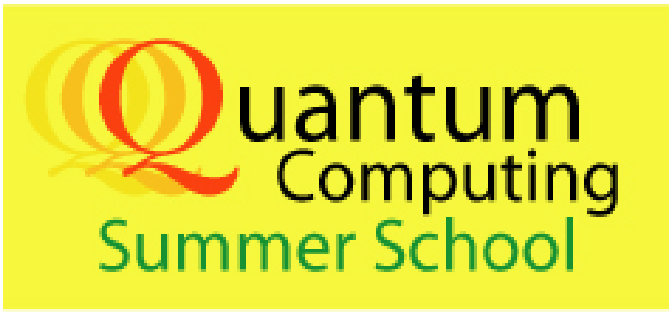
Quantum Computing Summer School

[Home]
[Members]
[Schedule]
[Overview]
[Sponsors]
[Archive/Links]
[Contact]



Home | Members | Schedule | Overview | Sponsors | Archive/Links | Contact

For problems or questions regarding this web contact V.Bulitko.
Last updated: 03/08/02.

Members

[Home]
[Members]
[Schedule]
[Overview]
[Sponsors]
[Archive/Links]
[Contact]

Presenters *(tentative)*		
	Angela Antoniu	aantoniu@ualberta.ca
	Vadim Bulitko *(chair)*	bulitko@ualberta.ca
	David Fortin	dcfortin@ualberta.ca
	Vahid Rezania	vrezania@Phys.ualberta.ca
	Arzu Sardarli	sardarli@ee.ualberta.ca
Participants *(tentative)*		
	Jason Blackstock	jblackst@Phys.ualberta.ca
	Robert Bryce	rbryce@edm.trlabs.ca

	Randy Goebel	Randy.Goebel@ualberta.ca
	Sanket Goel	sanket@ee.ualberta.ca
	Dave Gomboc	dave@cs.ualberta.ca
	Russ Greiner	greiner@cs.ualberta.ca
	Jeongwon Ho	jwho@Phys.ualberta.ca
	Jim Hoover	hoover@cs.ualberta.ca
	Govind Kaigala	govind@ee.ualberta.ca
	Jonathan Kelly	jkelly@cs.ualberta.ca
	Yaser Khamayseh	yaser@cs.ualberta.ca
	Dejan Kihas	kihas@ee.ualberta.ca
	Billie Sze-Hin Kwan	bkwan@ee.ualberta.ca
	Ilya Levner	ilya@cs.ualberta.ca

	Peter Xiaoping Liu	xpliu@ee.ualberta.ca
	Omid Madani	madani@cs.ualberta.ca
	Bruce Matichuk	bmatichuk@celcorp.com
	Samer Nassar	samer@cs.ualberta.ca
	Jim Nastos	nastos@cs.ualberta.ca
	Ashikur Rahman	ashikur@cs.ualberta.ca
	Lino Ramirez	l.ramirez@ieee.org
	Marlene Rodriguez	rodrigue@ee.ualberta.ca
	Daniel Salamon	salamon@ee.ualberta.ca
	Ajit Paul Singh	ajit@cs.ualberta.ca
	Dan Tzur	DTZUR@pharmacy.ualberta.ca
	Eric Woolgar	ewoolgar@math.ualberta.ca

	Herb Yang	yang@cs.ualberta.ca
	Peter Yap	peteryap@peteryap.com

Home | Members | Schedule | Overview | Sponsors | Archive/Links | Contact

For problems or questions regarding this web contact V.Bulitko.
Last updated: 03/08/02.

Schedule

[Home]
[Members]
[Schedule]
[Overview]
[Sponsors]
[Archive/Links]
[Contact]

Dates: every Tuesday and Thursday : May 2, 2002 through June 27, 2002
Time: 10:00am -- 11:20am
Place: Computing Science Centre, room B-43

The slides are here

The notes are here.
Please report all inaccuracies, comments, and observations to the author. Thanks!

Date	Topics	Presenter	Problems
May 2nd	Chapter 1 : Introduction and overview	Dave Fortin	
May 7th	Chapter 2 : Linear Algebra	Angela Antoniu	Ex. 2.11, 2.24, 2.17, 2.25, 2.18, 2.19, 2.27, 2.42, 2.48
May 9th	Chapter 2 : Postulates of Quantum Mechanics	Angela Antoniu	Ex. 2.51, 2.52, 2.53, 2.58, 2.59, 2.66
May 14th	Chapter 2 : Applications: super-dense coding, EPR	Dave Fortin	Ex. 2.69, 2.70
May 16th	Chapter 3 : Introduction to Computer Science, complexity classes	Vadim Bulitko	Ex. 3.7
May 21st	Chapter 3 : Reversible circuits	Vadim Bulitko	Ex. 3.32
May 23rd	Chapter 4 : Quantum circuits, part 1	Vahid Rezania	Ex. 4.3; 4.4; 4.6; 4.7; 4.8; 4.10; 4.12; 4.13; 4.15; 4.16; 4.18; 4.20; 4.21; 4.22; 4.23; 4.24; 4.25; 4.28; 4.31
May 28th	Chapter 4 : Quantum circuits, part 2	Vahid Rezania	Ex. 4.32; 4.34; 4.35; 4.37; 4.38; 4.39; 4.40; 4.41; 4.44
May 30th	Chapter 4 : Quantum circuits, part 3	Vahid Rezania	Ex. 4.46; 4.47; 4.49; 4.50; 4.51
June 4th	Chapter 5 : Quantum Fourier transform, part 1	Arzu Sardarli	Ex. 5.3, 5.8, 5.9, 5.18

June 6th	Chapter 4 : review and discussion; Chapter 5 : Quantum Fourier transform, part 2	Vadim Bulitko	Ex. 5.28, 5.3
June 13th	Chapter 6 : Quantum Search algorithm	Vahid Rezania	Ex. 6.1, 6.2, 6.3, 6.7, 6.12, 6.17
June 18th	Chapter 7 : Quantum Computers : physical realization, part 1	Arzu Sardarli	
June 20th	Chapter 7 : Quantum Computers : physical realization, part 2	Arzu Sardarli	
June 25th	Chapter 7 : Quantum Computers : physical realization, part 3	Arzu Sardarli	
June 27th	Quantum Computing for Artificial Intelligence	Ilya Levner	

Home | Members | Schedule | Overview | Sponsors | Archive/Links | Contact

For problems or questions regarding this web contact V.Bulitko.
Last updated: 03/08/02.

Quantum Computing Summer School

Lecture 1 : Introduction

Introduction

- Short-Term Objectives

  Introduce Quantum Computing Basics to interested parties in and around the University of Alberta

- Long-Term Objectives

  Engage into AI/CS/Math Research projects benefiting from Quantum Computing

- Format
  - Seminar-type meetings of 80 minute duration
  - Twice per week
- Prerequisite
  - No linear algebra or quantum mechanics assumed
  - A math or CS background would be beneficial

Introduction

- School Schedule (Days, Time and Place)

Dates:	Tuesdays and Thursdays : May 2, 2002 to June 27, 2002
Time:	10:00am -- 11:20am
Place:	Computing Science Centre, Room B-43

Introduction

- School Text

Quantum Computation &
Quantum Information

Michael A. Nielsen
Isaac L. Chuang

ISBN: 0 521 63503 9 Paperback
ISBN: 0 521 63235 8 Hardback

Cost: $48.00 New Paperback
$35.45 Used Paperback
(http://www.amazon.com)

Introduction

- Tentative Schedule (Week by Week)

May 2	Introduction and overview	Dave Fortin
May 7	Linear Algebra	Angela Antoniu
May 9	Postulates of Quantum Mechanics	Angela Antoniu
May 14	Applications: super-dense coding, EPR	Dave Fortin
May 16	Intro to Computer Science, complexity classes	Vadim Bulitko
May 21	Reversible circuits	Vadim Bulitko
May 23	Quantum circuits, part 1	Vahid Rezania / Angela Antoniu
May 28	Quantum circuits, part 2	
May 30	Quantum circuits, part 3	

Introduction

- Tentative Schedule (Week by Week)

June 4	Quantum Fourier transform	Arzu Sardarli
June 6	Quantum Fourier transform : Shor's algorithm	Vadim Bulitko
June 11	Quantum Search algorithm, part 1	Vahid Rezania
June 13	Quantum Search algorithm, part 2	Vahid Rezania
June 18	Quantum Computers : physical realization, part 1	Arzu Sardarli / Dave Fortin
June 20	Quantum Computers : physical realization, part 2	
June 25	Quantum Computers : physical realization, part 3	
June 27	Review and discussion	Vadim Bulitko

Introduction

- Presenters

Angela Antoniu
a.antoniu@ieee.org
Research Associate
Electrical & Computer Engineering Department

Vadim Bulitko
bulitko@ualberta.ca
Professor
Department of Computing Science

David Fortin
dcfortin@ualberta.ca
Administrator,
The Centre for Nanoscale Physics

Vahid Rezania
vrezania@phys.ualberta.ca
Postdoctoral Fellow
Department of Physics

Arzu Sardarli
sardarli@ee.ualberta.ca
Research Associate/Sessional Lecturer
Electrical & Computer Engineering Department

Introduction

- Resources: Web-Pages, Links, etc.
  - Information about the course can be found at:

Quantum Computing Summer School
http://www.cs.ualberta.ca/~bulitko/qc/

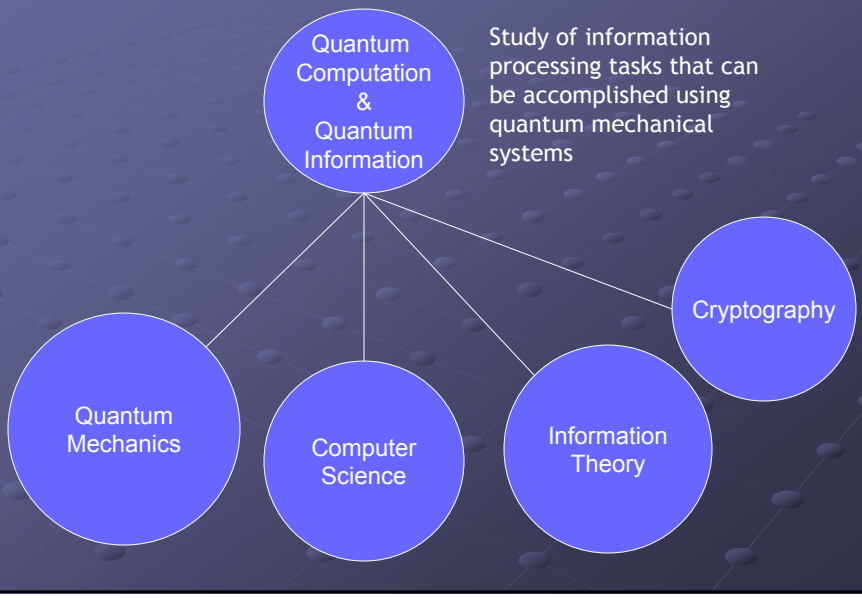
The Centre for Nanoscale Physics
http://nanoscale.phys.ualberta.ca

  - Links to other sites may also be obtained from above

Presentation Overview

Qubits	1 Qubit -> Bloch Sphere, 2 Qubits -> Bell States, n Qubits
Quantum Computation	Gates: Single Qubit, Arbitrary Single Qubit -> Universal Quantum Gates, Multiple Qubit Gates -> CNOT Other Computational Bases
Quantum Circuits	Qubit Swap Circuit Qubit Copying Circuit Bell State Circuit -> Quantum Teleportation
Quantum Algorithms	Toffoli Gate -> Quantum Parallelism -> Hadamard Transform Deutsch's Algorithm, Deutsch-Josa Algorithm Other Algorithms - Fourier Transform, Quantum Search, Quantum Simulation
Quantum Information Processing	Stern-Gerlach, Optical Techniques, Traps, NMR, Quantum Dots

Historical Vantage Point



What's a qubit?

- A qubit has two possible states $|0\rangle \text{or} |1\rangle$
- Unlike bits, a qubit can be in a state other than $|0\rangle \text{or} |1\rangle$
- We can form linear combinations of states $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$
- A qubit is a vector in a 2D complex vector space

Qubits

Qubits are computational basis states

- orthonormal basis

$$\langle i|j\rangle = \delta_{ij} \qquad \delta_{ij} = \begin{cases} 0 \text{ for } i \neq j \\ 1 \text{ for } i = j \end{cases}$$

- we cannot examine a bit to determine its quantum state

How can a qubit be realized?

- Two polarizations of a photon
- Alignment of a nuclear spin in a uniform magnetic field
- Two states of an electron orbiting a single atom (ground or excited state)

Qubits Cont'd

- We may rewrite $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ as...

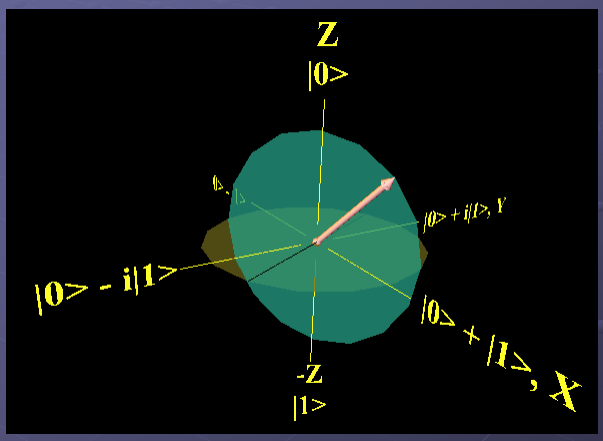
$$|\psi\rangle = e^{i\alpha}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle\right)$$

We can ignore $e^{i\alpha}$ as it has no observable effect

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle$$

- From a single measurement one obtains only a single bit of information about the state of the qubit
- There is "hidden" quantum information and this info grows exponentially

Bloch Sphere



How about 2 Qubits?

- Classically there are 4 possible states
- Quantum Mechanically there are 4 COMPUTATIONAL BASIS STATES

$$|00\rangle, |01\rangle, |10\rangle, |11\rangle$$

- a pair of qubits can also exist in a superpositions of these states where the amplitudes are complex numbers

How about 2 Qubits?

- The measurement result x occurs with a probability $|\alpha_x|^2$
- With the state of the qubits after the measurement being $|x\rangle$
- Which must sum to one

  ie: normalization condition

$$\sum_{x\in\{0,1\}^2} |\alpha_x|^2 = 1$$

How about 2 Qubits?

We could measure just a subset of the qubits

- Measuring the 1st one alone gives $|0\rangle$ with probability $|\alpha_{00}|^2 + |\alpha_{01}|^2$ leaving the post measurement state.

$$|\psi'\rangle = \frac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}$$

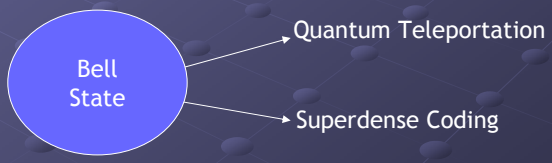
...which still satisfies the normalization condition.

How about 2 Qubits?

The "Bell State" or "EPR Pair"

is an important qubit state.

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}$$



How about 2 Qubits?

The Bell State has the property that upon measuring the 1st qubit one obtains two possible results.

- 0 with probability ½ leaving the post measurement state

$$|\phi'\rangle = |00\rangle$$

- 1 with probability ½ leaving the post measurement state

$$|\phi'\rangle = |11\rangle$$

- The measurement of the 2nd qubit always gives the same result as the measurement of the 1st qubit.
- ie: The measurements are CORRELATED

How about 2 Qubits?

John Bell State proved an amazing result:

The measurement correlations in the Bell State are STRONGER than could ever exist between classical systems

implies that quantum mechanics allows information processing beyond that of classical information processing

How about n qubits?

- Computational Basis States…

$$|x_1 x_2 x_3 \ldots x_n\rangle \qquad \therefore\ 2^n \text{ amplitudes}$$

if n=500

2^{500} is more than the number of atoms in the universe

Lets see a classical computer store that many numbers!!!

Quantum Computation

Changes to a quantum state can be described using the language of quantum computation

- Single Qubit Gates

Classical Not Gate - Truth table

$$0 \to 1 \text{ and } 1 \to 0$$

Quantum Not Gate - Truth table

$$|0\rangle \to |1\rangle \text{ and } |1\rangle \to |0\rangle$$

Quantum Computation

Superposition of states?

Not without further knowledge of the properties of quantum gates

The quantum NOT gate acts LINEARLY…

$$\alpha|0\rangle + \beta|1\rangle \to \alpha|1\rangle + \beta|0\rangle$$

Linear behaviour is a general property of quantum mechanics

Non-linear behaviour can lead to apparent paradoxes

- Time Travel
- Faster than light communication
- Violates the 2nd Law of Thermodynamics

Quantum Computation

NOT gate representation

$$X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad \text{for any} \quad \alpha|0\rangle + \beta|1\rangle \equiv \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

we get…

$$X\begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \beta \\ \alpha \end{bmatrix} \text{ or } \beta|0\rangle + \alpha|1\rangle$$

to summarize… $\alpha|0\rangle + \beta|1\rangle \rightarrow \alpha|1\rangle + \beta|0\rangle$

Quantum Computation

Are there any constraints on what matrices may be used as quantum gates? Of course!

We require the normalization condition

$$|\alpha|^2 + |\beta|^2 = 1 \quad \text{for} \quad |\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

and the result $|\psi'\rangle = \alpha'|0\rangle + \beta'|1\rangle$ after the gate has acted

The appropriate condition for this (of course) is that the matrix representing the gate is UNITARY

$$U^\dagger U = I \quad \text{where } U^\dagger \text{ is the adjoint of } U$$

That's it!!! Anything else is a valid quantum gate.

Quantum Computation

Two more important gates…

- Z gate

$$Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

leaves $|0\rangle$ unchanged
flips the sign of $|1\rangle$ to $-|1\rangle$

- Hadamard Gate

$$H \equiv \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

turns $|0\rangle$ into $(|0\rangle + |1\rangle)/\sqrt{2}$
turns $|1\rangle$ into $(|0\rangle - |1\rangle)/\sqrt{2}$

Note: Applying H twice to a state does nothing to it.

$$H^2 = I$$

Quantum Computation

Hadamard Gate: A most useful gate indeed!

if $H = \frac{1}{\sqrt{2}}(X + Z)$ and $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ *then*

$$H|\psi\rangle = \frac{1}{\sqrt{2}}\left(X|\psi\rangle + Z|\psi\rangle\right)$$

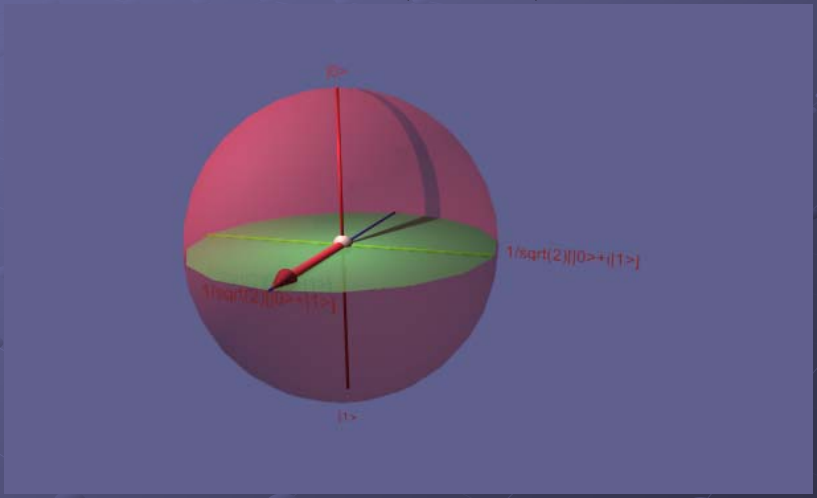
$$= \frac{1}{\sqrt{2}}\left(\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} \alpha \\ \beta \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} \alpha \\ \beta \end{bmatrix}\right) = \frac{1}{\sqrt{2}}\left(\begin{bmatrix} \beta \\ \alpha \end{bmatrix} + \begin{bmatrix} \alpha \\ -\beta \end{bmatrix}\right) = \frac{1}{\sqrt{2}}\begin{bmatrix} \alpha + \beta \\ \alpha - \beta \end{bmatrix}$$

for $H|0\rangle$ $\quad \alpha = 1, \beta = 0 \quad H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

for $H|1\rangle$ $\quad \alpha = 0, \beta = 1 \quad H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

Quantum Computation

Hadamard Gate: Bloch Sphere Representation



Quantum Computation

- Review: Important single-qubit gates

$\alpha|0\rangle+\beta|1\rangle$ — X — $\beta|0\rangle+\alpha|1\rangle$

$\alpha|0\rangle+\beta|1\rangle$ — Z — $\alpha|0\rangle-\beta|1\rangle$

$\alpha|0\rangle+\beta|1\rangle$ — H — $\alpha\frac{|0\rangle+|1\rangle}{\sqrt{2}}+\beta\frac{|1\rangle-|1\rangle}{\sqrt{2}}$

Quantum Computation

- Arbitrary Single Qubit Quantum Gate
  - complete set from properties of a much smaller set

$$U = e^{i\alpha}\begin{bmatrix} e^{-i\frac{\beta}{2}} & 0 \\ 0 & e^{i\frac{\beta}{2}} \end{bmatrix}\begin{bmatrix} \cos\frac{\gamma}{2} & -\sin\frac{\gamma}{2} \\ \sin\frac{\gamma}{2} & \cos\frac{\gamma}{2} \end{bmatrix}\begin{bmatrix} e^{-i\frac{\delta}{2}} & 0 \\ 0 & e^{i\frac{\delta}{2}} \end{bmatrix}$$

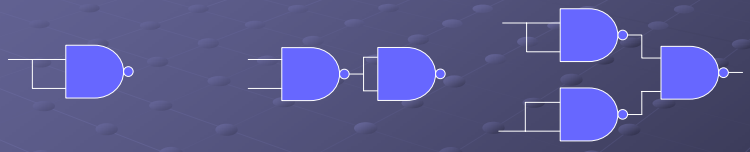
Global Phase Factor | Rotation about z | Rotation | Scaling Constant

α, β, γ and δ are all real valued

Quantum Computation

- Classical Universal Gates (example)
  - The NAND gate is a classical Universal Gate. Why?

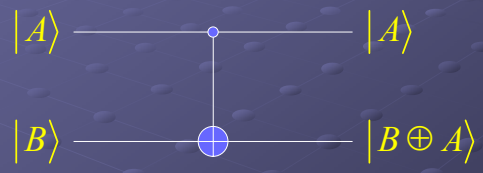
NOT gate using NAND | AND gate using NAND | OR gate using NAND



- Universal Quantum Gates
  - An arbitrary quantum Computation on n qubits can be generated by a finite set of gates that are UNIVERSAL for quantum computation
    - Need to introduce some multiple qubit quantum gates

Multiple Qubit Gates

- Controlled-NOT (CNOT) Gate
  - two input qubits: control and target

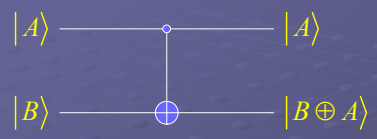


if control is 0 target left alone $|00\rangle \rightarrow |00\rangle$ or $|01\rangle \rightarrow |01\rangle$

else control is 1 target qubit is flipped $|10\rangle \rightarrow |11\rangle$ or $|11\rangle \rightarrow |10\rangle$

- In General $|A, B\rangle \rightarrow |A, B \oplus A\rangle$

CNOT quantum gate



$$U_{CN} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

$$|A\rangle|B\rangle \rightarrow \begin{bmatrix} A_0 \begin{bmatrix} B_0 \\ B_1 \end{bmatrix} \\ A_1 \begin{bmatrix} B_0 \\ B_1 \end{bmatrix} \end{bmatrix} = \begin{bmatrix} A_0 B_0 \\ A_0 B_1 \\ A_1 B_0 \\ A_1 B_1 \end{bmatrix}$$

if $|A\rangle = |0\rangle$ then $A_0 = 1$, $A_1 = 0$ we get $\begin{bmatrix} B_0 \\ B_1 \\ 0 \\ 0 \end{bmatrix}$

if $|A\rangle = |1\rangle$ then $A_0 = 0$, $A_1 = 1$ we get $\begin{bmatrix} 0 \\ 0 \\ B_0 \\ B_1 \end{bmatrix}$

Any multiple qubit logic gate may be composed from CNOT and Single Qubit Gates

Other Computational Bases

- Measurements
  - In terms of $|+\rangle = \frac{(|0\rangle + |1\rangle)}{\sqrt{2}}, |-\rangle = \frac{(|0\rangle - |1\rangle)}{\sqrt{2}}$ basis states

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \alpha\frac{|+\rangle + |-\rangle}{\sqrt{2}} + \beta\frac{|+\rangle - |-\rangle}{\sqrt{2}} = \frac{\alpha+\beta}{\sqrt{2}}|+\rangle + \frac{\alpha-\beta}{\sqrt{2}}|-\rangle$$

  - Generally any basis state can represent an arbitrary qubit state

$$|\psi\rangle = \alpha|a\rangle + \beta|b\rangle$$

  - If orthonormal then we can perform a measurement in keeping with probability interpretation

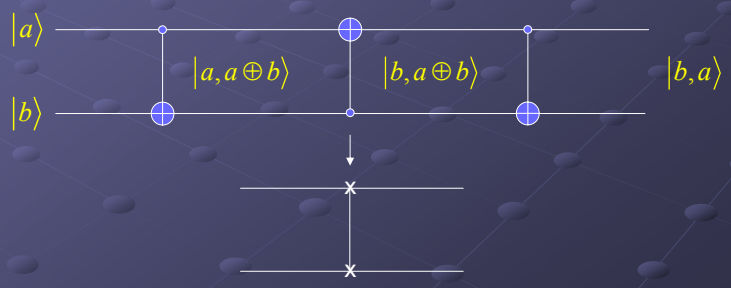
Quantum Circuits

- Elements of a Quantum Circuit
  - each line in a circuit represents a "wire"
    - passage of time
    - photon moving from one location to another
  - assume the state input is a computational basis state
  - input is usually the state consisting of all $|0\rangle$s
  - no loops allowed ie: acyclic
  - No FANIN(not reversible therefore not Unitary)
  - FANOUT (can't copy a qubit)

Quantum Circuits

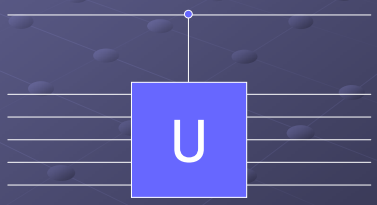
- Quantum Qubit Swap Circuit

$$|a,b\rangle \rightarrow |a,a\oplus b\rangle$$
$$\rightarrow |a\oplus(a\oplus b),a\oplus b\rangle = |b,a\oplus b\rangle$$
$$\rightarrow |b,(a\oplus b)\oplus b\rangle = |b,a\rangle$$



Quantum Circuits

- Controlled-U Gate
  - A Controlled-U Gate has one control qubit and n target qubits
  - where U is any unitary matrix acting on n qubits

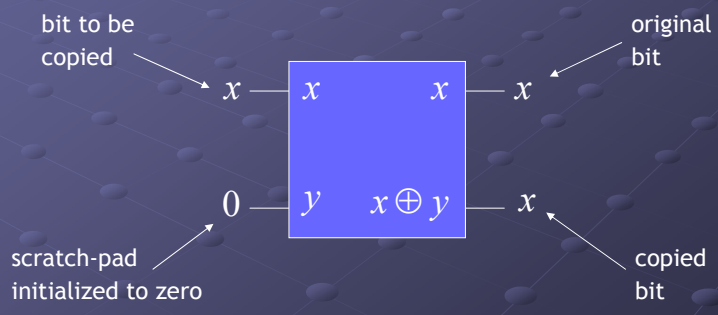


Quantum Circuits

- Measurement Operation
  - Converts a single qubit state into a probabilistic classical bit M

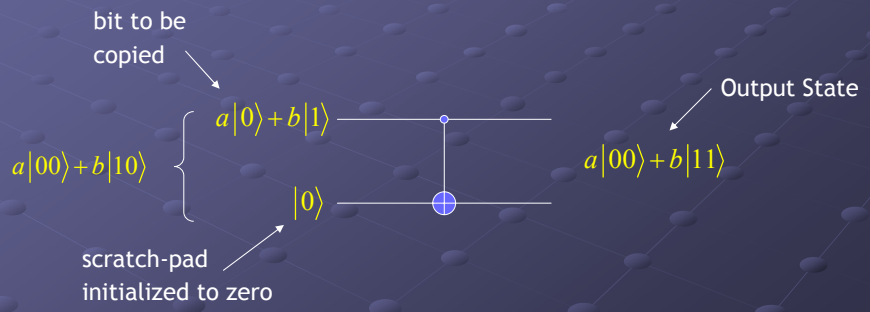
Quantum Circuits

- Can we make a Qubit Copying Circuit?
  - Copying a classical bit can be done with the Classical CNOT gate



Quantum Circuits

- Can we make a Qubit Copying Circuit?
  - How about copying a qubit in an unknown state using a controlled-CNOT gate? $|\psi\rangle = a|0\rangle + b|1\rangle$



Quantum Circuits

- Can we make a Qubit Copying Circuit?
  - Does $|\psi\rangle|\psi\rangle = a|00\rangle + b|11\rangle$?

$$|\psi\rangle|\psi\rangle = (a|0\rangle + b|1\rangle)(a|0\rangle + b|1\rangle) = a^2|00\rangle + ab|01\rangle + ab|10\rangle + b^2|11\rangle$$

  - Unless $ab = 0$ this does not copy the quantum state input

$$a^2|00\rangle + ab|01\rangle + ab|10\rangle + b^2|11\rangle \neq a|00\rangle + b|11\rangle$$

  - It is impossible to make a copy of the unknown quantum state

- NO CLONING THEOREM -

Quantum Circuits

- Bell States, EPR States, EPR Pairs

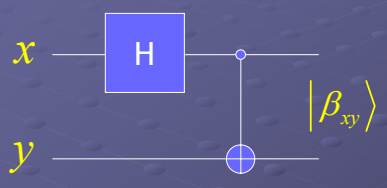
$$|\beta_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \qquad |\beta_{01}\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$$

$$|\beta_{10}\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}} \qquad |\beta_{11}\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$$

$$|\beta_{xy}\rangle = \frac{|0, y\rangle + (-1)^x |1, \bar{y}\rangle}{\sqrt{2}}$$

Quantum Circuits

- Bell States, EPR States, EPR Pairs



In	Out
$\|00\rangle$	$(\|00\rangle + \|11\rangle)/\sqrt{2} \equiv \|\beta_{00}\rangle$
$\|01\rangle$	$(\|01\rangle + \|10\rangle)/\sqrt{2} \equiv \|\beta_{01}\rangle$
$\|10\rangle$	$(\|00\rangle + \|11\rangle)/\sqrt{2} \equiv \|\beta_{00}\rangle$
$\|11\rangle$	$(\|00\rangle + \|11\rangle)/\sqrt{2} \equiv \|\beta_{00}\rangle$

$$\left.\begin{array}{l} |0\rangle \rightarrow \dfrac{|0\rangle + |1\rangle}{\sqrt{2}} \\ |0\rangle \rightarrow \end{array}\right\} \rightarrow \frac{|00\rangle + |10\rangle}{\sqrt{2}} \rightarrow \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

Quantum Circuits

- Quantum Teleportation
  - technique for moving quantum states around
  - Alice & Bob generate an EPR pair together

$$|\beta_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

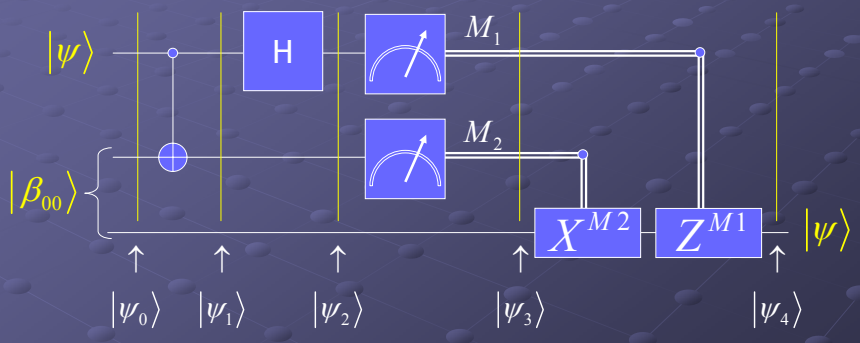
  - Each takes one qubit of the EPR pair
  - Alice must deliver a qubit to Bob but does not know the state of that qubit

$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ where α, β are unknown

  - Alice can only send classical information to Bob

Quantum Circuits

- Quantum Teleportation Circuit



Quantum Circuits

- Quantum Teleportation Calculations

$$|\psi_0\rangle = |\psi\rangle|\beta_{00}\rangle = \frac{1}{\sqrt{2}}\left[\alpha|0\rangle\left(|00\rangle+|11\rangle\right)+\beta\left(|00\rangle+|11\rangle\right)\right]$$

$$|\psi_0\rangle \xrightarrow{CNOT} |\psi_1\rangle = \frac{1}{\sqrt{2}}\left[\alpha|0\rangle\left(|00\rangle+|11\rangle\right)+\beta|1\rangle\left(|10\rangle+|01\rangle\right)\right]$$

$$|\psi_1\rangle \xrightarrow{H} |\psi_2\rangle = \frac{1}{2}\left[\alpha\left(|0\rangle+|1\rangle\right)\left(|00\rangle+|11\rangle\right)+\beta\left(|0\rangle+|1\rangle\right)\left(|10\rangle+|01\rangle\right)\right]$$

$$|\psi_2\rangle = \frac{1}{2}\left[\begin{array}{l}|00\rangle\left(\alpha|0\rangle+\beta|1\rangle\right)+|01\rangle\left(\alpha|1\rangle-\beta|0\rangle\right)+\\ |10\rangle\left(\alpha|0\rangle-\beta|1\rangle\right)+|11\rangle\left(\alpha|1\rangle-\beta|0\rangle\right)\end{array}\right]$$

Quantum Circuits

- Quantum Teleportation Measurements

  - Depending on Alice's measurement outcome, Bob's qubit will end up in one of these 4 possible states.

$$00 \mapsto |\psi_3(00)\rangle \equiv \alpha|0\rangle+\beta|1\rangle$$
$$01 \mapsto |\psi_3(01)\rangle \equiv \alpha|1\rangle-\beta|0\rangle$$
$$10 \mapsto |\psi_3(10)\rangle \equiv \alpha|0\rangle-\beta|1\rangle$$
$$11 \mapsto |\psi_3(11)\rangle \equiv \alpha|1\rangle-\beta|0\rangle$$

  - Bob must know the results of Alice's measurement to know which state the information is in.

Quantum Circuits

- Quantum Teleportation Results

  - Once Bob knows Alice's measurements he can discover the state by applying the appropriate quantum gate

    If 00 then Bob doesn't need to do anything

    If 01 then Bob needs to apply the X gate

    If 10 then Bob needs to apply the Z gate

    If 11 then Bob needs to apply the X gate then the Z gate

Quantum Circuits

- Quantum Teleportation Questions…

  - Does quantum teleportation allow one to transmit quantum states faster than light?

    No. Alice must send Bob her measurements over classical communication lines

  - Does quantum teleportation violate the no-cloning theorem?

    No. Only target qubit is in that state

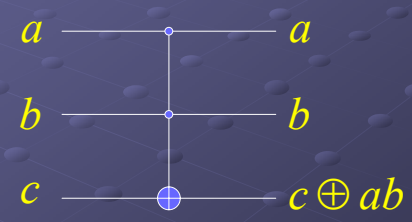
    the original data qubit ends up in one of the computational basis states depending on the measurement results of the first qubit

Quantum Algorithms

- Classical Computations on a Quantum Computer
  - Many classical gates are irreversible while all quantum gate are unitary and therefore reversible
  - Any classical circuit can be replaced by an equivalent circuit containing only reversible elements
  - This is accomplished using the TOFFOLI GATE…

Quantum Algorithms

- Toffoli Gate (Reversible Classical Gate)
  - two control bits one target bit
  - target bit flipped only if both control bits are set to one



  - The Toffoli gate is it's own inverse since…

$$(a,b,c) \rightarrow (a,b,c \oplus ab) \rightarrow (a,b,c)$$

Quantum Algorithms

- Quantum Toffoli Gate
  - Acts in same way as classical toffoli gate

$$|110\rangle \rightarrow |111\rangle$$

- Classical Simulation on a Quantum Computer
  - Can simulate irreversible classical logic gates
  - Can perform any calculation a classical deterministic computer can.
  - Can simulate a classical non-deterministic (probabilistic) computer

$$|0\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \xrightarrow{M} \begin{cases} |0\rangle \text{ with probability } 1/2 \\ |1\rangle \text{ with probability } 1/2 \end{cases}$$

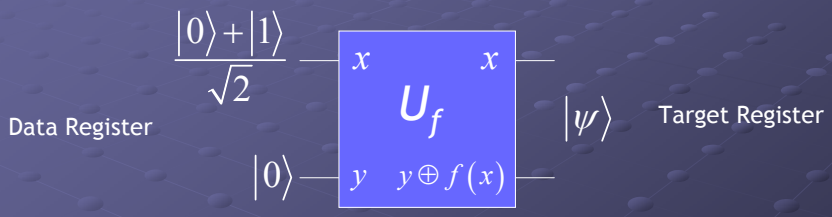
Quantum Algorithms

- Quantum Parallelism
  - Fundamental feature of many quantum algorithms
  - Simple Terms: it allows a quantum computer to evaluate a function f(x) for many different values of x simultaneously
- Ex: A two-qubit quantum computer
  - Suppose f(x) is a function with a one-bit domain and range

$$f(x): \{0,1\} \rightarrow \{0,1\}$$

Quantum Algorithms

Initial State $|x, y\rangle \rightarrow |x, y \oplus f(x)\rangle$ Final State



$$|x, y\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

$$|\psi\rangle = \frac{|0, 0 \oplus f(0)\rangle + |1, 0 \oplus f(1)\rangle}{\sqrt{2}} = \frac{|0, f(0)\rangle + |1, f(1)\rangle}{\sqrt{2}}$$

Quantum Algorithms

Eureka!!!! Both values of the function show up in the final state solution.

