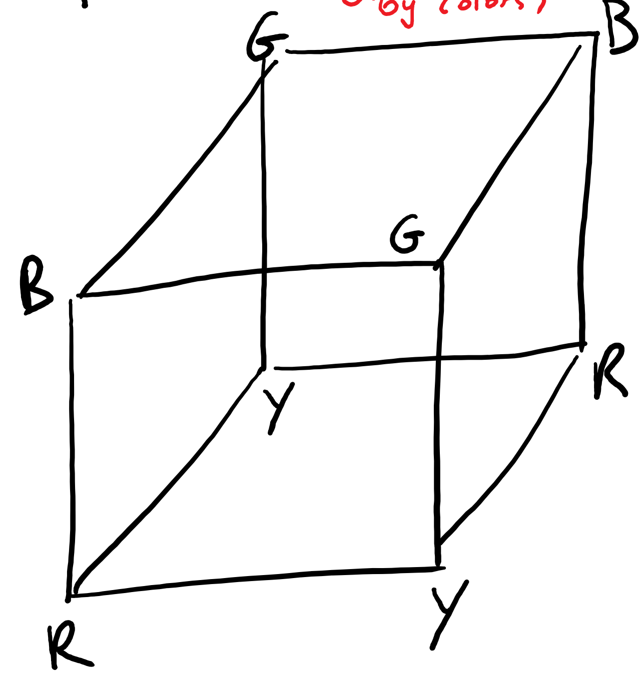
$F : \{0,1\}^n \to \text{COLORS} \subseteq \{0,1\}^m$

(not necessary all strings in F's range)

e.g. $n=3$:

x	$F(x)$
000	Red
001	Yellow
010	Blue
011	Green
100	Yellow
101	Red
110	Green
111	Blue

F: (labels hypercube vertices by colors)



Special promise on F...

F is "L-periodic" for some "secret" string $L \in \{0,1\}^n$. (In e.g. above, $L = 101$.)

def: (usual math definition in $\mathbb{F}_2^n$ context)

F is <u>L-periodic</u> for $L \in \{0,1\}^n$, $L \neq 00\cdots0$

$\forall x, \quad F(x+L) = F(x)$

coord-wise addition mod 2

(or negating bits according to "bitmask" L)

(Go over the n=3 example.)

(Normally, "periodicity" implies lots of value repetition, due to...)

$$F(x) = F(x+L) = F(\underbrace{x+L+L}_{x}) = \cdots\cdot$$

(due to addition mod (Recall: $L \neq 00\cdots0$))

(So the condition only enforces...)

F gives same color to all x, x+L pairs (same as —)

Let's add (nonstandardly) to definition:

"F gives different colors to different pairs."

That is $F(x) = F(y)$ if & <u>only if</u> $y = x+L$.

$\therefore$ L-periodic F always uses exactly $2^n/2$ diff. colors.

<u>Simon's Problem</u>: Given "black-box access" to Q_F implementing some L-periodic F, determine L.

Classical Solutions? [[Meaning: if you only plug classical inputs into Q_F?]]

Really hard!

<u>Claim</u>: Even allowing randomization, $\gtrsim \sqrt{N} = \sqrt{2^n} \approx 1.4^n$ applications of Q_F needed.

<u>Proof sketch</u>: (Similar to Birthday Attack on homework.)

Suppose $L \in \{0,1\}^n \setminus \{00\cdots0\}$ was chosen randomly, as were colors (subject to L-periodicity).

(And you know this fact.)

(may be randomly chosen)

Say you use Q_F T times, on $x^{(1)}, \ldots, x^{(T)} \in \{0,1\}^n$

If, luckily, $F(x^{(i)}) = F(x^{(j)}) \rightarrow$ you learn $L = x^{(i)} + x^{(j)}$ ($\pm$)

Otherwise, you just see T random distinct colors.

When this happens, you've ruled out $\binom{T}{2} \leq T^2$ possible L's.

But L is one of $2^n - 1$ possibilities, so <u>need</u>

$T^2 \geqslant 2^n - 1$ (or $\gtrsim$ if tolerating a little error) $\Rightarrow T \gtrsim \sqrt{2^n}$. "■"

Theorem [Simon]: Quantumly, can do it with $\leq 4n$ applications of Q_F! (Or. $50n$ apps $\Rightarrow$ Prob. failure $\leq 10^{-6}$.)

