LECTURE 11 September 26^{th}, 2023

PART II Fundamental Quantum Algorithms

$\boxed{\text{Today}}$ Qiskit Demo & Simons' Algorithm

RECAP Last time we looked at Deutsch's algorithm:

Given $f: \{0,1\} \to \{0,1\}$, decide if f is constant or balanced

Black-box access to f $\quad |x\rangle|y\rangle — \boxed{f} — |x\rangle|y \oplus f(x)\rangle$
(mystery unitary U_f)

Can solve it with one quantum query while two classical queries are needed

Key idea Create the state $\frac{1}{\sqrt{2}}(-1)^{f(0)}|0\rangle + \frac{1}{\sqrt{2}}(-1)^{f(1)}|1\rangle$ by making a superposition query!

This gives a 2X speedup!

Today we will look at Simons' algorithm which gives an exponential advantage in the number of queries!!

This is still in the black-box model and the problem is still mostly of theoretical interest, it directly inspired Shor's factoring algorithm!

Simons' Problem Here the mystery black-box function maps $f: \{0,1\}^n \to \{0,1\}^m$

It is useful to think of the output of f as a color assigned to a bit-string

E.g. (for $n=3$)

x	$f(x)$
000	RED
001	YELLOW
010	BLUE
011	GREEN
100	YELLOW
101	RED
110	GREEN
111	BLUE

Special promise on f $\quad$ f is assumed to be "L-periodic" for some unknown "secret" string $L \in \{0,1\}^n$ where $L \neq 00\cdots0$

$\forall x \in \{0,1\}^n$, $f(x) = f(x+L)$

addition mod 2

and $f(x) = f(y)$ if and only if $y = x + L$ or $y = x$

In other words, f gives the same color to $(x, x+L)$
but gives different colors to different pairs $\Big\}$ # COLORS $= 2^{n-1}$

What is L in the above example ?

Simon's problem is the following :

Given black-box access to f that is L-periodic, determine L

$$\underbrace{|x\rangle}_{n}\underbrace{|y\rangle}_{m} \text{ --- } \boxed{U_f} \text{ --- } \underbrace{|x\rangle}_{n}\underbrace{|y \oplus f(x)\rangle}_{m}$$

What about classical algorithms? Really hard for classical algorithms!

(In-class Exercise) What's the best classical algorithm?

Claim Even allowing randomized algorithms $\gtrsim \sqrt{2^n} \approx 1.4^n$ applications of U_f

Sketch Imagine L was chosen randomly and f is also a random L-periodic function

Say we apply U_f T times on $x^{(1)}, \dots, x^{(T)}$

- If we see two of the same color e.g. $x^{(i)}$ and $x^{(j)}$, then $L = x^{(i)} + x^{(j)}$ and we are done

- If all colors are different, we have ruled out that

$$L \neq x^{(i)} + x^{(j)} \quad \text{for all} \quad 1 \le i < j \le T$$

There are atmost T^2 such pairs, but 2^{n-1} possibilities for L

So, $T^2 \gtrsim 2^{n-1}$ if there is no error ■

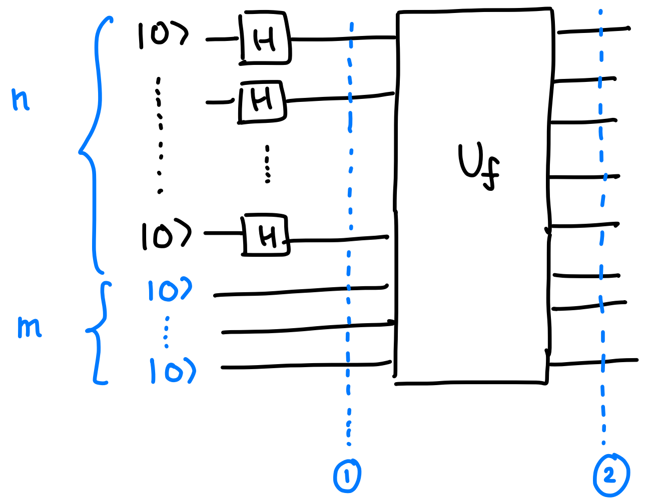
Is there a matching classical algorithm ?

Theorem (Simon) Quantumly one only needs $4n$ queries, i.e. $4n$ applications of U_f

If we repeat it 50 times, we can make $\mathbb{P}[\text{fail}] \le 10^{-10}$.

Summary $\underset{\text{quantum}}{4n}$ vs $\underset{\text{classical}}{1.4^n}$ ← Exponential quantum advantage

<u>The algorithm</u> Let us first try to evaluate f on all the inputs in superposition



$$= \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x, f(x)\rangle$$ ← All queries evaluated in a superposition

Why?