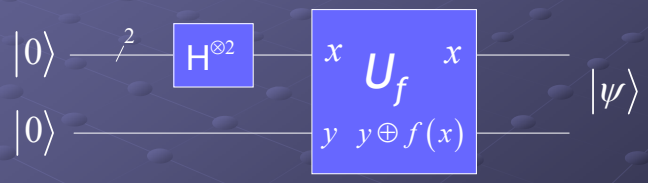
$$|\psi\rangle = \frac{|0, f(0)\rangle + |1, f(1)\rangle}{\sqrt{2}}$$

This can be generalized to functions on arbitrary number of bits using the…

HADAMARD TRANSFORM
or
WALSH-HADAMARD TRANSFORM

Quantum Algorithms

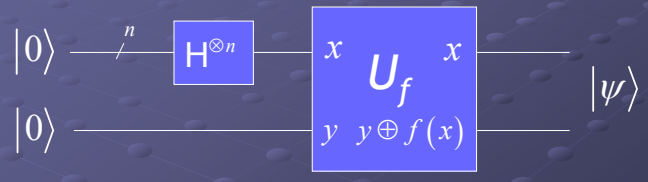
- Hadamard Transform Example
  - n=2 with qubits initially prepared as $|0\rangle$
  - $H^{\otimes 2}$ denotes the parallel action of two Hadamard gates



$$\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)=\frac{|00\rangle+|01\rangle+|10\rangle+|11\rangle}{2}$$

Quantum Algorithms

- Hadamard Transform
  - n Hadamard gates acting in parallel on n qubits



Quantum Algorithms

- Hadamard Transform
  - n Hadamard gates acting in parallel on n qubits
  - prepare n+1 qubit states

$$|0\rangle^{\otimes n}|0\rangle$$

  - Apply Hadamard transform to the first n qubits
  - Use this as the x-input to the quantum circuit U_f

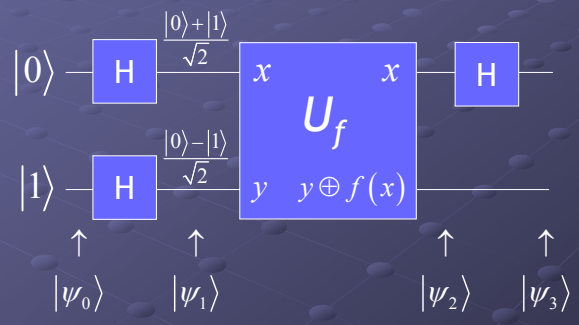
$$|\psi\rangle = \frac{1}{\sqrt{2^n}}\sum_x |x\rangle|f(x)\rangle$$

  - BUT in previous example can only get info about $|0, f(0)\rangle$ or $|1, f(1)\rangle$ not both. How can this be done?

Deutsch's Algorithm

Quantum Algorithms

- Deutsch's Algorithm Circuit
  - Combines quantum parallelism and interference



Quantum Algorithms

- Deutsch's Algorithm Calculations
  - Combines quantum parallelism and interference

$$|\psi_0\rangle = |01\rangle$$

$$|\psi_0\rangle \rightarrow |\psi_1\rangle = \left[\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$

$$|\psi_1\rangle \rightarrow |\psi_2\rangle = \begin{cases} \pm\left[\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] & \text{if } f(0) = f(1) \\ \pm\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] & \text{if } f(0) \neq f(1) \end{cases}$$

Quantum Algorithms

- Deutsch's Algorithm Conclusion

$$|\psi_2\rangle \rightarrow |\psi_3\rangle = \begin{cases} \pm|0\rangle\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] & \text{if } f(0) = f(1) \\ \pm|1\rangle\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] & \text{if } f(0) \neq f(1) \end{cases}$$

realizing $f(0) \oplus f(1)$ is 0 if $f(0) = f(1)$ and 1 otherwise…

$$|\psi_3\rangle = \pm|f(0) \oplus f(1)\rangle\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$

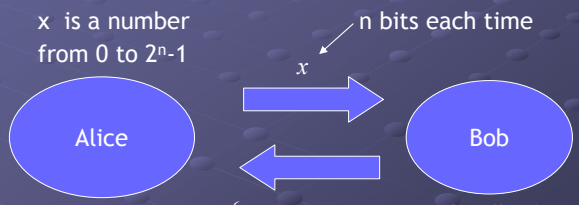
measuring the 1st qubit gives $f(0) \oplus f(1)$

Quantum Algorithms

- Deutsch's Algorithm Results
  - The quantum circuit has given us the ability to determine a GLOBAL PROPERTY of $f(x)$ namely $f(0) \oplus f(1)$ using only ONE evaluation of $f(x)$
  - A classical computer would require at least two evaluations!
  - Difference between quantum parallelism and classical randomized algorithms
    - One might think the state $|0\rangle|f(0)\rangle + |1\rangle|f(1)\rangle$ corresponds to probabilistic classical computer that evaluates $f(0)$ with probability 1/2 or $f(1)$ with probability ½. These are classically mutually exclusive.
    - Quantum mechanically these two alternatives can INTERFERE to yield some global property of the function f and by using a Hadamard gate can recombine the different alternatives

Quantum Algorithms

- Deutsch-Josa Algorithm
  - A simple case of a more general algorithm
  - Application is called Deutsch's Problem



$$f(x)\begin{cases}\text{Constant for all values of } x \\ \text{Balanced: 1 for 1/2 the values of } x \text{ or 0 otherwise}\end{cases}$$

  - Classically Alice can only send one value of x each time
  - Best classical algorithm requires up to $2^n/2+1$ queries

$2^n/2$ 0's and one $1 \Rightarrow$ Balanced

Quantum Algorithms

- Deutsch-Josa Algorithm
  - If Bob and Alice were able to exchange qubits instead of classical bits and if Bob calculated *f(x)* using a unitary transform U_f then Alice could determine the function in one query.

$|\psi_0\rangle$ - Alice has an n qubit register and a single qubit register which she gives to Bob

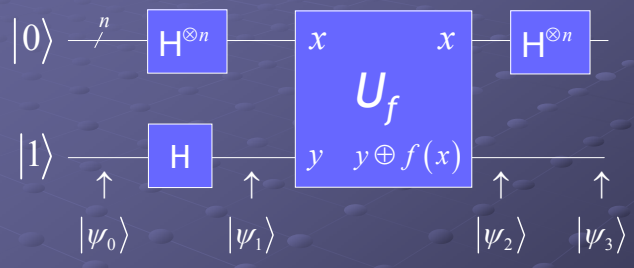
$|\psi_1\rangle$ - Prepares query and answer register in a superposition state

$|\psi_2\rangle$ - Bob evaluates f(x) and puts result into answer register

$|\psi_3\rangle$ - Alice interferes the states in the superposition using a hadamard transform on the query register

Quantum Algorithms

- Deutsch-Josa Algorithm Circuit



$$|\psi_0\rangle = |0\rangle^{\otimes n}|1\rangle \rightarrow |\psi_1\rangle = \sum_{x\in\{0,1\}^n} \frac{|x\rangle}{\sqrt{2^n}}\left[\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right]$$

$$|\psi_1\rangle \rightarrow |\psi_2\rangle = \sum_{x\in\{0,1\}^n} \frac{(-1)^{f(x)}|x\rangle}{\sqrt{2^n}}\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]$$

Bob's function evaluation is stored in the amplitude

Quantum Algorithms

- Deutsch-Josa Algorithm - detour

Hadamard transform: helps to calculate effect on a state $|x\rangle$
By checking the cases x=0 and x=1 separately for a single qubit...

$$H|x\rangle = \sum_z (-1)^{xz} \frac{|z\rangle}{\sqrt{2}}$$

thus $H^{\otimes n}|x_1,\ldots,x_n\rangle = \sum_{z_1,\ldots,z_n} (-1)^{x_1z_1+\ldots+x_nz_n} \frac{|z_1,\ldots,z_n\rangle}{\sqrt{2^n}}$

$$H^{\otimes n}|x\rangle = \sum_z (-1)^{x\bullet z} \frac{|z\rangle}{\sqrt{2^n}}$$

where $x \bullet z$ is the bitwise inner product of x and z, modulo 2

Quantum Algorithms

- Deutsch-Josa Algorithm Circuit

$$|\psi_2\rangle \rightarrow |\psi_3\rangle = \underbrace{\sum_z \sum_x \frac{(-1)^{x\bullet z + f(x)}|z\rangle}{2^n}}_{\text{query register}} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$

- amplitude for $|0\rangle^{\otimes n}$ is... $\sum_x \frac{(-1)^{f(x)}}{2^n}$

Case 1: If f is constant the amplitude for $|0\rangle^{\otimes n}$ is +1 or -1 depending on the constant value f(x) takes. Since $|\psi_3\rangle$ is unit length then all other amplitudes must be zero.

- An observation will yield 0s for all qubits in the register

Quantum Algorithms

- Deutsch-Josa Algorithm Circuit

Case 2: If f is balanced then the positive and negative contributions to the amplitude for $|0\rangle^{\otimes n}$ cancel, leaving an amplitude of 0

- A measurement must yield a result other than 0 on at least one qubit

Summary:

- If Alice measures all zeros then the function is constant
- Otherwise the function is balanced.
- Deutsch's problem on a quantum computer can be solved in one evaluation.

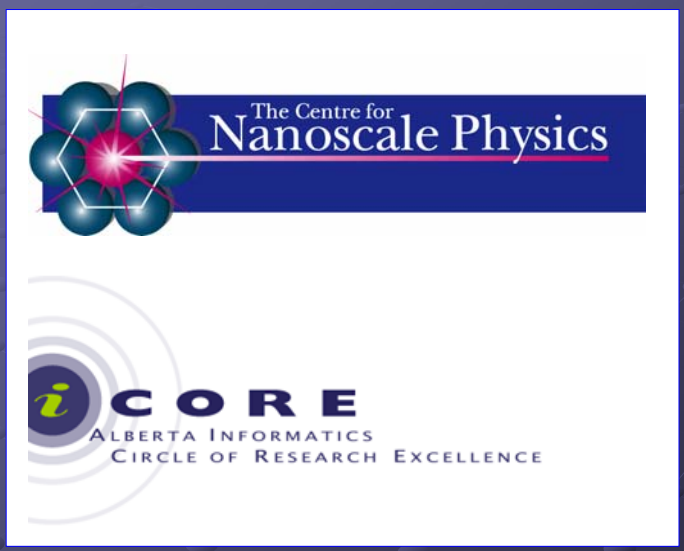
Quantum Algorithms

- Other Quantum Algorithms
  - Generally there are three classes
    * Discrete Fourier Transform Algorithms
      ~Deutsch-Jozsa Algorithm
      ~Shor's Algorithm for Factoring
      ~Shor's Discrete Logarithm Algorithm
    * Quantum Search Algorithms
    * Quantum Simulation Algorithms
      ~Quantum Computer is used to simulate quantum systems

Experimental Quantum Information Processing

- The Stern-Gerlach Experiment
- Optical Techniques
- Nuclear Magnetic Resonance
- Quantum Dots
- Traps: Ion Traps & Neutral Atom Traps

Thanks!



On Quantum Computing and AI

(Notes for a Graduate Class)

Vadim V. Bulitko bulitko@ualberta.ca
Department of Computing Science
University of Alberta
Edmonton, AB T6G 2H1, CANADA

Abstract

This evolving document serves as a repository for quantum computing related notes and thoughts. As it features summary of and solutions to the exercises found in (Nielsen et al. 2000), it doubles as a foundation for the author's forthcoming class on Quantum Computing and AI.

Contents

1. (Nielsen et al. 2000) Summary

The purpose of this section is to provide a highly compressed collection of facts presented in (Nielsen et al. 2000). This is helpful when refreshing material in the past sections.

1.1 NC Section 2.1: Hilbert Spaces

Complex numbers are specified by the real and imaginary parts: $a + ib$ where $a, b \in \mathbb{R}$ and $i^2 = -1$.

Polar representation: $ue^{i\theta} = u(\cos\theta + i\sin\theta)$ where $\theta, u \in \mathbb{R}$ and u is called the modulus of the complex number.

Complex conjugate: $(a + ib)^* = a - ib$.

Vectors are represented by columns: $|v\rangle = \begin{bmatrix} v_1 \\ v_2 \end{bmatrix}$.

Dual vectors are represented by rows: $|v\rangle^\dagger = \langle v| = [v_1^* , v_2^*]$.

Matrix multiplication: each element of the new matrix is a sum of products of the first factor's row and the second factor's column rotated to be superimposed on top of the row: $\begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} \times \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} a_1 x + a_2 y \\ a_3 x + a_4 y \end{bmatrix}$.

Linear dependence: *non-zero* vectors $|v_1\rangle, \ldots, |v_n\rangle$ are linearly dependent iff at least one of them is expressible through the others: $|v_j\rangle = \sum_i a_i |v_i\rangle$ where $a_m \in \mathbb{C}$.

The Pauli matrices: are given as:

- $\sigma_0 = I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$;
- $\sigma_1 = \sigma_x = X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
- $\sigma_2 = \sigma_y = Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
- $\sigma_3 = \sigma_z = Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$.

Properties:

1. unitary: $(\sigma_k)^\dagger \sigma_k = I$ for all k;
2. Hermitian: $(\sigma_k)^\dagger = \sigma_k$ for all k;
3. *eigen-decomposition:*
   (a) $\sigma_0 = I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ has the following eigenvectors: $|0\rangle$ with the eigenvalue of 1 and $|1\rangle$ with the eigenvalue of 1. Thus:

$$
\begin{aligned}
I &= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} && (1.1.1)\\
&= 1 \cdot |0\rangle\langle 0| + 1 \cdot |1\rangle\langle 1| && (1.1.2)\\
&= |\mathbf{0}\rangle\langle\mathbf{0}| + |\mathbf{1}\rangle\langle\mathbf{1}|. && (1.1.3)
\end{aligned}
$$

(b) $\sigma_1 = \sigma_x = X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ has the following eigenvectors: $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ with the eigenvalue of 1 and $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$ with the eigenvalue of -1. Thus:

$$\begin{aligned} X &= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} && (1.1.4)\\ &= 1 \cdot \frac{|0\rangle + |1\rangle}{\sqrt{2}} \frac{\langle 0| + \langle 1|}{\sqrt{2}} + (-1) \cdot \frac{|0\rangle - |1\rangle}{\sqrt{2}} \frac{\langle 0| - \langle 1|}{\sqrt{2}} && (1.1.5)\\ &= |\mathbf{1}\rangle \langle \mathbf{0}| + |\mathbf{0}\rangle \langle \mathbf{1}|. && (1.1.6) \end{aligned}$$

(c) $\sigma_2 = \sigma_y = Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$ has the following eigenvectors: $\frac{-i|0\rangle+|1\rangle}{\sqrt{2}}$ with the eigenvalue of 1 and $\frac{|0\rangle-i|1\rangle}{\sqrt{2}}$ with the eigenvalue of -1. Thus:

$$\begin{aligned} Y &= \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} && (1.1.7)\\ &= 1 \cdot \frac{-i\,|0\rangle + |1\rangle}{\sqrt{2}} \frac{i\,\langle 0| + \langle 1|}{\sqrt{2}} + (-1) \cdot \frac{|0\rangle - i\,|1\rangle}{\sqrt{2}} \frac{\langle 0| + i\,\langle 1|}{\sqrt{2}} && (1.1.8)\\ &= \mathbf{i}\,|\mathbf{1}\rangle \langle \mathbf{0}| - \mathbf{i}\,|\mathbf{0}\rangle \langle \mathbf{1}|. && (1.1.9) \end{aligned}$$

(d) $\sigma_3 = \sigma_z = Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ has the following eigenvectors: $|0\rangle$ with the eigenvalue of 1 and $|1\rangle$ with the eigenvalue of -1. Thus:

$$\begin{aligned} Z &= \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} && (1.1.10)\\ &= 1 \cdot |0\rangle \langle 0| + (-1) \cdot |1\rangle \langle 1| && (1.1.11)\\ &= |\mathbf{0}\rangle \langle \mathbf{0}| - |\mathbf{1}\rangle \langle \mathbf{1}|. && (1.1.12) \end{aligned}$$

Inner Product: $(|v_1\rangle, |v_2\rangle) \in \mathbb{C}$. **Properties:**

1. *matrix product representation:* $(\begin{bmatrix} v_1 \\ v_2 \end{bmatrix}, \begin{bmatrix} w_1 \\ w_2 \end{bmatrix}) = (|v\rangle, |w\rangle) = \langle v| \times |w\rangle = \langle v \mid w\rangle = [v_1^*, v_2^*] \times \begin{bmatrix} w_1 \\ w_2 \end{bmatrix} = v_1^* w_1 + v_2^* w_2$.
2. $\forall |v\rangle\, [\mathbb{R} \ni \langle v \mid v\rangle \geq 0]$, furthermore: $\langle v \mid v\rangle = 0 \implies |v\rangle = 0$;
3. $\langle v \mid \alpha w\rangle = \langle \alpha^* v \mid w\rangle = \alpha \langle v \mid w\rangle$;
4. $\langle v \mid x + y\rangle = \langle v \mid x\rangle + \langle v \mid y\rangle$;
5. $(|v\rangle, |w\rangle) = (|w\rangle, |v\rangle)^* = (|w\rangle^*, |v\rangle^*)$;
6. *the Cauchy-Schwartz inequality:* $|\langle v \mid w\rangle|^2 \leq \langle v \mid v\rangle \langle w \mid w\rangle$.

Vector norm: $\| |v\rangle \| = \sqrt{(|v\rangle, |v\rangle)} = \sqrt{\langle v \mid v\rangle}$. Unit vectors: $\| |v\rangle \| = 1$.

Orthogonality: $|v\rangle \neq 0$ and $|w\rangle \neq 0$ are orthogonal iff $\langle v \mid w\rangle = 0$.

Orthonormality: $\langle v_i \mid v_j\rangle = \delta_{ij}$ where the Dirac's delta is: $\delta_{ij} = 1$ if $i = j$ and 0 otherwise.

Gram-Schmidt procedure: given a linearly-independent vector set $\{|v_i\rangle\}$ we can create an orthonormal set that (i) spans the same subspace and (ii) the first vector is the normalized first vector of the original set: $|w_1\rangle = \frac{|v_1\rangle}{\||v_1\rangle\|}$.

Outer product: $|v\rangle\langle w|$ is a linear operator A such that $A|u\rangle = |v\rangle\langle w|u\rangle = |v\rangle\langle w \mid u\rangle = \langle w \mid u\rangle |v\rangle$. Here $\langle w \mid u\rangle \in \mathbb{C}$. It is easily understood in terms of matrices as $|v\rangle\langle w|$ is an $N \times N$ matrix and does, therefore, represent a linear operator. **Properties:**

1. *completeness relation:* for any orthonormal basis $\{|j\rangle\}$: $\sum_j |j\rangle\langle j| = I$.
2. *projectors:* if $\{|i\rangle\}$ is a set of orthonormal vectors (i.e., $\langle i \mid j\rangle = \delta_{ij}$) then the projection operator (or projector) $|i\rangle\langle i|$ *projects* any vector $|v\rangle$ onto the axis of $|i\rangle$: $|i\rangle\langle i|v\rangle = |i\rangle\langle i|(\sum_k v_k |k\rangle) = v_k |i\rangle$.

Eigenvalues and eigenvectors: linear operator A has λ_i as its i^{th} eigenvalue and $|v_i\rangle$ as the corresponding eigenvector iff $A|v_i\rangle = \lambda_i |v_i\rangle$. **Properties:**

1. *eigenspace* corresponding to eigenvalue λ is the set of eigenvectors corresponding to λ: $\{|w\rangle \mid A|w\rangle = \lambda|w\rangle\}$. Eigenspace is degenerate when its dimension is above 1 (i.e., it has two linearly independent eigenvectors). Non-degenerate eigenspaces are of the form: $\alpha|v\rangle$ where $\alpha \in \mathbb{C}$.
2. eigenvectors corresponding to different eigenvalues are linearly-independent. Therefore, one can speak of an orthonormal set of eigenvectors for an operator. Gram-Schmidt procedure can be used to generate one.
3. *computing eigenvalues and eigenvectors:* eigenvalues are [complex] roots to the characteristic equation of A's matrix: $c(\lambda) = \det|A - \lambda I| = 0$. Here det is the determinant*. Once $\{\lambda_i\}$ are computed we can solve the system of linear equations: $A|v\rangle = \lambda_i|v\rangle$ or $A|v\rangle - \lambda_i I = 0$ for $|v\rangle$ and it will be the eigenvector $|v_i\rangle$.
4. *spectral decomposition:* A is normal (i.e., $A^\dagger A = AA^\dagger$) iff (i) its eigenvectors are orthogonal and (ii) their normalized (i.e., orthonormal) versions $\{|w_i\rangle\}$ can be used to diagonalize the operator:
$$A = \sum_i \lambda_i |w_i\rangle\langle w_i|.$$
The matrix of this operator is diagonal: $\begin{bmatrix} \lambda_1 & 0 & 0 \\ 0 & \lambda_k & 0 \\ 0 & 0 & \lambda_n \end{bmatrix}$. In terms of matrix product this can be represented as $A = UDU^\dagger$ where D is a diagonal matrix and U is a unitary operator.

Adjoint/Hermitian and Normal operators: linear operator $A^\dagger$ is adjoint to A iff for any $|v\rangle, |w\rangle$ the following holds: $(|v\rangle, A|w\rangle) = (A^\dagger|v\rangle, |w\rangle)$. Alternatively: $\langle v \mid Aw\rangle = \langle vA^\dagger \mid w\rangle$. **Properties:**

1. by definition: $(|v\rangle)^\dagger = \langle v|$;
2. $(AB)^\dagger = B^\dagger A^\dagger$;
3. $(A|v\rangle)^\dagger = \langle v|A^\dagger$ but **not** $A|v\rangle = \langle v|A^\dagger$;
4. $(A^\dagger)^\dagger = A$;
5. $(\alpha A + \beta B)^\dagger = \alpha^* A^\dagger + \beta^* B^\dagger$;

---

*. Determinant of a 2×2 matrix is defined as $\det\left|\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right| = ad - bc$. Determinants of larger matrices can be decomposed into determinants of 2×2 matrices. For example: $\det\left|\begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix}\right| = a \cdot \det\left|\begin{bmatrix} e & f \\ h & i \end{bmatrix}\right| + b \cdot \det\left|\begin{bmatrix} d & f \\ g & i \end{bmatrix}\right| + c \cdot \det\left|\begin{bmatrix} d & e \\ g & h \end{bmatrix}\right|$.

6. $A^\dagger = (A^*)^T$;
7. *Normal operators:* $AA^\dagger = A^\dagger A$;
8. *Self-adjoint or Hermitian:* $A = A^\dagger$;
9. Hermitian $\implies$ normal;
10. A is normal then A is Hermitian iff A has real eigenvalues;
11. any operator A can be represented as $A = B + iC$ where B, C are Hermitian ($C = 0$ is A is Hermitian itself);
12. Hermitian operators have orthogonal eigenvectors?;
13. for any unitary $|v\rangle$ (i.e., of modulus 1), $V = |v\rangle \langle v|$ is Hermitian ($V^\dagger = V$) and, furthermore, $V^2 = V$;
14. if H is Hermitian then for any $|v\rangle$ $(|v\rangle, H|v\rangle) \in \mathbb{R}$;
15. *positive operators*: Hermitian (and therefore normal) A is positive iff for any $|v\rangle$ $\mathbb{R} \ni \langle v \mid Av\rangle = \langle vA \mid v\rangle \geq 0$. Positive operators have non-negative real eigenvalues.

Unitary operators: U is unitary iff $U^\dagger U = I$. **Properties:**

1. unitary $\implies$ normal;
2. unitary $\implies$ allows for spectral decomposition;
3. unitary $\implies$ allows for reversal: $U^\dagger(U|v\rangle) = I|v\rangle = |v\rangle$;
4. unitary $\implies$ preserves inner product: $(U|v\rangle, U|w\rangle) = (|v\rangle, |w\rangle)$;
5. unitary $\implies$ preserves norm: $\|U|v\rangle\| = \||v\rangle\|$;
6. if $\{|v_i\rangle\}$ is an orthonormal basis set then $\{U|v_i\rangle\} = \{w_i\}$ is also an orthonormal basis and $U = \sum_i |w_i\rangle \langle v_i|$;
7. unitary $\implies$ has modulus 1 eigenvalues (i.e., $\lambda_j = e^{i\theta_j}$).

Relationship between the operator classes is presented in Figure 1.

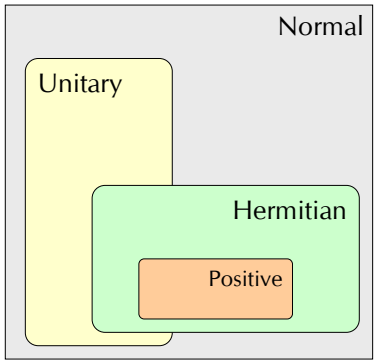


Figure 1: Relationship between the operators

Tensor products: If $\{|i\rangle\}$ is a basis for V and $\{|j\rangle\}$ is a basis for W then $\{|i\rangle \otimes |j\rangle\}$ is a basis for $V \otimes W$. **Properties:**

1. notation: $|i\rangle \otimes |j\rangle = |i\rangle |j\rangle = |i, j\rangle = |ij\rangle$;

2. linearity:

$$z(|v,w\rangle) = |zv,w\rangle = |v,zw\rangle \tag{1.1.13}$$
$$|v_1+v_2,w\rangle = |v_1,w\rangle + |v_2,w\rangle \tag{1.1.14}$$
$$|v,w_1+w_2\rangle = |v,w_1\rangle + |v,w_2\rangle \tag{1.1.15}$$

3. non-commutative: $|vw\rangle \neq |wv\rangle$;
4. if A, B are linear operators then $A \otimes B(|vw\rangle) = A|v\rangle \otimes A|w\rangle$;
5. *Kronecker product:* $A \otimes B = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \otimes \begin{bmatrix} x & y \\ v & w \end{bmatrix} = \begin{bmatrix} aB & bB \\ cB & dB \end{bmatrix} = \begin{bmatrix} ax & ay & bx & by \\ av & aw & bv & bw \\ cx & cy & dx & dy \\ cv & cw & dv & dw \end{bmatrix}$;
6. inner product: $(|vw\rangle, |v'w'\rangle) = (|v\rangle, |v'\rangle) \cdot (|w\rangle, |w'\rangle)$ or simply: $\langle vw \mid v'w'\rangle = \langle v \mid v'\rangle \langle w \mid w'\rangle$;
7. notation: $|v\rangle^{\otimes k} = (|v\rangle \otimes \cdots \otimes |v\rangle)_{k \text{ times}}$. This is left associative: $|v\rangle^{\otimes k} = |v\rangle^{\otimes k-1} \otimes |v\rangle$?
8. $(A \otimes B)^* = A^* \otimes B^*$;
9. $(A \otimes B)^T = A^T \otimes B^T$;
10. $(A \otimes B)^\dagger = A^\dagger \otimes B^\dagger$;
11. consequently: $|ab\rangle^\dagger = |a\rangle^\dagger |b\rangle^\dagger = \langle a|\langle b| = \langle ab|$;
12. if N_1, N_2 are normal then $N_1 \otimes N_2$ is normal;
13. if H_1, H_2 are Hermitian then $H_1 \otimes H_2$ is Hermitian;
14. if U_1, U_2 are unitary then $U_1 \otimes U_2$ is unitary;
15. if P_1, P_2 are positive then $P_1 \otimes P_2$ is positive;

Operator functions: if A is a normal operator and $A = \sum_a a|a\rangle\langle a|$ is its spectral decomposition then $f(A) = \sum_a f(a)|a\rangle\langle a|$.

Matrix traces: if A is a matrix then $\mathrm{tr}(A) = \sum_i A_{ii}$ (sum of diagonal elements). **Properties:**

1. $\mathrm{tr}(AB) = \mathrm{tr}(BA)$;
2. $\mathrm{tr}(A+B) = \mathrm{tr}(A) + \mathrm{tr}(B)$;
3. $\mathrm{tr}(zA) = z\,\mathrm{tr}(A)$;
4. *similarity transformation:* if U is unitary then $\mathrm{tr}(UAU^\dagger) = \mathrm{tr}(A)$;
5. if $|u\rangle$ is a unitary (i.e., modulus of 1) vector then $\mathrm{tr}(A|u\rangle\langle u|) = \langle u|A|u\rangle$;
6. consequently for any unitary vector $|v\rangle$, $\mathrm{tr}(|v\rangle\langle v|) = \mathrm{tr}(|v\rangle\langle v|v\rangle\langle v|) = \langle v|(|v\rangle\langle v|)|v\rangle = \langle v \mid v\rangle\langle v \mid v\rangle = |\,|v\rangle\,|^4 = 1$.

Anti-commutator: $\{A,B\} = AB + BA$, A anti-commutes with B iff $\{A,B\} = 0$.

Commutator: $[A,B] = AB - BA$, A commutes with B iff $[A,B] = 0$. **Properties:**

1. *Simultaneous diagonalization theorem:* suppose H_1, H_2 are Hermitian. Then $[H_1,H_2] = 0$ iff there exists an orthonormal set of eigenvectors for H_1, H_2 such that: $H_1 = \sum_i \lambda'_i |i\rangle\langle i|$ and $H_2 = \sum_i \lambda''_i |i\rangle\langle i|$;

2. $AB = \frac{[A,B]+\{A,B\}}{2}$;
3. $[A,B]^\dagger = [B^\dagger, A^\dagger]$;
4. $[A,B] = -[B,A]$;
5. $i[H_1, H_2]$ is Hermitian for any Hermitian H_1, H_2;

Polar decomposition: for any linear operator A it can be represented as $A = U\sqrt{A^\dagger A} = \sqrt{AA^\dagger}U$ where U is a unitary operator (unique (and equal to A?) if A is invertible).

Singular value decomposition: for any linear operator A of the same input and output dimensions (i.e., with a square matrix) there exists unitary U_1, U_2 and a diagonal matrix D with real non-negative elements such that:

$$A = U_1 D U_2.$$

Properties:

1. *Proof:* by the polar decomposition theorem: $A = U\sqrt{A^\dagger A}$, by spectral decomposition for positive (and, thus, normal) operators $\sqrt{A^\dagger A} = U' D U'^\dagger$ where D is diagonal with real non-negative elements (since $\sqrt{A^\dagger A}$ is positive). Therefore, $A = U\sqrt{A^\dagger A} = UU'DU'^\dagger = (UU')D(U'^\dagger) = U_1 D U_2$.

1.2 NC Section 2.2: The Postulates of Quantum Mechanics

Postulate 1. Any *isolated* quantum system can be completely described by a *state vector* which is a unit vector in a Hilbert space. **Notes:**

1. figuring out the specific Hilbert space and the state vector are non-trivial tasks;
2. the smallest system of interest is a *qubit*. Its state space is $\mathbb{C}^2$ and its state vector is a unit $|v\rangle \in \mathbb{C}$. We often fix an orthonormal basis such as $|0\rangle$ and $|1\rangle$. The a qubit can be described as $|v\rangle = \alpha|0\rangle + \beta|1\rangle$ where $\alpha, \beta \in \mathbb{C}$ are called *amplitudes*. Quantum mechanically we say that the system is in a *superposition* of states $|0\rangle$ and $|1\rangle$.

Postulate 2. Evolution of an isolated quantum system can be expressed as:

$$|v(t_2)\rangle = U(t_1, t_2)\,|v(t_1)\rangle$$

where t_1, t_2 are moments of time and $U(t_1, t_2)$ is a unitary operator. **Notes:**

1. U may vary with time. Hence, the corresponding segment of time explicitly specified: $U(t_1, t_2)$;
2. the process is in a sense Markovian (history doesn't matter) and reversible (since $U^\dagger U\,|v\rangle = |v\rangle$);

Postulate 2'. We can also re-write this with a stationary operator (*Schrödinger Equation*):

$$i\hbar\frac{d\,|v\rangle}{dt} = H\,|v\rangle$$

where H is a *fixed* (for a closed/isolated system) Hermitian operator (called Hamiltonian of the system) and $\hbar$ is Planck's constant. **Notes:**

1. since H is Hermitian it is also normal and therefore allows for the following spectral decomposition:
$$H = \sum_E E\,|E\rangle\,\langle E|$$
where eigenvalues E are real-valued and correspond the energy levels of stationary states expressed by normalized eigenvalues $|E\rangle$. The stationary state with the lowest energy is called the ground-state;
2. example: suppose a single qubit system can be described by the following Hamiltonian: $H = \hbar\omega X$ where X is one of the Pauli matrices: $X = \sigma_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ and ω is a physical parameter. Then the eigenvalues (the energy levels) are $\hbar\omega$ and $-\hbar\omega$ and the corresponding normalized eigenvectors (the stationary states) are $(|0\rangle+|1\rangle)/\sqrt{2}$ and $(|0\rangle-|1\rangle)/\sqrt{2}$ (with the latter being the ground state).
3. *Postulate 2' → Postulate 2:* a solution to the Schrödinger Equation can be given as:
$$U(t_1, t_2) = \exp\left[\frac{-i}{\hbar}(t_2 - t_1)H\right]$$
and, in fact, *any* unitary operator $U = \exp(iH)$ for some Hermitian H;
4. most practically occurring quantum systems are not isolated as they interact with a larger system they are a part of. It turns out, however, that the non-isolated system can be described by a different Hamiltonian as if it were isolated. The "trick" is that the new Hamiltonian (called *atomic Hamiltonian*) is *not* constant but changes with time. In fact, in physical experiments we can often *control* the changes in such an atomic Hamiltonian.

5. for any commuting (i.e., $AB = BA$ or $[A, B] = 0$) Hermitian operators A, B the following holds: $\exp(A)\exp(B) = \exp(A + B)$;
6. for any unitary U, $H = -i\log(U)$ is Hermitian.

Postulate 3. Quantum measurements are described by a set of linear operators $\{M_m\}, 1 \leq m \leq n$ where n is the number of possible outcomes. For the system in state $|v\rangle$ the probability of outcome m is given by $p(m) = (M_m|v\rangle, M_m|v\rangle) = \|M_m|v\rangle\|^2$. If the outcome is indeed m then the state of the system collapses to $\frac{M_m|v\rangle}{\|M_m|v\rangle\|}$. **Notes:**

1. $p(m) = (M_m|v\rangle, M_m|v\rangle) = \langle v|M_m^\dagger M_m|v\rangle$;
2. probabilities have to add up to one:

$$1 = \sum_m p(m) = \sum_m (M_m|v\rangle, M_m|v\rangle)$$

   which is equivalent (since for every $|v\rangle$) to $\sum_m M_m^\dagger M_m = I$;
3. example: if $|0\rangle$ and $|1\rangle$ form an orthonormal basis for a qubit $|v\rangle$ then we can define $M_0 = |0\rangle\langle 0|, M_1 = |1\rangle\langle 1|$. Since $|v\rangle = a|0\rangle + b|1\rangle$, $M_0|v\rangle = a|0\rangle$ and $M_1|v\rangle = b|1\rangle$. Thus, $p(0) = (a|0\rangle, a|0\rangle) = \langle 0|a^* a|0\rangle = |a|^2$. Likewise, $p(1) = |b|^2$. The outcomes are $\frac{a}{|a|}|0\rangle$ xor $\frac{b}{|b|}|1\rangle$;
4. open question: measurement is nothing but an interaction of the measured quantum system with the measuring tools (i.e., another quantum system). Two of them together form a single [larger] closed system that can be described with Postulate 2/2'. The question is: can we derive postulate 3 from postulate 2/2'?
5. *indistinguishability of non-orthogonal quantum states:* no quantum measurement can reliably distinguish between $|v_1\rangle$ and $|v_2\rangle$ if they are not orthogonal (i.e., $\langle v_1 \mid v_2\rangle \neq 0$.

Projective measurements: if we have a system of orthonormal $\{|m\rangle\}$ then each $P_m = |m\rangle\langle m|$ is Hermitian and $M = \sum_m mP_m$ is Hermitian as well (m's are the eigenvalues of M) . M is called an *observable* and each *projector* P_m projects onto the axis of $|m\rangle$. Clearly, $P_m^\dagger = P_m$ and $P_m P_m = P_m$ and thus the probability of outcome m measured with the observable M is

$$p(m) = (P_m|v\rangle, P_m|v\rangle) = \langle v|P_m|v\rangle$$

and if the outcome m does occur then the system will end up in the state

$$\frac{P_m|v\rangle}{\sqrt{p(m)}}.$$

Clearly, $p(m) = |\alpha_m|^2$ where $|v\rangle = \sum_m \alpha_m|m\rangle$. **Notes:**

1. Clearly: $P_i P_j = \delta_{ij} P_i = \delta_{ij} P_j$;
2. Define the expected/average value of observable M on vector $|v\rangle$ as: $\langle M\rangle = E[M] = \sum_m mp(m) = \sum_m m\langle v|P_m|v\rangle = \langle v|\sum_m mP_m|v\rangle = \langle v|M|v\rangle$.
3. Standard deviation of observable M on vector $|v\rangle$ is defined as: $\Delta(M) = \langle M^2\rangle - (\langle M\rangle)^2$.
4. *The Heisenberg uncertainty principle:* if C, D are two observables then for any vector $|v\rangle$: $\Delta(C)\Delta(D) \geq \frac{|\langle v|[C,D]|v\rangle|}{2}$.
5. If we are measuring with observable $M = \sum_m m|m\rangle\langle m|$ or (postulate 3) with operators $M_m = |m\rangle\langle m|$ then we are also said to be measuring in a basis $\{|m\rangle\}$.

6. *Repeatability:* if we measure with an observable M and get an outcome m then another measurement with M will gives us m again. This is not true with many physical measurements indicating that they are not projective. This is also not true with general M_m (postulate 3) since in general: $M_m^\dagger \neq M_m$ and $M_i M_j \neq \delta_{ij} M_j$.

