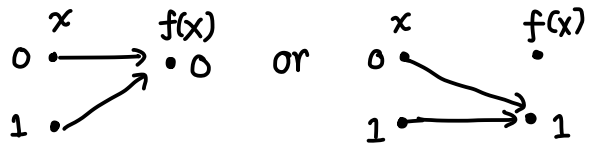
Lecture 11 February 25th

Today Quantum Speedups — Deutsch's & Simon's Algorithm

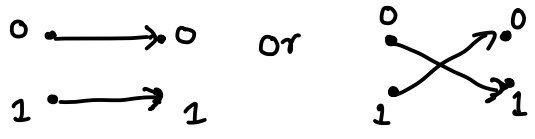
RECAP Deutsch's Algorithm

Given a function $f: \{0,1\} \to \{0,1\}$, determine if it is constant or balanced

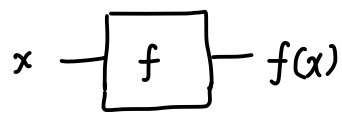
constant : $f(0) = f(1)$



balanced : $f(0) \neq f(1)$



How's the function given to you ? Only "black-box" or "query" access



One is given an API which allows you to get the value of f on any input. This is the only way to access f. In particular, you can't see the code of how f is implemented.

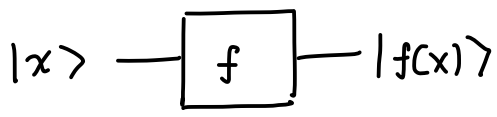
How many queries are needed classically to solve the problem (with no error) ?

- 2 queries are necessary and sufficient

Deutsch's algorithm does it in a single query ← 2× speedup over classical algorithms

Quantum Queries

What does it mean to query a function as a black-box ?



is not reversible and hence not unitary in general

e.g. f = AND

We need to implement it reversibly as we have seen :

$$|x\rangle|y\rangle \xrightarrow{U_f} |x\rangle|y \oplus f(x)\rangle$$

input output

Let us call this unitary U_f

A quantum algorithm can query in superposition

It is easy to see that 2 queries are still required if we only use a classical reversible circuit

Suppose we put the first qubit in $|+\rangle$ state

$$|+\rangle|0\rangle \xrightarrow{U_f} ? = \frac{1}{\sqrt{2}} U_f|00\rangle + \frac{1}{\sqrt{2}} U_f|10\rangle$$

$$= \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|10\rangle \qquad = \frac{1}{\sqrt{2}}|0\rangle|f(0)\rangle + \frac{1}{\sqrt{2}}|1\rangle|f(1)\rangle$$

↑ Contains information about both f(0) and f(1)!

How do we extract it though?

Measuring 1st qubit collapses to

$|0\rangle|f(0)\rangle$ or $|0\rangle|f(1)\rangle$ w\prob $\frac{1}{2}$ each

We could have done this classically as well by querying on a random bit

Let us try putting the 2nd qubit in superposition:

$$|x\rangle|-\rangle \xrightarrow{U_f} ? = \frac{1}{\sqrt{2}} U_f|x\rangle|0\rangle - \frac{1}{\sqrt{2}} U_f|x\rangle|1\rangle$$

$$= \frac{1}{\sqrt{2}}|x0\rangle - \frac{1}{\sqrt{2}}|x1\rangle \qquad = \frac{1}{\sqrt{2}}|x\rangle|0\oplus f(x)\rangle - \frac{1}{\sqrt{2}}|x\rangle|1\oplus f(x)\rangle$$

$$= |x\rangle\left(\frac{1}{\sqrt{2}}|0\oplus f(x)\rangle - \frac{1}{\sqrt{2}}|1\oplus f(x)\rangle\right)$$

$$= \begin{cases} \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle & \text{if } f(x)=0 \\ \frac{1}{\sqrt{2}}|1\rangle - \frac{1}{\sqrt{2}}|0\rangle & \text{if } f(x)=1 \end{cases}$$

$$= \begin{cases} |-\rangle & \text{if } f(x)=0 \\ -|-\rangle & \text{if } f(x)=1 \end{cases}$$

$$= (-1)^{f(x)}|x\rangle|-\rangle$$

f is implemented in the global phase, but still measurement will not help with a global phase

In summary: First qubit in superposition $|+\rangle|0\rangle \xrightarrow{U_f} \frac{1}{\sqrt{2}}|0\rangle|f(0)\rangle + \frac{1}{\sqrt{2}}|1\rangle|f(1)\rangle$

Second qubit in superposition $|x\rangle|-\rangle \xrightarrow{U_f} (-1)^{f(x)}|x\rangle|-\rangle$

Let's put both qubits in superposition :

$$|+\rangle|-\rangle \;\text{—}\boxed{U_f}\text{—}\; \frac{1}{\sqrt{2}}U_f|0\rangle|-\rangle + \frac{1}{\sqrt{2}}U_f|1\rangle|-\rangle$$

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

Let's focus on the first qubit and ignore the second

What we have is a qubit $\frac{1}{\sqrt{2}}(-1)^{f(0)}|0\rangle + \frac{1}{\sqrt{2}}(-1)^{f(1)}|1\rangle$

$$= \begin{cases} |+\rangle & \text{if } f(0)=f(1) \\ |-\rangle & \text{if } f(0)\neq f(1) \end{cases}$$

up to global phase

These two states can be distinguished perfectly! Interference at work!