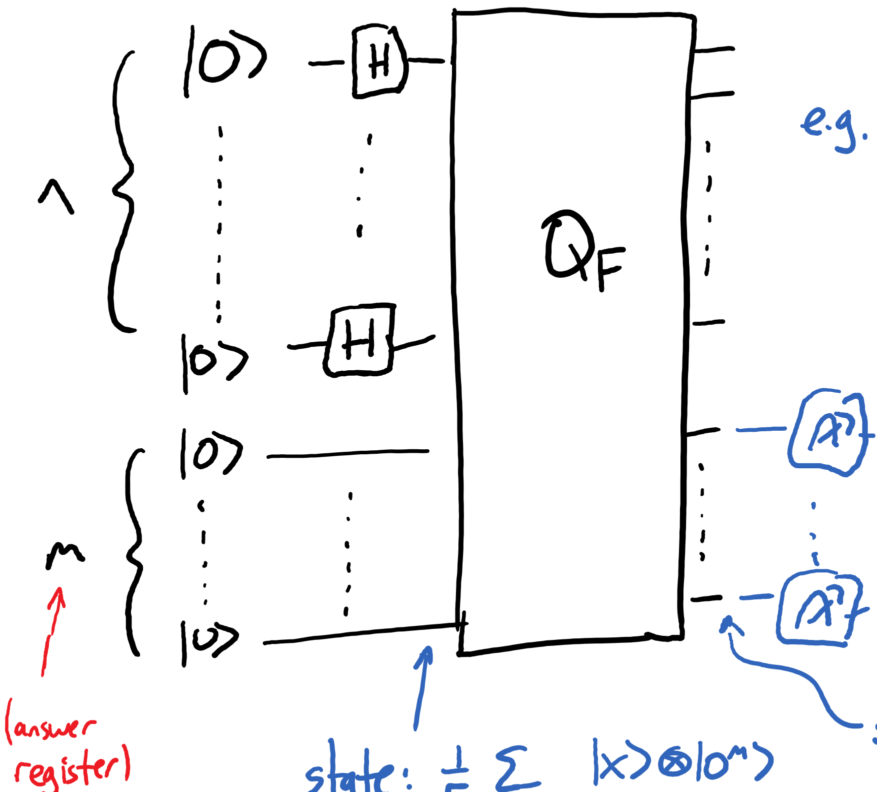
$4n$ vs. $\approx 1.4^n$: an exponential advantage!

(Remark: doesn't prove quantum computers are exponentially superior to classical ones in the "usual" sense, for usual "compute a function" probs. This "count the # of uses of a black-box Q_F" is highly stylized/contrived. Not allowed to "look inside Q_F"! Still.)

(Again, will use Fourier sampling paradigm.)

LOADING DATA

(Phase is a little different, because F has >1 output bit. We don't have "$Q_F^{\pm}$".)



e.g. $\frac{1}{\sqrt{8}}\big(|000\rangle \otimes |Red\rangle$
$+ |001\rangle \otimes |Yellow\rangle$
$+ |010\rangle \otimes |Blue\rangle$
$\vdots$
$+ |111\rangle \otimes |Blue\rangle\big)$

state: $\frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} |x\rangle \otimes |0^m\rangle$

state: $\frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} |x\rangle \otimes |F(x)\rangle$

(Same idea so far: get unif. superposition of all (input, output) pairs.)

New idea: <u>measure</u> the answer register qubits

(In fact, the final algorithm will not actually <u>look</u> at the measurement outcome (!). ∴ by Principle of Deferred Measurement, alg. could just as well <u>not</u> measure. But it simplifies/clarifies analysis.)

Recall partial measurement rules:

- for each string/color c in answer register, prob. of measuring it: p_c = sum of squared (magnitude of) amplitudes next to them.
- if measurement outcome is, say, c^*, state collapses to piece with $|c^*\rangle$'s, normalized by $\frac{1}{\sqrt{p_{c^*}}}$.

Since F is L-periodic, each color c occurs <u>twice</u>, amplitude $\frac{1}{\sqrt{N}}$.

$\therefore$ each $p_c = \frac{2}{N}$. (Recall: $\frac{N}{2}$ colors in use.)

$\therefore$ measurement outcome is some uniformly random color c^*.

State collapses to just two components!

e.g. $\frac{1}{\sqrt{2}}|010\rangle \otimes |\text{Blue}\rangle + \frac{1}{\sqrt{2}}|111\rangle \otimes |\text{Blue}\rangle$!

Generally: Say measurement outcome c^*.

State collapses to

$$\frac{1}{\sqrt{2}}|x^*\rangle \otimes |c^*\rangle + \frac{1}{\sqrt{2}}|x^*+L\rangle \otimes |c^*\rangle,$$

where $F(x^*) = F(x^*+L) = c^*$.

$$\boxed{\left(\frac{1}{\sqrt{2}}|x^*\rangle + \frac{1}{\sqrt{2}}|x^*+L\rangle\right)} \otimes |c^*\rangle$$

discard

(it's unentangled; won't need it any more)

End of "DATA LOADING".

(!! Looks like we're practically done! If we could just peer at the state's amplitudes, we'd easily discover L...)

$$\boxed{\frac{1}{\sqrt{2}}|x^*\rangle + \frac{1}{\sqrt{2}}|x^*+L\rangle}$$

If we could just measure this state twice... 50% chance of seeing x^* once & x^*+L once.

XOR these to get L.

[Alas... can't do that. Measuring it once collapses the state.

Wait... can't we just RELOAD? Get another copy to measure?

