Intro To Quantum Computing.

Simon's Algorithm.

- It concerns again Boolean functions, but the task now is more complicated.
- Break-through algorithm: Inspired many other, including Shor's algorithm.
- It contains a (i) Quantum component
  (ii) a Classical component,
  (iii) and incorporates Randomness.

- Before we define the problem, we will talk about

Binary String Addition Modulo 2

- Let a, b be two n-bit strings : $a, b \in \{0,1\}^n$
- $a = a_0 a_1 \cdots a_n$
- $b = b_0 b_1 \cdots b_n$

$\Big\}$ $a_i, b_i \in \{0,1\}$.

- Remember the XOR (exclusive OR) operator on two bits:

$$0 \oplus 0 = 0, \quad 0 \oplus 1 = 1, \quad 1 \oplus 0 = 1, \quad 1 \oplus 1 = 0$$

XOR = Binary addition modulo two

- We can perform $\oplus$ on whole strings : $a \oplus b = c$ where $c_i = a_i \oplus b_i$

$$\begin{array}{r} 1011 \\ \oplus\ 1100 \\ \hline 0111 \end{array}$$

$\Big\}$ Bit-wise addition modulo 2.

Simon's Problem

- Let $f:\{0,1\}^n \to \{0,1\}^n$.
- I.e. f sends n-lenght Binary Strings to other n-lenght Binary Strings.

- f has the following Peculiar Property:

$f(x) = f(y)$ if and only if $x = y$ or $x \oplus s = y$

for some n-Bit String $s \neq 0^n$

- Task: Find s !.
- In other words: How many times we need to "Query" f in order to deduce what the Unknown s is ?

Example: Les's assume $s = 110$ (we work with $n=3$).

Then:

$000 \oplus 110 = 110$.
$001 \oplus 110 = 111$
$010 \oplus 110 = 100$
$011 \oplus 110 = 101$
$100 \oplus 110 = 010$
$101 \oplus 110 = 011$
$110 \oplus 110 = 000$
$111 \oplus 110 = 001$

$x \oplus s \quad y$

This means:
$f(000) = f(110)$
$f(001) = f(111)$
$f(010) = f(100)$
$f(011) = f(101)$
$f(100) = f(010)$
$f(101) = f(011)$
$f(110) = f(000)$
$f(111) = f(001)$

The function is Periodic.

- THE POINT IS THAT WE DO NOT KNOW f OR s.
- BUT WE CAN ASK QUESTIONS TO f ("QUERIES").
- HOW MANY?

→ CLASSICALLY, WE CAN ASK FOUR DIFFERENT QUERIES I.E. "WHAT IS $f(x)$" FOR FOUR DIFFERENT STRINGS x AND GET DIFFERENT ANSWER EACH TIME.

→ THE FIFTH TIME WE QUERY f WE MUST NOTICE A COLLISION: I.E THE EVALUATION OF f ON THE 5TH QUERY $f(x_5)$ MUST BE THE SAME AS ONE OF THE $f(x_1), f(x_2), f(x_3), f(x_4)$, SAY $f(x_3)$.

- THEN, WE KNOW $x_5 = x_3 \oplus s$
  AND THEN s IS EASILY DETERMINED!
- FOR EXAMPLE, LET $x_5 = 011 \Rightarrow f(011) = f(101)$

$$\Rightarrow x_5 = x_3 \oplus s$$
$$011 = 101 \oplus s_1 s_2 s_3$$
$$\Rightarrow s_3 = 110 \quad \checkmark$$

$\Rightarrow 2^{n-1} + 1$ EVALUATIONS / QUERIES.

HOW MUCH BETTER WE CAN DO QUANTUMLY ?