At step ①, state is $|+\rangle^{\otimes n}|0\rangle^{\otimes m} = \left(\frac{1}{\sqrt2}|0\rangle + \frac{1}{\sqrt2}|1\rangle\right)^{\otimes n}|0\rangle^{\otimes m} = \left(\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle\right)\otimes|0\rangle^m$

At step ②, state is $U_f|+\rangle^{\otimes n}|0\rangle^{\otimes m} = \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n} U_f|x\rangle\underbrace{|0\cdots0\rangle}_{m}$

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

<u>E.g.</u> (for $n=3$)

x	$f(x)$
000	RED
001	YELLOW
010	BLUE
011	GREEN
100	YELLOW
101	RED
110	GREEN
111	BLUE

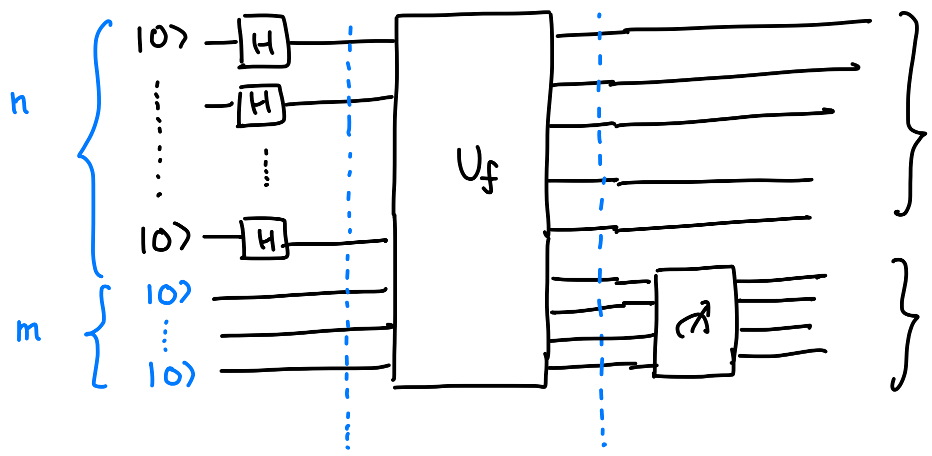
The state at ② is

$$\frac{1}{\sqrt8}\left(|000\rangle\otimes|\text{RED}\rangle + |001\rangle\otimes|\text{YELLOW}\rangle + \ldots\right)$$

So, far we have applied U_f once, i.e. made one quantum query
From this we will learn one bit of information and we can repeat this then

Let's see how to do that!

Let's measure all the ancillas and see what the state of the first n qubits collapses to



?

Measurement Outcome is a COLOR
Let's call it $c^* \in \{0,1\}^m$

Recalling the rules of partial measurement,

$\mathbb{P}[\text{measure } c^*] =$ sum of squared amplitudes where the color is c^*

$$= \frac{2}{2^n} = \frac{1}{2^{n-1}} = \frac{1}{\#\text{ COLORS}}$$

since by L-periodicity there are exactly two such terms in the state

$$\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle |\underbrace{f(x)}_{\text{COLOR}}\rangle$$

So, output is a uniformly random color

And the joint state becomes $\frac{1}{\sqrt{2}} |x^*\rangle |c^*\rangle + \frac{1}{\sqrt{2}} |x^* + L\rangle |c^*\rangle$

where x^* and $x^* + L$ are the pairs where f has value c^*

E.g. $\frac{1}{\sqrt{8}} \left(|000\rangle \otimes |\text{RED}\rangle + |001\rangle \otimes |\text{YELLOW}\rangle + \dots + |101\rangle \otimes |\text{RED}\rangle + \dots \right)$

$\mathbb{P}[\text{each color}] = \frac{1}{4}$

and if we measure RED, (joint) state collapses to

$$\frac{1}{\sqrt{2}} |000\rangle \otimes |\text{RED}\rangle + \frac{1}{\sqrt{2}} |101\rangle \otimes |\text{RED}\rangle$$

So, State of the first n qubits becomes $\frac{1}{\sqrt{2}} |x^*\rangle + \frac{1}{\sqrt{2}} |x^* + L\rangle$

This is very simple state! Almost looks like we are done! But are we?