POVM measurements: given a general (postulate 3) system of measurement operators M_m we can define *POVM elements* as $E_m = M_m^\dagger M_m$. **Properties/notes:**

1. $\sum_m E_m = I$ (follows from $\sum_m M_m^\dagger M_m = I$);
2. $p(m) = \langle v| E_m |v\rangle$;
3. E_m are positive operators;
4. the resulting state (in the case of outcome m) is $\frac{M_m|v\rangle}{\sqrt{\|M_m|v\rangle\|}}$ which is not easily expressible with E_m. So POVM elements are used when the resulting states are not important;
5. given a set of positive operators $\{E_m\}$ that satisfy the completeness relation ($\sum_m E_m = I$) we can define the general measurement operators as $M_m = \sqrt{E_m}$ (therefore $M_m^\dagger M_m = E_m$).
6. projectors $P_m = |m\rangle \langle m|$ comprise a special case of POVMs: $E_m = P_m$ would do.
7. *phase:* suppose we have a basis $\{|i\rangle\}$. Then any vector $|v\rangle$ has an amplitude α_i when represented in the basis: $|v\rangle = \sum_i \alpha_i |i\rangle$. We can associate *phase factors* $\theta_i \in \mathbb{R}$ with each $|i\rangle$. Then:
   (a) *relative phase difference:* two states $|v\rangle$ and $|w\rangle$ differ by a relative phase $\{\theta_j\}$ in a basis $\{|j\rangle\}$ iff each $|v\rangle$'s amplitude α_j differs by a relative phase θ_j from each $|w\rangle$'s amplitude β_j: $\alpha_j = e^{i\theta_j}\beta_j$. The differences between $|v\rangle$ and $|w\rangle$ *can* be detected with appropriate measurement operators.
   (b) *global phase difference:* occurs when *all* all amplitudes are shifted by $e^{i\theta}$ (i.e., when all θ_j are equal to θ). This *cannot* be detected by any measurement operator M_m since $\langle v| e^{-i\theta} M_m^\dagger M_m e^{i\theta} |v\rangle = \langle v| M_m^\dagger M_m |v\rangle$.
   (c) *note:* For any two orthonormal bases $(\{|v_i\rangle\}, \{|w_i\rangle\})$ the operator converting between them ($U|v_i\rangle = |w_i\rangle$) is indeed unitary and can be encoded as: $U = \sum |v_i\rangle \langle w_i|$. HOWEVER, the difference between a vector expressed in one basis and in the other vector can be a *relative* phase shift and not necessarily a global phase shift.
   Example: suppose we are converting from basis $\{|0\rangle, |1\rangle\}$ to $\{|0\rangle, -|1\rangle\}$. The unitary operator is simply $U = |0\rangle\langle 0| - |1\rangle\langle 1|$. So if we take an arbitrary vector $|v\rangle = \alpha|0\rangle + \beta|1\rangle$ then $U|v\rangle = \alpha|0\rangle - \beta|1\rangle$. Thus, the vector $\begin{bmatrix} \alpha \\ \beta \end{bmatrix}$ in basis $\{|0\rangle, |1\rangle\}$ and the vector $\begin{bmatrix} \alpha \\ \beta \end{bmatrix}$ in basis $\{|0\rangle, -|1\rangle\}$ are related through a *relative* phase shift $\{e^{i0}, e^{i\pi}\}$. In other words, there is no single θ such that $\alpha|0\rangle + \beta|1\rangle = e^{i\theta}(\alpha|0\rangle - \beta|1\rangle)$.

Postulate 4: Composite Systems: if a composite quantum system consists of n subsystem each evolving in its Hilbert space V_i then the state of the entire system evolves in $\bigotimes_i V_i$. Furthermore, if each subsystem is in a particular state $|v_i\rangle$ then the state of the entire system is $\bigotimes_i v_i$. **Notes:**

1. *motivation:* assume *super-position principle*: if $|v\rangle$ and $|w\rangle$ are possible states of a system then for any $\alpha, \beta \in \mathbb{C}$ such that $|\alpha|^2 + |\beta|^2 = 1$ the linear combination $\alpha|v\rangle + \beta|w\rangle$ is also a possible state. Then we can derive postulate 4 using the properties of tensor products.

2. *Bell/EPR states.* Define:

$$|b_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \quad (1.2.1)$$

$$|b_{01}\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}} \quad (1.2.2)$$

$$|b_{10}\rangle = \frac{|10\rangle + |01\rangle}{\sqrt{2}} \quad (1.2.3)$$

$$|b_{11}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}} \quad (1.2.4)$$

It turns out that they form an orthonormal basis for two qubits. Furthermore, for any single qubit linear operator V the value of $\langle b_{ij}| V \otimes I |b_{ij}\rangle = const_V$ for all i, j. Therefore, it is impossible to distinguish between Bell states by measuring only the first qubit†. It is, however, possible to distinguish between the Bell states reliably since they are orthonormal. Indeed, all one needs to do is to use a set of projective measurement operators: $P_{ij} = |b_{ij}\rangle \langle b_{ij}|$.

3. *Super-dense coding:* if Alice has the first qubit of $|b_{00}\rangle$ she can apply I, Z, X, iY to it. This is equivalent to applying $I \otimes I, Z \otimes I, X \otimes I, iY \otimes I$ to the entire Bell state $|b_{00}\rangle$ and results in $|b_{00}\rangle, |b_{01}\rangle, |b_{10}\rangle, |b_{11}\rangle$ correspondingly. Therefore, we can encode two classical bits (i.e., 4 choices) in just one qubit (hence the name).

   This is, however, hardly surprising since a single qubit is really a pair of arbitrary complex numbers (with the normality condition on top) and thus we can encode not just 4 choices (2 bits) but the whole irrational π number in it! The trick is, of course, to be able to read this off easily on the receiving end as well as to use simple transformations (such as the Pauli matrices) to do so. See below for a proposed method for transmitting 2^m bits with a single qubit...

   Also note, that in the example with Alice and Bob above, Alice changes the single qubit she has (i.e., the first qubit of the entangled pair $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$). However, since the first qubit is present in both $|0\rangle$ and $|1\rangle$ states in the original entangled state, her operators have to produce meaningful results in both cases:

op_1	$\|0\rangle$	$op_1 \|0\rangle$
op_1	$\|1\rangle$	$op_1 \|1\rangle$
...	...	...
op_n	$\|0\rangle$	$op_n \|0\rangle$
op_n	$\|1\rangle$	$op_n \|1\rangle$

   or specifically:

I	$\|0\rangle$	$I \|0\rangle = \|0\rangle$
I	$\|1\rangle$	$I \|1\rangle = \|1\rangle$
Z	$\|0\rangle$	$Z \|0\rangle = \|0\rangle$
Z	$\|1\rangle$	$Z \|1\rangle = -\|1\rangle$
X	$\|0\rangle$	$X \|0\rangle = \|1\rangle$
X	$\|1\rangle$	$X \|1\rangle = \|0\rangle$
iY	$\|0\rangle$	$iY \|0\rangle = -\|1\rangle$
iY	$\|1\rangle$	$iY \|1\rangle = \|0\rangle$

   A question: can we transmit more than 2 classical bits with a single qubit? **Proposed question**

†. how about the second qubit?

method: to transmit 2^m classical bits prepare an entangled state of m qubits. Give the last $m-1$ of them ($|q_2 \dots q_m\rangle$) to Bob and the first one ($|q_1\rangle$) to Alice. Then Alice applies one of her 2^m linear operators (the one with the index $1 \leq i \leq 2^m$ where i is the classical message she is transmitting) on $|q_1\rangle$ and sends the result to Bob. This is equivalent to applying $op_i \otimes I \otimes \dots \otimes I$ on the initial entangled state. Let's call the resulting m-qubit state $|b_i\rangle$ ($1 \leq i \leq 2^m$). The only requirement is that $\{|b_1\rangle, \dots, |b_{2^m}\rangle\}$ are orthonormal and therefore can be reliably distinguished (e.g., with the observable $M = \sum_{i=1}^{2^m} i\,|b_i\rangle\langle b_i|$).

4. *Entanglement, correlation, and anti-correlation:*

   (a) Bell states in H^2 have components (for each qubit) that project both on $|0\rangle$ and $|1\rangle$. Therefore, measuring either qubit in the basis $\{|0\rangle, |1\rangle\}$ gives $|0\rangle$ with the probability $1/2$ and $|1\rangle$ with the probability $1/2$. In other words:

   $$\langle b_{ij}|\,|0\rangle\langle 0|\,|b_{ij}\rangle = \frac{1}{2} \quad (1.2.5)$$

   $$\langle b_{ij}|\,|1\rangle\langle 1|\,|b_{ij}\rangle = \frac{1}{2}. \quad (1.2.6)$$

   So, if we measure the first qubit of any $|b_{ij}\rangle$ with say the observable $M = \alpha\,|0\rangle\langle 0| + \beta\,|1\rangle\langle 1|$ then we get α in half cases and β in half cases (i.e., $p(\alpha) = p(\beta) = \frac{1}{2}$). Suppose, we make a measurement and get α. Then if the original Bell state was $\frac{|0x\rangle \pm |1y\rangle}{\sqrt{2}}$ then the resulting state collapses to $|0x\rangle$ (the $\frac{1}{\sqrt{2}}$ is removed by the normalization). Therefore, now if we measure the second qubit we are *bound* to see $|x\rangle$. So if $|x\rangle$ happens to be $|0\rangle$ we will get *correlation* (the second qubit measurement is bound to give the same result as the first qubit measurement) or (if $|x\rangle = |1\rangle$) *anti-correlation* (the second qubit measurement is bound to be opposite to the first qubit measurement).

   (b) Generally speaking, we want two properties here:

      i. the first measurement (of any qubit) can give us either $|0\rangle$ or $|1\rangle$ equally likely;

      ii. the second measurement (of the *other* qubit) gives us the result deterministically dependant on the first measurement (i.e., correlation or anti-correlation).

HYPOTHESIS

Hypothesis: this *cannot* be accomplished with a non-entangled state. Example: suppose we have non-entangled $|v\rangle = (a\,|0\rangle + b\,|1\rangle)(c\,|0\rangle + d\,|1\rangle)$. Then depending on a, b, c, d we will get two cases:

i. one of the qubits in $|v\rangle$ is the same (e.g., $|v\rangle = (|0\rangle + |1\rangle)\,|0\rangle = |00\rangle + |10\rangle$ and the measurement on the 2nd qubit always gives $|0\rangle$);

ii. there are elements in the sum that start/end with the same qubit but end/start with different ones (e.g., $|v\rangle = (|0\rangle + |1\rangle)^2 = |00\rangle + |01\rangle + |10\rangle + |11\rangle$ and no matter what we measure first the second measurement will be *non-deterministic*).

5. *Bell inequalities.* Suppose we have two particles: one in the possession of Alice and one in the possession of Bob. Suppose Alice and Bob take measurements (outside of the null cone so that one doesn't affect the other) of two quantities each: $Q = \pm 1, R = \pm 1; S = \pm 1, T = \pm 1$. Consider, the quantity: $QS + RS + RT - QT = (Q+R)S + (R-Q)T = \pm 2$. Suppose, there is a state of the system and it is $Q = q, R = r, S = s, T = t$ with the probability of $p(q, r, s, t)$ before the measurement. The expected value is: $E(QS + RS + RT - QT) \leq 2$. On the other hand, $E(QS + RS + RT - QT) = E(QS) + E(RS) + E(RT) - E(QT)$. Thus, the Bell inequality is $E(QS) + E(RS) + E(RT) - E(QT) \leq 2$.

   Quantum mechanically, however, we can take $|b_{11}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$ and measure the following observables: $Q = Z_1, R = X_1, S = \frac{-Z_2 - X_2}{\sqrt{2}}, T = \frac{Z_2 - X_2}{\sqrt{2}}$. On the entangled state $|b_{11}\rangle$ their expected values are: $\langle QS\rangle = \frac{1}{\sqrt{2}}, \langle RS\rangle = \frac{1}{\sqrt{2}}, \langle RT\rangle = \frac{1}{\sqrt{2}}, \langle QT\rangle = -\frac{1}{\sqrt{2}}$ and,

therefore, the expected value of the entire quantity is: $\langle QS\rangle + \langle RS\rangle + \langle RT\rangle - \langle QT\rangle = 2\sqrt{2} > 2$!

Experiments show that Nature follows the second way and the measured value of the observables is greater than 2. This means that at least one of the following assumptions doesn't hold:

(a) *realism:* Q, R, S, T have values independent of observation;

(b) *locality:* Alice's measurement doesn't affect Bob's measurement.

Note that the same trick doesn't work with a non-entangled state such as $|00\rangle$ which results in $\langle QS\rangle = -\frac{1}{\sqrt{2}}, \langle RS\rangle = 0, \langle RT\rangle = 0, \langle QT\rangle = \frac{1}{\sqrt{2}}$ and, therefore, the expected value of the entire quantity is: $\langle QS\rangle + \langle RS\rangle + \langle RT\rangle - \langle QT\rangle = -\sqrt{2} < 2$.

1.3 NC 3.1.2: Circuits

Universality: the following gates seem to be needed:

1. Auxilary gates: wires + ancilla bits + fanout + crossover;
2. NAND / AND+NOT / XOR;

are the crossover/ancilla bits really needed?

1.4 NC 3.2: Computational Complexity

Complexity classes can be defined as follows:

L (*logarithmic space*) is the class of languages that can be decided by a deterministic TM running in $O(\log(n))$ space (the restriction applies to the working tape only);

P (*polynomial time*) is the class of languages that can be decided by a deterministic TM running in $O(n^k)$ time;

NP (*non-deterministic polynomial time*) is the class of languages that can be verified by a deterministic TM running $O(n^k)$ time. More technically: $L \in$ **NP** if $\exists M \exists k \forall \ell [(\ell \in L \implies \exists w M(\ell, w) = 1 \text{ in } O(|\ell|^k)) \ \& \ (\ell \notin L \implies \forall w M(\ell, w) = 0 \text{ in } O(|\ell|^k))]$. In other words, we require a witness w for each positive (i.e., $\ell \in L$) instance. Example: $L = \{\ell \in \mathbb{N} | \ell \text{ is not prime}\} \in$ **NP** .

coNP is the class of languages where we require a witness for every negative (i.e., $\ell \notin L$) instance. Clearly, $\forall L [L \in$ **NP** $\iff \overline{L} \in$ **coNP** $]$. Example: $\overline{L} = \{\ell \in \mathbb{N} | \ell \text{ is prime}\} \in$ **coNP** .

NP -complete is the class of languages from **NP** such that for any language L from **NP** L can be polynomially reduced to that **NP** -complete language;

NPI (**NP** *intermediate*) is the class of languages that are **NP** but not **NP** -complete;

PSPACE (*polynomial space*) is the class of languages that can be decided in polynomial space by a deterministic TM;

EXP (*exponential time*) is the class of languages that can be decided by a deterministic TM running in $O(2^{n^k})$ time;

Notes:

1. $TIME(f(n)) \subset TIME(f(n)\log^2(f(n)))$ (the time hierarchy theorem);
2. $SPACE(f(n)) \subset SPACE(f(n)\log(f(n)))$ (the space hierarchy theorem);
3. **P** $\subset$ **EXP** ;
4. **L** $\subset$ **PSPACE** ;

5. **L** $\subseteq$ **P** $\subseteq$ **NP** $\subseteq$ **PSPACE** $\subseteq$ **EXP** ;
6. factoring is not proven to be **NP** -complete and is suspected to be **NPI** ;
7. graph isomorphism is not proven to be **NP** -complete and is suspected to be **NPI** ;

Quantum computational power is currently believed (but not proven) to be higher than that of conventional computing devices insomuch as:

1. Polynomial quantum algorithms are known to be in **PSPACE** ;
2. QC are believed to be able to do **NPI** problems in polynomial time but not **NP** -complete tasks.

1.5 NC 3.2.5: Energy and reversibility

Landauer's principle: any time a bit of information is erased an amount of energy dissipated into the environment is lower bounded by $k_B T \ln 2$. Alternatively, the entropy goes up by at least $k_B T \ln 2$. **Notes:**

1. I think the intuition here is that erasing information makes things more uniform (since it reduces a certain [unknown/chaotic] state to a known brand-new erased state. Therefore, the amount of order increases raising the entropy.
2. Reversible computations can be *theoretically* carried out with no energy used! However, in practice, noise correction requires keeping track of errors, and, therefore, erasing these temporary working records. Thus, in practice one needs to dissipate energy while computing.

Fredkin Gate is a universal reversible gate. It has two data (A, B) and one control (C) input and outputs (A', B', C'). In other words, $F(A, B, C) = (A', B', C')$. The control always passes through unchanged: $C' = C$ while the gate swaps A, B if $C = 1$ and passes them straight otherwise. **Notes:**

1. $F(0, y, x) = (xy, \overline{x}y, x)$ (and);
2. $F(1, 0, x) = (\overline{x}, x, x)$ (not, fanout);
3. $F(x, y, 1) = (y, x, 1)$ (cross-over);
4. any classical [irreversible] function $f()$ can be computed with Fredkin's gates and ancilla bits: $(x, a) \rightarrow (f(x), g(x))$. The problem lies with the "garbage" bits that *depend* on x (i.e., $g(x)$). The following is a trick to get rid of them – or rather produce them in a more standard way.

WHY are garbage bits bad?

5. Use a CNOT-gate ($CNOT(c, t) = (c, c \oplus t)$[‡]) to prepare all ancilla 1's. Thus, only ancilla 0's are needed and
$$(x, a) \rightarrow (f(x), g(x))$$
becomes
$$(x, 0) \rightarrow (f(x), g(x)).$$
Also notice that $CNOT(0, x) = (x, x)$. Thus, we can use it to propagate a copy of x all along
$$(x, 0, 0) \rightarrow (x, f(x), g(x)).$$

‡. here $a \oplus b = a + b \mod 2$.

6. We now add a forth register that starts in a random state y: $(x, 0, 0, y)$. We compute $f(x)$ using Fredkin's gates and add it modulo 2 with the y:

$$(x, 0, 0, y) \stackrel{U_1}{\to} (x, f(x), g(x), y) \stackrel{U_2}{\to} (x, f(x), g(x), y \oplus f(x)).$$

Since U_1 is reversible and didn't touch y we can undo it (called *uncomputation*):

$$(x, f(x), g(x), y \oplus f(x)) \stackrel{(U_1)^{-1}}{\longrightarrow} (x, 0, 0, y \oplus f(x)).$$

Dropping 0's we get

$$(x, y) \to (x, y \oplus f(x)).$$

This is reversible and there are no garbage bits depending on x.

7. The overhead of making a computation reversible is a constant factor and thus **P** and **NP** classes don't change.

???
$\oplus f(x)$???

Toffoli gate is defined as $T(A, B, C) = (A, B, C \oplus AB)$. **Notes:**

Crossover?

1. $T(x, y, 1) = (x, y, \overline{xy})$ (nand);
2. $T(x, y, 0) = (x, y, xy)$ (and);
3. $T(x, 1, 0) = (x, 1, x)$ (fanout);
4. $T(1, 1, x) = (1, 1, \overline{x})$ (not);
5. *Toffoli → Fredkin:* 9 Fredkin gates are enough to simulate a Toffoli gate. Is this the minimum?
6. *Fredkin → Toffoli:* 15 Toffoli gates are enough to simulate a Fredkin gate. Is this the minimum?

References

[Bulitko et al. 2002] Bulitko, V., Levner, I., Greiner, R. (2002). State Abstraction and Lookahead Control Policies. *In Proceedings of the American Association for Artificial Intelligence (AAAI) Conference*. AAAI Press. (submitted)

[Korf 1990] Korf, R.E. (1990). Real-time heuristic search. *Artificial Intelligence*, Vol. 42, No. 2-3, pp. 189-211.

[Mitchell 1997] Mitchell, T. (1997). *Machine Learning*. WCB/McGraw-Hill.

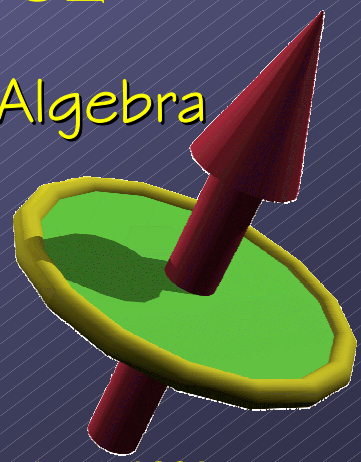
[Nielsen et al. 2000] Nielsen, M., Chuang, L., (2000). *Quantum Computation and Quantum Information*. Cambridge University Press.

Quantum Computing Summer School

Lecture 2: Linear Algebra

Angela Antoniu

Department of Electrical and Computing Engineering



May 7, 2002

Introduction to Quantum Mechanics

- Chapter objective (lectures 2,3,4):
  - *To introduce all of the fundamental principles of Quantum mechanics*
- Quantum mechanics
  - *The most realistic known description of the world*
  - *The basis for quantum computing and quantum information*
- Why Linear Algebra?
  - *L A is the prerequisite for understanding Quantum Mechanics*
- What is Linear Algebra?
  - *… is the study of vector spaces… and of*
  - *linear operations on those vector spaces[1]*

Linear algebra -Lecture objectives

- Review basic concepts from Linear Algebra:
  - *Complex numbers*
  - *Vector Spaces and Vector Subspaces*
  - *Linear Independence and Bases Vectors*
  - *Linear Operators*
  - *Pauli matrices*
  - *Inner (dot) product, outer product, tensor product*
  - *Eigenvalues, eigenvectors, Singular Value Decomposition (SVD)*
- Describe the standard notations (the Dirac notations) adopted for these concepts in the study of Quantum mechanics
- … which, in the next lecture, will allow us to study the main topic of the Chapter: the postulates of quantum mechanics

Complex numbers

- A complex number $z_n \in C$ is of the form $z_n = a_n + ib_n$ where $a_n, b_n \in R$ and $i^2=-1$
- Polar representation
  $z_n = u_n e^{i\theta_n}$, where $u_n, \theta_n \in R$
  - With $u_n = \sqrt{a_n^2 + b_n^2}$ the modulus or magnitude
  - And the phase $\theta_n = \arctan\left(b_n / a_n\right)$
- Trigonometric representation
  $z_n = u_n(\cos\theta_n + i\sin\theta_n)$
- *Complex conjugate*
  $z_n^* = (a_n + ib_n)^* = a_n - ib_n$

Vectors

- Characteristics:
  - *Modulus (or magnitude)*
  - *Orientation*
- Matrix representation of a vector

$$|\mathbf{v}\rangle = \begin{bmatrix} z_1 \\ \vdots \\ z_n \end{bmatrix} \text{(a column), and its dual}$$

$$|\mathbf{v}\rangle^{\dagger} = \langle \mathbf{v}| = [z_1^*, \cdots, z_n^*] \quad \text{(row vector)}$$

Vector Space, definition:

- A vector space (of dimension n) is a set of n vectors satisfying the following axioms (rules):
  - ***Addition:*** *add any two vectors* $|\mathbf{v}\rangle$ *and* $|\mathbf{v}'\rangle$ *pertaining to a vector space, say* C^n*, obtain a vector,*

$$|\mathbf{v}\rangle + |\mathbf{v}'\rangle = \begin{bmatrix} z_1 + z_1' \\ \vdots \\ z_n + z_n' \end{bmatrix} \quad \textit{the sum, with the properties :}$$

  - Commutative: $|\mathbf{v}\rangle + |\mathbf{v}'\rangle = |\mathbf{v}'\rangle + |\mathbf{v}\rangle$
  - Associative: $(|\mathbf{v}\rangle + |\mathbf{v}'\rangle) + |\mathbf{v}''\rangle = |\mathbf{v}\rangle + (|\mathbf{v}'\rangle + |\mathbf{v}''\rangle)$
  - Any $|\mathbf{v}\rangle$ has a zero vector (called the origin): $|\mathbf{v}\rangle + \mathbf{0} = |\mathbf{v}\rangle$
  - To every $|\mathbf{v}\rangle$ in C^n corresponds a unique vector $-|\mathbf{v}\rangle$ such as

$$|\mathbf{v}\rangle + (-|\mathbf{v}\rangle) = \mathbf{0}$$

  - *Scalar* ***multiplication:*** → *next slide*

Vector Space (cont)

- *Scalar multiplication: for any scalar*

  $z \in C$ and vector $|\mathrm{v}\rangle \in C^n$ there is a vector

  $z|\mathbf{v}\rangle = \begin{bmatrix} zz_1 \\ \vdots \\ zz_n \end{bmatrix}$, the scalar product, in such way that

  - Multiplication by scalars is Associative: $z(z'|\mathbf{v}\rangle) = (zz')|\mathbf{v}\rangle$
  - $1|\mathbf{v}\rangle = |\mathbf{v}\rangle$
  - Distributive with respect to vector addition:

    $$z(|\mathbf{v}\rangle + |\mathbf{v}'\rangle) = z|\mathbf{v}\rangle + z|\mathbf{v}'\rangle$$

  - Multiplication by vectors is

    Distributive with respect to scalar addition: $(z+z')|\mathbf{v}\rangle = z|\mathbf{v}\rangle + z'|\mathbf{v}\rangle$

- A Vector subspace in an n-dimensional vector space is a non-empty subset of vectors satisfying the same axioms

Basis vectors

- Or SPANNING SET for C^n: any set of n vectors such that any vector in the vector space C^n can be written using the n base vectors
  - Example for C^2 (n=2):

$|0\rangle$ corresponds to $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$

$|1\rangle$ corresponds to $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$

$\alpha_0|0\rangle + \alpha_1|1\rangle$ corresponds to $\alpha_0\begin{pmatrix} 1 \\ 0 \end{pmatrix} + \alpha_1\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix}$

which is a linear combination of the 2 dimensional basis vectors and $|\mathbf{0}\rangle$ $|\mathbf{1}\rangle$

Bases and Linear Independence

Spanning set: a set of vectors such that any vector in the space can be written as a linear combination of vectors in the set

$$\{|v_1\rangle,\ldots,|v_n\rangle\} \longrightarrow |v\rangle = \sum_{j=1}^{n} a_j |v_j\rangle \quad \text{for any } |v\rangle$$

Linear independence: a set of vectors is linearly independent if there is no linear combination of them which adds to zero non-trivially

$$\sum_{j=1}^{n} a_j |v_j\rangle = 0 \quad \text{iff every } a_j = 0$$

Basis: a linearly independent spanning set (always exists!)

Quantum Notation

z^*	Complex conjugate of z
$\|\psi\rangle$	Vector (a ket) -- this will represent a possible state of the discrete quantum system
$\langle\psi\|$	Vector dual to $\|\psi\rangle$ (a bra)
$\langle\psi\|\varphi\rangle$	Inner product of two vectors
$\|\psi\rangle\otimes\|\varphi\rangle$	Tensor product of two vectors
$\mathbf{A}$	A matrix -- this will represent an operator which can modify a quantum state
$\langle\psi\|\mathbf{A}\|\varphi\rangle$	Inner product of $\|\psi\rangle$ and $\mathbf{A}\|\varphi\rangle$

Linear Operators

Physical operations on quantum states are represented by linear operators which act on the states

Linear operator: An operator which maps one vector space into another that is linear in its arguments

$$\mathbf{A}\left(\sum_{j=1}^{n} a_j |v_j\rangle\right) = \sum_{j=1}^{n} a_j \mathbf{A}(|v_j\rangle)$$

Linear operators ⟷ matrices (matrix elements determined by specifying action on a basis)

Basis for V ↓ Basis for W ↓

$$\mathbf{A}(|v_i\rangle) = \sum_j A_{ij} |w_j\rangle$$

Pauli Matrices

A useful set of matrices which acts on a 2-dimensional vector space are the Pauli matrices:

$$\sigma_0 = I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad \sigma_1 = \sigma_x = X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$\sigma_2 = \sigma_y = Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \qquad \sigma_3 = \sigma_z = Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

- Properties: Unitary $(\boldsymbol{\sigma}_k)^\dagger \boldsymbol{\sigma}_k = \mathbf{I}, \forall k$

  and Hermitian $(\boldsymbol{\sigma}_k)^\dagger = \boldsymbol{\sigma}_k$

Inner Products

Inner Product: A method for combining two vectors which yields a complex number $(|\psi\rangle,|\varphi\rangle)\equiv\langle\psi|\varphi\rangle\mapsto C$ that obeys the following rules

- $(\ ,\ )$ is linear in its 2nd argument

$$\left(|v\rangle,\sum_k a_k|w_k\rangle\right)=\sum_k a_k(|v\rangle,|w_k\rangle)$$

- $(|v\rangle,|w\rangle)=(|w\rangle,|v\rangle)^*$
- $(|v\rangle,|v\rangle)\geq 0$

Example: C^n

$$((w_1,\ldots,w_n),(z_1,\ldots,z_n))=w_1^*z_1+\cdots w_n^*z_n$$

More on Inner Products

Hilbert Space: the inner product space of a quantum system

Orthogonality: $|w\rangle$ and $|v\rangle$ are orthogonal if $\langle v|w\rangle=0$

Norm: $\||v\rangle\|\equiv\sqrt{\langle v|v\rangle}$ Unit: $\dfrac{|v\rangle}{\sqrt{\langle v|v\rangle}}$ is the unit vector parallel to $|v\rangle$

Orthonormal basis: a basis set $\{|v_1\rangle,\ldots,|v_n\rangle\}$ where $\langle v_i|v_j\rangle=\delta_{ij}$

Gram-Schmidt Orthogonalization: an algorithmic procedure for finding an orthonormal basis $|j\rangle$ from a given basis

$$\left.\begin{aligned}|v\rangle&=\sum_{j=1}^n v_j|j\rangle\\ |w\rangle&=\sum_{j=1}^n w_j|j\rangle\end{aligned}\right\}\Rightarrow\langle v|w\rangle=\sum_j v_j^*w_j$$

(inner product of 2 vectors is equal to inner product of the matrix reps of the 2 vectors)

Outer Products

Let $|w\rangle$ be a vector in the vector space W

Let $|v\rangle$ be a vector in the vector space V

Outer product: $|w\rangle\langle v|$ is the outer product of $|w\rangle$ and $|v\rangle$
It is a linear map from V into W defined by

$$|w\rangle\langle v|\big(|v'\rangle\big)=|w\rangle\langle v|v'\rangle$$

Completeness relation: Let $|j\rangle$ be a basis for V. It is easy to show that $\sum_j |j\rangle\langle j| = \mathbf{I}$

$$\text{i.e.} \sum_j |j\rangle\langle j|\big(|v\rangle\big)=|v\rangle \text{ for every } |v\rangle$$

Eigenvalues and Eigenvectors

$$\mathbf{A}|v\rangle = \lambda_v|v\rangle = v|v\rangle$$

Eigenvalue — obtain by finding all roots to the eqn $\det(\mathbf{A}-\lambda\mathbf{I})=0$

Eigenvector

Diagonalizable: A matrix $\mathbf{A}$ is diagonalizable if it can be written as $\mathbf{A}=\sum_j \lambda_j |j\rangle\langle j|$ (orthonormal basis)

e.g. $Z=\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}=|0\rangle\langle 0|-|1\rangle\langle 1|$

Degeneracy: when two (or more) eigenvalues are equal
In this case the eigenspace is larger than one dimension

Hermitian Operators

Adjoint: $\mathbf{A}^\tau$ is the adjoint of $\mathbf{A}$ if $\left(\mathbf{A}^\tau|v\rangle, |w\rangle\right) = \left(|v\rangle, \mathbf{A}|w\rangle\right)$ for all vectors $|v\rangle, |w\rangle$ in the vector space V

Properties: $\mathbf{A}^\tau = \mathbf{A}^{*T}$ $\qquad \left(\mathbf{A}^\tau\right)^\tau = \mathbf{A}$ $\qquad (\mathbf{AB})^\tau = \mathbf{B}^\tau\mathbf{A}^\tau$

$|v\rangle^\tau = \langle v|$

Hermiticity: $\mathbf{A}$ is Hermitian if $\mathbf{A}^\tau = \mathbf{A}$

e.g. $\mathbf{P} = \sum_{j=1}^{k} |j\rangle\langle j|$ Projects any vector into a k-dim'l subspace

Normal: $\mathbf{A}$ is Normal if $\mathbf{A}^\tau\mathbf{A} = \mathbf{A}\mathbf{A}^\tau$

can show: Normal ⟷ Diagonalizable (spectral decomposition)

Unitary and Positive Operators

Unitary: $\mathbf{U}$ is unitary if $\mathbf{U}^\tau\mathbf{U} = \mathbf{I}$

can write: $\mathbf{U} = \sum_j |\hat{j}\rangle\langle j|$ where $|j\rangle$ and $|\hat{j}\rangle$ are any two distinct orthonormal bases for the vector space V, such that $\mathbf{U}|j\rangle = |\hat{j}\rangle$

Note:

$\left(\mathbf{U}|v\rangle, \mathbf{U}|w\rangle\right) = \langle v|\mathbf{U}^\tau\mathbf{U}|w\rangle = \langle v|w\rangle = \left(|v\rangle, |w\rangle\right)$ (preserves inner product)

Positive: $\mathbf{B}$ is positive if $\left(|v\rangle, \mathbf{B}|v\rangle\right) \geq 0$ for every $|v\rangle$ in V
(no negative eigenvalues!)

If $\left(|v\rangle, \mathbf{B}|v\rangle\right) > 0$ for every $|v\rangle$ in V ➡ $\mathbf{B}$ is positive definite
(all positive eigenvalues!)

Tensor Products

A tensor product is a larger vector space formed from two smaller ones simply by combining elements from each in all possible ways that preserve both linearity and scalar multiplication

If V is a vector space of dimension n & W is a vector space of dimension m then V⊗W is a vector space of dimension mn

$|v\rangle$
$|w\rangle$
$|v\rangle \otimes |w\rangle$

e.g.

$|0\rangle \otimes |0\rangle = |00\rangle \quad |1\rangle \otimes |1\rangle = |11\rangle$ are elements of V⊗V

and so is $|00\rangle + |11\rangle$ ⟹ qualitatively new feature: entangled states!

More on Tensor Products

$z(|v\rangle \otimes |w\rangle) = (z|v\rangle \otimes |w\rangle) = (|v\rangle \otimes z|w\rangle)$ scalar multiplication

$|v\rangle \otimes (|w_1\rangle + |w_2\rangle) = |v\rangle \otimes |w_1\rangle + |v\rangle \otimes |w_2\rangle$

$(|v_1\rangle + |v_2\rangle) \otimes |w\rangle = |v_1\rangle \otimes |w\rangle + |v_2\rangle \otimes |w\rangle$

} linearity

$\mathbf{A}$ acts on $|v\rangle$ $\quad$ $\mathbf{B}$ acts on $|w\rangle$

$(\mathbf{A} \otimes \mathbf{B})(|v\rangle \otimes |w\rangle) = \mathbf{A}|v\rangle \otimes \mathbf{B}|w\rangle$

} tensor product of operators

e.g. $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ $\quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$ ⟹ $X \otimes Y = \begin{bmatrix} 0 \bullet Y & 1 \bullet Y \\ 1 \bullet Y & 0 \bullet Y \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & -i \\ 0 & 0 & i & 0 \\ 0 & -i & 0 & 0 \\ i & 0 & 0 & 0 \end{bmatrix}$

Functions of Operators

Can define the function of an operator from its power series:

$$f(x)=\sum_n a_n x^n \Rightarrow f(\mathbf{A})=\sum_n a_n \mathbf{A}^n$$

e.g. $\exp(\theta X)=I+\theta X+\frac{1}{2!}(\theta X)^2+\frac{1}{3!}(\theta X)^3+\cdots$

$$=I+\frac{1}{2!}\theta^2 I+\cdots+\left(\theta+\frac{1}{3!}\theta^3+\cdots\right)X$$

$$=I\cos\theta+X\sin\theta$$

For normal operators, can go beyond this using their spectral decomposition:

$$\mathbf{A}=\sum_j \lambda_j |j\rangle\langle j| \Rightarrow f(\mathbf{A})=\sum_j f(\lambda_j)|j\rangle\langle j|$$

Trace and Commutator

Trace: $\mathrm{tr}(\mathbf{A})=\sum_j A_{jj}$ (sum over the diagonal elements)

$$\mathrm{tr}(\mathbf{AB})=\mathrm{tr}(\mathbf{BA}) \quad \mathrm{tr}(z\mathbf{A}+\mathbf{B})=z\,\mathrm{tr}(\mathbf{A})+\mathrm{tr}(\mathbf{B})$$

Commutator: $[\mathbf{A},\mathbf{B}]\equiv\mathbf{AB}-\mathbf{BA}$

Anti-commutator: $\{\mathbf{A},\mathbf{B}\}\equiv\mathbf{AB}+\mathbf{BA}$

Simultaneous Diagonalization: Two Hermitian operators $\mathbf{A}$ and $\mathbf{B}$ are diagonalizable in the same basis if and only if $[\mathbf{A},\mathbf{B}]=0$

Polar Decomposition

For any linear operator acting on a vector space we can write

$$\mathbf{A} = \mathbf{U}\sqrt{\mathbf{A}^{\dagger}\mathbf{A}}$$ (left polar decomposition)

where $\mathbf{U}$ is a unitary matrix -- it is unique if $\mathbf{A}$ has an inverse

Alternatively $\mathbf{A} = \sqrt{\mathbf{A}\mathbf{A}^{\dagger}}\mathbf{U}'$ (right polar decomposition)

Singular-value decomposition:
For all square matrices, can write $\mathbf{A} = \mathbf{U}\mathbf{D}\mathbf{U}'$
where $\mathbf{D}$ is a diagonal matrix

Bibliography & acknowledgements

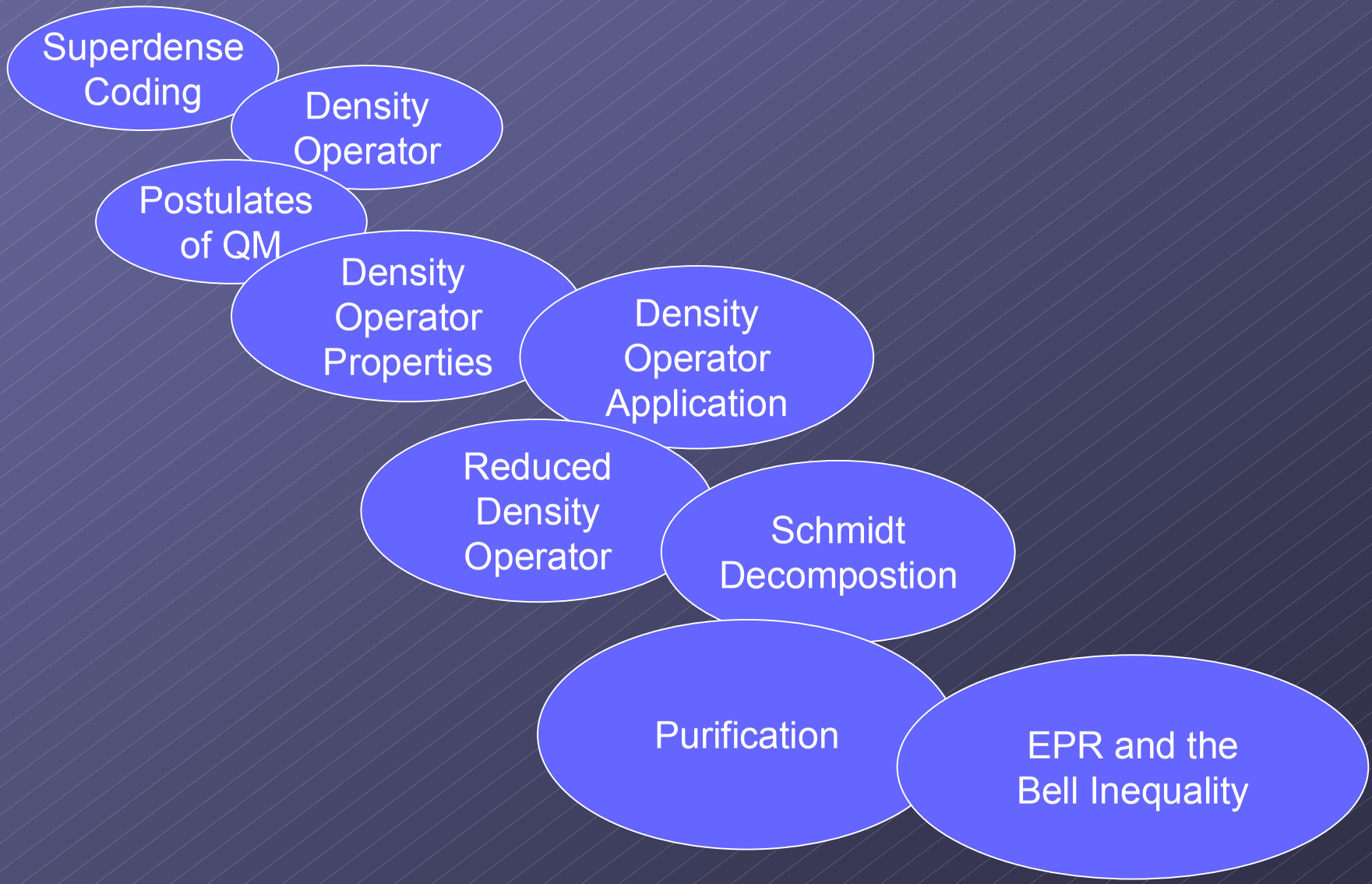
- Michael A. Nielsen and Isaac L. Chuang, Quantum Computation and Quantum Information, Cambridge University Press, Cambridge, UK, 2002
- R. Mann,M.Mosca, Introduction to Quantum Computation, Lecture series, Univ. Waterloo, 2000 http://cacr.math.uwaterloo.ca/~mmosca/quantumcoursef00.htm
- Paul Halmos, Finite-Dimensional Vector Spaces, Springer Verlag, New York, 1974
- V. Bulitko, On quantum Computing and AI, Notes for a graduate class, University of Alberta, 2002
- D. Fotin, Introduction to "Quantum Computing Summer School", University of Alberta, 2002.
- A. Antoniu, Localization of the sources of the electroencephalogram, Thesis, University of Alberta , Edmonton, Canada, 2000

Quantum Computing Summer School

Lecture 4:

Super-Dense Coding, EPR

Presentation Overview



SuperDense Coding

- Alice & Bob have the long distance feeling
- Goal: to transmit some CLASSICAL information from Alice to Bob.
- Alice is in possession of two classical bits of information which she wishes to send to Bob but can only send one qubit to Bob.
- Can she achieve her goal?

