L25

Monday, April 5, 2021 6:24 PM

Quantum Algorithms

$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

$\alpha^2 + \beta^2 = 1$

- Why Quantum Computers can be faster
- Superposition, making Measurement
  - → Quantum Parallelism
  - → Classical Computers – one input at a Time
- But output of the Quantum Computers can be in superposition state – thus many possible answers
- Role of the Quantum Algorithms

Input: Superposition states → $\boxed{\text{Algorithms}}$ → Output: Measurements?

⇒ Speed of Algorithms

– Complexity Classes P and NP

– Consider the followin problem

		n
E	1) Find two Prime Numbers with the product 35	2
H1	2) Find two prime Numbers with the product 187	3
A H2	3) Find two prime Numbers with × 2407	4
H3	4) Find two prime Numbers with × 88631	5

$T \sim \exp$

Ramanujan

– Consider now "opposite" problem

		n
e	1) Multiply 7 by 5 and check that it = 35	2
h1	2) Multiply 11 by 17 — check = 187	4
B h2	3) Multiply 29 × 83 — check = 2407	4
h3	4) Multiply 337 × 263 — check = 88631	6

$T \sim$ polynomial

– B is easier than A – amount of thime grows more slowly

– Denote number of digits of the input n

A 1) $n=2$, 2) $n=3$, 3) $n=4$ 4) $n=5$

B

– Define $T(n)$ – time or number of steps to solve the question of the input length n

– Complexity ≡ how $T(n)$ grows with n

a) If one can find some positive k and p such that $T(n) \le k n^p$ (problem can be solved in Polinomial Time)

b) If on the other hand we can find k and $c>1$ such that $T(n) > k c^n$ (problem requires an Exponential Time)

Property There is always some n That $T^{EXP}(n) > T^{Pol}(n)$

– Question that can be solved in $T^{Pol}(n)$ – Tractable (in classical computation)

$T^{EXP}(n)$ – Untractable — n – manageable.

→ Potentialy Solvable with increase power of computation

→ Need classical computer ~ Universe

- Our factoring and product problem

  $B \longrightarrow T(n)^{Pol}$

  $A \longrightarrow T(n)^{EXP}$?

- 1991, RSA Laboratories challenge to factor Numbers 100 – 600 decimal digits
  300

- If the problem can be solved in $T(P)^{P}$ – complexity class P

- Say you have a problem and you know the answer → B
  - if checking the answer is complexity class P
  Then we say problem belongs to complexity class NP
  (Nondeterministic Polynomial)

- The problem A – is NP
  - Problem B → Class P

⇒ Theorem: Every P – is also NP

  Inverse is every NP is P   Not proven

  - B – is P
  - A – is NP but is it P?

⇒ Problem of whether NP is equal to P is on of the most important in computer Science

  - Clay Mathematics Institute's one of the "Millennium Prize problems"
    - "P versus NP Problem"

⇒ Are Quantum Algorithms Faster Than Classical Ones

- Most quantum computer (QC) scientists believe $P \neq NP$

- But QC can solve $NP \neq P$ problems in Polynomial Time

- How to compare speed of CC with QC
  Theoretical and Practical

⇒ Complexity for Quantum Computing
Query Complexity

- Algorithms – related to evaluating functions
- Consider functions that belong to two classes of functions.
- Two functions are given in random – We have to determine which of two classes the function belongs

- In running these Algorithms – we have to evaluate these functions

- the query complexity – counts the number of times that we have to evaluate the function to get our answer !

- The function is called Black Box – Oracle

- Querying the Black Box or Oracle

- we track the number of questions – querys

$0 \oplus f = f$

$1 \oplus f =$

P	Q	$P \oplus Q$
0	0	0
1	0	1
0	1	1
1	1	0

we ... asset to BB Oracle

⇒ Deutsch's Algorithm

David Deutsch – founders of Q.C., 1985

– function of One Variable: input 0 or 1 → f → output 0, or 1

$y(x) = $ const

– There are four of these functions $f_0\ f_1\ f_2\ f_3$

– f_0	$0,1 \to f_0 \to 0$	$f_0(0) = 0$ (IN, OUT)	$f_0(1) = 0$ (IN, OUT)	Constant
– f_1	$1 \to 1$, $0 \to 0$	$\to f_1(0) = 0$	$f_1(1) = 1$	Balanced
– f_2	$1 \to 0$, $0 \to 1$	$\to f_2(0) = 1$	$f_2(1) = 0$	Balanced
– f_3	$1 \to 1$, $0 \to 1$	$f_3(0) = 1$	$f_3(1) = 1$	Constant

– $f_0\ \ f_3$ – $\boxed{\text{constant functions}}$

– $f_1\ \ f_2$ – $\boxed{\text{Balanced functions}}$

– Question: given f_0, f_1, f_2, f_2 at random
how many queryies need to be make
do determine function is constant
or Balanced ?!?!

⇒ Classical Analysis: Need to make two evaluations

2 queryes:

input 0 — $f_0\ f_1$ — output 0
1 — $f_1 =$ Balanced — output 1

answer.