Let us try some natural things

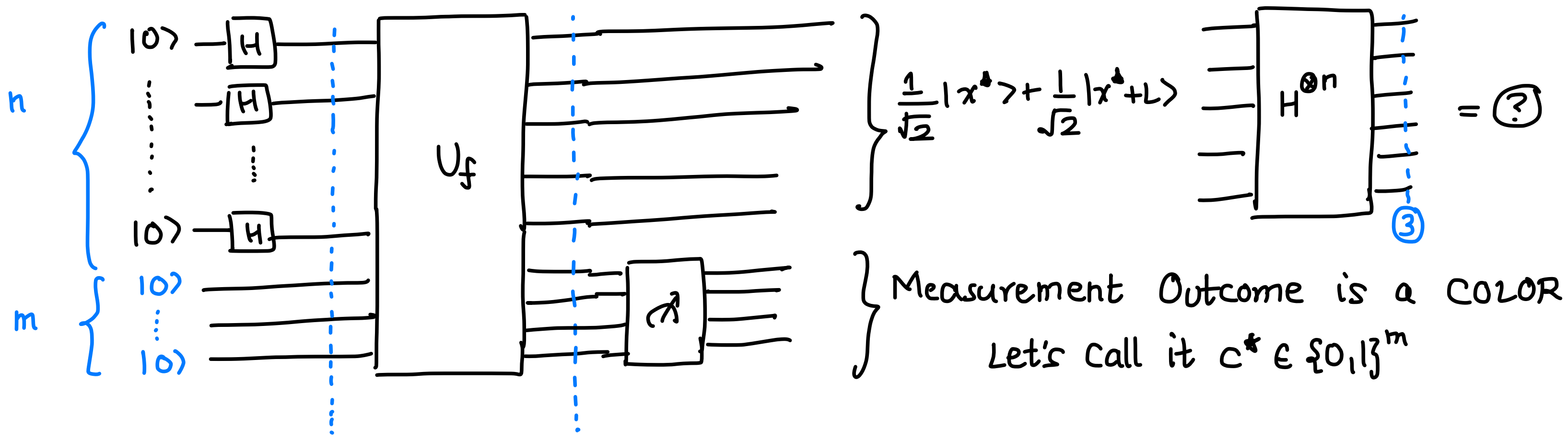
Try 1 Measure — with 50% chance get x^* and $x^* + L$
but can't do it twice with one copy of the state
since it's destroyed after measurement

Try 2 Prepare another copy

but we will get a different c^* and the pair associated to that → Again not helpful

Try 3 Unitary transformation on $\frac{1}{\sqrt{2}} |x^*\rangle + \frac{1}{\sqrt{2}} |x^* + L\rangle$

Let's apply a Hadamard gate H on each qubit and see what happens!



At step 3, the state is $H^{\otimes n}\left(\frac{1}{\sqrt{2}}|x^*\rangle + \frac{1}{\sqrt{2}}|x^*+L\rangle\right)$

$$= \frac{1}{\sqrt{2}} H^{\otimes n}|x^*\rangle + \frac{1}{\sqrt{2}} H^{\otimes n}|x^*+L\rangle$$

What is $H^{\otimes n}|x\rangle$? E.g. if $|x\rangle = |0\cdots0\rangle$

$$H^{\otimes}|0\cdots0\rangle = (H|0\rangle)\otimes(H|0\rangle)\otimes\cdots\otimes(H|0\rangle)$$

$$= |+\rangle^{\otimes n} = \left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right)^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{s\in\{0,1\}^n} |s\rangle$$

$$H^{\otimes n}|x_1\cdots x_n\rangle = (H|x_1\rangle)\otimes(H|x_2\rangle)\otimes\cdots\otimes(H|x_n\rangle)$$

$H|0\rangle = |+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$

$$= \left(\frac{1}{\sqrt{2}}|0\rangle + (-1)^{x_1}|1\rangle\right)\otimes\cdots\otimes\left(\frac{1}{\sqrt{2}}|0\rangle + (-1)^{x_n}|1\rangle\right)$$

$H|1\rangle = |-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$

$$= \frac{1}{\sqrt{2^n}} \sum_{s\in\{0,1\}^n} (-1)^{x_1\cdot s_1 + \cdots + x_n s_n} |s\rangle$$

So, the state at step 3 is

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

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

either $\begin{cases} 2 \text{ if } L\cdot s = 0 \mod 2 \\ 0 \text{ if } L\cdot s = 1 \mod 2 \end{cases}$

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

Half of all $s \in \{0,1\}^n$ satisfy $s\cdot L = 0 \mod 2$
i.e. $\frac{2^n}{2}$ such string s in the sum

What happens if we measure this state now ?

We get a uniformly random $s \in \{0,1\}^n$ such that $s \cdot L = 0 \mod 2$

Note · All the information about x^* went away !!

This is one bit of information about L
For example if $s = 0 \cdots 1 0 \cdots 0$ had a single 1 coordinate
we learn that particular bit of L

In general, we get a linear equation $s \cdot L = 0 \mod 2$ for a random s

We know s explicitly e.g. $s = 1001110000$
$L = L_1 L_2 \cdots L_n$

$\Rightarrow L_1 + L_4 + L_5 + L_6 = 0 \mod 2$

We can repeat this whole quantum subroutine T times and get T linear equations

$$s^{(1)} \cdot L = 0$$
$$s^{(2)} \cdot L = 0$$
$$\vdots$$
$$s^{(T)} \cdot L = 0$$

$\longrightarrow$ Each equation reduces # of possible L's by $\frac{1}{2}$
and we can stop if there are exactly 2 solutions
the true secret string L & 0

If these contain $n-1$ linearly independent equations, we know L exactly $\leftarrow$ Classical algorithm such as Gaussian Elimination

To summarize:
- Quantum subroutine gives us a random s satisfying $s \cdot L = 0$
- Collect T such strings which gives T linear equations (mod 2)
- Solve them classically

$\boxed{\text{NEXT TIME}}$ Buildup to Shor's Algorithm via Quantum Fourier Transform