SuperDense Coding

- SuperDense Coding says YES!

  - They both initially share a pair of qubits in the entangled state.

$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

  - Alice initially has the first qubit and Bob has the second qubit.

  - Note the qubit is prepared ahead of time by a third party who then sends one to Alice and one to Bob

  - By sending a single qubit to Bob, Alice can communicate two bits of classical information

SuperDense Coding

$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

1 qubit 1 qubit

Alice

$00 : I \quad 01 : Z$

$10 : X \quad 11 : iY$

Bob

CIRCUIT CNOT

SuperDense Coding

- Procedure:
  - If Alice wants to send...

00	Bob does nothing
01	She applies the phase flip Z to her qubit
10	She applies quantum NOT gate X
11	She applies the iY gate

CIRCUIT

SuperDense Coding

- Four Resulting States

$$00 : |\psi\rangle \rightarrow \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

$$01 : |\psi\rangle \rightarrow \frac{|00\rangle - |11\rangle}{\sqrt{2}}$$

$$10 : |\psi\rangle \rightarrow \frac{|10\rangle + |01\rangle}{\sqrt{2}}$$

$$11 : |\psi\rangle \rightarrow \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

Bell States

SuperDense Coding

- Notice that the Bell States…

  1. Form an orthonormal basis

     eg:

$$\left(\frac{\langle 00| + \langle 11|}{\sqrt{2}}\right)\left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right)$$

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

$$= \frac{1}{2}(2) = 1$$

…therefore can be distinguished by an appropriate quantum measurement

Density Operator

- We have formulated quantum mechanics using the language of the state vector.
- Alternative formulation is a tool called the
  DENSITY OPERATOR or DENSITY MATRIX

- Mathematically equivalent but more convenient for thinking about some common quantum mechanics scenarios

Density Operator

Ensemble of Quantum States

- Suppose a quantum system is in one of a number of states $|\psi_i\rangle$ where i is an index, with probabilities p_i
- We call $\{p_i, |\psi_i\rangle\}$ an ENSEMBLE OF PURE STATES.

$$\rho \equiv \sum_i p_i |\psi_i\rangle\langle\psi_i|$$

Density Operator

- All postulates of quantum mechanics can be reformulated in terms of the density operator language.

Density Operator

Ensemble of Quantum States

Evolution of a closed system is described by a unitary operator U.

- If the system was initially in the state $|\psi_i\rangle$ with probability p_i then after the evolution has occurred the system will be in the state $U|\psi_i\rangle$ with probability p_i

The evolution of the density operator is described by …

$$\rho \equiv \sum_i p_i |\psi_i\rangle\langle\psi_i| \xrightarrow{U} \sum_i p_i U|\psi_i\rangle\langle\psi_i|U^\dagger = U\rho U^\dagger$$

Evolution of the Density Operator

Density Operator

Ensemble of Quantum States

Measurements…

- Suppose we perform a measurement described by the measurement operators M_m
- If the initial state was $|\psi_i\rangle$ then the probability of getting result m is …

$$p(m|i) = \langle \psi_i | M_m^\dagger M_m | \psi_i \rangle = tr\left(M_m^\dagger M_m |\psi_i\rangle\langle\psi_i| \right)$$

Probability of getting result m if the intial state was $|\psi_i\rangle$

Density Operator

Ensemble of Quantum States

By the LAW of TOTAL PROBABILITY…

- The probability of obtaining result m if the initial state was $|\psi_i\rangle$ is…

$$p(m) = \sum_i p(m|i)\, p_i$$

$$= \sum_i \mathrm{p_i} \mathrm{tr}\left(M_m^\dagger M_m |\psi_i\rangle\langle\psi_i| \right)$$

$$= \mathrm{tr}\left(M_m^\dagger M_m \rho \right)$$

Probability of getting result m

Density Operator

Ensemble of Quantum States

State of the system after obtaining the result m is …

$$\left|\psi_i^m\right\rangle = \frac{M_m \left|\psi_i\right\rangle}{\sqrt{\left\langle\psi_i\right| M_m^\dagger M_m \left|\psi_i\right\rangle}}$$

- We have an ensemble of states $\left|\psi_i^m\right\rangle$ with respective probabilities $p(i|m)$
- Corresponding density operator ρ_m is …

$$\rho_m = \sum_i p(i|m)\left|\psi_i^m\right\rangle\left\langle\psi_i^m\right| = \sum_i p(i|m)\frac{M_m \left|\psi_i\right\rangle\left\langle\psi_i\right| M_m^\dagger}{\left\langle\psi_i\right| M_m^\dagger M_m \left|\psi_i\right\rangle}$$

Density Operator

- Ensemble of Quantum States

by elementary probability theory …

$$p(i \mid m) = p(m \mid i)\, p_i / p(m)$$

$$\rho_m = \sum_i p_i \frac{M_m |\psi_i\rangle\langle\psi_i| M_m^\dagger}{tr\left(M_m^\dagger M_m \rho\right)} = \frac{M_m \rho M_m^\dagger}{tr\left(M_m^\dagger M_m \rho\right)}$$

Density Operator

Ensemble of Quantum States

Language of Density Operators …

- A quantum system whose state $|\psi\rangle$ is known exactly is said to be in a PURE STATE
  - * The density operator is simply $\rho = |\psi\rangle\langle\psi|$
  - * A pure state satisfies $\mathrm{tr}\left(\rho^2\right) = 1$

- Otherwise the density operator is in a MIXED STATE.
  - * It is a mixture of different pure states
  - * A mixed state satisfies $\mathrm{tr}\left(\rho^2\right) < 1$

Density Operator

Ensemble of Quantum States

- Imagine a quantum system is prepared in the state ρ_i with probability p_i
  - The density matrix that describes it is...

$$\rho = \sum_i p_i \rho_i$$

proof

Density Operator

Ensemble of Quantum States

- If our record of the result m of the measurement is lost we would have a quantum system in the state ρ_m with probability $p(m)$ but would no longer know the value of m
- The state of the system would be described by the density operator …

$$\rho = \sum_m p(m)\rho_m = \sum_m tr\left(M_m^\dagger M_m \rho\right)\frac{M_m \rho M_m^\dagger}{tr\left(M_m^\dagger M_m \rho\right)}$$

$$= \sum_m M_m \rho M_m^\dagger$$

Density Operator

- Ensemble of Quantum States
  - Compact formula which may be used for the analysis of operations on the system

$$\rho = \sum_m M_m \rho M_m^\dagger$$

Density Operator

- General Properties of the Density Operator

- Used to describe ensembles of quantum states

- The class of the operators that are density operators are characterized by ...

Characterization of Density Operators

* An operator ρ is the density operator associated to some ensemble $\{p_i, |\psi_i\rangle\}$ if and only if it satisfies the conditions

1) (Trace Condition) ρ has trace equal to one

2) (Positivity Condition) ρ is a positive operator

Density Operator

The Density Operator is a positive operator ρ such that...

$$\mathrm{tr}(\rho) = 1$$

We will reformulate
POSTULATES OF QUANTUM MECHANICS
using this definition

Postulates of Quantum Mechanics

Density Operator Formulation

Postulate 1:

- Associated to any isolated physical system is a complex vector space with inner product known as the STATE SPACE of the system
- The system is completely described by its DENSITY OPERATOR acting on the state of the system.
- If a quantum system is in the state ρ_i with probability p_i then the density operator for the system is ...

$$\rho = \sum_i p_i \rho_i$$

DENSITY OPERATOR FOR THE SYSTEM

Postulates of Quantum Mechanics

Density Operator Formulation

Postulate 2:

- The evolution of a CLOSED quantum system is described by a UNITARY TRANSFORMATION.
- In other words: The state ρ of the system at time t_1 is related to the state ρ' of the system at time t_2 by a unitary operator U which depends only on the times t_1 and t_2

$$\rho' = U \rho U^{\dagger}$$

Postulates of Quantum Mechanics

Density Operator Formulation

Postulate 3:

- Quantum measurements are described by a collection M_m of MEASUREMENT OPERATORS
- These are operators acting on the state space of the system being measured
  * index m refers to the measurement outcomes that may occur in the experiment.
- If the state of the quantum system is ρ immediately before the measurement then the probability that result m occurs is given by

$$p(m) = tr\left(M_m^\dagger M_m \rho\right)$$

Postulates of Quantum Mechanics

Density Operator Formulation

Postulate 3 (continued):

- The state of the system after the measurement is

$$\frac{M_m \rho M_m^\dagger}{\mathrm{tr}\left(M_m^\dagger M_m \rho\right)}$$

- Measurement operators satisfy the COMPLETENESS RELATION

$$\sum_m M_m^\dagger M_m = I$$

Postulates of Quantum Mechanics

Density Operator Formulation

Postulate 4:

- The state space of a composite physical system is the tensor product of the state spaces of the component physical systems.
- If we have systems numbered $1,\ldots,n$ and the system number 1 is prepared in the state ρ_i, then the joint state of the total system is ...

$$\rho_1 \otimes \rho_2 \otimes \ldots \rho_n$$

State Space of a Composite Physical System

Density Operator: Properties

Density Operator approach shines for two applications

1) Description of Quantum Systems who state is unknown
2) Description of Subsystems of a Composite Quantum System

Ex: One might assume that the quantum system with

$$\rho = \frac{3}{4}|0\rangle\langle 0| + \frac{1}{4}|1\rangle\langle 1|$$

must be in the state $|0\rangle$ with probability ¾ and in state $|1\rangle$ with probability ¼

However…

Density Operator: Properties

- Suppose we define

$$|a\rangle = \sqrt{\frac{3}{4}}|0\rangle + \sqrt{\frac{1}{4}}|1\rangle \qquad |b\rangle = \sqrt{\frac{3}{4}}|0\rangle - \sqrt{\frac{1}{4}}|1\rangle$$

and the quantum system is prepared in the state $|a\rangle$ with probability ½ and in the state $|b\rangle$ with probability ½ then the corresponding density matrix is…

$$\rho = \frac{1}{2}|a\rangle\langle a| + \frac{1}{2}|b\rangle\langle b| = \frac{3}{4}|0\rangle\langle 0| + \frac{1}{4}|1\rangle\langle 1|$$

These Two DIFFERENT ensembles
give rise to
the SAME density matrix.

Density Operator: Properties

- Properties of the Density Operator

  - In general, the eigenvectors and eigenvalues of a density matrix just indicate ONE of the many possible ensembles that may give rise to a specific density matrix

Density Operator: Properties

What Class of Ensembles gives rise to a particular density matrix?

- The set of vectors $|\tilde{\psi}_i\rangle$ which may not be normalized to unit length GENERATES the operator…

$$\rho \equiv \sum_i |\tilde{\psi}_i\rangle\langle\tilde{\psi}_i|$$

- The connection to the usual ensemble picture of density operators is expressed by

$$|\tilde{\psi}_i\rangle = \sqrt{p_i}\,|\psi_i\rangle$$

Density Operator: Application

So, when do two sets of vectors $|\tilde{\psi}_i\rangle$ and $|\tilde{\varphi}_i\rangle$ generate the same operator ρ ?

Theorem:

Unitary Freedom in the Ensemble for Density Matrices

- The sets $|\tilde{\psi}_i\rangle$ and $|\tilde{\varphi}_i\rangle$ generate the same density matrix iff...

$$|\tilde{\psi}_i\rangle = \sum_j u_{ij} |\tilde{\varphi}_j\rangle$$

Unitary Matrix (Complex)

- *we "pad" whichever set of vectors $|\tilde{\psi}_i\rangle$ or $|\tilde{\varphi}_i\rangle$ is smaller with additional vectors 0 so that the two sets have the same number of elements*

Density Operator: Application

Consequence?

note that...

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i| = \sum_j q_j |\varphi_j\rangle\langle\varphi_j|$$

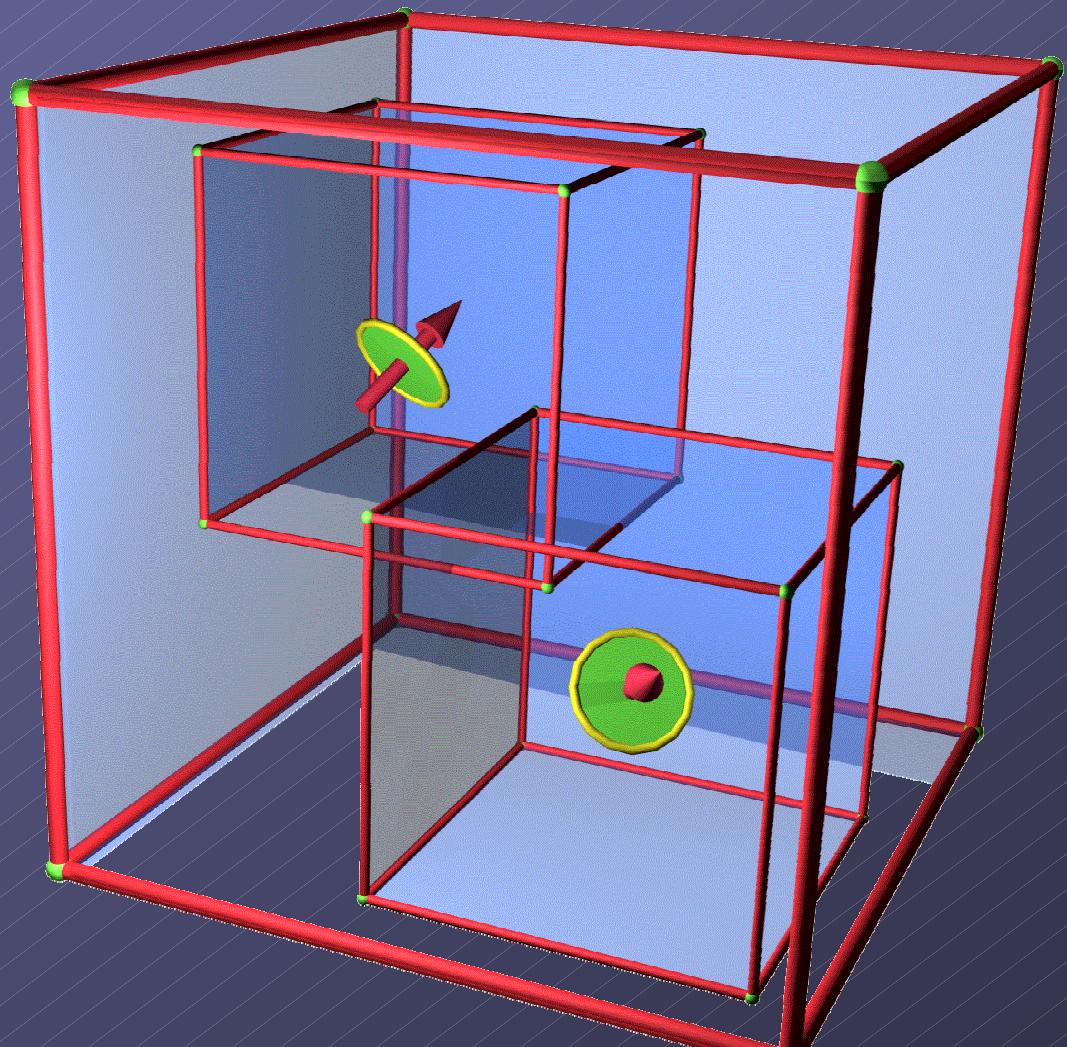
for normalized states $|\psi_i\rangle$, $|\varphi_j\rangle$ and probability distributions p_i and q_j iff

$$\sqrt{p_i}\,|\psi_i\rangle = \sum_i u_{ij}\sqrt{q_j}\,|\varphi_j\rangle$$

Unitary Matrix (Complex)

Reduced Density Operator

The Reduced Density Operator is a descriptive tool for SUBSYSTEMS of a composite quantum system



Reduced Density Operator

- Suppose we have physical systems A and B whose state is described by a density operator ρ^{AB}
- Reduced density operator for the system is defined by…

$$\rho^{A} \equiv tr_{B}\left(\rho^{AB}\right)$$

PARTIAL TRACE over System B

$|a_1\rangle$ and $|a_2\rangle$ are any two vectors in the state space of A

$|b_1\rangle$ and $|b_2\rangle$ are any two vectors in the state space of B

Partial Trace over B is defined by…

$$\mathrm{tr}_{B}\left(|a_1\rangle\langle a_2| \otimes |b_1\rangle\langle b_2|\right) \equiv |a_1\rangle\langle a_2| \underbrace{\mathrm{tr}\left(|b_1\rangle\langle b_2|\right)}$$

$$\mathrm{tr}\left(|b_1\rangle\langle b_2|\right) = \langle b_2|b_1\rangle$$

Reduced Density Operator

- Partial trace operation is defined only on the special subclass of operators on AB
- The specification is completed by requiring that the partial trace be linear in its input.

Is the Reduced Density Operator for the system A a description for the state of the system?

- Suppose a quantum system is in the product state

$$\rho^{AB} = \rho \otimes \sigma$$

ρ is the density operator for system A

σ is a density operator for system B

$$\rho^{A} = \mathrm{tr}_{B}\left(\rho \otimes \sigma\right) = \rho \mathrm{tr}\left(\sigma\right) = \rho$$

similarly…

$$\rho^{B} = \sigma$$

Reduced Density Operator

- Example: The Bell State $\left(|00\rangle + |11\rangle/\sqrt{2}\right)$
  - The density operator is…

$$\rho = \left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right)\left(\frac{\langle 00| + \langle 11|}{\sqrt{2}}\right)$$

$$= \frac{|00\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 00| + |11\rangle\langle 11|}{2}$$

  - Reduced density operator for the 1 st qubit is…

$$\rho^1 = \mathrm{tr}_2(\rho) = \frac{\mathrm{tr}_2(|00\rangle\langle 00|) + \mathrm{tr}_2(|00\rangle\langle 11|) + \mathrm{tr}_2(|11\rangle\langle 00|) + \mathrm{tr}_2(|11\rangle\langle 11|)}{2}$$

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

$$= \frac{|0\rangle\langle 0| + |1\rangle\langle 1|}{2} = \frac{I}{2}$$

Reduced Density Operator

- Example: The Bell State $\left(|00\rangle + |11\rangle / \sqrt{2}\right)$
  - This is in a mixed state since...

$$\mathrm{tr}_2\left(\rho^2\right) = \mathrm{tr}_2\left(\left(\frac{I}{2}\right)^2\right) = \frac{1}{2} < 1$$

  - The state of the joint system of two qubits is a PURE STATE and is known exactly
  - The 1st qubit is in a mixed state (a state that we don't have maximal knowledge) → quantum entanglement

Reduced Density Operator

- Example: Quantum Teleportation

  - Quantum Teleportation is a procedure for sending quantum information from Alice to Bob

    * Alice & Bob share an EPR pair
    * Alice & Bob have a classical communications channel

$$|\psi_2\rangle = \frac{1}{2}\Big[|00\rangle(\alpha|0\rangle+\beta|1\rangle)+|01\rangle(\alpha|1\rangle-\beta|0\rangle)+ |10\rangle(\alpha|0\rangle-\beta|1\rangle)+|11\rangle(\alpha|1\rangle-\beta|0\rangle)\Big]$$

Quantum state of the system immediately before Alice makes her measurement

CIRCUIT

Reduced Density Operator

- Example: Quantum Teleportation cont'd

  $|00\rangle,|01\rangle,|10\rangle,|11\rangle$

  - Measuring in Alice's computational basis, the state of the system after measurement is...

$$|00\rangle\left[\alpha|0\rangle+\beta|1\rangle\right] \text{ with probability } \frac{1}{4}$$

$$|01\rangle\left[\alpha|1\rangle-\beta|0\rangle\right] \text{ with probability } \frac{1}{4}$$

$$|10\rangle\left[\alpha|0\rangle-\beta|1\rangle\right] \text{ with probability } \frac{1}{4}$$

$$|11\rangle\left[\alpha|1\rangle-\beta|0\rangle\right] \text{ with probability } \frac{1}{4}$$

Reduced Density Operator

- Example: Quantum Teleportation cont'd
  - The density operator of the system is then...

$$\rho = \frac{1}{4}\left[\begin{array}{l} |00\rangle\langle 00|\left(\alpha|0\rangle+\beta|1\rangle\right)\left(\alpha^*\langle 0|+\beta^*\langle 1|\right)+ \\ |01\rangle\langle 01|\left(\alpha|1\rangle+\beta|0\rangle\right)\left(\alpha^*\langle 1|+\beta^*\langle 0|\right)+ \\ |10\rangle\langle 10|\left(\alpha|0\rangle-\beta|1\rangle\right)\left(\alpha^*\langle 0|-\beta^*\langle 1|\right)+ \\ |11\rangle\langle 11|\left(\alpha|1\rangle-\beta|0\rangle\right)\left(\alpha^*\langle 1|-\beta^*\langle 0|\right) \end{array}\right]$$

Reduced Density Operator

- Example: Quantum Teleportation cont'd

  - Tracing out Alice's system, the REDUCED DENSITY OPERATOR for Bob's system is...

$$\rho^B = \frac{1}{4}\begin{bmatrix} (\alpha|0\rangle+\beta|1\rangle)(\alpha^*\langle 0|+\beta^*\langle 1|)+ \\ (\alpha|1\rangle+\beta|0\rangle)(\alpha^*\langle 1|+\beta^*\langle 0|)+ \\ (\alpha|0\rangle-\beta|1\rangle)(\alpha^*\langle 0|-\beta^*\langle 1|)+ \\ (\alpha|1\rangle-\beta|0\rangle)(\alpha^*\langle 1|-\beta^*\langle 0|) \end{bmatrix}$$

$$= \frac{2\left(|\alpha|^2+|\beta|^2\right)|0\rangle\langle 0|+2\left(|\alpha|^2+|\beta|^2\right)|1\rangle\langle 1|}{4} = \frac{|0\rangle\langle 0|+|1\rangle\langle 1|}{2} = \frac{I}{2}$$

State of Bob's system AFTER Alice has performed the measurement but BEFORE Bob has learned the measurement result is I/2

Reduced Density Operator

- Example: Quantum Teleportation cont'd

  - This state has no dependence on the state $|\psi\rangle$ being teleported

    * Any measurement performed by Bob will contain no information about $|\psi\rangle$

  - Therefore Alice can't use teleportation to transmit information to Bob faster than light.

Schmidt Decomposition

Another tool in the arsenal of tools useful for the study of composite quantum systems

- Suppose $|\psi\rangle$ is a pure state of a composite system AB then there exists orthonormal states $|i_A\rangle$ for system A and orthonormal states $|i_B\rangle$ of system B such that

$$|\psi\rangle = \sum_i \lambda_i |i_A\rangle |i_B\rangle$$

Schmidt Co-efficients

where $\lambda_i \geq 0$ and $\lambda_i \in \Re$ satisfying $\sum_i \lambda_i^2 = 1$

Schmidt Decomposition

We can use this result…

- Let $|\psi\rangle$ be a pure state of the composite system AB
- By Schmidt decomposition…

$$\rho^A = \sum_i \lambda_i^2 |i_A\rangle\langle i_A| \text{ and } \rho^B = \sum_i \lambda_i^2 |i_B\rangle\langle i_B|$$

- eigenvalues of ρ^A and ρ^B are identical → λ_i^2

Schmidt Decomposition

- Consider the state of two qubits…

$$\left(|00\rangle+|01\rangle+|11\rangle\right)/\sqrt{3}$$

- There is no obvious symmetry property, yet…

$$\mathrm{tr}\left(\left(\rho^{A}\right)^{2}\right)=\frac{7}{9} \text{ and } \mathrm{tr}\left(\left(\rho^{B}\right)^{2}\right)=\frac{7}{9}$$

- For the PURE STATE of a composite system AB, the properties with be the same for both systems A & B.

Purification

Purification allows us to
associate pure states with mixed states

Suppose we are given a state ρ^A of a quantum system A

- It is possible to introduce another system R and define a PURE STATE, $|AR\rangle$ for the joint system AR such that…

$$\rho^A = \mathrm{tr}_R \left(|AR\rangle\langle AR| \right)$$

- The pure state reduces to ρ^A when we look at system A alone

??? OOPS ran out of time ☺

EPR and the Bell inequality

...a compelling example of an
essential difference between quantum and classical physics

- Classically we assume the physical properties of an object have an existence independent of observation

  (eg: position, or momentum of a ball)
- Quantum Mechanically an unobserved particle does not possess physical properties that exist independent of observation.

  - such properties arise as a consequence of measurements performed on the system.
- Quantum Mechanics gives a set of rules which specify, given the state vector, the probabilities for the possible measurement outcomes when an observable is measured

EPR and the Bell inequality

EPR was interested in the "elements of reality" and presumed that any complete physical theory MUST include them.

The goal of the argument in the EPR paper was to show that Quantum Mechanics was an incomplete theory

- A sufficient condition for a physical property to be an element of reality was that it be possible to predict with certainty the value of that property will have just prior to measurement

EPR and the Bell inequality

- The Anti-Correlations in the EPR experiment shows that if we measure the first qubit we can predict what the measurement outcome of the second qubit will be with certainty
  - Suppose we have a two qubit state…

$$|\psi\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

spin singlet state

  - Suppose we perform a measurement of spin along the $\vec{v}$ axis on both qubits ie: we measure the observable

$$\vec{v}\cdot\vec{\sigma} = v_1\sigma_1 + v_2\sigma_2 + v_3\sigma_3$$

$\vec{v}$ is any real three dimensional unit vector

EPR and the BELL inequality

- [more to come]

Quantum Circuits

- Bell States, EPR States, EPR Pairs

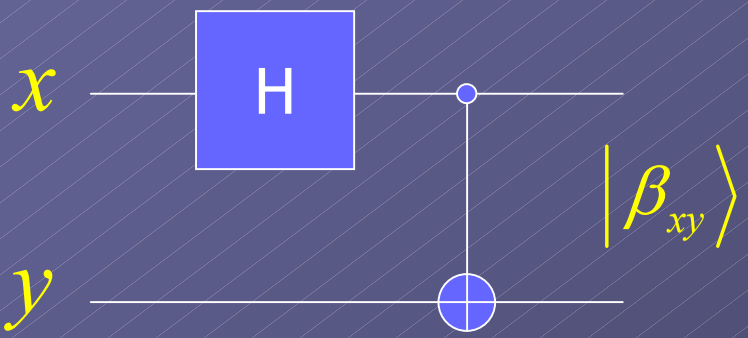
$$|\beta_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \qquad |\beta_{01}\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$$

$$|\beta_{10}\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}} \qquad |\beta_{11}\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$$

$$|\beta_{xy}\rangle = \frac{|0, y\rangle + (-1)^x |1, \bar{y}\rangle}{\sqrt{2}}$$

Quantum Circuits

- Bell States, EPR States, EPR Pairs



In	Out
$\|00\rangle$	$(\|00\rangle+\|11\rangle)/\sqrt{2} \equiv \|\beta_{00}\rangle$
$\|01\rangle$	$(\|01\rangle+\|10\rangle)/\sqrt{2} \equiv \|\beta_{01}\rangle$
$\|10\rangle$	$(\|00\rangle+\|11\rangle)/\sqrt{2} \equiv \|\beta_{00}\rangle$
$\|11\rangle$	$(\|00\rangle+\|11\rangle)/\sqrt{2} \equiv \|\beta_{00}\rangle$

$$\left.\begin{array}{l} |0\rangle \rightarrow \dfrac{|0\rangle+|1\rangle}{\sqrt{2}} \\ |0\rangle \rightarrow \end{array}\right\} \rightarrow \frac{|00\rangle+|10\rangle}{\sqrt{2}} \rightarrow \frac{|00\rangle+|11\rangle}{\sqrt{2}}$$

$$tr\left(A|\psi_i\rangle\langle\psi_i| \right) = \sum_i \langle i|A|\psi\rangle\langle\psi||i\rangle = \langle\psi|A|\psi\rangle$$

$$\rho = \sum_{ij} p_i p_{ij} \left|\psi_{ij}\right\rangle\left\langle\psi_{ij}\right|$$

$$= \sum_{i} p_i \rho_i$$

$$\text{where } \rho_i = \sum_{i} p_{ij} \left|\psi_{ij}\right\rangle\left\langle\psi_{ij}\right|$$

rho is a MIXTURE of the states rhosubi with probabilities psubi

Proof:

Characterization of Density Operators

suppose $\rho = \sum_{ij} p_i \left|\psi_{ij}\right\rangle\left\langle\psi_{ij}\right|$ is a density operator

Then

$$\left\langle\varphi\right|\rho\left|\varphi\right\rangle = \sum_i p_i \left\langle\varphi|\psi_i\right\rangle\left\langle\psi_i|\varphi\right\rangle$$

$$= \sum_i p_i \left|\left\langle\varphi|\psi_i\right\rangle\right|^2 \geq 0$$

so positivity condition is satisfied

Proof:

Characterization of Density Operators

Suppose ρ is any operator satisfying the trace and positivity conditions

Since ρ is positive, it must have a spectral decomposition.

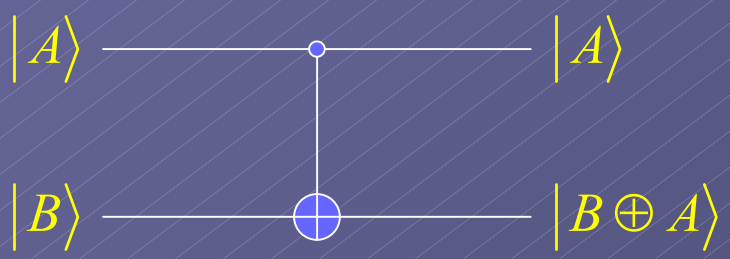
$\rho = \sum_j \lambda_j |j\rangle\langle j|$ where vectors $|j\rangle$ are orthogonal, and λ_j are real, non-negative eigenvalues of ρ.

From the trace condition we see that $\sum_j \lambda_j = 1$

Therefore a system in state $|j\rangle$ with probability λ_j will have a density operator ρ

That is the ensemble $\{\lambda_j, |j\rangle\}$ is an ensemble of states giving rise to the density operator ρ.

CNOT QUANTUM GATE



$$U_{CN} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

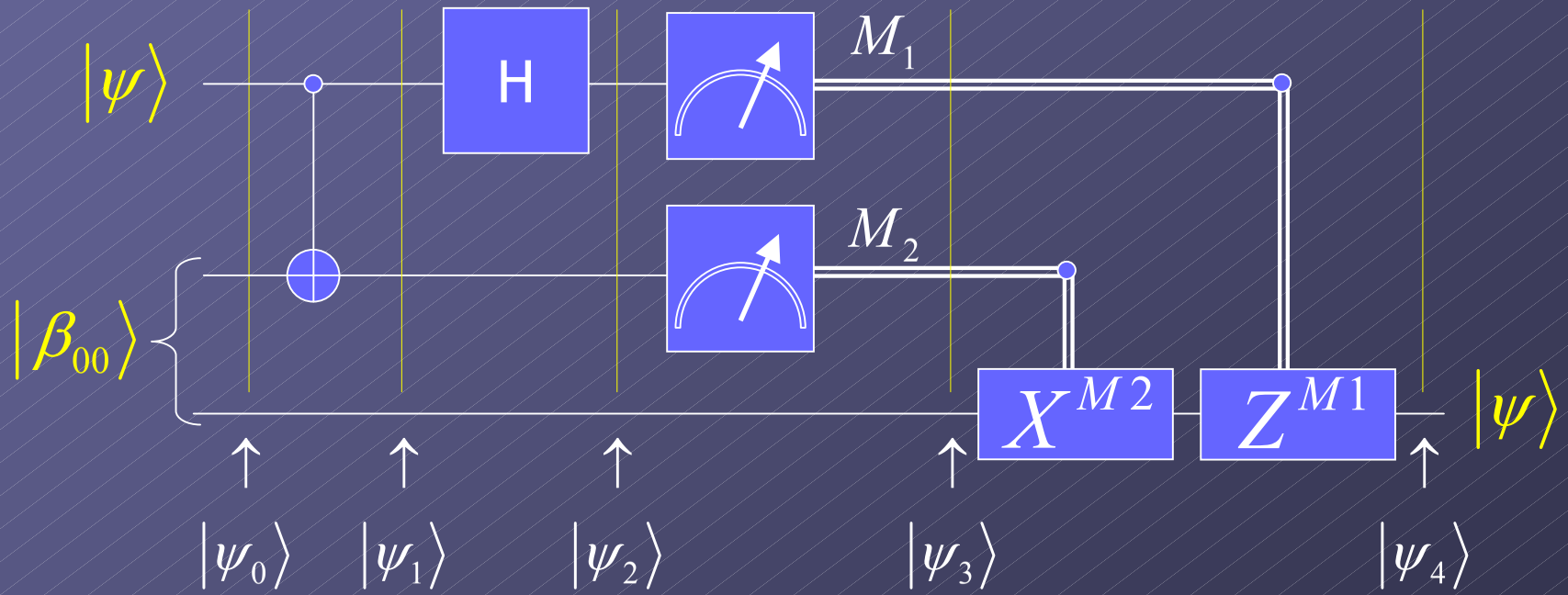
$$|A\rangle|B\rangle \rightarrow \begin{bmatrix} a_0 \begin{bmatrix} b_0 \\ b_1 \end{bmatrix} \\ a_1 \begin{bmatrix} b_0 \\ b_1 \end{bmatrix} \end{bmatrix} = \begin{bmatrix} a_0 b_0 \\ a_0 b_1 \\ a_1 b_0 \\ a_1 b_1 \end{bmatrix}$$

if $|A\rangle = |0\rangle$ then $a_0 = 1$, $a_1 = 0$ we get $\begin{bmatrix} b_0 \\ b_1 \\ 0 \\ 0 \end{bmatrix}$

if $|A\rangle = |1\rangle$ then $a_0 = 0$, $a_1 = 1$ we get $\begin{bmatrix} 0 \\ 0 \\ b_0 \\ b_1 \end{bmatrix}$

Quantum Circuits

- Quantum Teleportation Circuit



Quantum Computing Summer School

Lecture 3: Postulates of Quantum Mechanics

Angela Antoniu

Department of Electrical and Computing Engineering

May 9, 2002

Postulates of Quantum Mechanics Lecture objectives

- Why are postulates important?
  - *… they provide the **connections** between the physical, real, world and the quantum mechanics mathematics used to model these systems*
- Lecture Objectives
  - *Description of connections*
  - *Introduce the postulates*
  - *Learn how to use them*
  - *…and when to use them*

Physical Systems - Quantum Mechanics Connections

Postulate 1	Isolated physical system	⇄	Hilbert Space
Postulate 2	Evolution of a physical system	⇄	Unitary transformation
Postulate 3	Measurements of a physical system	⇄	Measurement operators
Postulate 4	Composite physical system	⇄	Tensor product of components

Postulate 1: State Space

- *Postulate I defines "the setting" in which Quantum Mechanics take place, which is the Hilbert space (inner product space which satisfy the condition of completeness)*
- **Postulate I :** Any isolated physical space is associated with a complex vector space with inner product called the ***State Space*** of the system.
  - *The system is completely described by a* state vector*, a unit vector, pertaining to the state space.*
  - *The state space describes all possible states the system can be in.*
  - *Postulate 1 does NOT tell us either what the state space or state vector is.*

A Qubit: The Simplest State Space

The simplest quantum system is a state space with 2 dimensions -- there are two possible states the system can be in! $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$ ⟹ a qubit!

Recall: state vector is a unit vector, so

$$\langle\psi|\psi\rangle = 1 \Rightarrow |\alpha_0|^2 + |\alpha_1|^2 = 1$$ (normalization condition)

A linear combination of states is called a *superposition* of states ⟹ qualitatively new feature: a qubit can be a mixture of two classical bits!