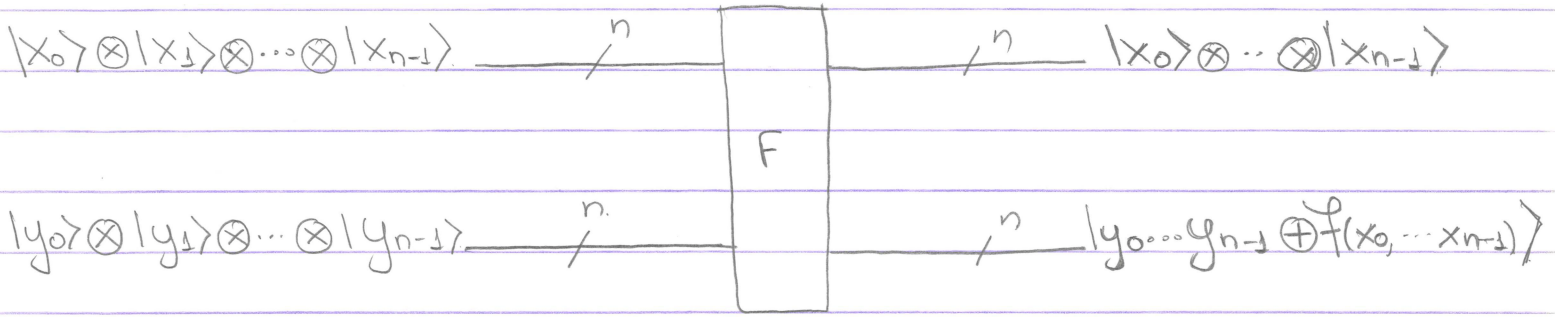
- A LOT...

- DOT PRODUCT OF TWO BINARY STRINGS:
- LET $a = a_0 a_1 \cdots a_{n-1}$, $b = b_0 b_1 \cdots b_{n-1}$ BE TWO n-BIT BINARY STRINGS.
- $a \cdot b = a_0 b_0 \oplus a_1 b_1 \oplus \cdots \oplus a_{n-1} b_{n-1}$.
  I.E. $101 \cdot 111 = (1 \cdot 1) \oplus (1 \cdot 0) \oplus (1 \cdot 1)$
  $= 1 \oplus 0 \oplus 1$
  $= 0$

DETERMINES IF a, b DIFFER IN AN ODD/EVEN NUMBER OF POSITIONS.

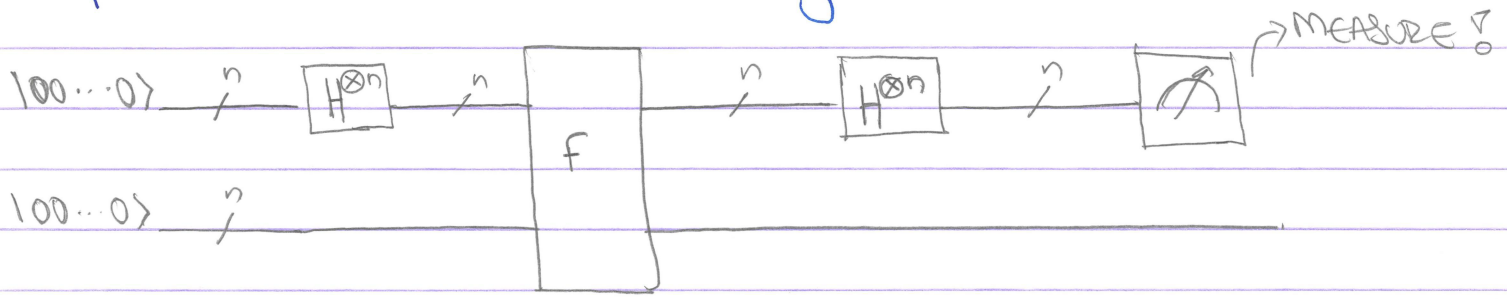
Quantum Circuit for Simon's Problem

- As in previous algorithms, we construct a black box (quantum circuit) that implements f:



- The 2nd output is the function evaluated on the 1st input string ($|x_0\rangle \otimes \cdots \otimes |x_{n-1}\rangle$) added bitwise to the bottom string $|y_0\rangle \otimes \cdots \otimes |y_{n-1}\rangle$.

- Given the above black box, Simon implemented the following circuit (seems very familiar).



Analysis of Simon's Circuit.

Just for the sake of easiness, we will work with $n=2$.

1st Step: 1st input passes through Hadamard:

$$|00\rangle \longrightarrow \frac{1}{2}\left(|00\rangle + |01\rangle + |10\rangle + |11\rangle\right).$$

2nd input remains unchanged.

THE COMPOSITE STATE AFTER THIS STEP IS:

$$\frac{1}{2}\left(|00\rangle + |01\rangle + |10\rangle + |11\rangle\right) \otimes |00\rangle =$$

$$= \frac{1}{2}\left(|00\rangle \otimes |00\rangle + |01\rangle \otimes |00\rangle + |10\rangle \otimes |00\rangle + |11\rangle \otimes |00\rangle\right)$$

2ND STEP: NOW THE QBITS PASS THROUGH THE BLACK-BOX IMPLEMENTING f.

