QC17

Monday, April 5, 2021 6:24 PM

Quantum Algorithms

- Why Quantum Computers can be faster

- Superposition, making Measurement

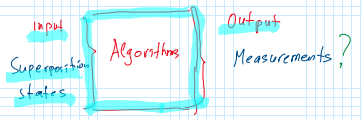
  → Quantum Parallelism

  → Classical computers - one input at a Time

$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, $\alpha^2 + \beta^2 = 1$

- But output of the Quantum Computers can be in superposition state - thus many possible answers

- Role of the Quantum Algorithms



⇒ Speed of Algorithms

- Complexity classes P and NP

- Consider the following problem

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

Ramanujan

- Consider now "opposite" problem

		n	
e	1) Multiply 7 By 5 and check that it = 35	2	
H	2) Multiply 11 By 17 — check = 187	4	
B	H 3) Multiply 29 × 83 — check = 2407	4	T ~ polynomial
	H3 4) Multiply 337 × 263 — check = 88631	6	

- B is easier than A - amount of time 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 $T(n) \leq Kn^P$

(problem can be solved in Polynomial Time)

b) If on the other hand we can find K and C>1 such that $T(n) > KC^n$

(problem requires an Exponential Time)

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

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

$T(n)^{EXP}$ - Untractable — n - many all.

→ Potentially Solvable with increase power of computation

→ Need classical computer ~ Universe

- Our factoring and product problem

B → $T(n)^{Pol}$

A → $T(n)^{EXP}$?

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

300

- If the problem can be solved in $T(n)^{P}$ - 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 NP~~

⇒ 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 ≠ P problems in Polynomial Time

- How to compare speed of CC with QC

Theoretical and Practical

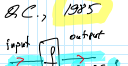
⇒ Complexity for Quantum Computing
Query Complexity

- 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 - queries asked to BB Oracle

⇒ Deutsch's Algorithm

David Deutsch - founders of Q.C., 1985

- function of One Variable



$y(x) =$ Const ⇒

- There are four of these functions $f_0\ f_1\ f_2\ f_3$
  - f_0  $f_0(0) = 0$ $f_0(1) = 0$ Constant
  - f_1  $f_1(0) = 0$ $f_1(1) = 1$ Balanced
  - f_2  $f_2(0) = 1$ $f_2(1) = 0$ Balanced
  - f_3  $f_3(0) = 1$ $f_3(1) = 1$ Constant
  - f_0 f_3 - Constant functions
  - f_1 f_2 - Balanced functions
  - Question: given f_0, f_1, f_2, f_3 at random how many queries need to be made to determine function is Constant or Balanced

⇒ Classical Analysis: Need to make two evaluations

2 queries

Input 0 f_0 f_1 output 0

Input 1 f_1 = Balanced output 1

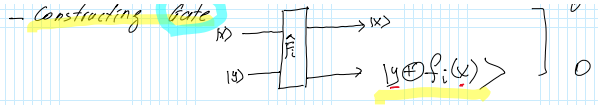
answer.

⇒ Quantum Analysis:

0 ⊕ f = f

1 ⊕ f =

P	Q	P ⊕ Q
0	0	0
1	0	1
0	1	1
1	1	0



Analysing

$|x\rangle$ $|1\rangle$ $|1\rangle$ $|0\rangle$ $|0\rangle$ F_i $|0\rangle$ $|0\rangle$ $|1\rangle$ $|1\rangle$

$|y\rangle$ $|1\rangle$ $|0\rangle$ $|1\rangle$ $|0\rangle$ $|f_i(0)\rangle$ $|f_i(0)\oplus 1\rangle$ $|f_i(1)\rangle$ $|f_i(1)\oplus 1\rangle$

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

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

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

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

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

$|x\rangle$ $|1\rangle$ $|y\rangle$ $|0\rangle$ $|b \oplus f_i(0)\rangle$

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

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

$i=2$

$|0\rangle \otimes f_2(0) =$

$|1\rangle \otimes f_2(1) =$

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

$|x\rangle$ $|0\rangle$ $|0\rangle$ F_i $|f_i(0)\rangle$ $|y\rangle$

$i=0$ $|0\rangle$ $|f_0(0)\rangle = |0\rangle$

$i=1$ $|0\rangle$ $|f_1(0)\rangle = |0\rangle$

$i=2$ $|0\rangle$ $|f_2(0)\rangle = |1\rangle$

$i=3$ $|0\rangle$ $|f_3(0)\rangle = |1\rangle$

- with this measurement one can not distinguish f_0 - from f_1 or f_2 from f_3 $|0\rangle$ $|1\rangle$

- Say output was $|0\rangle \otimes |0\rangle$ then it is either f_0 or f_1

- Need to do another measurement with different input

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

$|x\rangle$ $|1\rangle$ $|0\rangle$ $|1\rangle$ $|f_i(x)\rangle$

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

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

- if this measurement yields $|1\rangle|0\rangle$ then it is f_0

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

⇒ Deutsch

Gate.

Scheme

Top ↓

Measure.

$|x\rangle$ $|0\rangle$

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

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

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

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

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

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

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

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

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

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

$\Rightarrow |f_i(0) - |f_i(0)\oplus 1\rangle \begin{cases} |0\rangle - |1\rangle & (\text{if } f_i(0) = 0) \\ |1\rangle - |0\rangle & (\text{if } f_i(0) = 1) \end{cases}$

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

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

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

Same ways

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

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

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

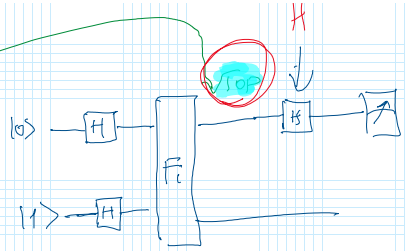
$= \frac{1}{2}((-1)^{f_i(0)}|0\rangle + (-1)^{f_i(1)}|1\rangle) \otimes (|0\rangle - |1\rangle) = //$

Normalized state

$= \frac{1}{\sqrt{2}}\left((-1)^{f_0(0)}|0\rangle + (-1)^{f_0(1)}|1\rangle\right) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

Normalized state — Top — Bottom

- Qubits are not Entangled
- Top qubit is $\frac{1}{\sqrt{2}}\left((-1)^{f_1(0)}|0\rangle + (-1)^{f_1(1)}|1\rangle\right)$ — Top



- Examine the top state

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

$\hat{H}$ = $|0\rangle$, $|1\rangle$, $-|1\rangle$, $-|0\rangle$

- Apply $\hat{H}$ gate

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

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

- 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

1 if f_1 and f_2 — Balanced