Postulate 2: Evolution

- Evolution of an isolated system can be expressed as:

$$|v(t_2)\rangle = U(t_1, t_2)|v(t_1)\rangle$$

where t_1, t_2 are moments in time and $U(t_1, t_2)$ is a unitary operator.

  - *U may vary with time. Hence, the corresponding segment of time is explicitly specified:*

$$U(t_1, t_2)$$

  - *the process is in a sense Markovian (history doesn't matter) and reversible, since*

$$U^\dagger U|v\rangle = |v\rangle$$

Postulate 2: Evolution of States

The evolution of a closed system is described by a unitary transformation.

$$|\psi(t_2)\rangle = \mathbf{U}(t_2,t_1)|\psi(t_1)\rangle$$ Heisenberg picture

$$\longleftrightarrow \quad \mathbf{U}(t,t_1) = \exp\left[-\frac{i}{\hbar}\mathbf{H}(t-t_1)\right]$$

$$\longleftrightarrow \quad i\hbar\frac{\partial}{\partial t}|\psi(t)\rangle = \mathbf{H}|\psi(t)\rangle$$ Schroedinger picture

Planck's constant (set to unity)

Hamiltonian (must be input from physical considerations)

$\mathbf{H}^\dagger = \mathbf{H}$ ⟹ Hamiltonian has a spectral decomposition

$$\Longrightarrow \quad \mathbf{H} = \sum_E E|E\rangle\langle E| \quad \Longrightarrow \quad |E\rangle = e^{-iEt/\hbar}|E\rangle$$

Energy eignvalues — Stationary states

Example: Hadamard Gate

Hadamard Gate:
$$\left.\begin{aligned} H|0\rangle &= \frac{1}{\sqrt{2}}\left(|0\rangle+|1\rangle\right) \\ H|1\rangle &= \frac{1}{\sqrt{2}}\left(|0\rangle-|1\rangle\right) \end{aligned}\right\} \Rightarrow H = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$$

$$|0\rangle = \begin{bmatrix}1\\0\end{bmatrix} \Rightarrow H|0\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}1\\0\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix} = \frac{1}{\sqrt{2}}\left(|0\rangle+|1\rangle\right)$$

$$|1\rangle = \begin{bmatrix}0\\1\end{bmatrix} \Rightarrow H|1\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}0\\1\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix} = \frac{1}{\sqrt{2}}\left(|0\rangle-|1\rangle\right)$$

(in this case the unitary matrix H has trivial time dependence)

Postulate 3: Quantum Measurement

The measurement of a closed system is described by a collection of operators $\mathbf{M}_m$ which act on the state space such that

1) $p(m) = \langle\psi|\mathbf{M}_m^\dagger\mathbf{M}_m|\psi\rangle$ describes the probability the measurement outcome m occurred

2) $|\psi'\rangle = \dfrac{\mathbf{M}_m|\psi\rangle}{\sqrt{\langle\psi|\mathbf{M}_m^\dagger\mathbf{M}_m|\psi\rangle}}$ is the state of the system after measurement outcome m occurred

3) $\sum_m \mathbf{M}_m^\dagger\mathbf{M}_m = \mathbf{I} \Leftrightarrow \sum_m p(m) = 1$ Completeness relation

Notes: Measurement is an external observation of a system and so disturbs its unitary evolution

Qubit Measurement

There are two possible outcomes in the measurement of a qubit: $|0\rangle$ and $|1\rangle$

$\Rightarrow \mathbf{M}_0 = |0\rangle\langle 0| \qquad \mathbf{M}_1 = |1\rangle\langle 1| \qquad (\mathbf{M}_0 + \mathbf{M}_1 = \mathbf{I})$

So the probability that $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$ is in the state $|0\rangle$ is

$$p(0) = \langle\psi|\mathbf{M}_0^\dagger\mathbf{M}_0|\psi\rangle = \left(\alpha_0^*\langle 0| + \alpha_1^*\langle 1|\right)\left(|0\rangle\langle 0|\right)^\dagger\left(|0\rangle\langle 0|\right)\left(\alpha_0|0\rangle + \alpha_1|1\rangle\right)$$
$$= |\alpha_0|^2\left|\langle 0|0\rangle\right|^2 = |\alpha_0|^2$$

And the state vector changes: $|\psi\rangle \to \dfrac{\mathbf{M}_0}{|\alpha_0|}|\psi\rangle = \dfrac{\alpha_0}{|\alpha_0|}|0\rangle$

Distinguishability

Only orthogonal states can be distinguished in a measurement!

Why? Suppose $|\psi_1\rangle$ and $|\psi_2\rangle$ are not orthogonal, but can be distinguished by two measurement operators, $\mathbf{E}_1$ and $\mathbf{E}_2$ where $\mathbf{E}_1+\mathbf{E}_2=\mathbf{I}$, and $\mathbf{E}_i=\mathbf{M}_i^\dagger\mathbf{M}_i$ We must have

$$\langle\psi_1|\mathbf{E}_1|\psi_1\rangle=1 \quad \text{and} \quad \langle\psi_2|\mathbf{E}_2|\psi_2\rangle=1$$

since by assumption the states can be distinguished. However we can also write $|\psi_2\rangle=\alpha|\psi_1\rangle+\beta|\varphi\rangle$ where $\langle\psi|\varphi\rangle=0$ and $|\alpha|^2+|\beta|^2=1$

Since $\mathbf{E}_1+\mathbf{E}_2=\mathbf{I}$ we have $\langle\psi_1|\mathbf{E}_2|\psi_1\rangle=0$. But then

$$\langle\psi_2|\mathbf{E}_2|\psi_2\rangle=|\beta|^2\langle\varphi|\mathbf{E}_2|\varphi\rangle\le|\beta|^2<1$$ ⊗

(Unless $\alpha=0$ in which case states are orthogonal)

Projective Measurements

Observable: A Hermitian operator on the state space.

Can write: $\mathbf{M}=\sum_m m\mathbf{P}_m \Rightarrow p(m)=\langle\psi|\mathbf{P}_m^\dagger\mathbf{P}_m|\psi\rangle=\langle\psi|\mathbf{P}_m|\psi\rangle$

(each measurement operator is a projector!)

Average value of a measurement:

$$\mathrm{E}(\mathbf{M})=\sum_m mp(m)=\sum_m m\langle\psi|\mathbf{P}_m|\psi\rangle=\langle\psi|\sum_m m\mathbf{P}_m|\psi\rangle=\langle\psi|\mathbf{M}|\psi\rangle$$

(expectation value)

Standard deviation of a measurement:

$$\Delta(\mathbf{M})=\sqrt{\left\langle(\mathbf{M}-\langle\mathbf{M}\rangle)^2\right\rangle}=\sqrt{\langle\mathbf{M}^2\rangle-\langle\mathbf{M}\rangle^2}$$ where $\langle\mathbf{M}\rangle=\langle\psi|\mathbf{M}|\psi\rangle$

Uncertainty Principle

$$\Delta(\mathbf{p})\Delta(\mathbf{q}) \geq \frac{|\langle\psi|[\mathbf{p},\mathbf{q}]\psi\rangle|}{2}$$

Why? $\langle\psi|\mathbf{A}^2|\psi\rangle\langle\psi|\mathbf{B}^2|\psi\rangle \geq |\langle\psi|\mathbf{AB}|\psi\rangle|^2 = \frac{1}{4}|\langle\psi|[\mathbf{A},\mathbf{B}]+\{\mathbf{A},\mathbf{B}\}\psi\rangle|^2$

$$\frac{1}{4}\left(|\langle\psi|[\mathbf{A},\mathbf{B}]\psi\rangle|^2 + |\langle\psi|\{\mathbf{A},\mathbf{B}\}\psi\rangle|^2\right) \geq \frac{1}{4}|\langle\psi|[\mathbf{A},\mathbf{B}]\psi\rangle|^2$$

Set $\mathbf{A} = \mathbf{p} - \langle\mathbf{p}\rangle, \mathbf{B} = \mathbf{q} - \langle\mathbf{q}\rangle$ and the result follows!

Measurement errors are not arbitrarily reducible!

Positive Operator-Valued Measurements (POVM)

POVM: Any complete set $\{\mathbf{E}_m\}$ of positive operators $\left(\sum_m \mathbf{E}_m = 1\right)$

Recall $|\psi_1\rangle$ and $|\psi_2\rangle = \alpha|\psi_1\rangle + \beta|\varphi\rangle$. Write

$$\mathbf{E}_1 = |\varphi\rangle\langle\varphi|$$

$$\mathbf{E}_2 = \frac{(\beta^*|\psi_1\rangle - \alpha^*|\varphi\rangle)(\beta\langle\psi_1| - \alpha\langle\varphi|)}{|\alpha|^2 + |\beta|^2}$$

$$\mathbf{E}_3 = I - \mathbf{E}_1 - \mathbf{E}_2$$

If you observe $\mathbf{E}_1$ then you know the state is $|\psi_2\rangle$. If you observe $\mathbf{E}_2$ then you know the state is $|\psi_1\rangle$. If you observe $\mathbf{E}_3$ then you don't know the state

POVMs:

Advantage: can never mis-identify a state

Disadvantage: sometimes you get no information

Phase

Global Phase: $e^{i\theta}|\psi\rangle$ is physically indistinguishable from $|\psi\rangle$

$$\langle\psi|e^{-i\theta}\mathbf{M}_m^\tau\mathbf{M}_m e^{i\theta}|\psi\rangle = \langle\psi|\mathbf{M}_m^\tau\mathbf{M}_m|\psi\rangle$$

Relative Phase: $|\psi\rangle = |\chi\rangle + |\varphi\rangle$ can be physically distinguished from $|\psi\rangle = |\chi\rangle + e^{i\theta}|\varphi\rangle$

⟹ a basis-dependent concept

Local Phase: If the phase is a function of position and/or time we say that it is local

$\theta = \theta(\vec{x}, t)$ (not relevant (yet) for quantum computing)

Postulate 4: Composite Systems

The state space of a composite system is the tensor product of the state spaces of its components.

System A: $|\chi\rangle$
System B: $|\varphi\rangle$
} System AB: $|\chi\rangle \otimes |\varphi\rangle$

Common usage:

$|\chi\rangle \otimes |\varphi\rangle$

Physical system (call it V)

Ancilla system (corresponds to measurement outcomes -- call it M)

Unitary Dynamics + Projective Measurements = General Measurement

General Measurements

Let $\mathbf{U} : V \otimes M \to V \otimes M$ be defined so that

$$\mathbf{U}|\psi\rangle|0\rangle \equiv \sum_m \mathbf{M}_m |\psi\rangle|m\rangle$$

for a fixed state $|0\rangle$ in M and a general state $|\psi\rangle$ in V

$$\Rightarrow \left(\mathbf{U}|\varphi\rangle|0\rangle\right)^\dagger \left(\mathbf{U}|\psi\rangle|0\rangle\right) \equiv \langle\varphi|\langle 0|\mathbf{U}^\dagger\mathbf{U}|\psi\rangle|0\rangle = \sum_{m,m'} \langle\varphi|\mathbf{M}^\dagger_m \mathbf{M}_{m'}|\psi\rangle\langle m|m'\rangle$$

$$= \sum_m \langle\varphi|\mathbf{M}^\dagger_m \mathbf{M}_m|\psi\rangle = \langle\varphi|\psi\rangle \Rightarrow \mathbf{U} \text{ can be defined on entire space } V \otimes M$$

Now set $\mathbf{P}_m = \mathbf{I}_V \otimes |m\rangle\langle m|$

$$\Rightarrow p(m) = \langle\psi|\langle 0|\mathbf{U}^\dagger \mathbf{P}_m \mathbf{U}|\psi\rangle|0\rangle = \sum_{m',m''} \langle\psi|\mathbf{M}^\dagger_{m'}\langle m'|\left(I_V \otimes |m\rangle\langle m|\right)\mathbf{M}_{m''}|\psi\rangle|m''\rangle$$

$$= \sum_m \langle\psi|\mathbf{M}^\dagger_m \mathbf{M}_m|\psi\rangle \Rightarrow \text{General Measurement!}$$

Superdense Coding

Idea: exploit entanglement to send more information from point A to point B that would classically be allowed

Problem: Alice has 2 classical bits of information she wants to send to Bob, but is only allowed to send Bob a single qubit. Can she do it?

Solution: Yes! Put Alice's qubit in an entangled state with Bob's! Alice acts on her qubit and then sends it to Bob -- this allows Bob to uniquely deduce Alice's 2 classical bits!

Bibliography & acknowledgements

- Michael A. Nielsen and Isaac L. Chuang, Quantum Computation and Quantum Information, Cambridge University Press, Cambridge, UK, 2002
- V. Bulitko, On quantum Computing and AI, Notes for a graduate class, University of Alberta, 2002
- R. Mann,M.Mosca, Introduction to Quantum Computation, Lecture series, Univ. Waterloo, 2000 http://cacr.math.uwaterloo.ca/~mmosca/quantumcoursef00.htm D. Fotin, Introduction to "Quantum Computing Summer School", University of Alberta, 2002.

Quantum Computing Summer School

Vadim Bulitko

Lecture 5:

EPR, Topics in CS

Presentation Overview

- Super dense Coding
- EPR & Bell Inequality
- Topics in CS

Super Dense Coding

- Alice & Bob have the long distance feeling
- Goal: to transmit some CLASSICAL information from Alice to Bob.
- Alice is in possession of two classical bits of information which she wishes to send to Bob but can only send one qubit to Bob.
- Can she achieve her goal?

Super Dense Coding

- Super Dense Coding says YES!

- They both initially share a pair of qubits in the entangled state.

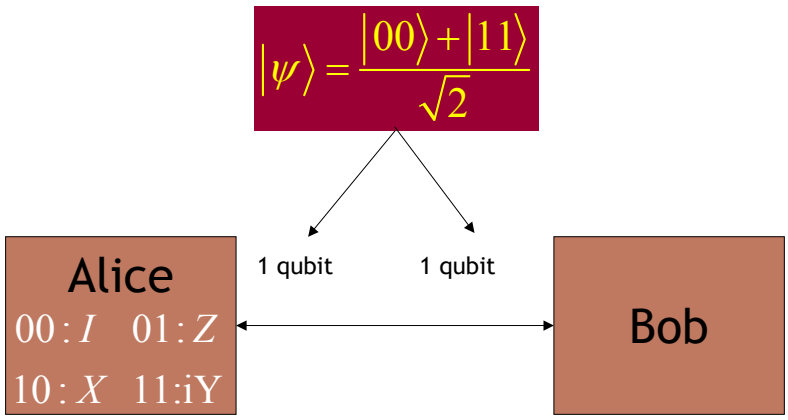
$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

- Alice initially has the first qubit and Bob has the second qubit.

- Note the qubit is prepared ahead of time by a third party who then sends one to Alice and one to Bob

- By sending a single qubit to Bob, Alice can communicate two bits of classical information

Super Dense Coding



Super Dense Coding

- Procedure:
  - If Alice wants to send…

00	She does nothing
01	She applies the phase flip Z to her qubit
10	She applies quantum NOT gate X
11	She applies the iY gate

- Then Bob applies an appropriate measurement operator

Super Dense Coding

- Four Resulting States

$$00:|\psi\rangle \rightarrow \frac{|00\rangle+|11\rangle}{\sqrt{2}}$$
$$01:|\psi\rangle \rightarrow \frac{|00\rangle-|11\rangle}{\sqrt{2}}$$
$$10:|\psi\rangle \rightarrow \frac{|10\rangle+|01\rangle}{\sqrt{2}}$$
$$11:|\psi\rangle \rightarrow \frac{|01\rangle-|10\rangle}{\sqrt{2}}$$

Bell States

Super Dense Coding

- Notice that the Bell States…

Form an orthonormal basis

eg:

$$\left(\frac{\langle 00|+\langle 11|}{\sqrt{2}}\right)\left(\frac{|00\rangle+|11\rangle}{\sqrt{2}}\right)$$
$$=\frac{1}{2}\left(\langle 00|00\rangle+\langle 00|11\rangle+\langle 11|00\rangle+\langle 11|11\rangle\right)$$
$$=\frac{1}{2}(2)=1$$

…therefore can be distinguished by an appropriate quantum measurement. Example:

$$P_{ij} = |b_{ij}\rangle \langle b_{ij}|$$

More on The Measurement

- So what is the measurement operator Bob should use?
- Switch to the white board...

Entanglement & Correlation

Bell states in H^2 have components (for each qubit) that project both on $|0\rangle$ and $|1\rangle$. Therefore, measuring either qubit in the basis $\{|0\rangle, |1\rangle\}$ gives $|0\rangle$ with the probability $1/2$ and $|1\rangle$ with the probability $1/2$. In other words:

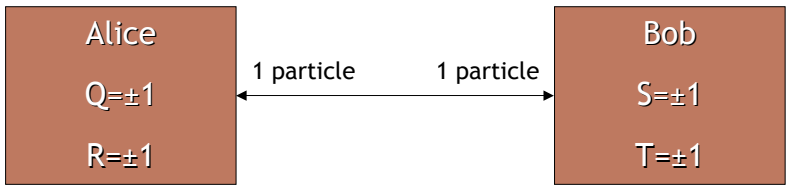
$$\langle b_{ij}| |0\rangle \langle 0| |b_{ij}\rangle = \frac{1}{2} \quad (1.2.5)$$

$$\langle b_{ij}| |1\rangle \langle 1| |b_{ij}\rangle = \frac{1}{2}. \quad (1.2.6)$$

So, if we measure the first qubit of any $|b_{ij}\rangle$ with say the observable $M = \alpha |0\rangle \langle 0| + \beta |1\rangle \langle 1|$ then we get α in half cases and β in half cases (i.e., $p(\alpha) = p(\beta) = \frac{1}{2}$). Suppose, we make a measurement and get α. Then if the original Bell state was $\frac{|0x\rangle \pm |1y\rangle}{\sqrt{2}}$ then the resulting state collapses to $|0x\rangle$ (the $\frac{1}{\sqrt{2}}$ is removed by the normalization). Therefore, now if we measure the second qubit we are *bound* to see $|x\rangle$. So if $|x\rangle$ happens to be $|0\rangle$ we will get *correlation* (the second qubit measurement is bound to give the same result as the first qubit measurement) or (if $|x\rangle = |1\rangle$) *anti-correlation* (the second qubit measurement is bound to be opposite to the first qubit measurement).

EPR "Paradox"

- Suppose we have 2 particles: one with Alice and one with Bob
- Suppose Alice and Bob measure 2 properties of their particle each:



Classical View

- Suppose the system has a state:
  - $Q = q$
  - $R = r$
  - $S = s$
  - $T = t$

with probability p(q,r,s,t)

- Then $E[QS + RS + RT\text{-}QT] \leq 2$
- Thus $E[QS + RS + RT\text{-}QT] =$ $E[QS] + E[RS] + E[RT]\text{-}E[QT] \leq 2$ (Bell ineq.)

Quantum View

Quantum mechanically, however, we can take $|b_{11}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$ and measure the following observables: $Q = Z_1, R = X_1, S = \frac{-Z_2 - X_2}{\sqrt{2}}, T = \frac{Z_2 - X_2}{\sqrt{2}}$. On the entangled state $|b_{11}\rangle$ their expected values are: $\langle QS\rangle = \frac{1}{\sqrt{2}}, \langle RS\rangle = \frac{1}{\sqrt{2}}, \langle RT\rangle = \frac{1}{\sqrt{2}}, \langle QT\rangle = -\frac{1}{\sqrt{2}}$ and, therefore, the expected value of the entire quantity is: $\langle QS\rangle + \langle RS\rangle + \langle RT\rangle - \langle QT\rangle = 2\sqrt{2} > 2$!

So what is the truth?

$$E[QS] + E[RS] + E[RT] - E[QT] \leq 2$$

Or

$$E[QS] + E[RS] + E[RT] - E[QT] > 2$$

Nature's Response

- The Mother Nature says:

$$E[QS] + E[RS] + E[RT] - E[QT] > 2$$

- Assumptions of the classical view:
  - P,Q,R,S,T have definite values independent of observation (realism)
  - Alice's measurement doesn't affect Bob's measurement if they are causally disconnected (locality)
- So the verdict?
  - Nature is NOT locally realistic

Does The Reality Exist?

- *I recall that during one walk Einstein suddenly stopped, turned to me and asked whether I really believed that the moon exists only when I look at it.*

Abraham Pais

Computer Science

- Goal: *Brush up on CS aspects relevant to QC*
- Models of computation:
  - Turing machines
  - Circuits
- Computation problems
  - Description
  - Algorithms
  - Complexity : asymptotic notation
  - Complexity : classes
- Energy & computation : reversibility

Models Of Computation

- Why do we need a model of computation?
- When someone says *"This function is incomputable"* or *"f(x) is computable but intractable"*, etc. what does it really mean?
- What if I say *"I can compute this"* or *"I have an algorithm for this"* ?
- Intuition?
- Well, David Hilbert felt that any true formula can be proven by a mechanical procedure.
- ...Need a formalization

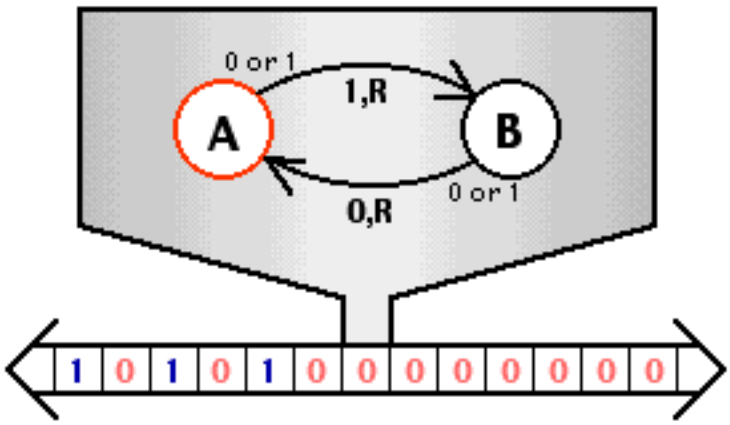
Turing Machines

- Need a formalization of what it means to have an algorithm for (or to be able to compute)

LCMs can do anything that could be described as 'rule of thumb' or 'purely mechanical'.
Alan Mathison Turing (1948)

- So what is LCM (or as it's now known Turing Machine) ?

Turing Machines

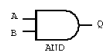


Demos

- Classical implementation
  http://www.warthman.com/ex-turing.htm
- Conway's Game of Life implementation
  http://www.rendell.uk.co/gol/tmdetails.htm

Circuits

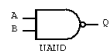
- Circuit : wires + gates
- Gates : function $\{0,1\}^k \rightarrow \{0,1\}^m$
- No loops
- Elementary circuits
  - AND, OR, NOT, NAND, NOR, XOR
  - Fanout
  - Crossover
  - Work (ancilla) bits



$Q = A \cdot B$

AND

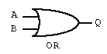
A	B	Q
0	0	0
0	1	0
1	0	0
1	1	1



$Q = \overline{A \cdot B}$

NAND

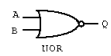
A	B	Q
0	0	1
0	1	1
1	0	1
1	1	0



$Q = A + B$

OR

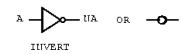
A	B	Q
0	0	0
0	1	1
1	0	1
1	1	1



$Q = \overline{A + B}$

NOR

A	B	Q
0	0	1
0	1	0
1	0	0
1	1	0



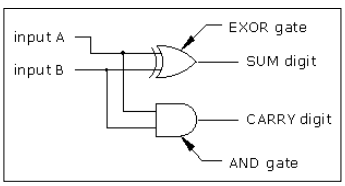
$Q = \overline{A}$

NOT

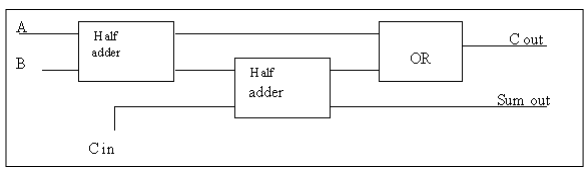
A	Q
0	1
1	0

Putting Circuits Together

- Here is a half-adder (half because doesn't take carry as in an input):



- Here is a full-adder then:



Universality

- Any function $\{0,1\}^k \rightarrow \{0,1\}^m$ can be computed with:
  - Wires
  - Work (ancilla) bits prepared in some fixed state
  - Fanout operation
  - Crossover
  - AND, XOR gates (or just NAND)
- *How is crossover different from crossed wires?*
- *Why cannot we do crossover with XOR?*

Families Of Circuits

- A single function $\{0,1\}^k \rightarrow \{0,1\}^m$ is merely a 2^k row look-up table.
- Obviously, any such function is computable. Furthermore, it doesn't correspond to our notion of algorithm which can be defined for arbitrarily large numbers (e.g., $f(n) = n^2$)
- What do we do?
- Families of circuits…

Families Of Circuits

- Thus, define a uniform circuit family as:
  - a set $\{C_n\}$ of circuits
  - C_n handles inputs of size up to n
  - For all $m > n$ for all x $C_m(x) = C_n(x)$
  - There is a Turing machine T_C such that $T_C(n)$ produces description of circuit C_n
- Then $\{C_n\}$ computes function $C()$ iff for all x $C(x) = C_{|x|}(x)$

Turing-Church Thesis

- Anything that can be computed mechanically/algorithmically can be computed on a Turing machine
- Corollary: anything that can be computed mechanically/algorithmically can be computed with a uniform family of circuits
- Proof?
- "computed mechanically/algorithmically" is too fuzzy to use in a proof…

Why A Formalization?

- Allows us to answer several questions:
  - What is a computational problem?
  - Is there an algorithm to solve it?
  - What are the resources to solve a problem?

Mass Problems

- Consider this problem:

  "Is X entailed by a set of axioms?"
- The answer is 'yes' or 'no' as X is just a single constant expression
- Therefore, there exists a program which takes X and outputs 'yes' or 'no' (it will just contain one print statement (e.g., print('yes')))
- We might not know how to write that program but it trivially exists

Mass Problems

- This doesn't capture the fact that the problem of proving a given FOPC statement is undecidable
- Thus, need a mass problem:

"Is there a computable function f(X) such that f(X) = 'yes' iff X is a FOPC statement entailed by a given set of axioms and f(x) = 'no' iff X isn't."

- Undecidable – no such computable function exists

Decision Problems

- The answers are:
  - What is a computational problem?
    - Here : a mass problem with 'yes'/'no' answer
    - Example: "Function f(n) such that f(n) = yes iff n is prime and f(n) = no iff n is not prime"

Another Example

- Mass problem :

  "Given a Turing machine number m, can we algorithmically determine if T_m will halt on the empty input?"

- Known as the Halting Problem
- Undecidable

Decidability

- Decidability == computability of the corresponding decision mass problem
  - What is a computational problem?
    - Here : a mass problem with 'yes'/'no' answer
  - Is there an algorithm to solve it?
    - Not always

More Cheerful Examples

- Fortunately, some tasks are more doable
- Examples:

"For any given 3 numbers a,b,c return 'yes' if a=bc and 'no' otherwise"

"For any given number n return its prime factors"

- Both are computable
- But the complexity is different
- So need finer distinctions

Complexity

- On to the last bullet:
  - What is a computational problem?
    - Here : a mass problem with 'yes'/'no' answer
  - Is there an algorithm to solve it?
    - Not always
  - What are the resources to solve a problem?
    - Coarse division : tractable / intractable
    - Finer division : asymptotic notation

Asymptotic Notation

- Big O : $f = O(g)$ iff there exists a constant c that starting from some x_0 holds $f(x) < cg(x)$ (i.e., g upper-bounds f)
- Example: $sum_{i=1..n}\ i\ =\ O(n^2)$
- Good for worst-case performance analysis
- Example: linear search is $O(n)$

Asymptotic Notation

- Big Omega : $f = \Omega(g)$ iff there exists a constant $c \neq 0$ that starting from some x_0 holds $f(x) > cg(x)$ (i.e., g lower-bounds f)
- Sometimes used for the best case analysis
- Example: any binary-comparison based sorting is $\Omega(n \log n)$

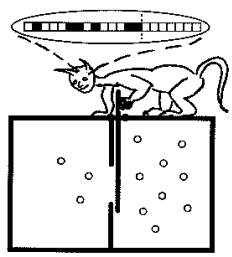
QCSS

"Quantum Computing Summer School"

Prof. Vadim Bulitko
University of Alberta

Today

- Computability
  - Turing-Church thesis
  - Turing machines
  - Circuits
- Computational complexity
  - Computable/non-computable
  - Asymptotic notation
  - P, NP, etc. classes



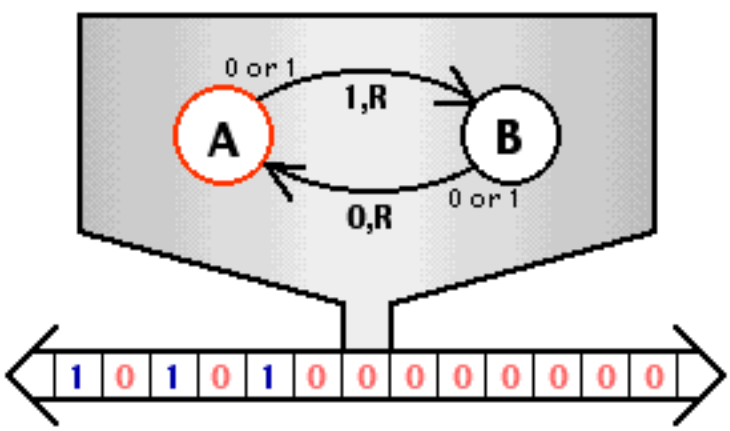
- Reversibility

Outline

- What does it mean if a function is computable?
- What device is to be used?
- Does it matter?

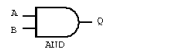
- Turing machines can compute anything computable – thereby formalizing the definition of computability

Turing Machines



Circuits

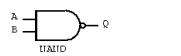
- Circuit : wires + gates
- Gates : function $\{0,1\}^k \rightarrow \{0,1\}^m$
- No loops
- Elementary circuits
  - AND, OR, NOT, NAND, NOR, XOR
  - Fanout
  - Crossover
  - Work (ancilla) bits



AND

A	B	Q
0	0	0
0	1	0
1	0	0
1	1	1

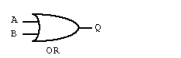
$Q = A \cdot B$



NAND

A	B	Q
0	0	1
0	1	1
1	0	1
1	1	0

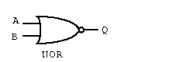
$Q = \overline{A \cdot B}$



OR

A	B	Q
0	0	0
0	1	1
1	0	1
1	1	1

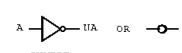
$Q = A + B$



NOR

A	B	Q
0	0	1
0	1	0
1	0	0
1	1	0

$Q = \overline{A + B}$



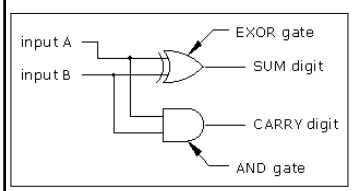
NOT

A	Q
0	1
1	0

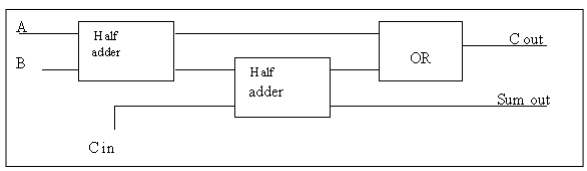
$Q = \overline{A}$

Putting Circuits Together

- Here is a half-adder (half because doesn't take carry as in an input):



- Here is a full-adder then:



Circuit Universality

- Any function $\{0,1\}^k \rightarrow \{0,1\}^m$ can be computed with:
  - Wires
  - Work (ancilla) bits prepared in some fixed state
  - Fanout operation
  - Crossover
  - AND, XOR gates (or just NAND)
- Need crossover to keep things planar
- *Why cannot we do crossover with XOR?*

Inputs of arbitrary lengths

- A single function $\{0,1\}^k \rightarrow \{0,1\}^m$ is merely a 2^k row look-up table.
- Obviously, any such function is computable. Furthermore, it doesn't correspond to our notion of algorithm which can be defined for arbitrarily large numbers (e.g., $f(n) = n^2$)
- What do we do?

Families Of Circuits

- Thus, define a uniform circuit family as:
  - a set $\{C_n\}$ of circuits
  - C_n handles inputs of size up to n
  - For all $m > n$ for all x $C_m(x) = C_n(x)$
  - There is a Turing machine T_C such that $T_C(n)$ produces description of circuit C_n
- Then $\{C_n\}$ computes function $C()$ iff for all x $C(x) = C_{|x|}(x)$

- Uniform circuit families are equivalent to Turing machines and therefore can compute anything computable

Turing Machine Countability

- All Turing machines / circuits can be algorithmically enumerated

- What it means is:
  - Every possible Turing machine/circuit can be assigned a unique integer ID number
  - There is a Turing machine/circuit that given index j produces the full description of Turing machine/circuit #j

Why A Formalization?

- Allows us to answer several questions:
  - What is a computational problem?
  - Is there an algorithm to solve it?
  - What are the resources to solve a problem?

Computability / Decidability

- A problem is computationally solvable (or computable) if there exists a program that computes the answer
- If the answer is of the Yes/No type then the problem is called a decision problem
- If such a problem is computable we say it is decidable

Single Instance Problems

- It is not interesting to pose a single instance problem
- For example: is the problem of answering "Can machines think?" computationally decidable?
- Sure – there exists a program that prints out "Yes" and there exists a program that prints out "No"
- By our definition on the previous slide the problem is decidable

Mass Problems

- To make computability/decidability definitions meaningful we can use mass problems
- A mass problem consists of inputs and desired outputs (e.g., $n \rightarrow n^2$)
- Mass Yes/No problems ➔ mass decision problems
- We say that a mass problem is computable/decidable iff there exists an algorithm for finding the desired answer for any valid input

Computability / Decidability

- Decidability problems are often described by languages:
  - the input are members of a larger set
  - the output is Yes/No on whether the input belongs to a given language (set) L
- Examples:
  - $L = \{n \mid n \text{ is a prime number}\}$ — **decidable**
  - $L = \{n \mid n \text{ is an index of Turing machine that halts on input } 0\}$ — **undecidable**

Asymptotic Notation

- Upper bound
- Big O : $f = O(g)$ iff there exists a constant c that starting from some x_0 holds $f(x) < cg(x)$ (i.e., g upper-bounds f)
- Example: $\text{sum}_{i=1..n}\ i = O(n^2)$
- Example: linear search is $O(n)$

Asymptotic Notation

- Lower bound
- Big Omega : $f = \Omega(g)$ iff there exists a constant $c \neq 0$ that starting from some x_0 holds $f(x) > cg(x)$ (i.e., g lower-bounds f)
- Example: any binary-comparison based sorting is $\Omega(n \log n)$

Coarse Division : Tractable/Intractable

- Often we want to make a statement if an algorithm is tractable/feasible or intractable/infeasible
- The crude formalization is this:

If the worst case running time is polynomial (i.e., $O(n^k)$ where k is a constant) then the algorithm is tractable in running time

- Here n is the input size in a reasonable (e.g., binary) representation
- The running time measured on a deterministic Turing machine

Slightly finer division

- Class P – time to solve: O(poly(|input|))
- Class NP – time to verify : O(poly(|input|))
- Class NP-complete -- any other NP problem is reducible to it
- Class NPI – NP but not NP-complete
- Class PSPACE -- space to solve: O(poly(|input|))
- Class EXP – space to solve : $O(2^{poly(|input|)})$

Class P

- Thus can define:

P (*polynomial time*) is the class of languages that can be decided by a deterministic TM running in $O(n^k)$ time;

Class P

- Examples:
  - Search: $n < n^1$
  - Sorting: $n\log n < n^2$
  - Etc.
- Counter examples:
  - Sure, take a number n, idle for 2^n time ticks, output 'yes'. This algorithm is exponential but the function it represents is O(1)

Class NP

- Some problems appear harder
- Example: "Is a given number composite (i.e., not prime)?". No polynomial algorithm is known.
- Define:

NP (*non-deterministic polynomial time*) is the class of languages that can be verified by a deterministic TM running $O(n^k)$ time. More technically: $L \in \mathbf{NP}$ if $\exists M \exists k \forall \ell [(\ell \in L \implies \exists w M(\ell, w) = 1 \text{ in } O(|\ell|^k)) \ \& \ (\ell \notin L \implies \forall w M(\ell, w) = 0 \text{ in } O(|\ell|^k))]$. In other words, we require a witness w for each positive (i.e., $\ell \in L$) instance. Example: $L = \{\ell \in \mathbb{N} | \ell \text{ is not prime}\} \in \mathbf{NP}$.

A Corollary

- Given an input x of size $|x| = n$ and an appropriate witness w there must be a polynomial time algorithm to check if x belongs to L
- This means that $|w| = O(poly(|x))$

- Why?
- Otherwise, the Turing Machine won't be even able to read in w

Class Co-NP

- What about "Is n prime?"
- Can easily check if n is not a prime if given a witness (e.g., a factor of n)

- Define:

coNP is the class of languages where we require a witness for every negative (i.e., $\ell \notin L$) instance. Clearly, $\forall L[L \in \mathbf{NP} \iff \overline{L} \in \mathbf{coNP}]$. Example: $\overline{L} = \{\ell \in \mathbb{N} | \ell \text{ is prime}\} \in \mathbf{coNP}$.

Class NP-Complete

- Some NP-problem are especially hard insomuch as any other NP problem can be reduced to any of them
- Reduction : if I have a NP decision problem L (i.e., I am asking a question "Is x in L?") and an NP-complete problem M then for any x it takes polynomial time to produce y such that y is in M iff x is in L
- In other words, the time complexity of L is O(poly(t)) where t is the time complexity of M

Class NP-Complete

- Formally:

NP -complete is the class of languages from **NP** such that for any language L from **NP** L can be polynomially reduced to that **NP** -complete language;

- Examples:
  - CSAT : given a Boolean circuit of AND and NOT gates, is there an assignment of its inputs such that the entire circuit produces 1 (true)?

HC

- Hamiltonian cycle is an ordering of all graph vertices such that no vertices are repeated except the starting vertex. The cycle has to have the edges present in the graph.
- Decision-problem : does a given graph have a Hamiltonian cycle?

EC

- Euler cycle is an ordering of all edges of a graph such that:
  - every edge is visited exactly once
  - any two consecutive edges in the sequence share a vertex
  - the sequence forms a cycle
- Decision-problem : does a given graph have an Euler cycle?