Final Algorithm

(i) Create the state $|+\rangle|-\rangle$

(ii) Apply U_f

(iii) Measure the first qubit in $|\pm\rangle$ basis

If outcome is "+", output "f is constant"

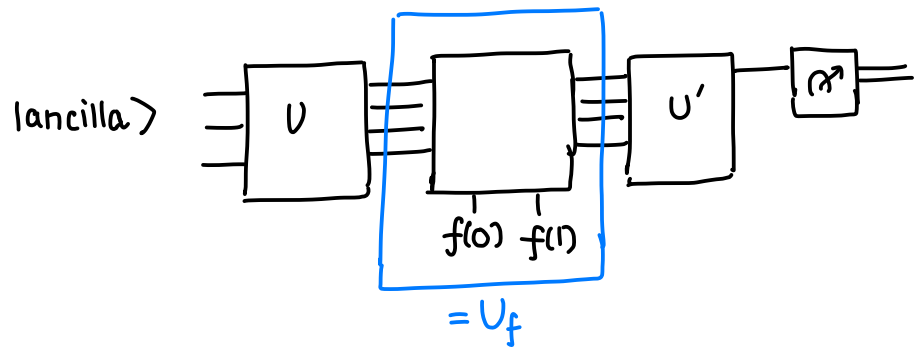
If outcome is "−", output "f is balanced"

Exercise Draw a circuit diagram for this algorithm

Warning You may wonder that this algorithm has no input qubits

The input is the truth table of the function f
but it can only be accessed as a "black-box" or "oracle"

Basically, the circuit can be drawn as



In summary, we take our input ≡ the truth table of f and the ancillas and write a subroutine to compute f reversibly
The quantum algorithm is then allowed to use U_f as a gate in the circuit

The subroutine is the only way to access the input but it may be very complex to implement

So, number of queries is not the final word for efficiency

So, why study this model ?

① Theoretically interesting and one can rigorously compare quantum vs classical

② For most practical quantum algorithms, # queries ≅ # gates

③ We don't know how to prove that there are no efficient classical circuits in terms of # gates

This model is called query complexity model or "black-box model" or "oracle model"

Simon's Algorithm

Deutsch's algorithm gives a 2X speedup !

Now 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, but 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 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

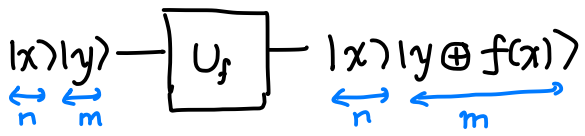
and $f(x) = f(y)$ if and only if $y = x + L$ or $y = x$

In other words, f gives the same color to $(x, x+L)$ but gives different colors to different pairs } # 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



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 ■

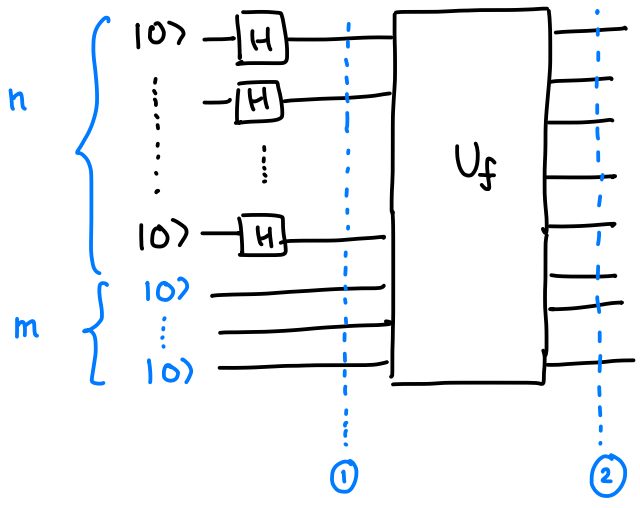
Is there a matching classical algorithm ?

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 $4n$ vs 1.4^n ← Exponential quantum advantage
quantum classical

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

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

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

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

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

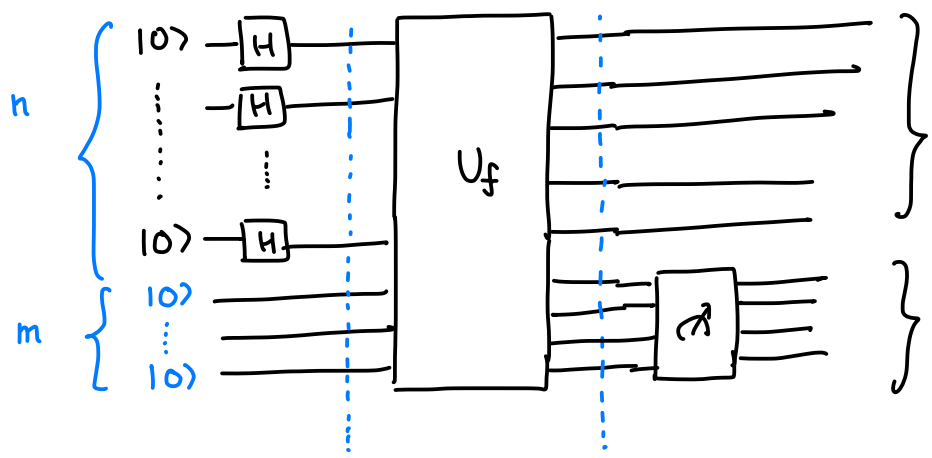
The state at ② is

$$\frac{1}{\sqrt{8}} \left(|000\rangle \otimes |\text{RED}\rangle + |001\rangle \otimes |\text{YELLOW}\rangle + \ldots \right)$$

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



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

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

↳ COLOR

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

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

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

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