- REMEMBER: OUTPUT IS $|x_0\rangle \otimes \cdots \otimes |x_{n-1}\rangle \otimes |y_0 \cdots y_{n-1} \oplus f(x_0 \cdots x_{n-1})\rangle$

$\Rightarrow$ THE COMPOSITE QUANTUM STATE AFTER THEY PASS F IS

$$\frac{1}{2}\left(|00\rangle \otimes |f(00)\rangle + |01\rangle \otimes |f(01)\rangle + |10\rangle \otimes |f(10)\rangle + |11\rangle |f(11)\rangle\right).$$

THIS IS BECAUSE $|y_0 y_1\rangle = |00\rangle$ AND $|00 \oplus f(x_0 x_1)\rangle = |f(x_0 x_1)\rangle$.

3RD STEP: TOP QBITS PASS THROUGH HADAMARD (AGAIN) ...

SO, FOR THE TOP QBIT WE HAVE:

$$H^{\otimes 2}|00\rangle = \frac{1}{2}\left(|00\rangle + |01\rangle + |10\rangle + |11\rangle\right)$$

$$H^{\otimes 2}|01\rangle = \frac{1}{2}\left(|00\rangle - |01\rangle + |10\rangle - |11\rangle\right)$$

$$H^{\otimes 2}|10\rangle = \frac{1}{2}\left(|00\rangle + |01\rangle - |10\rangle - |11\rangle\right)$$

$$H^{\otimes 2}|11\rangle = \frac{1}{2}\left(|00\rangle - |01\rangle - |10\rangle - |11\rangle\right)$$

AND SO THE STATE NOW BECOMES:

$$\frac{1}{4}\left(|00\rangle + |01\rangle + |10\rangle + |11\rangle\right) \otimes |f(00)\rangle +$$
$$+ \frac{1}{4}\left(|00\rangle - |01\rangle + |10\rangle - |11\rangle\right) \otimes |f(01)\rangle +$$
$$+ \frac{1}{4}\left(|00\rangle + |01\rangle - |10\rangle - |11\rangle\right) \otimes |f(10)\rangle +$$
$$+ \frac{1}{4}\left(|00\rangle - |01\rangle - |10\rangle + |11\rangle\right) \otimes |f(11)\rangle \; . = |\Phi\rangle$$

NOW, WE SIMPLY REARRANGE WITH RESPECT TO $|00\rangle, \dots, |11\rangle$:

$$\Rightarrow |\Phi\rangle = \frac{1}{4}|00\rangle \otimes \left(|f(00)\rangle + |f(01)\rangle + |f(10)\rangle + |f(11)\rangle\right) +$$
$$+ \frac{1}{4}|01\rangle \otimes \left(|f(00)\rangle - |f(01)\rangle + |f(10)\rangle - |f(11)\rangle\right) +$$
$$+ \frac{1}{4}|10\rangle \otimes \left(|f(00)\rangle + |f(01)\rangle - |f(10)\rangle - |f(11)\rangle\right) +$$
$$+ \frac{1}{4}|11\rangle \otimes \left(|f(00)\rangle - |f(01)\rangle - |f(10)\rangle + |f(11)\rangle\right)$$

↑ THE SAME PATTERN OF +,− AS IN PREVIOUS EXPRESSION. IT COMES FROM STRUCTURE OF $H^{\otimes 2}$

- BY THE NATURE OF f, WE KNOW THAT $f(\alpha) = f(\alpha \oplus s)$ FOR THE SECRET s WE ARE TRYING TO FIND.
- SO, THE TERMS IN THE PARENTHESIS ABOVE CAN BE SIMPLIFIED CONSIDERABLY.
- THE DETAILS ARE INVOLVED, BUT WE WILL ILLUSTRATE THIS WITH AN EXAMPLE:

- Say, $f(00) = f(10)$, $f(01) = f(11)$ $\Rightarrow$ $00 = 10 \oplus s_1 s_2$ $\Rightarrow$ $s = 10$