HC vs. EC

- Hamiltonian cycle is NP-complete
- EC is in P (can be solved in $O(|\text{input}|^3)$)

Class NPI

- How about problems that are in NP but not NP-complete?
- They would belong to NPI (NP Intermediate)
- Do they exist?
- Unknown but suspected that:
  - Factoring is in NPI
  - Graph isomorphism is in NPI

Classes PSPACE & EXP

- **PSPACE**: Problems that can be decided in *space* $O(\text{poly}(|\text{input}|))$
- **EXP**: Problems that can be decided in *space* $O(2^{\text{poly}(|\text{input}|)})$

Class Inclusion

- What do we know?
  - $P \subseteq NP \subseteq PSPACE \subseteq EXP$
  - NP-complete $\subseteq$ NP
  - NPI $\subseteq$ NP
  - $P \subset EXP$
- What don't we know but really believe that it is true?
  - $P \subset NP$?
  - NPI $\neq \varnothing$?
  - $P \subset SPACE$?

What is in all this for us?

- Well, we know that:
  - Polynomial quantum algorithms are in PSPACE
- It's believed:
  - Polynomial quantum algorithms can do MORE than polynomial classical algorithms
  - Specifically: they can do NPI but NOT all NP (i.e., not NP-complete)

Energy & Computation

- Erasing information ➔ increase in entropy ➔ will dissipate some energy
- Reversible computations can go without erasing information and can be done with NO energy dissipated at all!
- How much: at least $k_B T \ln 2$ joules per 1 classical bit (Landauer's principle)
- *Can we erase a qubit? Not without storing this information somewhere else. Why? Because otherwise it won't be reversible (i.e., no unitary transformation)*

Reversibility of Computation

- Can we make any computation reversible?
- Yes
- Hand-waving argument :
  - the laws of physics are reversible (given a closed system we can compute its previous states given the current state)
- Quantum computation is reversible (can undo the unitary operator)

Questions For Discussion...

- So what happens to two bits of information when I apply an AND gate and get one bit out?
- Using an AND gate I erased some info, yet the underlying physical processes must be reversible. So where did that information go to? How do I reverse the AND gate?
- Comments???

Reversible Gates

- Classical computation can be made reversible so that no information is lost
- How?
- Instead of using AND, OR, etc. we will gates that are:
  - universal (e.g., allow us to implement any circuit)
  - explicitly reversible
- The gates: Fredkin & Toffoli

Fredkin Gate

- The first reversible universal gate
- Invented by a former US Air Force pilot Ed Fredkin in 1974, Caltech
- Has 3 inputs (a,b,c), 3 outputs (a′,b′,c′)
- Swaps a and b when c = 1

Professor Ed Fredkin.

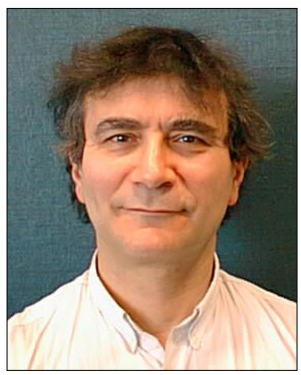
http://digitalphilosophy.org

Fredkin Gate Universality

- Wires — still need them
- Ancilla bits prepared in some fixed state — still need them
- Fanout, NOT — F(1,0,x)=(not(x),x,x)
- Crossover — F(x,y,1)=(y,x,1)
- AND — F(0,y,x)=(x&y,not(x)&y,x)

Toffoli Gate

- Another universal reversible gate
- Has 3 inputs (a,b,c) and 3 outputs (a′,b′,c′):
  - a′ = a
  - b′ = b
  - c′ = c XOR (a AND b)
  - (the target bit c is flipped when both a and b are set)



http://pm1.bu.edu/~tt/

Toffoli Gate Universality

• Wires	still need them
• Ancilla bits prepared in some fixed state	still need them
• Fanout operation	T(x,1,0)=(x,1,x)
• Crossover	?? a quick way ??
• NAND	T(x,y,1)=(x,y,nand(x,y))

Fredkin ⇔ Toffoli

- Exercise 3.32 : simulate Fredkin by Toffoli and back
- 9 Fredkin gates appear enough to simulate a Toffoli gate
- 15 Toffoli gates seem to be able to simulate a Fredkin gate
- Challenge: can anyone do better?

Garbage Bits

- Suppose we have a classical computation: x → f(x)
- With ancilla bits a and reversible gates we can simulate it as : (x,a)→(f(x),g(x))
- Garbage bits g(x) depend on x --- not good… Why?
- Need to produce garbage bits in some standard state independent of x

Uncomputation - 1

- Here is the trick…
- Define CNOT(c,t) = (c,c XOR t) [reversible]
- Use CNOTs to prepare ancilla 1's
- Thus:

(x,a) → (f(x),g(x))

- Becomes

(x,0) → (f(x),g(x))

Uncomputation - 2

- Notice that CNOT(0,x) = (x,x) (fanout)
- Use it to drag x along:

  $(x,0,0) \rightarrow (x,f(x),g(x))$
- Add another input in a random state y:

  $(x,0,0,y) \rightarrow (x,f(x),g(x),y)$
- Add another input in a random state y:

  $(x,0,0,y) \rightarrow (x,f(x),g(x),y)$

Uncomputation - 3

- So far just dragging x and y along:

  $(x,0,0,y) \xrightarrow{U} (x,f(x),g(x),y)$
- Now, CNOT f(x) and y:

  $(x,f(x),g(x),y) \rightarrow (x,f(x),g(x),y \text{ XOR } f(x))$
- U was reversible – undo it (i.e., apply U^{-1}):

  $(x,f(x),g(x), y \text{ XOR } f(x)) \rightarrow (x,0,0,y \text{ XOR } f(x))$
- Thus, by applying U, CNOT, U^{-1} we
  $(x,0,0,y) \rightarrow (x,0,0,y \text{ XOR } f(x)$
- Drop 0s:

  $(x,y) \rightarrow (x,y \text{ XOR } f(x))$

• Reversible
• No garbage bits dependent on x
• The uncomputation overhead doesn't change the class hierarchy

Check - point

- Done with Part I of the book :
  - Chapter 1 : Intro
  - Chapter 2 : Linear Algebra + postulates
  - Chapter 3 : Computer Science
- Now on to Part II and specifically:
  - Chapter 4 : Quantum Circuits
  - Chapter 5 : Quantum Fourier Transform
  - Chapter 6 : Quantum Search
  - Chapter 7 : Physical Realization of QMs

Chapter 4

QUANTUM CIRCUITS

Part I

Lecture 7

Vahid Rezania
May-June 2002

Motivation

- Quantum circuit model :
  fundamental model for quantum computing

- Universal Gates:
  any quantum computation can be expressed by these gates

Outline

- Quantum Algorithms
- Single qubit operations
- Controlled operations (Multi-qubits operations)
- Measurement
- Universal quantum gates

4.1 Quantum Algorithms

-Why quantum computer?

many problems are impossible to solve by classical computers (astronomical resources required)

Quantum Algorithms

-Two quantum algorithms:

(a) Shor's quantum Fourier transformation

- factoring, discrete logarithmic problems
- exponential speed up

(b) Grover's quantum search algorithm

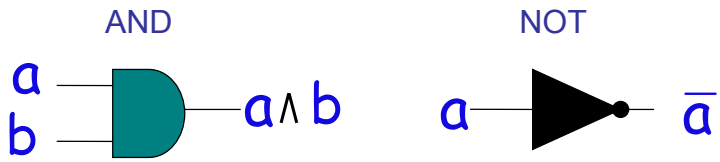
- quadratic speed up

Quantum Algorithms

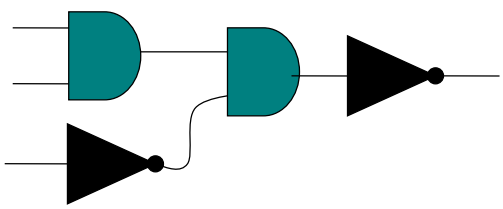
- Why two?
  - finding an efficient and optimal algorithm is very difficult
  - should more efficient than classical one

4.2 Single qubit operations

A gate is a function from *m* bits (qubits) to *n* Bits (qubits):



To compute a Boolean function, ‘ glue ’ different gates ⇒ Circuits



Properties of quantum circuits:

- time proceeds from left to right
- wires represent qubits

Single qubit operations

- A single qubit vector is shown as
  $|\psi> = a\ |0> + b\ |1>$ with $|a|^2 + |b|^2 = 1$.

- Operations must preserve the norm.
- 2 x 2 unitary matrices.

Single qubit operations

- The Pauli matrices

$$\sigma_0 = I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad \sigma_1 = \sigma_x = X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$\sigma_2 = \sigma_y = Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \qquad \sigma_3 = \sigma_z = Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Single qubit operations

$$H = (1/\sqrt{2}) \begin{vmatrix} 1 & 1 \\ 1 & -1 \end{vmatrix}$$ Hadamard gate

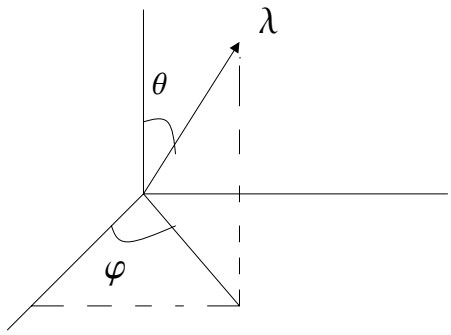
$$S = \begin{vmatrix} 1 & 0 \\ 0 & i \end{vmatrix}$$ phase gate

$$T = \begin{vmatrix} 1 & 0 \\ 0 & \exp(i\pi/4) \end{vmatrix}$$ $\pi/8$ gate

- qubit represented by a point (θ,φ) on a sphere – Bloch sphere

- Bloch vector :

  $(\cos\varphi \sin\theta, \sin\varphi \sin\theta, \cos\theta)$



- Rotation operators:

about x-direction:

$R_x(\theta) = \exp(-i\theta X/2) = \cos(\theta/2)\, I - i \sin(\theta/2)\, X$

about y-direction:

$R_y(\theta) = \exp(-i\theta Y/2) = \cos(\theta/2)\, I - i \sin(\theta/2)\, Y$

about z-direction:

$R_z(\theta) = \exp(-i\theta Z/2) = \cos(\theta/2)\, I - i \sin(\theta/2)\, Z$

Note: $\exp(iAx) = \cos(x)\, I + i \sin(x)\, A$ if $A^2 = I$ and x is a real number

- for any unit vector $n = (n_x, n_y, n_z)$ the rotation operator is defined by :

$R_n(\theta) = \exp(-i\theta\, n.\sigma/2)$

$= \cos(\theta/2)\, I - i \sin(\theta/2)(n_x\sigma_x + n_y\sigma_y + n_z\sigma_z)$

$R_n^{\dagger}(\theta) = R_n(-\theta) = \exp(i\theta\, n.\sigma/2)$

- Why rotation operators?

  any arbitrary unitary operator on a single qubit can written as a combination of rotations and global phase shift.

$$U = \exp(i\alpha) R_n(\theta)$$

Example:

for $\alpha=0$, $\theta=-\pi/2$: $U = H$

for $\alpha=\pi/4$, $\theta=\pi/2$: $U = S$

Theorem 4.1: *Z-Y* decomposition

Let U is a unitary operation. There is real numbers $\alpha, \beta, \gamma,$ and δ such that

$$U = \exp(i\alpha) R_z(\beta) R_y(\gamma) R_z(\delta)$$

$$U = \begin{vmatrix} e^{i(\alpha-\beta/2-\delta/2)}\cos(\gamma/2) & -e^{i(\alpha-\beta/2+\delta/2)}\sin(\gamma/2) \\ e^{i(\alpha+\beta/2-\delta/2)}\sin(\gamma/2) & e^{i(\alpha+\beta/2+\delta/2)}\cos(\gamma/2) \end{vmatrix}$$

In general for two non-parallel unit vectors *m* and *n*, one can decompose an arbitrary Single qubit unitary *U* as

$$U = \exp(i\alpha) R_n(\beta_1) R_m(\gamma_1) R_n(\beta_2) R_m(\gamma_2) \ldots$$

for appropriate choice of α and β_k, γ_k .

Corollary 4.2: Let *U* is a unitary gate on a single qubit. There exist operators *A*, *B*, and *C* on single qubit such that $ABC=I$ and

$$U = \exp(i\alpha)\, A\, X\, B\, X\, C$$

where α is a phase.

proof: Set $A = R_z(\beta) R_y(\gamma/2)$,

$B = R_y(-\gamma/2) R_z(-(\delta+\beta)/2)$, $C = R_z((\delta-\beta)/2)$

Example:

$H = \exp(i\pi/2)\, A\, X\, B\, X\, C$

for $A=R_y(\pi/4)$, $B= R_y(-\pi/4)R_z(-\pi/2)$, $C=R_z(\pi/2)$

Circuit identities

- To simplify a circuit one can use following identities:

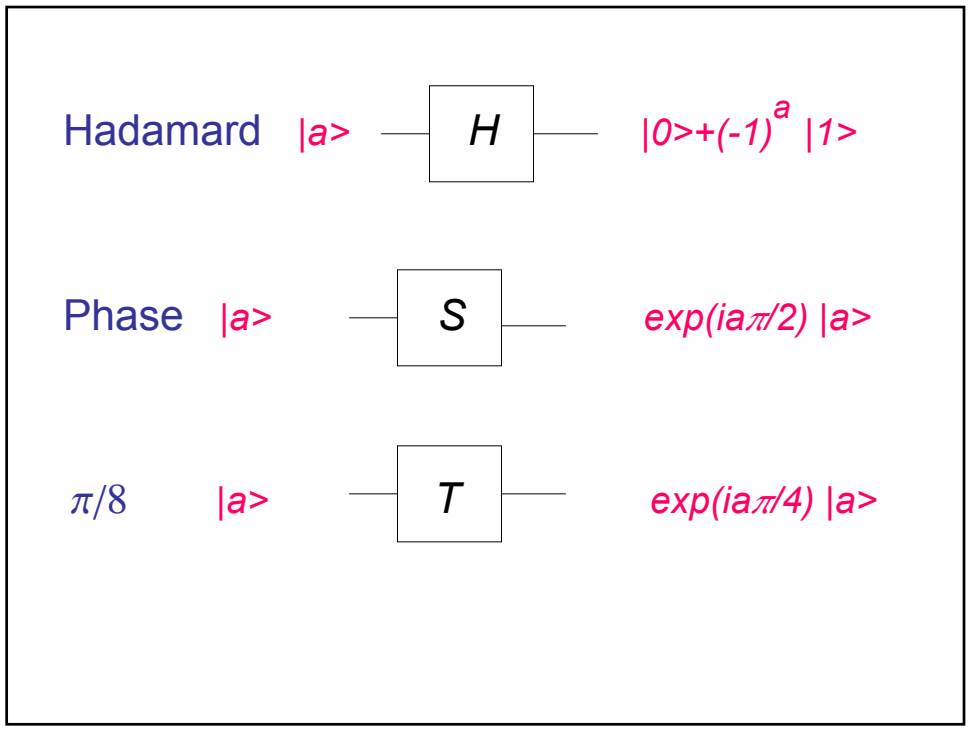
$$H X H = Z$$
$$H Y H = - Y$$
$$H Z H = X$$
$$H T H = R_x(\pi/4)$$

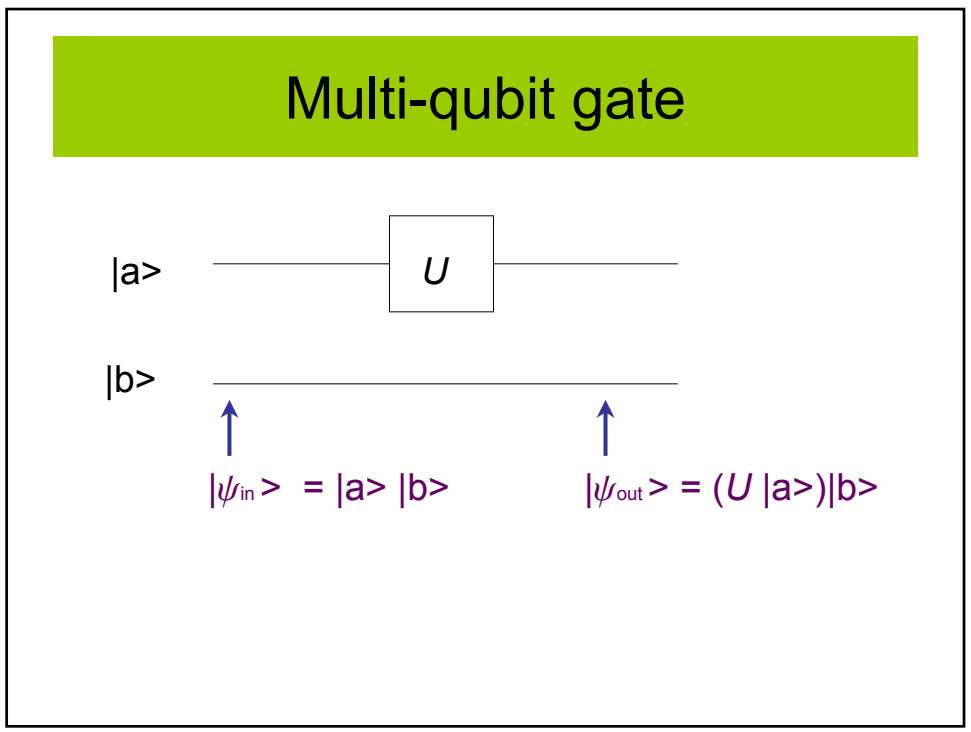
Single qubit gates:

Pauli – X $|a\rangle$ — [X] — $|1-a\rangle$

Pauli – Y $|a\rangle$ — [Y] — $(-1)^a i\,|1-a\rangle$

Pauli - Z $|a\rangle$ — [Z] — $(-1)^a\,|a\rangle$


Hadamard
|a>
H
|0>+(-1)^a |1>
Phase
|a>
S
exp(iaπ/2) |a>
π/8
|a>
T
exp(iaπ/4) |a>


Multi-qubit gate
|a>
U
|b>
|ψin> = |a> |b>
|ψout> = (U |a>)|b>

4.3 Controlled Operations

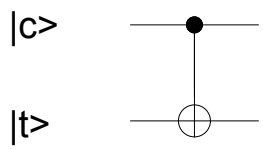
if ‘ A ’ is true then do ‘ B ’

- controlled qubit: |c>
- target qubit : |t>

- C – NOT (*If* |c> = |1> *then flip* |t>):

- |c>|t> —— operation ——→ |c> |t⊕c>

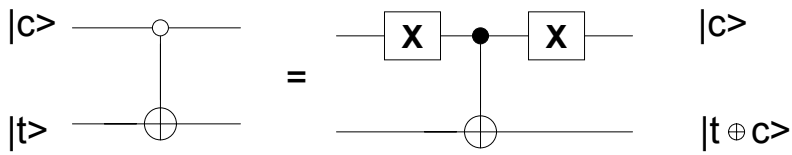
	00	01	10	11
00	1	0	0	0
01	0	1	0	0
10	0	0	0	1
11	0	0	1	0



- C – NOT (*if* $|c\rangle = |0\rangle$ *then flip* $|t\rangle$):

- $|c\rangle|t\rangle$ —operation→ $|c\rangle\ |t \oplus c\rangle$

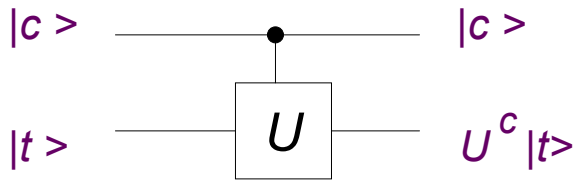
	00	01	10	11
00	0	1	0	0
01	1	0	0	0
10	0	0	1	0
11	0	0	0	1



The Controlled-*U*

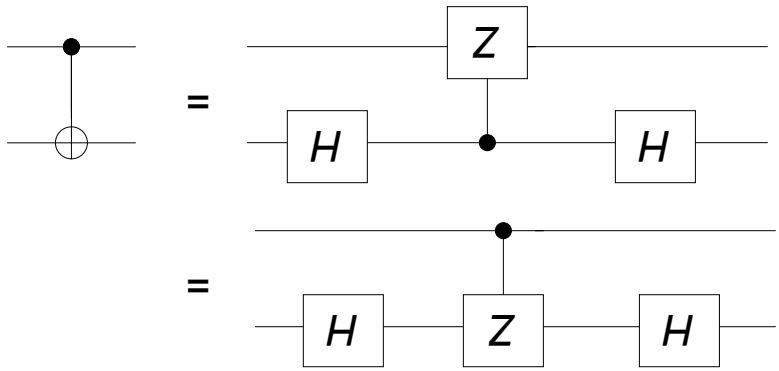
- is a two qubits operation as

$$|c\rangle|t\rangle \Rightarrow |c\rangle U^{c} |t\rangle$$



Example

- C-NOT is a controlled-Z gate:



See Ex. 4.17 and 4.18

C-NOT

- The role of 'control' and 'target' qubits depends on the chosen basis:

  the role of control and target qubits is completely interchanged in the basis

$|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ $\quad |-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$

$|0\rangle|0\rangle \xrightarrow{C\text{-}N} |0\rangle|0\rangle$ $\quad |+\rangle|+\rangle \xrightarrow{C\text{-}N} |+\rangle|+\rangle$

$|0\rangle|1\rangle \longrightarrow |0\rangle|1\rangle$ $\quad |-\rangle|+\rangle \longrightarrow |-\rangle|+\rangle$

$|1\rangle|0\rangle \longrightarrow |1\rangle|1\rangle$ $\quad |+\rangle|-\rangle \longrightarrow |-\rangle|-\rangle$

$|1\rangle|1\rangle \longrightarrow |1\rangle|0\rangle$ $\quad |-\rangle|-\rangle \longrightarrow |+\rangle|-\rangle$

Blue = control qubit Red = target qubit

See Exe. 4.20

The Controlled-*U*

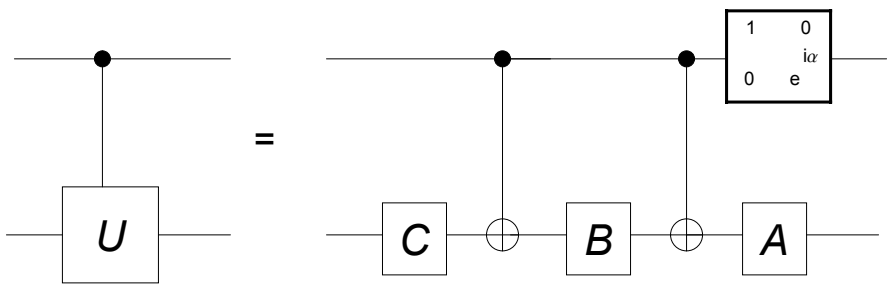
- Can we express the controlled-*U* in terms of single qubit operations and CNOT gate?

yes

$$U = \exp(i\alpha)\, A\, X\, B\, X\, C$$

The Controlled-*U*

- We can simulate the controlled-*U* gate by using the CNOT and any single qubit gates:

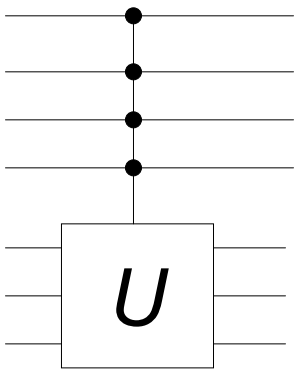


The Controlled-*U*

In general for $n+k$ qubits and U is a k qubit unitary operator :

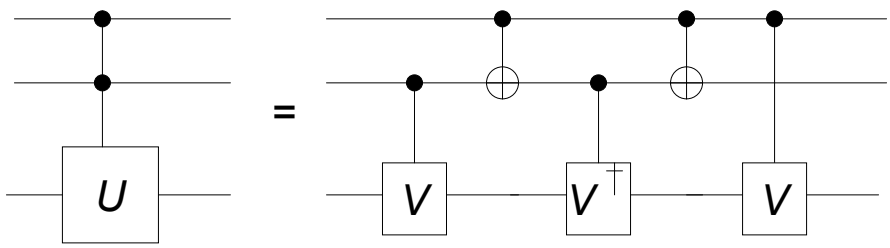
$$C^n(U)|x_1x_2..x_n\rangle|\psi\rangle = |x_1x_2\ldots x_n\rangle U^{x_1x_2\ldots x_n}|\psi\rangle$$

$n=4,\ k=3$



$C^2(U)$:

we can express $C^2(U)$ by using any unitary operator V such that $V^2=U$

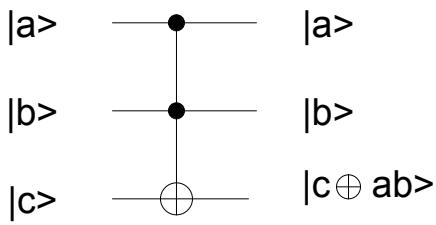


$C^2(U)$:

- $|a,b,x\rangle \rightarrow |a\rangle|b\rangle V^b |x\rangle$ (V)
- $\rightarrow |a\rangle |b \oplus a\rangle V^b |x\rangle$ (C-NOT)
- $\rightarrow |a\rangle |b \oplus a\rangle (V^\dagger)^{b \oplus a} V^b |x\rangle$ ($V^\dagger$)
- $\rightarrow |a\rangle |b \oplus a \oplus a\rangle (V^\dagger)^{b \oplus a} V^b |x\rangle$ (C-NOT)
- $\rightarrow |a\rangle |b\rangle V^a (V^\dagger)^{b \oplus a} V^b |x\rangle$ (V)
- $U^{ab} = V^a (V^\dagger)^{b \oplus a} V^b$ if $V^2 = U$

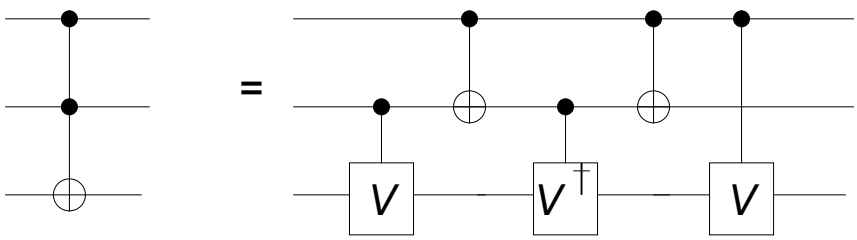
- One and two qubit reversible gates are sufficient to simulate $C^2(U)$
- This decomposition is *valid* in quantum computing *only*.
- In classical computation you cannot build a circuit using only one and two bit reversible logic gates, see problem 3.5
- We can simulate Toffoli gate by using one and two qubit unitary operations

The Toffoli gate



$$|a\rangle|b\rangle|c\rangle \longrightarrow |a\rangle|b\rangle X^{ab} |c\rangle$$

Toffoli Gate: $C^2(X)$



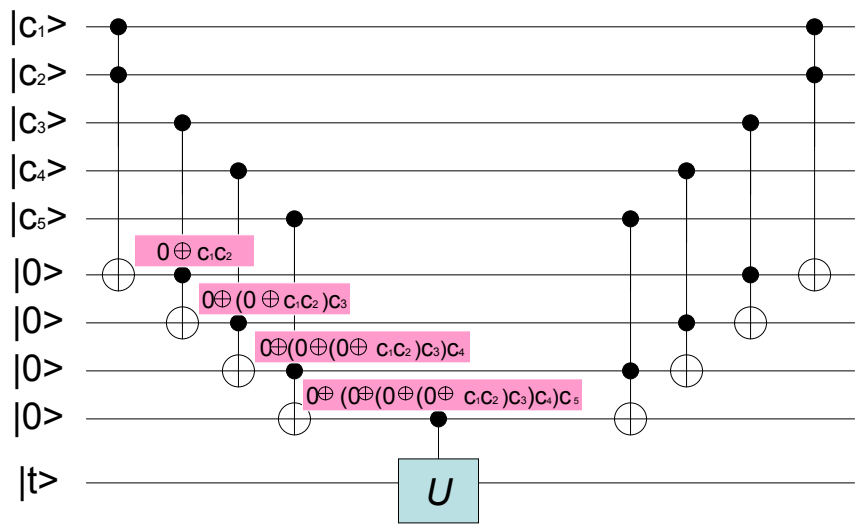
$V=(1-i)(I+iX)/2, \quad V^2=X$

$C^n(U)$

- How we can implement $C^n(U)$ for an unitary operator U by using our known gates?

- simplest way:
  - n control qubits
  - $n-1$ working qubits (all start and end in the state |0>)
  - target qubit

$C^5(U)$



$C^5(U)$ - matrix operations

$|c_1 \ldots c_5;\ 0,0,0,0;\ t\rangle \longrightarrow$

c_1c_2 $(0 \oplus c_1c_2)c_3$ $(0 \oplus (0 \oplus c_1c_2)c_3)c_4$ $(0 \oplus (0 \oplus (0 \oplus c_1c_2)c_3)c_4)c_5$

X X X X

$0 \oplus (0 \oplus (0 \oplus (0 \oplus c_1c_2)c_3)c_4)c_5$

U

$(0 \oplus (0 \oplus (0 \oplus c_1c_2)c_3)c_4)c_5$ $(0 \oplus (0 \oplus c_1c_2)c_3)c_4$ $(0 \oplus c_1c_2)c_3$ c_1c_2

X X X X

$|c_1 \ldots c_5;\ 0,0,0,0;\ t\rangle = |c_1 \ldots c_5;\ 0,0,0,0;\ t \oplus [\ 0 \oplus (0 \oplus (0 \oplus (0 \oplus c_1c_2)c_3)c_4)c_5]\rangle$

Exercises:

- Ex. 4.3; 4.4; 4.7; 4.8; 4.10; 4.12; 4.13; 4.15; 4.16; 4.18; 4.20; 4.21; 4.22; 4.23; 4.24; 4.25; 4.28; 4.31

Chapter 4

QUANTUM CIRCUITS

Part II

Lecture 8

Vahid Rezania

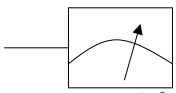
May-June 2002

Overview

- Deferred and implicit measurements
- Universality

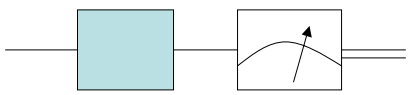
4.2 Measurement

- final element in a circuit

- $|\psi>$  denotes a projective measurement in the computational basis
- general measurement can always represented by unitary transforms with ancilla qubits followed by projective measurement, see sect. 2.2.6

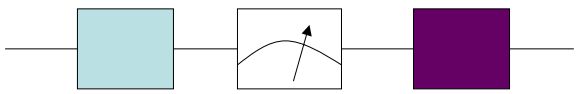
Measurement

- the role of measurements in quantum circuits is considered as an interface between quantum and classical worlds
- measurement is an irreversible operation, destroying quantum information and replacing with classical information (except teleportation and quantum error correction, see chap. 10)



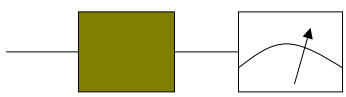
Deferred Measurement

- Principle of deferred measurement:
- Consider we have an algorithm that performs some quantum operations, measures, and then applies more quantum operations (depending on the outcome of the quantum measurement).



Deferred Measurement

- We can simulate this entire algorithm by a completely quantum algorithm with only one final measurement

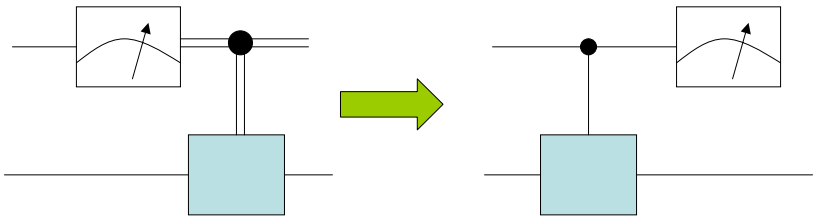


- How?

Deferred Measurement

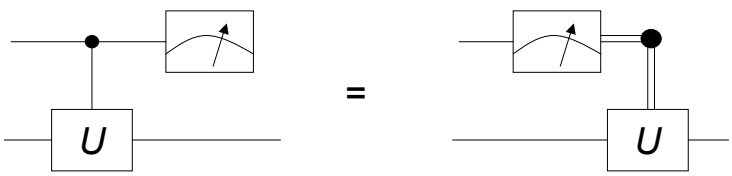
- Replace classically controlled operations with controlled quantum operations,

see figure 1.13



Measurement commutes with controlled operation

- Suppose we use a qubit to control a quantum operation U, and then we measure the qubit.
- We could equivalently first measure the control qubit, and then use the measurement result to classically control the application of U



Implicit Measurement

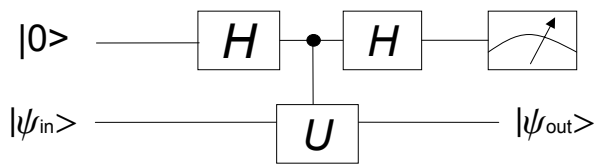
- Principle of implicit measurement:

  If some qubits in a computation are never used again, you can assume that they have been measured (and the result ignored)

⇨ The reduced density matrix is not affected by the measurement, see Ex. 4.32

The kicked-back trick

Consider the following circuit



if $U|\psi_{in}\rangle = \lambda|\psi_{in}\rangle$, $\lambda = +1, -1$ (U Hermitian-unitary)

$|\psi_{out}\rangle = |0\rangle|\psi_{in}\rangle$ for $\lambda = +1$

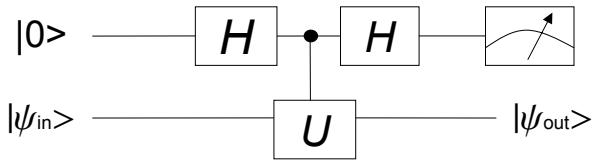
$|\psi_{out}\rangle = |1\rangle|\psi_{in}\rangle$ for $\lambda = -1$

⇨ result indicate one its eigenvalues

⇨ U is measured

The kicked-back trick

generally if $U|\psi_{in}\rangle = e^{i\varphi}|\psi_{in}\rangle$



$|0\rangle|\psi_{in}\rangle \rightarrow (|0\rangle + |1\rangle)|\psi_{in}\rangle$ *(H)*

$\rightarrow (|0\rangle + e^{i\varphi}|1\rangle)|\psi_{in}\rangle$ *(C-U)*

$\rightarrow [(1+e^{i\varphi})|0\rangle + (1-e^{i\varphi})|1\rangle]|\psi_{in}\rangle$ *(H)*

$= e^{i\varphi/2}[\cos(\varphi/2)|0\rangle + \sin(\varphi/2)|1\rangle]|\psi_{in}\rangle$

⇨ $|\psi_{in}\rangle$ is not altered (auxiliary state)

⇨ $e^{i\varphi}$ is kicked-back

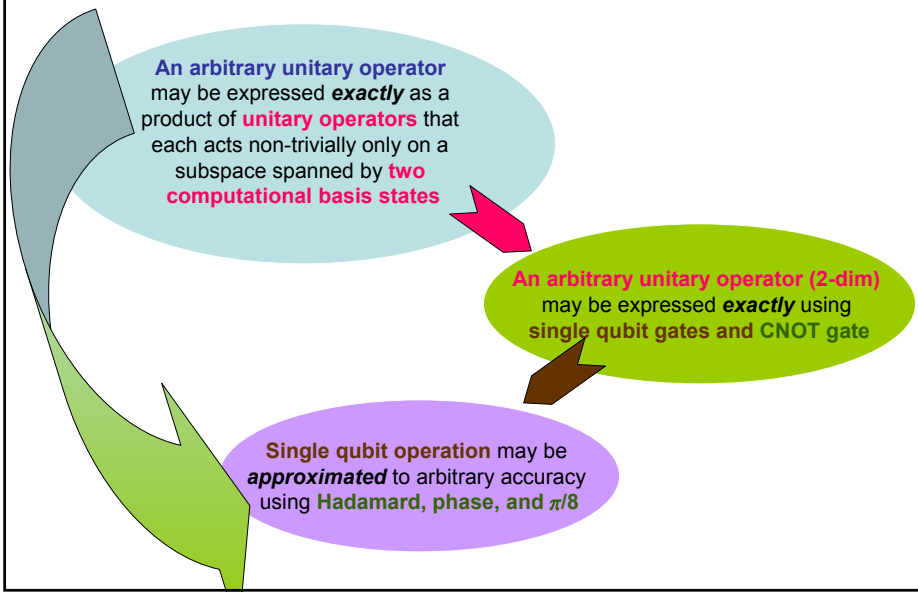
4.5 Universal quantum gates

- In classical computation any classical function can be computed by a small set of gates like AND, OR, XOR, NOT, NAND ⇨ Universal gates
- What is universal gate in quantum computing?

  a set of gates is called universal for quantum computation, if any unitary operation may be approximated to arbitrary accuracy $\epsilon > 0$ by a quantum circuit involving universal gates, for example:

  { Hadamard, CNOT, phase, $\pi/8$ }

Universality construction



Universality construction

How many gates must be composed to create a given unitary operation?

- Depends on initial qubits
- There exist unitary operations which require exponentially many gates to approximate.