⇒ Quantum Analysis:

– Constructing Gate

$|x\rangle \to \hat{F}_i \to |x\rangle$

$|y\rangle \to \hat{F}_i \to |y \oplus f_i(x)\rangle$

0

0

Analysing

$\lvert x\rangle$	$\lvert 1\rangle$	$\lvert 1\rangle$	$0\rangle$	$\lvert 0\rangle$	F_i	$\lvert 0\rangle$	$\lvert 0\rangle$	$\lvert 1\rangle$	$\lvert 1\rangle$
$\lvert y\rangle$	$\lvert 1\rangle$	$\lvert 0\rangle$	$\lvert 1\rangle$	$\lvert 0\rangle$		$\lvert f_i(0)\rangle$	$\lvert f_i(0) \oplus 1\rangle$	$\lvert f_i(1)\rangle$	$\lvert f_i(1) \oplus 1\rangle$

$1 \quad 0$

$|x\rangle \quad |y\rangle$

$|0 \oplus f_i(0)\rangle$

$f_i(0) = 0$: $f_i(0)$: $|0 \oplus 0\rangle = |0\rangle$ — $f_i(0)$.

$f_i(0) = 1$: $|0 \oplus 1\rangle = |1\rangle$ — $f_i(0)$ — $f_i(1)$

$|x\rangle \quad |y\rangle$

$$|0\rangle \otimes |0\rangle \xrightarrow{|0\rangle|0\rangle F_i} |0\rangle \otimes |0 \oplus f_i(0)\rangle = \boxed{|0\rangle \otimes |f_i(0)\rangle}$$

$$|0\rangle \otimes |1\rangle \xrightarrow{|0\rangle|1\rangle F_i} |0\rangle \otimes |1 \oplus f_i(0)\rangle = |0\rangle \otimes |f_i(0) \oplus 1\rangle$$

$$|1\rangle \otimes |0\rangle \xrightarrow{|1\rangle|0\rangle F_i} |1\rangle \otimes |0 \oplus f_i(1)\rangle = \boxed{|1\rangle \otimes |f_i(1)\rangle}$$

$$|1\rangle \otimes |1\rangle \xrightarrow{|1\rangle|1\rangle F_i} |1\rangle \otimes |1 \oplus f_i(1)\rangle = |1\rangle \otimes |f_i(1) \oplus 1\rangle$$

!

⇒ Let's make first measurement with $|0\rangle \otimes |0\rangle$ input

$|x\rangle$: $|0\rangle \to F_i \to |0\rangle$

$|y\rangle$: $|0\rangle \to F_i \to |f_i(0)\rangle$

$|0\rangle\ |0\rangle \quad |0\rangle\ |1\rangle$

$i=0$	$i=1$	$i=2$	$i=3$
$\lvert 0\rangle$	$\lvert 0\rangle$	$\lvert 0\rangle$	$\lvert 0\rangle$
$\lvert f_0(0)\rangle = \lvert 0\rangle$	$\lvert f_1(0)\rangle = \lvert 0\rangle$	$\lvert f_2(0)\rangle = \lvert 1\rangle$	$\lvert f_3(0)\rangle = \lvert 1\rangle$

– with this measuremen one can not distinguish f_0 – from f_1 or f_2 from f_3

$|0\rangle\ |0\rangle$ $|0\rangle\ |1\rangle$

– Say output was $\boxed{|0\rangle \otimes |0\rangle}$ then it is either f_0 or f_1

f_2

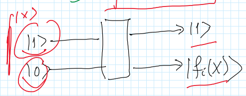
$i = 2$ $\qquad$ $i = 3$

$|0\rangle \otimes f_2(0) = \boxed{|0\rangle \otimes |1\rangle}$ $\qquad$ $|0\rangle \otimes f_3(0)$

$|1\rangle \otimes f_2(1) = \boxed{|1\rangle \otimes |0\rangle}$ $\qquad$ $|1\rangle \otimes f_3(1$

– Need to do another measurement with different input

⇒ Say $|1\rangle \otimes |0\rangle$ output $|1\rangle \otimes |0\rangle$



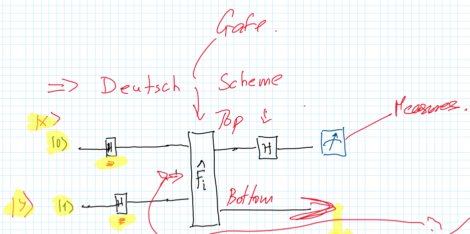
$i=0$: $|1\rangle$, $|f_0(1)\rangle = |0\rangle$

$i=1$: $|1\rangle$, $|f_1(1)\rangle = |1\rangle$

– if this measuremen yields $|1\rangle|0\rangle$ then it is f_0

if $|1\rangle|1\rangle$ it is f_1

⇒ Deutsch Scheme



$\hat{H}|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ $\quad \hat{H}\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle) = |0\rangle$