- Then the previous expression for $|\phi\rangle$ simplifies to:

$$|\phi\rangle = \frac{1}{4}|00\rangle \otimes \left(2|f(00)\rangle + 2|f(01)\rangle\right) +$$
$$+ \frac{1}{4}|01\rangle \otimes \left(2|f(00)\rangle - 2|f(01)\rangle\right) +$$
$$+ \frac{1}{4}|10\rangle \otimes (0) +$$
$$+ \frac{1}{4}|11\rangle \otimes (0).$$

$$= \frac{1}{2}|00\rangle \otimes \left(|f(00)\rangle + |f(01)\rangle\right) + \frac{1}{2}|01\rangle \otimes \left(|f(00)\rangle - |f(01)\rangle\right)$$

$$= \frac{1}{\sqrt{2}}|00\rangle \otimes \frac{1}{\sqrt{2}}\left(|f(00)\rangle + |f(01)\rangle\right) + \frac{1}{\sqrt{2}}|01\rangle \otimes \frac{1}{\sqrt{2}}\left(|f(00)\rangle - |f(01)\rangle\right).$$

4TH STEP: MEASUREMENT.

- ACCORDING TO THE LAST EXPRESSION, WHEN WE MEASURE THE TOP QBITS (TOP TWO QBITS IN OUR EXAMPLE) WE SHALL GET EITHER $|00\rangle$ OR $|01\rangle$, EACH WITH PROBABILITY $1/2$.

- Why? WHAT DOES IT MEAN?

- NOTICE THAT BOTH STRINGS 00, 01 HAVE DOT PRODUCT WITH OUR SECRET STRING ($s = 10$) EQUAL TO ZERO:

$$00 \cdot 10 = (0 \cdot 1) \oplus (0 \cdot 0) = 0 \oplus 0 = 0$$
$$01 \cdot 10 = (0 \cdot 1) \oplus (1 \cdot 0) = 0 \oplus 0 = 0.$$

YEAH... SO WHAT?
NEITHER OF THEM IS s...

- But we know that, no matter what, the dot product of the measurement outcome and s must be zero.
- (The details are ommized for now).
- Assume we measure 00.
  $\Rightarrow 00 \cdot s_1 s_2 = 0 \Rightarrow (0 \cdot s_1) \oplus (0 \cdot s_2) = 0$
- Still no info about $s_1 s_2 = s$.

But... let's repeat the entire procedure one more time.

- When we make the new measurement, now we have a chance to get 01.
- So... we keep repeating till we get a different than 00 outcome
- Expected number of re-runs = 2.
- For 01 we have the same property:
  $01 \cdot s_1 s_2 = 0 \Rightarrow (0 \cdot s_1) \oplus (1 \cdot s_2) = 0$.
  $\Rightarrow s_2$ must be 0 !.
  s_1 could be anything
- But we know that $s = s_1 s_2 \neq 00$!
  $\Rightarrow s_1$ must be 1 !

We have found s!.

Example: Let's work with $n=5$. $\Rightarrow 2^5 - 1$ possible candidates for s (we exclude $s=0000$).

- We run Simon's circuit and say we got 10100 = a. as result of measurement
- We know a dot s $= 0 \Rightarrow$
  $\Rightarrow (a_0 s_0) \oplus (a_1 s_1) \oplus (a_2 s_2) \oplus (a_3 s_3) \oplus (a_4 s_4) = 0$
  $\Rightarrow s_0 \oplus s_2 = 0 \Rightarrow s_0 = s_2 = 0$ or
  $s_0 = s_2 = 1$.
- We rerun Simon's circuit till we get measurement different than 10100.

- It turns out that there can be 2^{n-1} possible such strings. (16 if $n=5$).
- Say we got on second time the measurement outcome $b = 00100$
- Same as before $b \cdot s = 0 \Rightarrow$
  $\Rightarrow (b_0 s_0) \oplus (b_1 s_1) \oplus (b_2 s_2) \oplus (b_3 s_3) \oplus (b_4 s_4) = 0$
  $\Rightarrow b_2 s_2 = 0 \Rightarrow s_2 = 0$.
  $\Rightarrow s_0 = 0$.
- So far we have the partially constructed answer.
  $s = 0\, s_1\, 0\, s_3\, s_4$.

- How many times we shall repeat the process?
- Each time we run Simon's circuit, we get a measurement outcome whose dot product with s must be 0.
- This alone gives us a linear equation on the n unknowns
- Each subsequent distinct measurement gives a new equation on n unknowns

$\Rightarrow (n-1)$ such different measurements are enough ($n-1$ and not n since $s \neq 0$ all zero string).

- We have $N = 2^{n-1}$ objects, each one equally probable.
- We keep sampling with replacement till we hit $n-1$ different objects.
- This is a variant of the coupon collector problem.