Nope... if we reload, we'll get $\frac{1}{\sqrt{2}}|x'\rangle + \frac{1}{\sqrt{2}}|x'+L\rangle$ for some new, uniformly random x', not x^*.]

$$H^{\otimes n}\left(\boxed{\frac{1}{\sqrt{2}}|x^*\rangle + \frac{1}{\sqrt{2}}|x^*+L\rangle}\right)$$

(But this is Simon's Alg! We have to use his slogan, Rotate Compute Rotate! Must put this state thru Hadamard transform!)

$$\frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{N}}\sum_{s\in\{0,1\}^n}(-1)^{x^*\cdot s}|s\rangle + \frac{1}{\sqrt{N}}\sum_{s}(-1)^{(x^*+L)\cdot s}|s\rangle\right)$$

$$= \frac{1}{\sqrt{2N}}\sum_{s\in\{0,1\}^n}(-1)^{x^*\cdot s}|s\rangle\underbrace{\left(1+(-1)^{L\cdot s}\right)}_{\begin{cases}2 & \text{if } L\cdot s=0\\ 0 & \text{if } L\cdot s=1\end{cases}}$$

$$= \sqrt{\frac{2}{N}}\sum_{s:\,L\cdot s=0}(-1)^{x^*\cdot s}|s\rangle$$

(there are $\frac{N}{2}=2^{n-1}$ such s)

$$\sqrt{\frac{2}{N}} \sum_{s : s \cdot L = 0} (-1)^{x^* \cdot s} |s\rangle$$

(This is output of Hadamard transform.)

Now <u>measure</u>:

Receive a uniformly random $s \in \{0,1\}^n$ such that $s \cdot L = 0$. ☺

Remark: ☺ occurs independent of c^*, x^*.

- all "pattern strengths" super-tiny: $\sqrt{\frac{2}{N}}$
- but the XORs with nonzero strength all satisfy $s \cdot L = 0$

$$\begin{gathered} s \cdot L = 0 \\ \| \\ s_1 L_1 + s_2 L_2 + \cdots + s_n L_n = 0 \mod 2 \end{gathered}$$

e.g. if measured "$s = 100110\ldots$",

you learn $L_1 + L_4 + L_5 + \ldots = 0 \bmod 2$

"One bit of info. about secret L."

<u>Now</u> repeat the whole megillah.

Each repetition: $\approx 2n$ H gates

1 Q_F gate

n meas. gates

$\downarrow$

Get a random equation $s \cdot L = 0$,
from all 2^{n-1} possible s.

A system of equations in n unknowns $L_1, \ldots, L_n$ over $\mathbb{F}_2$:

$$\begin{bmatrix} \text{—} & s^{(1)} & \text{—} \\ \text{—} & s^{(2)} & \text{—} \\ & \vdots & \\ \text{—} & s^{(n-1)} & \text{—} \end{bmatrix} \begin{bmatrix} \\ L \\ \\ \end{bmatrix} = 0$$

Repeat it $n-1$ times. $\underbrace{\text{Solve for } L.}_{\text{classical Gaussian Elim, } \approx n^3 \text{ steps.}}$

Always ≥ 2 solutions:
$\vec{0}$, and the true secret L.

If there are no <u>more</u> solutions, you've found L!

Recall (homework): $\begin{array}{c} \\ n-1 \end{array}\left[\quad A \quad\right]\left[\ \ \right]\begin{array}{c}\uparrow\\ n\\ \downarrow\end{array} = \left[0\right]$ has

exactly 2 solutions if and only if A's rows are linear indep. = span an $(n-1)$-dim subspace.

<u>Claim:</u> This occurs with prob. $\geq \frac{1}{4}$.

<u>Then</u>: Keep repeating the whole thing. Expected 4 overall trials

$\rightsquigarrow$. $4(n-1)$ applications of Q_F ✓

· $\approx n^3$ total "work"

Proof of claim:

Assume first i rows $s^{(1)}, \ldots, s^{(i)}$ lin. indep. $\rightarrow$ span an i-dim. subspace

$\hookrightarrow 2^i$ vectors in $\mathbb{F}_2^n$.

The next random $s^{(i+1)}$ (satisfying $s^{(i+1)} \cdot L$) continues the linear independence streak if not in the 2^i vectors.

$\Pr(\text{it } \underline{\text{is}} \text{ in}] = 2^i / 2^{n-1} \leftarrow$ # possibilities for rand. s

$\Rightarrow \Pr[\text{it's } \underline{\text{not}} \text{ in}] = 1 - 2^i/2^{n-1}$.
(hence lin. indep.)

$\therefore$ all $n-1$ $s^{(i)}$'s are lin. indep.

$$= \left(1 - \frac{1}{2^{n-1}}\right)\left(1 - \frac{2}{2^{n-1}}\right)\left(1 - \frac{4}{2^{n-1}}\right) \cdots \cdots \left(1 - \frac{2^{n-2}}{2^{n-1}}\right)$$

$$\geq \frac{1}{2} \cdot \frac{3}{4} \cdot \frac{7}{8} \cdot \frac{15}{16} \cdots \cdots \quad (\approx .288)$$

$$\geq \frac{1}{2} \cdot \left(1 - \frac{1}{4} - \frac{1}{8} - \frac{1}{16} - \frac{1}{32} - \cdots\right) \quad \left(\text{using } (1-a)(1-b) \geq (1-a-b)\right)$$

$$\geq \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4}. \checkmark$$

$\blacksquare$