First construction:
Two-level unitary gates

Two-level matrix:

Consider 3x3 matrix (in 3-dimensions vector space) as

$$A = \begin{vmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 1 \end{vmatrix}$$

Its operation changes the first two components of a vector (x, y, z) only:

$$\begin{vmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 1 \end{vmatrix} \begin{vmatrix} x \\ y \\ z \end{vmatrix} = \begin{vmatrix} ax+by \\ cx+dy \\ Z \end{vmatrix}$$

⇨ A is a two-level

First construction:
Two-level unitary gates

Note:

All following 3x3 matrices are two-level matrices:

$$\begin{vmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 1 \end{vmatrix} \quad \begin{vmatrix} a & 0 & b \\ 0 & 1 & 0 \\ c & 0 & d \end{vmatrix} \quad \begin{vmatrix} 1 & 0 & 0 \\ 0 & a & b \\ 0 & c & d \end{vmatrix}$$

First construction:
Two-level unitary gates

Suppose we have a unitary matrix (dxd) U as

$$U = \begin{vmatrix} a_{11} & a_{12} \dots & a_{1d} \\ a_{21} & a_{22} \dots & a_{2d} \\ \vdots & \vdots & \vdots \\ a_{d1} & a_{d2} \dots & a_{dd} \end{vmatrix}$$

We can find two-level matrices $U_1, \dots, U_{d-1}$ such that the matrix $U_{d-1}\, U_{d-2} \dots U_2 U_1 U$ has a one in the top left hand corner, and all zero elsewhere in the first row and column :

First construction:
Two-level unitary gates

$$U_{d-1}\, U_{d-2} \dots U_2 U_1 U = \begin{vmatrix} 1 & 0 \dots & 0 \\ 0 & b_{11} \dots & b_{1d-1} \\ \vdots & \vdots & \vdots \\ 0 & b_{d-1\,2} \dots & b_{d-1\,d-1} \end{vmatrix}$$

We then repeat this procedure for the *d-1* by *d-1* unitary submatrix, and so on, with the end result that

$$U = V_1 \dots V_K$$

where the matrices V_i are two-level unitary matrices with $K \leq d(d-1)/2$

First construction:
Two-level unitary gates

Example:

For $d = 3$ we can find two-level matrices U_1, U_2 and U_3 such that

$$U_3 U_2 U_1 U = I$$

or

$$U = U_1^\dagger U_2^\dagger U_3^\dagger$$

Second construction:
Single qubit and CNOT gates are universal

Consider a two-level unitary matrix U as

$$U = \begin{vmatrix} a & 0 & 0 & 0 & 0 & 0 & 0 & c \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ b & 0 & 0 & 0 & 0 & 0 & 0 & d \end{vmatrix}$$

U non-trivially acts on the states |000> and |111>:

U |000> = a |000> + b |111>

U |111> = c |000> + d |111>

U |x> = |x> for |x> $\neq$ |000> and |111>

Second construction:
Single qubit and CNOT gates are universal

We wish to implement U by using CNOT and a single qubit operation $\tilde{U}$ (submatrix of U) as

$$\tilde{U} = \begin{vmatrix} a & c \\ b & d \end{vmatrix}$$

Let set |s> = |000> and |t> = |111>. We can find a sequence between |s> and |t> such that adjacent members of the list differ in exactly one bit (Gray code) :

Second construction:
Single qubit and CNOT gates are universal

$\|g_1\rangle$	0	0	0
$\|g_2\rangle$	0	0	1
$\|g_3\rangle$	0	1	1
$\|g_4\rangle$	1	1	1

where $|g_1\rangle$ to $|g_4\rangle$ are Gray sequence. In general we can find m sequences between $|s\rangle = |g_1\rangle$ and $|t\rangle = |g_m\rangle$.

Second construction:
Single qubit and CNOT gates are universal

To express U as a product of CNOT and single qubit operation $\tilde{U}$ gates:

Step 1: apply the permutation (by CNOT gates) on the first m-1 sequences ($|g_1\rangle$, …, $|g_{m-1}\rangle$) such that (swap operation)

$$|g_1\rangle \longrightarrow |g_{m-1}\rangle$$
$$|g_2\rangle \longrightarrow |g_1\rangle$$
$$|g_3\rangle \longrightarrow |g_2\rangle$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$|g_{m-1}\rangle \longrightarrow |g_{m-2}\rangle$$

Second construction:
Single qubit and CNOT gates are universal

Step 2: suppose $|g_{m-1}\rangle$ and $|g_m\rangle$ differ in the j-th bit.

Apply a controlled-$\tilde{U}$ operation with j-th bit as target, conditional on the other qubits having the same values as appear in both $|g_{m-1}\rangle$ and $|g_m\rangle$.

Step 3: Undo the swap operations (inverse permutation): swap $|g_{m-1}\rangle$ with $|g_{m-2}\rangle$, then $|g_{m-2}\rangle$ with $|g_{m-3}\rangle$, …, and then $|g_2\rangle$ with $|g_1\rangle$.

Second construction:
Single qubit and CNOT gates are universal

Back to our example we need to swap

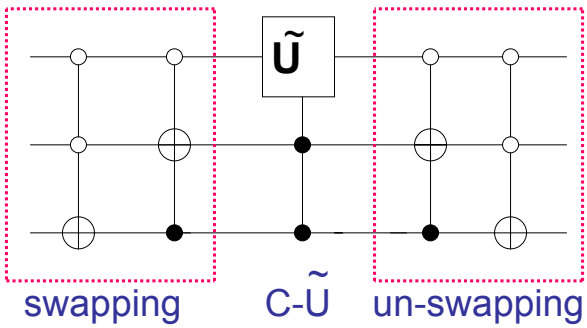
$|g_1\rangle$ with $|g_3\rangle$,

$|g_2\rangle$ with $|g_1\rangle$,

$|g_3\rangle$ with $|g_2\rangle$,

then apply controlled-$\tilde{U}$ on a different bit of $|g_3\rangle$ and $|g_4\rangle$ (the first bit on each) as target, and finally unswap. So one can build the following circuit:

Second construction:
Single qubit and CNOT gates are universal



Second construction:
Single qubit and CNOT gates are universal

- CNOT and Single qubit unitary gates together form a Universal set for quantum computation.

Third construction:
Approximating unitary operators

- Although CNOT and single qubit gates form a universal set, no method is known to implement all these gates in a fashion which is resistant to errors (see chap. 10).

- There is a discrete set to perform universal quantum computation.

Third construction: Approximating unitary operators

- Why approximate?

- The set of unitary operations is continuous.
  ($U = \exp(i\alpha) R_z(\beta) R_y(\gamma) R_z(\delta)$)

⇨ A discrete set cannot exactly implement an arbitrary unitary operation.

Third construction: Approximating unitary operators

We define the error when V is implemented instead of U by

$$E(U,V) = \max_{|\psi\rangle} \| (U-V)|\psi\rangle \|$$

where maximum is over all normalized quantum state $|\psi\rangle$.

Third construction: Approximating unitary operators

This definition has a reasonable interpretation that if $E(U,V) < \epsilon$, then the probability P of any outcome after measuring $U|\psi\rangle$ is within 2ϵ of the probability of obtaining the same outcome after measuring $V|\psi\rangle$. More precisely

$$| P_U - P_V | \leqq 2E(U,V) \leqq 2\epsilon$$

for any POVM operator M.

Third construction: Approximating unitary operators

- Further, if we have a sequence of gates $V_1,\ldots, V_m$ intended to approximate some other sequence of gates $U_1,\ldots, U_m$, then the errors add at most linearly:

$$E(U_m U_{m-1}\ldots U_1, V_m V_{m-1}\ldots V_1) \leqq \sum_{j=1}^{m} E(U_j, V_j)$$

so it suffices to have $E(U_j, V_j) \leqq \epsilon/(2m)$

Third construction: Approximating unitary operators

Now we need to show that the following set of gates is universal:

$$\{ \text{Hadamard, CNOT, phase, } \pi/8 \}$$

Remember (Ex. 4.4 and 4.11): up to global phase

$T = R_z(\pi/4)$

$HTH = R_x(\pi/4)$

Third construction: Approximating unitary operators

- The operation

$$THTH = R_{\mathbf{n}}(\theta)$$

$$\mathbf{n} = (\cos(\pi/8), \sin(\pi/8), \cos(\pi/8))$$

$$\cos(\theta) = \cos^2(\pi/8)$$

- As it clear with H and T gates we can construct $R_{\mathbf{n}}(\theta)$
- θ is irrational multiple of 2π

Third construction: Approximating unitary operators

- Repeated iteration of $R_n(\theta)$ can be used to approximate to arbitrary accuracy any rotation operation $R_n(\alpha)$.

Proof: Define θ_k such that $\theta_k \in [0, 2\pi)$ and $\theta_k = (k\,\theta) \bmod 2\pi$, for k=1,…, N (integer N > 1/desired accuracy). So the pigeonhole principle implies that there are distinct **j** and **k** **(k > j)** such that $|\theta_k - \theta_j| < 2\pi/\mathbf{N}$.

⇨ This means that $\mathbf{0} < |\theta_{k-j}| < 2\pi/\mathbf{N}$.

Third construction: Approximating unitary operators

⇨ it follows that the sequence θ_{k-j}, $\theta_{2(k-j)}$, $\theta_{3(k-j)}$, … fills up the interval $[0, 2\pi)$ and form a ' net ' of width $\delta < 2\pi/\mathbf{N}$

⇨ it follows that for any $\epsilon > 0$ there exists an k such that

$$E(R_n(\alpha), R_n^k(\theta)) < \epsilon/3$$

Third construction: Approximating unitary operators

Since

$$H\, R_n(\alpha)\, H = R_m(\alpha)$$

$$\mathbf{m} = \left(\cos(\pi/8),\ -\sin(\pi/8),\ \cos(\pi/8) \right)$$

we can write also

$$E(R_m(\alpha),\ R_m^k(\theta)) < \epsilon/3$$

Third construction: Approximating unitary operators

And finally from $U = \exp(i\alpha)\, R_n(\beta)\, R_m(\gamma)\, R_n(\delta)$

we find

$$E(U,\ R_n^{k_1}(\theta)\, H\, R_n^{k_2}(\theta)\, H\, R_n^{k_3}(\theta)) < \epsilon$$

For suitable positive integers k_1, k_2, and k_3

⇨ This means that *any* single qubit unitary operator U *can be approximated* up to given value $\epsilon > 0$ by a circuit composed of Hadamard and $\pi/8$ gates *only*.

Third construction: Approximating unitary operators

- Combining with result of the second step, one may approximate a given circuit with *m* gates, using Hadamard, CNOT and $\pi/8$ gates.

Third construction: Approximating unitary operators

How efficient is it?

Solovay and Kitaev showed that to approximate an arbitrary single qubit gate up to an accuracy ϵ, one needs to use $O(\log^c(1/\epsilon))$ gates from the discrete set, where c ~ 2 (Solovay-Kitaev theorem).

⇨ to approximate a circuit with *m* gates, we needs

$$O(m \log^c(m/\epsilon))$$

which is poly-logarithmic increase over the original circuit.

Approximating unitary gates is generically hard

- Is it always possible to build up an arbitrary unitary operator efficiently?
- or for given U on *n* qubits, does there always exist a circuit of size polynomial in *n* approximating U?
- NO
- How many gates does need to generate an arbitrary state of *n* qubits?
- Requires exponentially many operators:

$$\Omega(2^n \log(1/\epsilon)/\log n)$$

Approximating unitary gates is generically hard

- To within a polynomial factor the construction for universality is optimal

- But it does not address the problem of determining which families of unitary operators can be computed efficiently in the quantum circuit model.

Exercises

- Ex. 4.32; 4.34; 4.35; 4.37; 4.38; 4.39; 4.40; 4.41; 4.44

Chapter 4

QUANTUM CIRCUITS

Part III

Lecture 9

Vahid Rezania

May-June 2002

Overview

- Quantum computational complexity
- Simulation of quantum circuit

4.5.5 Quantum computational Complexity

- Classical classification of resources:
  - Class P - time to solve: $O(\text{poly}(|\text{input}|))$
  - Class NP - time to verify: $O(\text{poly}(|\text{input}|))$
  - Class NP-complete - any other NP problem is reducible to it
  - Class NPI - NP but not NP-complete

  - Class PSPACE - space to solve: $O(\text{poly}(|\text{input}|))$
  - class EXP - space to solve: $O(2^{\text{poly}(|\text{input}|)})$

Quantum Computation Complexity
PSAPCE - class

- Class PSPACE
  - class of decision problems
  - can be solved on a Turing machine
  - using space polynomial in the problem size
  - using an arbitrary amount of time.

Quantum Computation Complexity
BQP - class

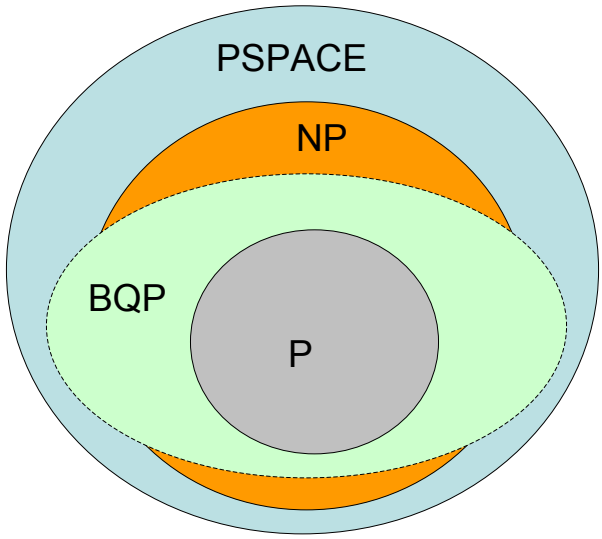
- Class BQP
  - an essentially quantum complexity class
  - contains decision problems that can be solved with bounded probability of error
  - using a polynomial size quantum circuit.

Quantum Computation Complexity
BPP - class

Class BPP
- classical complexity class
- contains decision problems that can be solved with bounded probability of error
- using polynomial time on a classical Turing machine

- It is clear that $BPP \subseteq BQP$

Quantum Computation Complexity



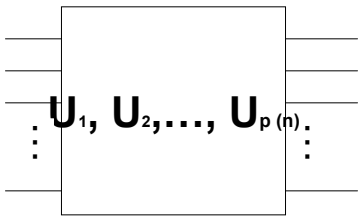
Quantum Computation Complexity
BQP in PSAPCE

- We wish to show that BQP $\subseteq$ PSAPCE, ie. any language L for which a quantum algorithm can decide with bounded error in polynomial size quantum circuit, *can* be decided by a classical machine using *only* space polynomial,

$$L \in BPQ \Rightarrow L \in PSPACE$$

Quantum Computation Complexity
BQP in PSAPCE

Suppose we have an *n* qubits quantum computer with *p(n)* gates, where *p(n)* is some polynomial in *n:*



and let the quantum circuit starts in the state |0>

Quantum Computation Complexity
BQP in PSAPCE

The probability that it ends up in the state |y> is

$$\langle y|\, U_{p(n)} \ldots U_2 U_1 |0\rangle$$

$$= \sum_{x_1, \ldots, x_{p(n)-1}} \langle y|U_{p(n)}|x_{p(n)-1}\rangle\langle x_{p(n)-1}|U_{p(n)-1}\ldots U_2|x_1\rangle\langle x_1|U_1|0\rangle$$

(inserting $\sum_x |x\rangle\langle x| = I$)

Quantum Computation Complexity
BQP in PSAPCE

- Each individual unitary gates are operations such as Hadamard gate, CNOT, etc.
- So each term can be calculated to high accuracy using only polynomial space on a classical computer

⇨ the whole can be calculated using polynomial space

⇨ BQP ⊆ PSAPCE

Quantum Computation Complexity

- Any arbitrary quantum computation can be simulated on a classical computer, no matter the length of the quantum computation

- The class of problems solvable on a quantum computer with unlimited time and space resources is no larger than the class of problems solvable on a classical computer

Quantum Computation Complexity

⇨ quantum computers do not violate the Church-Turing thesis:

any algorithmic process can be simulated using a Turing machine

4.6 Summary of the quantum circuit model

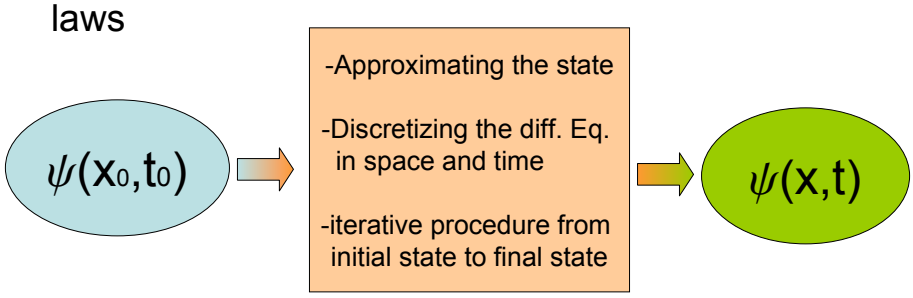
- Classical resources
- A suitable state space: $|x_1, \ldots, x_n\rangle$
  2^n-dimensional complex Hilbert space
- Ability to prepare states in computational basis
  any computational basis $|x_1, \ldots, x_n\rangle$ can be prepared in n steps

4.6 Summary of the quantum circuit model

- Ability to perform quantum gates
  - gates can be applied to any subset of qubits
  - universal gates
- Ability to perform measurements in the computational basis

4.7 Simulation of quantum systems

- Finding solution of integro-differential equations of a dynamical system which is governed by physics laws



- The error is *bounded*
- *Not* all dynamical systems can be simulated efficiently

4.7 Simulation of quantum systems

- Simulation of quantum systems by classical computers is possible, but *very inefficiently*
- The *exponential* of number of differential equations

$$i \frac{d}{dt} |\psi\rangle = H |\psi\rangle$$

- For *n* qubits $\longrightarrow$ 2^n equations

4.7.2 Quantum simulation algorithm time-independent Hamiltonian

- A system starting in $|\psi(0)\rangle$
- A time-independent Hamiltonian operator H, operates on the state over a period of time t
- System evolves to $|\psi(t)\rangle = e^{-iHt} |\psi(0)\rangle$
- The first order approximation

$$|\psi(t + \Delta t)\rangle \simeq (I - iH \Delta t)|\psi(t)\rangle$$

4.7.2 Quantum simulation algorithm time-independent Hamiltonian

Example:

the Hamiltonian of a spin - $\frac{1}{2}$ particle in a uniform magnetic field along the z-axis is

$$H = cZ = \begin{vmatrix} c & 0 \\ 0 & -c \end{vmatrix} \qquad c = (eB/mC)$$

Then after a time t

$$|0\rangle \longrightarrow e^{-ict}|0\rangle$$
$$|1\rangle \longrightarrow e^{ict}|1\rangle$$

4.7.2 Quantum simulation algorithm time-independent Hamiltonian

Example (continue):

for two non-interacting spin - $\frac{1}{2}$ particles in a uniform magnetic field along the z-axis will be

$$H = c_1 Z \otimes I + c_2 I \otimes Z = \begin{vmatrix} c_1 + c_2 & 0 & 0 & 0 \\ 0 & c_1 - c_2 & 0 & 0 \\ 0 & 0 & -c_1 + c_2 & 0 \\ 0 & 0 & 0 & -c_1 - c_2 \end{vmatrix}$$

4.7.2 Quantum simulation algorithm time-independent Hamiltonian

Example (continue):

but for two interacting spin - $\frac{1}{2}$ particles in a uniform magnetic field along the z-axis we have

$$H = c_1 Z \otimes I + c_2 I \otimes Z + j_{12} Z \otimes Z =$$

$$\begin{vmatrix} c_1 + c_2 + j_{12} & 0 & 0 & 0 \\ 0 & c_1 - c_2 - j_{12} & 0 & 0 \\ 0 & 0 & -c_1 + c_2 - j_{12} & 0 \\ 0 & 0 & 0 & -c_1 - c_2 + j_{12} \end{vmatrix}$$

4.7.2 Quantum simulation algorithm time-independent Hamiltonian

- Generally in most physical systems, the Hamiltonian can be written as a sum over many local interactions (subsystems)

$$H = \sum_{k=1}^{L} H_k$$

where H_k acts on small number of subsystems and L is a polynomial of number of subsystems

4.7.2 Quantum simulation algorithm
time-independent Hamiltonian

- We can choose the subsystems such that each $e^{iH_k t}$ would be easy to simulate

- But in general we have $[H_k, H_j] \neq 0$ then

$$e^{-iHt} \neq \prod_k e^{-iH_k t}$$

- How can construct e^{-iHt} from $e^{-iH_k t}$?

4.7.2 Quantum simulation algorithm
approximating Hamiltonian

- We can approximate e^{-iHt}

- Theorem 4.3: Let A and B be Hermitian operators. Then for any real t,

$$\lim_{n \to \infty} \left(e^{iAt/n} e^{iBt/n} \right)^n = e^{i(A+B)t}$$

(Trotter formula)

4.7.2 Quantum simulation algorithm approximating Hamiltonian

Example:

$$e^{i(A+B)\Delta t} = e^{iA\Delta t}\, e^{iB\Delta t} + O(\Delta t^2)$$

$$e^{i(A+B)\Delta t} = e^{iA\Delta t/2}\, e^{iB\Delta t}\, e^{iA\Delta t/2} + O(\Delta t^3)$$

time-independent Hamiltonian Simulation algorithm

- Inputs:

  - $H = \sum_k H_k$ H_k acting on N-dimensional system, where each H_k acts on small subsystem of size independent of N
  - initial state $|\psi_0\rangle$ of the system at t=0
  - a positive, non-zero accuracy $\delta > 0$
  - a final time t_f at which the evolved state is desired

time-independent Hamiltonian Simulation algorithm

- Outputs:

A state $|\tilde{\psi}(t_f)\rangle$ such that

$$|\langle\tilde{\psi}(t_f)|\, e^{-iHt_f} |\psi_0\rangle|^2 \geq 1 - \delta$$

- Runtime:

$O(\text{poly}(1/\delta, L, t_f))$ operations

time-independent Hamiltonian Simulation algorithm

- Procedure:

- choose a representation $|\tilde{\psi}\rangle$ of n=poly(log N) qubits to approximate the system
- choose Δt such that the expected error is acceptable and $m\Delta t = t_f$ for integer m
- approximate each $e^{-iH_k\Delta t}$ with accuracy $O(\delta/m)$ with efficient quantum circuit
- construct the corresponding quantum circuit $U_{\Delta t}$ for the iterative steps (see Ex. 4.50)

time-independent Hamiltonian
Simulation algorithm

- Procedure (continue):

do:

1- $|\tilde{\psi}_0\rangle \longleftarrow |\psi_0\rangle$; j=0 — initial state

2- $\longrightarrow |\tilde{\psi}_{j+1}\rangle = U_{\Delta t} |\tilde{\psi}_j\rangle$ — iterative update

3- $\longrightarrow$ j = j+1; goto 2 untile j $\geq$ m — loop

4- $\longrightarrow |\psi(t_f)\rangle = |\tilde{\psi}_j\rangle$ — final state

time-independent Hamiltonian

- Actually these methods do *not* require the H_k be local

- H_k can be tensor products of local Hamiltonian

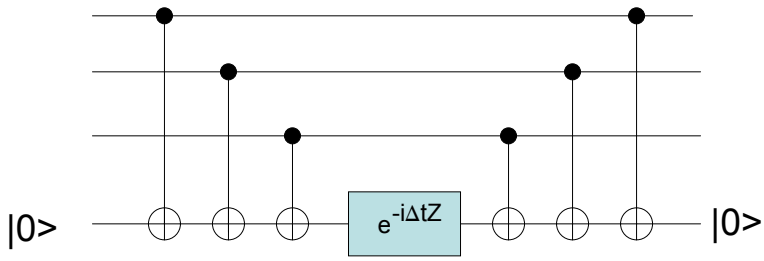
eg.

$$H = Z_1 \otimes Z_2 \otimes \ldots \otimes Z_n$$

which acts on an n qubit system.

time-independent Hamiltonian

For n=3 we can simulate the $e^{-iH\Delta t}$ by following quantum circuit



$H = Z_1 \otimes Z_2 \otimes Z_3$

time-independent Hamiltonian
Pauli matrices

- We can simulate arbitrary products of the Pauli matrices by using Hadamard gate *H*

Example:

$X = HZH \rightarrow e^{-iXt} = H\ e^{-iZt}\ H$

so

$e^{-iZ \otimes X \otimes X\, t} = I \otimes H \otimes H \,.\, e^{-iZ \otimes Z \otimes Z\, t} \,.\, I \otimes H \otimes H$

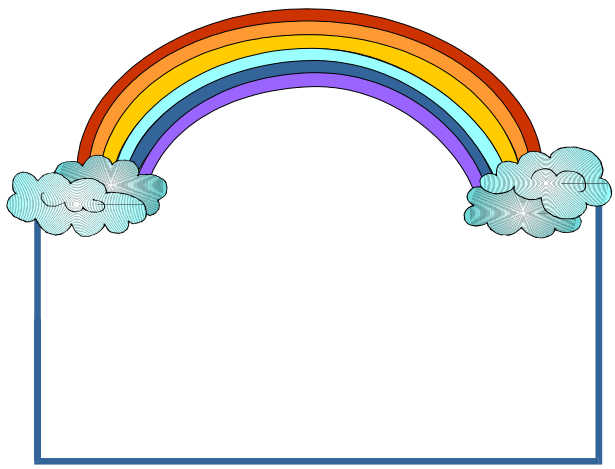
(prove it !)

Exercise

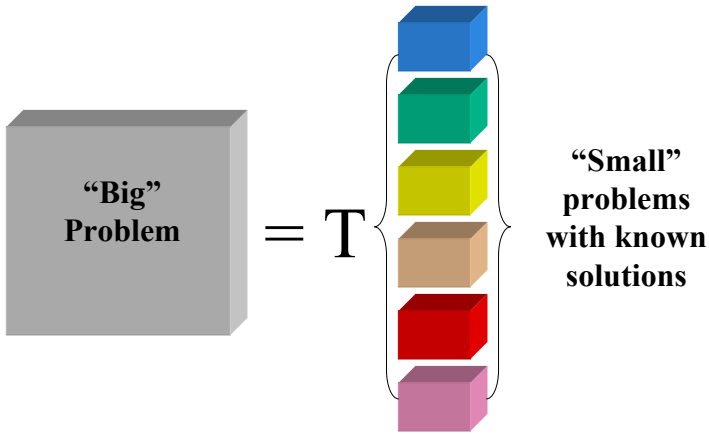
Ex. 4.46; 4.47; 4.49; 4.50; 4.51

The quantum Fourier transform and its application (Chapter 5)

Natural Fourier Transformer



5.1 The quantum Fourier transform



Discrete and quantum Fourier transforms

- Discrete Fourier transform

$$y_k \equiv \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{2\pi i j k / N}$$

- Quantum Fourier transform

$$|j\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} x_j e^{2\pi i j k / N} |k\rangle$$

- Equivalency

$$\sum_{j=0}^{N-1} x_j |j\rangle \rightarrow \sum_{k=0}^{N-1} y_k |k\rangle$$

Product Representation

For $N = 2^n$ and the basis

State $|j\rangle$ using the binary representation:

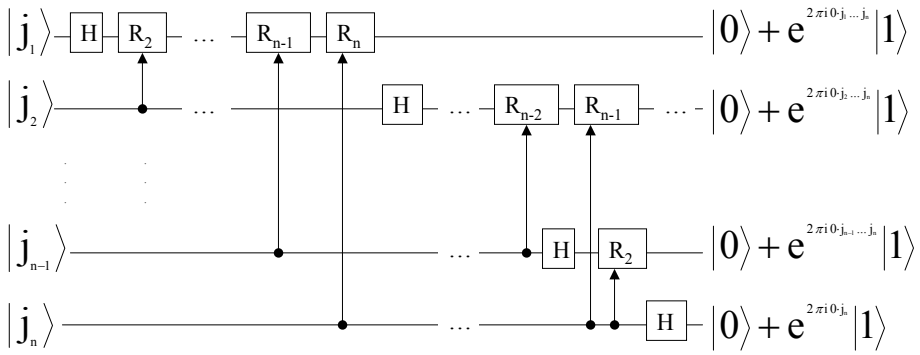
$$|0\rangle,\ldots,|2^n-1\rangle$$

$$j = j_1 j_2 \ldots j_n = j_1 2^{n-1} + j_2 2^{n-2} + \ldots + j_n 2^0$$

Product representation:

$$|j_1,\ldots,j_n\rangle \rightarrow \frac{(|0\rangle + e^{2\pi i 0.j_n}|1\rangle)(|0\rangle + e^{2\pi i 0.j_{n-1}j_n}|1\rangle)\cdots(|0\rangle + e^{2\pi i 0.j_1 j_2 \cdots j_n}|1\rangle)}{2^{n/2}}$$

Efficient circuit for the quantum Fourier transform

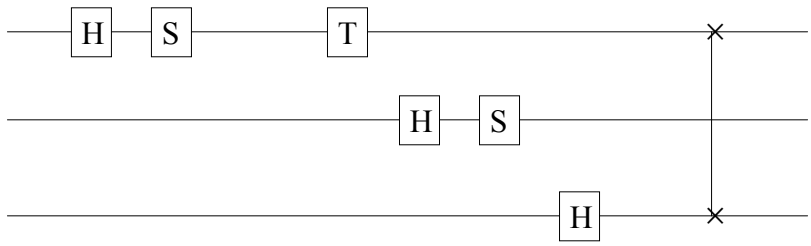


$$R_k \equiv \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{bmatrix}$$

Applying the Hadamard gate

$$\frac{1}{2^{1/2}}(|0\rangle + e^{2\pi i 0.j_1}|1\rangle)|j_2 \ldots j_n\rangle$$

Three qubit quantum Fourier transform



Recall that S and T are the phase and π/8 gates

Matrix representation of the quantum Fourier transform

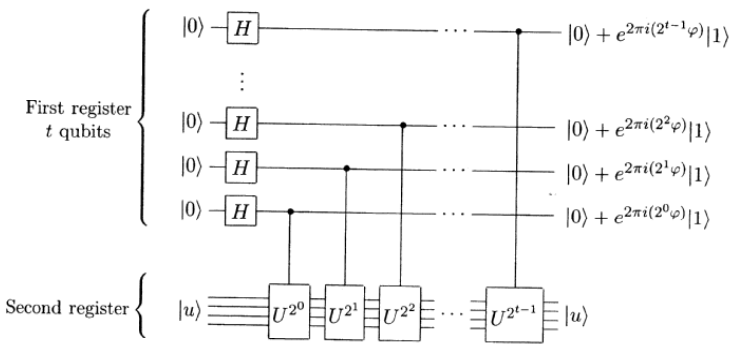
$$\omega = e^{2\pi i/8} = \sqrt{i}$$

$$\frac{1}{\sqrt{8}}\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 & \omega^7 \\ 1 & \omega^2 & \omega^4 & \omega^6 & 1 & \omega^2 & \omega^4 & \omega^6 \\ 1 & \omega^3 & \omega^6 & \omega^1 & \omega^4 & \omega^7 & \omega^2 & \omega^5 \\ 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 \\ 1 & \omega^5 & \omega^2 & \omega^7 & \omega^4 & \omega^1 & \omega^6 & \omega^3 \\ 1 & \omega^6 & \omega^4 & \omega^2 & 1 & \omega^6 & \omega^4 & \omega^2 \\ 1 & \omega^7 & \omega^6 & \omega^5 & \omega^4 & \omega^3 & \omega^2 & \omega^1 \end{bmatrix}$$

5.2 Phase estimation

- Suppose a unitary operator U has an eigenvector $|u\rangle$ with eigenvalue $e^{2\pi i\varphi}$
- The goal of the phase estimation algorithm is to estimate φ
- Phase estimation is performed in two stages:
  - Circuit representation by applying a Hadamard transform
  - Inverse quantum Fourier transform application

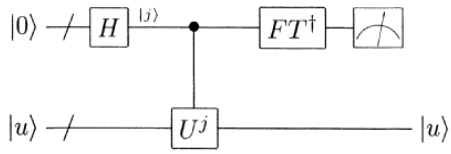
Phase estimation. First stage



$$\frac{1}{2^{t/2}}\left(|0\rangle + e^{2\pi i 2^{t-1}\varphi}|1\rangle\right)\left(|0\rangle + e^{2\pi i 2^{t-2}\varphi}|1\rangle\right)\ldots\left(|0\rangle + e^{2\pi i 2^{0}\varphi}|1\rangle\right)$$
$$= \frac{1}{2^{t/2}}\sum_{k=0}^{2^t-1} e^{2\pi i\varphi k}|k\rangle\,.$$

Phase estimation. Second stage

$$\frac{1}{2^{t/2}}\left(|0\rangle + e^{2\pi i 0.\varphi_t}|1\rangle\right)\left(|0\rangle + e^{2\pi i 0.\varphi_{t-1}\varphi_t}|1\rangle\right)\ldots\left(|0\rangle + e^{2\pi i 0.\varphi_1\varphi_2\cdots\varphi_t}|1\rangle\right)$$



$$\frac{1}{2^{t/2}}\sum_{j=0}^{2^t-1} e^{2\pi i\varphi j}|j\rangle|u\rangle \rightarrow |\tilde{\varphi}\rangle|u\rangle$$

5.2.1 Performance and requirements

$$\frac{1}{2^t}\sum_{k,l=0}^{2^t-1} e^{\frac{-2\pi i k l}{2^t}} e^{2\pi i\varphi k}|l\rangle \qquad \alpha_l \equiv \frac{1}{2^t}\sum_{k=0}^{2^t-1}\left(e^{2\pi i(\varphi-(b+l)/2^t)}\right)^k$$

$$\alpha_l = \frac{1}{2^t}\left(\frac{1-e^{2\pi i(2^t\varphi-(b+l))}}{1-e^{2\pi i(\varphi-(b+l)/2^t)}}\right) = \frac{1}{2^t}\left(\frac{1-e^{2\pi i(2^t\delta-l)}}{1-e^{2\pi i(\delta-l/2^t)}}\right)$$

$$p(|m-b|>e) = \sum_{-2^{t-1}<l\leq-(e+1)}|\alpha_l|^2 + \sum_{e+1\leq l\leq 2^{t-1}}|\alpha_l|^2$$

$$t = n + \left\lceil \log\left(2+\frac{1}{2\epsilon}\right)\right\rceil$$

Algorithm: Quantum phase estimation

Inputs: (1) A black box wich performs a controlled-U^j operation, for integer
(2) an eigenstate $|u\rangle$ of U with eigenvalue $e^{2\pi i\varphi_u}$, and (3) $t = n + \lceil \log\left(2 + \frac{1}{2\epsilon}\right)$
qubits initialized to $|0\rangle$.

Outputs: An n-bit approximation $\widetilde{\varphi_u}$ to φ_u.

Runtime: $O(t^2)$ operations and one call to controlled-U^j black box. Succeeds
with probability at least $1 - \epsilon$.

Procedure:

1.	$\|0\rangle\|u\rangle$	initial state
2.	$\rightarrow \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} \|j\rangle\|u\rangle$	create superposition
3.	$\rightarrow \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} \|j\rangle U^j\|u\rangle$	apply black box
	$= \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} e^{2\pi i j\varphi_u}\|j\rangle\|u\rangle$	result of black box
4.	$\rightarrow \|\widetilde{\varphi_u}\rangle\|u\rangle$	apply inverse Fourier transform
5.	$\rightarrow \widetilde{\varphi_u}$	measure first register

5.3 Applications: order-finding and factoring

- The fast quantum algorithm for order-finding and factoring are interesting for at least three reasons.
  - They provide evidence for the idea that quantum computers may be inherently more powerful than classical computers, and provide a credible challenge to the strong Church-Turing thesis.
  - Both problems are of sufficient intrinsic worth to justify interest in any novel algorithm, be it classical or quantum.
  - Efficient algorithms for order-finding and factoring can be used to break the RSA public-key cryptosystem.

5.3.1 Application: order-finding

$U|y\rangle \equiv |xy(\mathrm{mod}\ N)\rangle \qquad y \in \{0,1\}^L \ N \le y \le 2^L - 1$

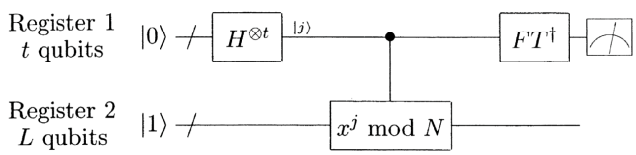
U only acts non-trivially when $0 \le y \le N-1$

$$|u_s\rangle \equiv \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \exp\left[\frac{-2\pi i s k}{r}\right] |x^k \bmod N\rangle$$

for integer $0 \le s \le r-1$ are eigenstates of U, since

$$\begin{aligned} U|u_s\rangle &= \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \exp\left[\frac{-2\pi i s k}{r}\right] |x^{k+1} \bmod N\rangle \\ &= \exp\left[\frac{2\pi i s}{r}\right] |u_s\rangle . \end{aligned}$$

Quantum circuit for the order-finding algorithm



Algorithm: Quantum order-finding

Algorithm: Quantum order-finding

Inputs: (1) A black box $U_{x,N}$ which performs the transformation $|j\rangle|k\rangle \rightarrow |j\rangle|x^j k \bmod N\rangle$, for x co-prime to the L-bit number N, (2) $t = 2L + 1 + \lceil \log\left(2 + \frac{1}{2\epsilon}\right) \rceil$ qubits initialized to $|0\rangle$, and (3) L qubits initialized to the state $|1\rangle$.

Outputs: The least integer $r > 0$ such that $x^r = 1 \pmod N$.

Runtime: $O(L^3)$ operations. Succeeds with probability $O(1)$.

Procedure:

1.	$\|0\rangle\|1\rangle$	initial state
2.	$\rightarrow \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} \|j\rangle\|1\rangle$	create superposition
3.	$\rightarrow \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} \|j\rangle\|x^j \bmod N\rangle$	apply $U_{x,N}$
	$\approx \frac{1}{\sqrt{r2^t}} \sum_{s=0}^{r-1} \sum_{j=0}^{2^t-1} e^{2\pi i s j / r} \|j\rangle\|u_s\rangle$	
4.	$\rightarrow \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} \|\widetilde{s/r}\rangle\|u_s\rangle$	apply inverse Fourier transform to first register
5.	$\rightarrow \widetilde{s/r}$	measure first register
6.	$\rightarrow r$	apply continued fractions algorithm

5.3.2 Application: factoring

Theorem 5.2: Suppose N is an L bit composite number, and x is a non-trivial solution to the equation $x^2 = 1 \pmod N$ in the range $1 \leq x \leq N$, that is, neither $x = 1 \pmod N$ nor $x = N - 1 = -1 \pmod N$. Then at least one of $\gcd(x - 1, N)$ and $\gcd(x + 1, N)$ is a non-trivial factor of N that can be computed using $O(L^3)$ operations.

Theorem 5.3: Suppose $N = p_1^{\alpha_1} \ldots p_m^{\alpha_m}$ is the prime factorization of an odd composite positive integer. Let x be an integer chosen uniformly at random, subject to the requirements that $1 \leq x \leq N - 1$ and x is co-prime to N. Let r be the order of x modulo N. Then

$$p(r \text{ is even and } x^{r/2} \neq -1 \pmod N) \geq 1 - \frac{1}{2^m}$$

Algorithm: Reduction of factoring to order-finding

Algorithm: Reduction of factoring to order-finding

Inputs: A composite number N

Outputs: A non-trivial factor of N.

Runtime: $O((\log N)^3)$ operations. Succeeds with probability $O(1)$.

Procedure:

1. If N is even, return the factor 2.
2. Determine whether $N = a^b$ for integers $a \geq 1$ and $b \geq 2$, and if so return the factor a (uses the classical algorithm of Exercise 5.17).
3. Randomly choose x in the range 1 to $N-1$. If $\gcd(x, N) > 1$ then return the factor $\gcd(x, N)$.
4. Use the order-finding subroutine to find the order r of x modulo N.
5. If r is even and $x^{r/2} \neq -1 \pmod{N}$ then compute $\gcd(x^{r/2} - 1, N)$ and $\gcd(x^{r/2} + 1, N)$, and test to see if one of these is a non-trivial factor, returning that factor if so. Otherwise, the algorithm fails.