$\hat{H}|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ $\quad \hat{H}\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle) = |1\rangle$

$$\hat{H}|0\rangle \otimes \hat{H}|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\otimes\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle) = \frac{1}{2}(|00\rangle-|01\rangle+|10\rangle-|11\rangle)$$

$$\frac{1}{2}(|00\rangle-|01\rangle+|10\rangle-|11\rangle)\hat{F}_i = \frac{1}{2}(|0\rangle\otimes|f_i(0)\rangle - |0\rangle\otimes|f_i(0)\oplus 1\rangle + |1\rangle\otimes|f_i(1)\rangle - |1\rangle\otimes|f_i(1)\oplus 1\rangle)$$

$|00\rangle\hat{F}_i = |0\rangle|0\rangle\hat{F}_i = |0\rangle\otimes f_i(0)$

$|01\rangle\hat{F}_i = |0\rangle|1\rangle\hat{F}_i = |0\rangle\otimes|f_i(0)\oplus 1\rangle$

$|10\rangle\hat{F}_i = |1\rangle|0\rangle\hat{F}_i = |1\rangle\otimes|f_i(1)\rangle$

$|11\rangle\hat{F}_i = |1\rangle|1\rangle\hat{F}_i = |1\rangle\otimes|f_i(1)\oplus 1\rangle$

$$= \frac{1}{2}\Big[\overset{|x\rangle}{|0\rangle}\otimes(|f_i(0)\rangle - |f_i(0)\oplus 1\rangle) + \overset{|x\rangle}{|1\rangle}\otimes(|f_i(1)\rangle - |f_i(1)\oplus 1\rangle)\Big]$$

$\Rightarrow |f_i(0)\rangle - |f_i(0)\oplus 1\rangle <$ $|0\rangle - |1\rangle$ (if $f_i(0) = 0$) ; $|1\rangle - |0\rangle$ (if $f_i(0) = 1$)

$|0\rangle - |1\rangle = (-1)^0(|0\rangle - |1\rangle)$

$|1\rangle - |0\rangle = (-1)^1(|0\rangle - |1\rangle)$

$$|f_i(0)\rangle - |f_i(0)\oplus 1\rangle = \boxed{(-1)^{f_i(0)}(|0\rangle - |1\rangle)}$$

Same way

$$|f_i(1)\rangle - |f_i(1)\oplus 1\rangle = \boxed{(-1)^{f_i(1)}(|0\rangle - |1\rangle)}$$

$$// = \frac{1}{2}\{|0\rangle \otimes ((-1)^{f_i(0)}(|0\rangle - |1\rangle)) + |1\rangle \otimes ((-1)^{f_i(1)}(|0\rangle - |1\rangle)) = //$$

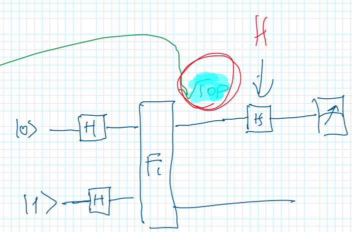
$$// = \frac{1}{2}\left((-1)^{f_i(0)}|0\rangle \otimes (|0\rangle - |1\rangle) + (-1)^{f_i(1)}|1\rangle \otimes (|0\rangle - |1\rangle)\right) = //$$

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

$$= \underbrace{\frac{1}{\sqrt{2}}\left((-1)^{f_i(0)}|0\rangle + (-1)^{f_i(1)}|1\rangle\right)}_{\text{Normalized state, Top}} \otimes \underbrace{\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)}_{\text{Bottom}}$$

Normalized state

- Qubits are not Entangled
- Top qubit is $\frac{1}{\sqrt{2}}\left((-1)^{f_i(0)}|0\rangle + (-1)^{f_i(1)}|1\rangle\right)$ Top



- Examine the top state

For f_0	$f_0(0)=0$, $f_0(1)=0$	$\left(\frac{1}{\sqrt{2}}\right)(|0\rangle + |1\rangle)$	$\hat{H} =$	$|0\rangle$
f_1	$f_1(0)=0$, $f_1(1)=1$	$\left(\frac{1}{\sqrt{2}}\right)(|0\rangle - |1\rangle)$		$|1\rangle$
f_2	$f_2(0)=1$, $f_2(1)=0$	$\left(-\frac{1}{\sqrt{2}}\right)(|0\rangle - |1\rangle)$		$-|1\rangle$
f_3	$f_3(0)=1$, $f_3(1)=1$	$\left(-\frac{1}{\sqrt{2}}\right)(|0\rangle + |1\rangle)$		$-|0\rangle$

- Apply $\hat{H}$ gate $\quad \hat{H}\left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right) = |0\rangle$

$\hat{H}\left(\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right) = |1\rangle$

- for

f_0	$|0\rangle$
f_1	$|1\rangle$
f_2	$-|1\rangle$
f_3	$-|0\rangle$

- If we make measurement for top state in standard basis

we get 0 if f_0 and f_3 — constant

Undo

1 if f_1 and f_2 — balanced