QCSS

"Quantum Computing Summer School"

Prof. Vadim Bulitko
University of Alberta

Today

- Summary of Chapter 4
- CS questions on QC

Jean Baptiste Joseph Fourier

- Fourier transform re-cap
- Fourier transform applications
  - Period-finding
  - Discrete logarithms
  - The hidden subgroup problem
- Discussion

Peter Shor

Chapter 4 Refresher

- **Universality :** any unitary operation on n qubits can be done exactly with single qubit gates and C-NOTs
- **Discrete set universality :** can approximate any single qubit unitary operator with Hadamard, C-NOT, pi/8
- The number of these universal gates can be **exponential** in the number of qubits for some "tricky" unitary gates

Chapter 4 Refresher

- Recall : **BPP** -- polynomial *time* on a non-deterministic Turing machine to get a bounded error solution
- Define : **BQP** -- polynomial *circuit size* of a quantum circuit to get a bounded error solution (a finite universal gate set is used)
- **BQP** $\subseteq$ **PSPACE** (Turing machines with polynomial space requirements)
  - Possibly exponential time of the simulation
- **BPP** $\subseteq$ **BQP** $\subseteq$ **PSPACE**

Chapter 4 Refresher

- No violation of Church-Turing thesis:
  - *Anything a quantum machine can do we can approximate on a Turing machine*
- A possible violation of the strong Church-Turing thesis:
  - any computable process can be done efficiently (with at most a polynomial increase in the number of operations) on a non-deterministic Turing machine (p. 140)
  - Possible counter-example : factoring : polynomial on QC and exponential (?) on classical machines
  - Quantum search is not a counter-example : the speed up is quadratic and, therefore, polynomial

Chapter 4 : The Model

- In the book 'quantum computer' = 'quantum circuit model'
  - What is 'quantum circuit model'?
  - Classical part (for convinience)
  - 2^n dimensional Hilbert space
  - Ability to prepare basis states in at most n steps (each). We always start with the basis states
  - Ability to apply quanum gates to subsets
  - Universal discrete gate set: e.g., Hadamard, phase, CNOT, pi/8
  - Ability to perform measurements on any qubits
- Cannot prepare arbitrary quantum states easily….

Chapter 4 : Extensions?

- Qutrits (3-level basic elements)?
- Infinite Hilbert spaces?
- Non-basis starting states?

Some CS questions on QC

- Why are Quantum Computers faster?
  - Are they : **PSCAPE** = **BPP** ➔ **BQP** = **BPP** ?
  - Grover's algorithm?
  - Quantum parallelism?
- Simulation of QC on classical machines?
  - Approximation of irrational numbers?

Quantum Parallelism : The Holly Grail

- Ideally, we would like to take complex numbers $\{x_j\}$ as the inputs 2^n of them
- A computable function $f : C \rightarrow C$
- And compute $\{f(x_j)\}$ on all of them in parallel on a poly(n)-gate quantum circuit
- Read the results back: $f(x_1),\ldots,f(x_{2n})$

- *Similar to* : analog (non-digital) electronic machines where currents/frequencies/etc. can be used to represent real-valued numbers (as opposed to their n-bit digital approximations)

Problem : noise

Quantum Parallelism : Naïve

- Have 2^n complex numbers x_j to run f on
- Prepare the input: $$|in\rangle = \sum_{j=0}^{2^N-1} x_j |j\rangle$$
- Run our function f (expressed as U_f) on $|in\rangle$, get: $$|out\rangle = U_f(\sum_{j=0}^{2^N-1} x_j |j\rangle) = \sum_{j=0}^{2^N-1} x_j U_f(|j\rangle)$$
- Well, U_f didn't touch x_j at all... ☹

Quantum Parallelism : Less Naïve

- Suppose have a Boolean function with one input $f : \{0,1\} \rightarrow \{0,1\}$
- Create a unitary circuit for computing f: U_f

Figure 1.17, p. 31

- Prepare input in superposition of $|0>$ and $|1>$
- Output is a superposition of f(0) and f(1)
- Can do the same for n bits

Quantum Parallelism : Less Naïve

- A problem : one measurement gives us just one integer number back (the index of the measurement operator in the observable)
- The state then collapses and no more information can be gathered
- Good-bye to the rest of $\{f(x_j)\}$

What can we do?

- Well, we can measure some global properties of f fast…
- Example #1 : Deutsch's algorithm (p. 33): can measure f(0) XOR f(1) with a single U_f circuit run.
- Example #2 : Deutsch-Jozsa's algorithm : can determine if f is balanced/constant in poly(n) steps where as need O(exp(n)) evaluations of f in the classical case (p. 34)
- Problems --- Eric?

Quantum Parallelism : Question

- We seem unable to use amplitudes of the basis vectors (even normalized) to encode inputs $\{x_j\}$
- …because any quantum gate is linear and will simply pass them through
- The solution suggested was to encode $\{x_j\}$ in binary (n bits) and use basis vectors (for n qubits) to represent all of them.

- *Here is a question* : Can we use phases of vectors to encode $\{x_j\}$?

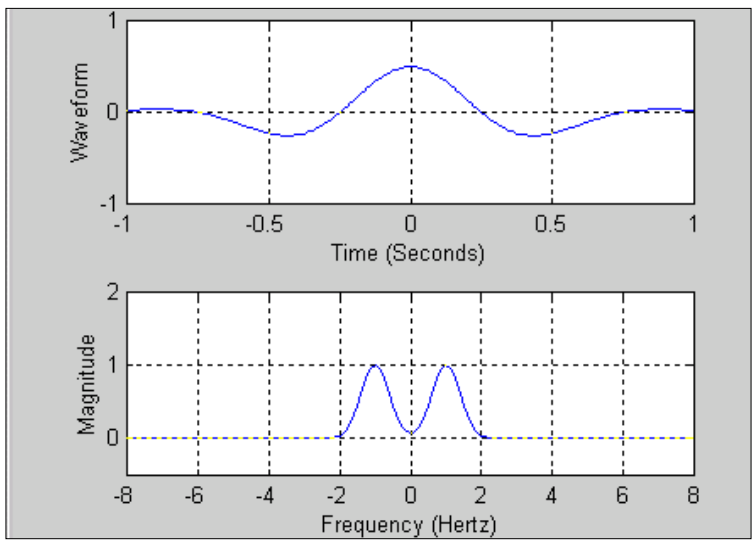
Fourier Tranform Recap (5.1)

- Classical (discrete) Fourier transform:
  - Input : $\{x_0,\ldots,x_{N-1}\}$ complex numbers
  - Output: $\{y_0,\ldots,y_{N-1}\}$ complex numbers

$$y_k \equiv \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{2\pi i j k / N}$$

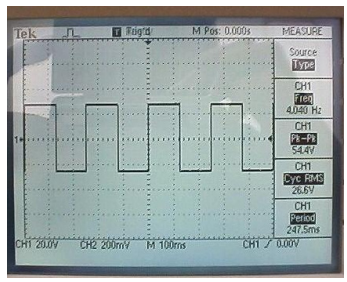
- Intuitive meaning – spectral analysis – find "basic" frequencies of sine/cosine waves in a complex waveform

Fourier Transform : Illustration

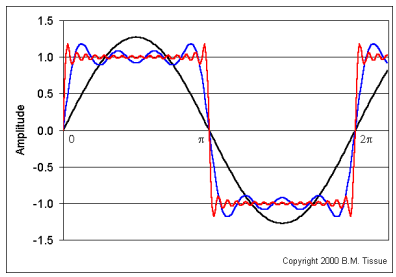


Fourier Transform : Illustration

- Suppose we have a square wave



- Can still approximate it with sine/cosine waves:



Fourier Tranform Recap

- Quantum Fourier transform is a linear operator over orthonormal basis $\{|0>,\ldots,|N\text{-}1>\}$ ($N = 2^n$ – thus n qubits):

$$|j\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} x_j e^{2\pi i jk/N} |k\rangle$$

- Here amplitudes x_j are the original imputs and y_k are the outputs:

$$\sum_{j=0}^{N-1} x_j |j\rangle \rightarrow \sum_{k=0}^{N-1} y_k |k\rangle$$

Fourier Tranform Recap

- If the input $|j> = |j_1 \ldots j_n>$ then QFT is:

$$|j_1,\ldots,j_n\rangle \rightarrow \frac{(|0\rangle + e^{2\pi i 0.j_n}|1\rangle)(|0\rangle + e^{2\pi i 0.j_{n-1}j_n}|1\rangle)\cdots(|0\rangle + e^{2\pi i 0.j_1 j_2 \ldots j_n}|1\rangle)}{2^{n/2}}$$

- Complexity:
  - Quantum: $O(n^2)$ gates
  - Classical: $O(2^n)$ operations

- Problems:
  - Cannot measure outputs y_j
  - Cannot efficiently prepare the input state $|j>$

$$\sum_{j=0}^{N-1} x_j |j\rangle \rightarrow \sum_{k=0}^{N-1} y_k |k\rangle$$

Why?

Phase Estimation Recap (5.2)

- Suppose I have a unitary operator U
- U has an eigenvector $|u>$:

$$U|u\rangle = \lambda|u\rangle, \lambda \in \mathbb{C}$$

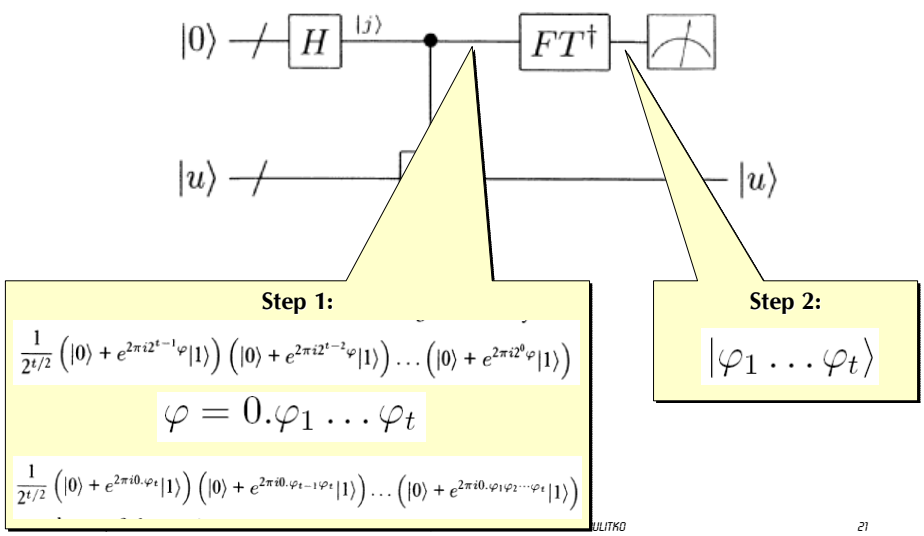
- Since U is unitary, its eigenvalue λ is a complex scalar of modulus 1:

$$\lambda = e^{i\theta} = e^{2\pi i\varphi}, \varphi \in \mathbb{R}$$

- What is the phase φ?

Can the phase be found by solving the characteristic equation?

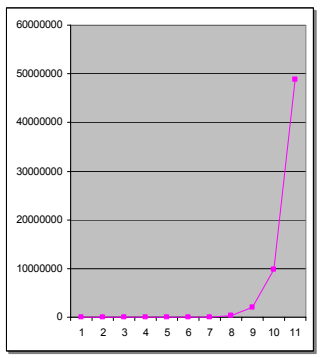
Phase Estimation Recap

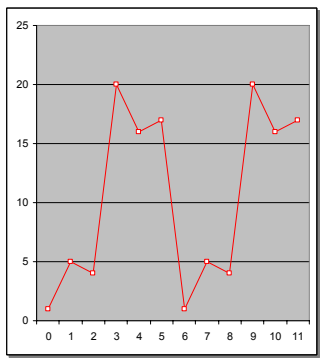


Application : Order Finding

- Find min $r > 0$ such that $x^r = 1 \pmod N$
- How is it related to Fourier transform?

	x=5	N=21
r	x^r	x^r mod N
0	1	1
1	5	5
2	25	4
3	125	20
4	625	16
5	3125	17
6	15625	1
7	78125	5
8	390625	4
9	1953125	20
10	9765625	16
11	48828125	17





Order-finding

- So, we will just form a unitary operator:

$$U\left|y\right\rangle \equiv \left|xy(\mathrm{mod}\ N)\right\rangle$$

- Its eigenvectors are (but of course!)

$$|u_s\rangle \equiv \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \exp\left[\frac{-2\pi i s k}{r}\right] |x^k \bmod N\rangle$$

- The eigenvalues then are:

$$e^{2\pi i \varphi} = e^{2\pi i \frac{s}{r}}$$

- And therefore the period is: $r = \frac{\varphi}{s}$

Problems & Solutions...

- So, yes, it seems like we will just do phase-estimation for φ, compute r, and happily go home...
- Well, maybe not quite: $|u_s\rangle \equiv \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \exp\left[\frac{-2\pi i s k}{r}\right] |x^k \bmod N\rangle$
  - How do we prepare $|u_s\rangle$ eigenvectors?
  - Need to know r... Hmm...
  - What if s and r have a common factor?
- Have efficient workarounds for all three (see pp. 227-230 in the book).

Application : Factoring

- Given a positive composite number N, find a non-trivial factor of it
- Why bother?
  - Don't we all do it before going to sleep?
  - Breaking RSA-like encryption systems – credit card number encoding, PGP, etc., etc., etc.
- Best classical methods : O(exp(N))
- Can reduce to order-finding : $O((\log N)^3)$

Factoring → Order-finding

- The reduction is based on this observation:

Theorem 5.2: Suppose N is an L bit composite number, and x is a non-trivial solution to the equation $x^2 = 1 \pmod N$ in the range $1 \leq x \leq N$, that is, neither $x = 1 \pmod N$ nor $x = N - 1 = -1 \pmod N$. Then at least one of $\gcd(x - 1, N)$ and $\gcd(x + 1, N)$ is a non-trivial factor of N that can be computed using $O(L^3)$ operations.

Theorem 5.3: Suppose $N = p_1^{\alpha_1} \ldots p_m^{\alpha_m}$ is the prime factorization of an odd composite positive integer. Let x be an integer chosen uniformly at random, subject to the requirements that $1 \leq x \leq N - 1$ and x is co-prime to N. Let r be the order of x modulo N. Then

Period-finding

- So, we will just form a unitary operator:

$$U\left|y\right\rangle \equiv \left|xy(\mathrm{mod}\ N)\right\rangle$$

- Its eigenvectors are (but of course!)

$$|u_s\rangle \equiv \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \exp\left[\frac{-2\pi i s k}{r}\right] |x^k$$

- The eigenvalues then are:

$$e^{2\pi i \varphi} = e^{2\pi i \frac{s}{r}}$$

- And therefore the period is:

$$r = \frac{\varphi}{s}$$

This finds a period of function f(k) = x^k mod N. Can we do it for a general periodic function? Sure (pp. 236-237)

Fast Quantum Algorithms

- Hidden subgroup formulation (section 5.4.3):
  - f : G → X
  - X is finite
  - G is a group
  - K is a subgroup of G
  - f is constant on gK and distinct for different g's
  - Have a quantum box for U|g>|h> = |g>|h⊕f(g)> where ⊕ is a specific binary operation on X
  - Task: find a generating set for K
- Can be done fast on quantum machines for Abelian (commutative) groups G

The Power of QC

- Again : What makes QC appear faster than classical machines?
  - Parallelism?
  - Promise (e.g., existence of generating subset for K)
- Question: why do we need a promise?

Check - point

- Done with these :
  - Chapter 1 : Intro
  - Chapter 2 : Linear Algebra + postulates
  - Chapter 3 : Computer Science
  - Chapter 4 : Quantum Circuits
  - Chapter 5 : Quantum Fourier Transform
- Now on to:
  - Chapter 6 : Quantum Search
  - Chapter 7 : Physical Realization of QMs

Why are QC faster?

How can *you* apply QC in your area?

Chapter 6

QUANTUM SEARCH ALGORITHM

Lecture 12

Vahid Rezania
May-June 2002

Overview

- The algorithm
- Quantum counting
- Search as quantum simulation

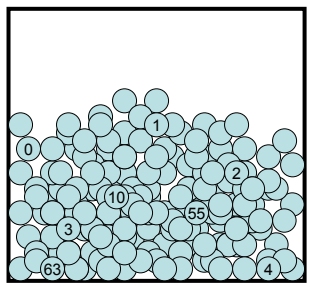
6.1 The quantum search algorithm

- $N = 2^n$ – elements
- $1 \leq M \leq N$ solutions
- $x \in \{0, N-1\}$

  $f: \{0,1\}^n \longrightarrow \{0,1\}$

  $f(x) = 1 \rightarrow$ x is solution

  $f(x) = 0 \rightarrow$ x is not solution



The quantum search algorithm Oracle qubit

- Suppose we have a quantum oracle with ability to recognize solutions to the search problem, ie. an unitary operator *O* which acts as

$$|x\rangle\,|q\rangle \xrightarrow{O} |x\rangle\,|q \oplus f(x)\rangle$$

Oracle qubit

$f(x) = 1$ q is flipped → x is a solution

$f(x) = 0$ q is unchanged

Example: $|x\rangle\,|0\rangle$

The quantum search algorithm
Oracle qubit

- Usually the state $(|0\rangle - |1\rangle)/\sqrt{2}$ is considered as oracle qubit, so

$$|x\rangle \left(|0\rangle - |1\rangle\right)/\sqrt{2} \xrightarrow{O} (-1)^{f(x)} |x\rangle \left(|0\rangle - |1\rangle\right)/\sqrt{2}$$

f(x) = 1 initial states are interchanged
f(x) = 0 initial states are unchanged

$$\Rightarrow \quad |x\rangle \xrightarrow{O} (-1)^{f(x)} |x\rangle$$

$\Rightarrow$ $O(\sqrt{N / M})$ for M solutions

The quantum search algorithm
the oracle

- What is the oracle?
- Consider the classical factoring problem:
  $m = p \,.\, q$ ($p < q$ and are prime). To find p we need to search all numbers from 2 to $\sqrt{m}$

- In quantum case, the action of the oracle depends on input state |x> : divide m by x, and check if the division is exact → flipping the oracle qubit. ($x \in \{0, m-1\}$)

The quantum search algorithm
the oracle

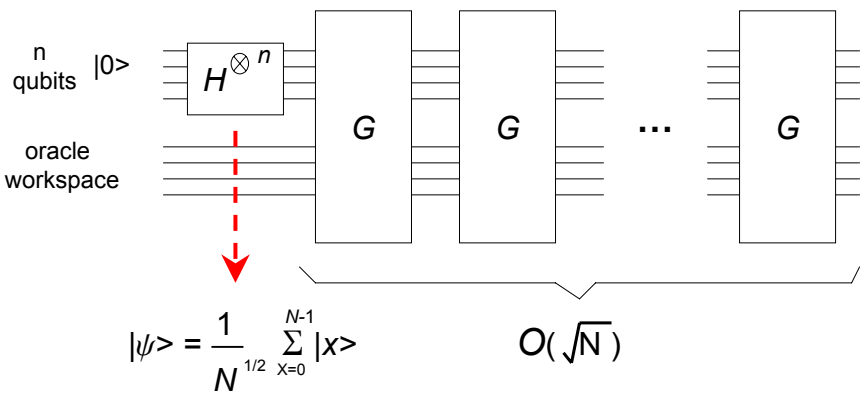
- How to implement the oracle efficiently?
- Note if x divides *m* ⟶ f(x) =1, otherwise f(x)=0
  so we need to compute f(x) : Sec. 3.2.5 : reversible classical circuit

$(x,0,0,q) \rightarrow (x,f(x),g(x),q) \rightarrow (x,f(x),g(x),q \oplus f(x)) \longrightarrow$
$\longrightarrow (x,0,0,q \oplus f(x))$

- Without knowing the prime factors of *m,* we can construct an oracle which recognize a solution to the search problem when it sees one ⟶ $O(m^{1/4})$ oracle calls

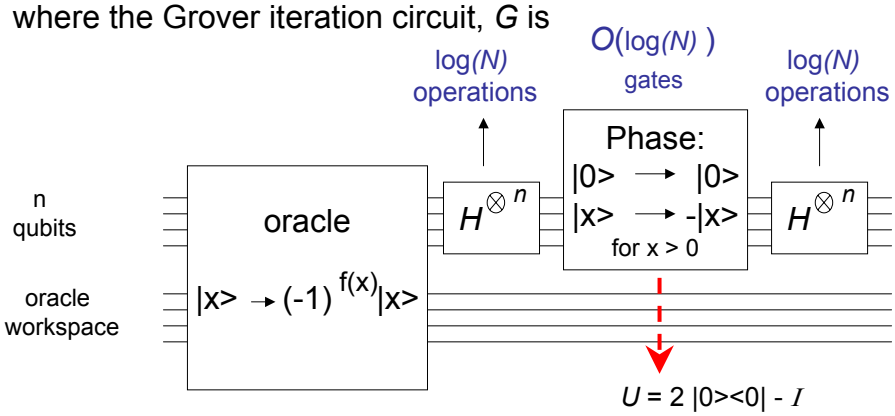
The quantum search algorithm
the procedure

The search algorithm operates as:



The quantum search algorithm
the procedure

where the Grover iteration circuit, G is



Note that: $H^{\otimes n}\,(2\,|0\rangle\langle 0| - I)\,H^{\otimes n} = 2\,|\psi\rangle\langle\psi| - I$

$\Rightarrow$ $G = (\,2\,|\psi\rangle\langle\psi| - I\,)\,O$

the Grover operator
is a rotation operator

- $G = (\,2\,|\psi\rangle\langle\psi| - I\,)\,O$
- let we have M solutions, we define ortho-normalized basis

$$|\alpha\rangle = \frac{1}{\sqrt{N-M}} \sum_x{}'' |x\rangle \qquad |\beta\rangle = \frac{1}{\sqrt{M}} \sum_x{}' |x\rangle$$

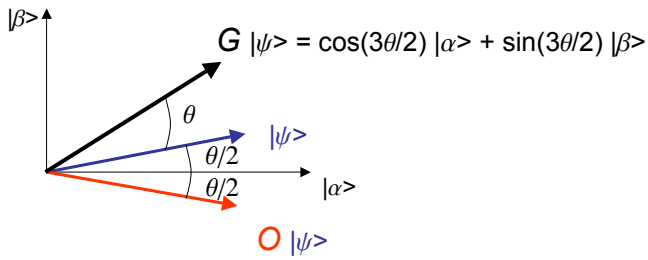
(sum over all x which are not solution) (sum over all x which are solution)

therefore

$$|\psi\rangle = \sqrt{\frac{N-M}{N}}\,|\alpha\rangle + \sqrt{\frac{M}{N}}\,|\beta\rangle$$

$$|\psi\rangle = \cos(\theta/2)\,|\alpha\rangle + \sin(\theta/2)\,|\beta\rangle \qquad \cos(\theta/2) = \sqrt{(N-M)/N}$$

the Grover iteration is a rotation operator



- after k iteration :

$$G^k|\psi\rangle = \cos\big((2k+1)\theta/2\big)\,|\alpha\rangle + \sin\big((2k+1)\theta/2\big)\,|\beta\rangle$$

$$\longrightarrow\ |\beta\rangle$$

the Grover iteration

- How many Grover iteration?

- note $\theta = 2\arcsin(\sqrt{M/N})$ so the number of iterations is

$$R = \mathrm{CI}\left(\frac{2\arcsin(\sqrt{M/N})}{\theta}\right) \qquad \theta/2 \le \pi/4$$

where CI(x) = integer closet to x, CI(3.5)=3, CI(3.6)=4

- note: *R* depends on knowing *M*

the Grover iteration

- For $M \leq N/2$:

R $\leq [\pi/2\theta]$, but $\theta/2 \geq \sin(\theta/2) = \sqrt{M/N}$

then we have

$$R \leq [(\pi/4)\sqrt{N/M}\,] \Rightarrow R = O(\sqrt{N/M})$$

- **Classically** $\longrightarrow$ ***O(N / M)***

- For $M \geq N/2$:

from $\theta =$ arcsin $(2\sqrt{M(N-M)}/N)$,

so as M gets closer to N, θ gets smaller

$\Rightarrow$ the iteration *increases* with M !!

the Grover iteration

- For $M \geq N/2$:

- if M is known, just pick up a solution and check it using the oracle. The success probability is ½ and requires one consultation with oracle only.

- if M is unknown, adds N extra items which you know that they are not solution. As a result, $M \leq N/2$. So

(1) add a single qubit |q> to the search index

(2) double the number of items to be searched to $2N$

New *augmented* oracle needs $R = \pi/4\sqrt{2N/M}$ calls (at most).

6.3 Quantum counting

- Up to now we assumed that the number of solutions is determined in advance - **if not: how fast we can find it?**
- **Classical:** $\Theta(N)$ consultations with oracle
- **Quantum:** Grover iteration **+** the phase estimation technique (faster)

⇨ possible finding a solution after first counting

⇨ existence of solution ⟶ **NP**-complete problems

Quantum counting
eigenvalue estimation

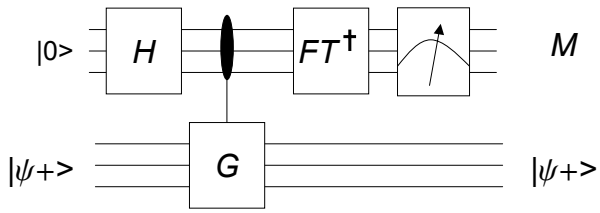
- $|\psi\rangle = \cos(\theta/2)\,|\alpha\rangle + \sin(\theta/2)\,|\beta\rangle$
- $G\,|\psi\rangle = \cos(3\theta/2)\,|\alpha\rangle + \sin(3\theta/2)\,|\beta\rangle$ (rotated by angle θ)
- What if θ is unspecified?
- Estimating the **eigenvalues** of the Grover iteration - G is rotation operator in two dimensions, using the phase estimation technique:

$$G = \begin{vmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{vmatrix} \longrightarrow \lambda = e^{i\theta}\ ,\quad e^{-i\theta}$$

$|\psi+\rangle = (|\alpha\rangle + i\,|\beta\rangle)/2$ $\qquad$ $G\,|\psi+\rangle = e^{i\theta}\,|\psi+\rangle$

$|\psi-\rangle = (|\alpha\rangle - i\,|\beta\rangle)/2$ $\qquad$ $G\,|\psi-\rangle = e^{-i\theta}\,|\psi-\rangle$

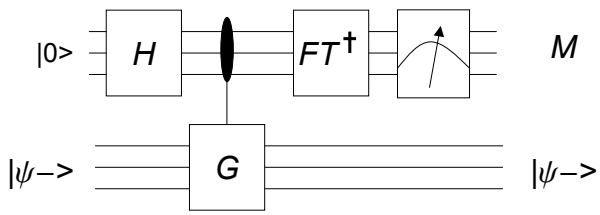
Quantum counting
eigenvalue estimation



-

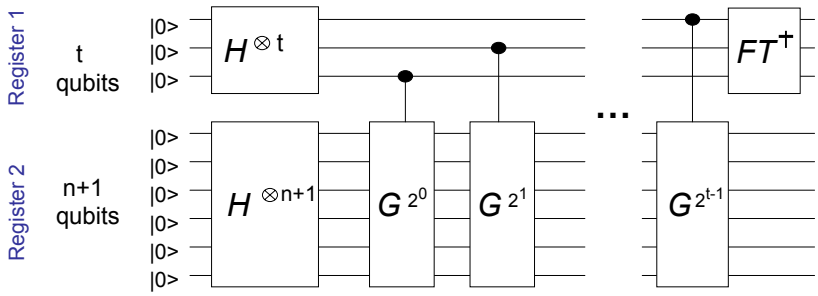
$$\frac{M}{N} \approx \sin^2(\theta/2)$$

Quantum counting
eigenvalue estimation



$$\frac{M}{N} \approx \sin^2((2\pi-\theta)/2)$$

Quantum counting
the circuit



- estimate θ to m bits of accuracy, with a probability of success $1 - \epsilon$
- $t = m + [\log(2+1/2\epsilon)]$
- $|\Delta\theta| \leq 2^{-m}$

The quantum search algorithm

- Input: (1) a black box oracle O which perform $O|x>|q>=|x>|q \oplus f(x)>$
  where $f(x)=0$ for all $0 \leq x < 2^n$ except x_0, $f(x_0)=1$.
  (2) $n+1$ qubits in the state $|0>$

  Output: x_0

  Runtime: $O(2^{n/2})$ operations.

  Procedure:

  1. $|0>^{\otimes n}|0>$
  2. $(1/2^{n/2}) \sum_{x=0}^{2^n-1} |x>\ (|0> - |1>)/2^{1/2} = |s>$ apply $H^{\otimes n}$ to first n, HX to last qubit
  3. $[(2|\psi><\psi| - I)O]^{\otimes R}|s> \sim |x_0>(|0> - |1>)/2^{1/2}$ apply G, R times
  4. $\rightarrow x_0$ measure the first n qubits

6.2 Search as simulation

Simulation (re-cap):

- initial state $|\psi\rangle$
- Hamiltonian H
- final state $|x\rangle$ after some prescribed time

Search :

- we need a H which solves the search problem ie. if x is a solution of search problem then

$$\exp(-iHt)|\psi\rangle \longrightarrow |x\rangle$$

What kind of H will do this job?

$|x\rangle\langle x|$, $|\psi\rangle\langle\psi|$

$|x\rangle\langle\psi|$, $|\psi\rangle\langle x|$

6.2 Search as simulation

- The simple way is

$$H_1 = |x\rangle\langle x| + |\psi\rangle\langle\psi|$$
$$H_2 = |x\rangle\langle\psi| + |\psi\rangle\langle x|$$

- both of them **works** for the search algorithm

- Find $|y\rangle$ s.t $|x\rangle$ and $|y\rangle$ are orthonormal (Gram-Schmidt procedure)
- Expand $|\psi\rangle = \alpha|x\rangle + \beta|y\rangle$, $\alpha^2 + \beta^2 = 1$
- $\longrightarrow$ $H_1 = I + \alpha(\beta X + \alpha Z)$

- $\exp(-iH_1 t)|\psi\rangle = \exp(-it)[\cos(\alpha t)|\psi\rangle - i\sin(\alpha t)|x\rangle]$

- So after $t = \pi/(2\alpha)$ we get $|x\rangle$ with probability **one !**

6.2 Search as simulation

- but time t depends on the α, the component of $|\psi>$ in the direction of |x>.
- choose $|\psi>$ be a uniform superposition of all |x>, so α is constant and

$$|\psi> = (1/N^{1/2}) \Sigma |x>$$

- the time will be $\pi N^{1/2}/2$
- easy to simulate, but
- to achieve accuracy $O(\Delta t)$, number of oracle calls $O(N)$
- for better accuracy $O(\Delta t^r)$, number of oracle calls $O(N^{r/2(r-1)})$
- only for **large** r, we get the same efficiency as search algorithm.

6.2 Search as simulation

- using $e^{i(A+B)\Delta t} = e^{iA\Delta t} e^{iB\Delta t} + O(\Delta t^2)$ we can construct
- $U(\Delta t) = \exp(-i|\psi><\psi|\Delta t) \exp(-i|x><x|\Delta t)$
- $U(\Delta t)$ is a **rotation** on Bloch sphere about an axis

$$\boldsymbol{r} = \cos(\Delta t/2)\ (\psi+\boldsymbol{z})/2 + \sin(\Delta t/2)\ (\psi\ \mathbf{x}\ \boldsymbol{z})/2$$

with angle

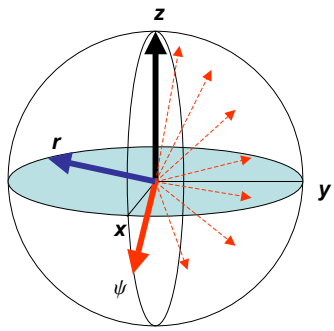
$$\cos(\theta/2) = 1 - 2\sin^2(\Delta t/2) / N$$

-
-

6.2 Search as simulation

- choose $\Delta t = \pi$, $\rightarrow \cos(\theta/2) = 1 - 2/N$
- for **large** N **:** $\theta \sim 4/N^{1/2}$
- No. of oracle calls to find |x> **:**

$$O(N^{1/2}) \text{ !}$$



- **Note:**
- $\exp(-i|\psi\rangle\langle\psi|\,\pi) = I - 2\,|\psi\rangle\langle\psi|$

$|\psi\rangle = (2\alpha\beta, 0, \alpha^2 - \beta^2)$

z = (0, 0, 1)

$\exp(-i|x\rangle\langle x|\,\pi) = I - 2\,|x\rangle\langle x|$

6.2 Search as simulation

- In summary
  - specify the problem, including the desired input and output
  - **guess** a Hamiltonian (rather than quantum circuit)
  - simulate the Hamiltonian
  - analyze the costs

Hamiltonian Cycle

- **Classical algorithm:** requires $O(\, p(n)\, 2^{n[\log n]}\,)$ operations to determine existence of Hamiltonian cycle.
  The success probability is 1.

- **Quantum algorithm:** requires $O(\, p(n)\, 2^{n[\log n]\,/2}\,)$ operations to determine existence of Hamiltonian cycle (using search algorithm).
  The probability of error is constant, say 1/6, which may reduced to $1/6^r$ by r repetitions of algorithm.

- Asymptotically the quantum algorithm needs the **square root** of the number of operations the classical algorithm requires.

Search algorithm

- The algorithm is essentially **optimal:** no quantum algorithm can perform searching using fewer than $\Omega(N^{1/2})$.

- No further improvement is **possible**.

- **NP-**complete problems can not be solved efficiently on quantum computers using search-based method.

- **BQP** does not contain **NP-**complete ?

Search algorithm

- **Polynomial** speedup for problems which are involved with evaluation of Boolean functions

- **D(F):** minimum number of oracle calls that a classical computer must perform to compute a function F with **certainty**.

- **$Q_2(F)$:** minimum number of oracle calls that a quantum computer must perform to produce an output which equals F with **probability** at least 2/3.

Example: for F = OR

$$Q_2(F) \geq \left[D(F)/13824 \right]^{1/6}$$

Exercises

- Ex.: 6.1, 6.2, 6.3, 6.7, 6.12, 6.17

7. Quantum computers: physical realization

To be or ***not to be***. That's a question…

William Shakespeare

The "classic" answers: ***"to be"*** or ***"not to be"***

The "quantum" answers:

"to be", ***"not to be"*** or $\mathbf{a} \times$ ***(to be)*** + $\mathbf{b} \times$ ***(not to be)***

7. Quantum computers: physical realization
(Outline)

- Section 7.1: An overview of the tradeoffs in selecting a physical realization of a quantum computer
- Section 7.2: Physical conditions for quantum computation
- Section 7.3: Harmonic oscillator quantum computer
- Section 7.4: Optical photon quantum computer
- Section 7.5: Optical cavity quantum electrodynamics
- Section 7.6: Ion traps
- Section 7.7: Nuclear magnetic resonance (NMR)
- Section 7.8: Other implementation schemes

7.1 Guiding principles

The elementary units of the theory are quantum bits – two-level quantum systems.

➢What are the experimental requirements for building a quantum computer?

- Robustly represent quantum information
- Perform a universal family of unitary transformation
- Prepare a fiducial initial state
- Measure the output result

The challenge of experimental realization is that these basic requirements can often only be partially met.

Crude estimates for typical times and maximum number of operations

System	τ_Q	τ_{op}	$n_{op} = \lambda^{-1}$
Nuclear spin	$10^{-2} - 10^{8}$	$10^{-3} - 10^{-6}$	$10^{5} - 10^{14}$
Electron spin	10^{-3}	10^{-7}	10^{4}
Ion trap (In^{+})	10^{-1}	10^{-14}	10^{13}
Electron – Au	10^{-8}	10^{-14}	10^{6}
Electron – GaAs	10^{-10}	10^{-13}	10^{3}
Quantum dot	10^{-6}	10^{-9}	10^{3}
Optical cavity	10^{-5}	10^{-14}	10^{9}
Microwave cavity	10^{0}	10^{-4}	10^{4}

$\tau_Q \equiv$ decoherence time (quantum noise)

$\tau_{op} \equiv$ operation time

$n_{op} = \lambda^{-1} = \tau_Q/\tau_{op}$

7.2.1 Representation of quantum information

- ***Quantum computation*** is based on transformation of quantum states
- ***Quantum bits*** are two-level quantum systems

Example spin-1/2 particle as a quantum bit

$$\left|\uparrow\right\rangle \quad \text{and} \left|\downarrow\right\rangle$$

Example spin-3/2 particle as two qubits

$$\left|\mathrm{m}=+3/2\right\rangle, \left|\mathrm{m}=+1/2\right\rangle, \left|\mathrm{m}=-1/2\right\rangle \quad \text{and} \quad \left|\mathrm{m}=-3/2\right\rangle$$

7.2.1 Representation of quantum information

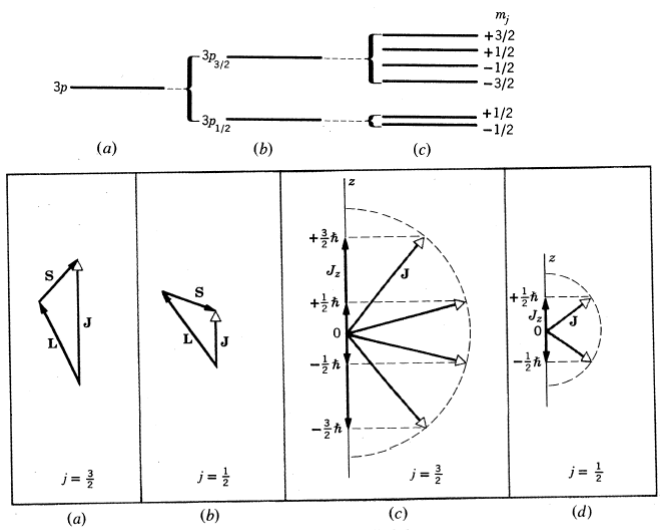


Figure 44–8 (*a*) **J** for a $p_{3/2}$ state; this is sometimes called the "stretch" mode. (*b*) **J** for a $p_{1/2}$ state; this is sometimes called the "jack-knife" mode. (*c*) The four values of J_z for the $p_{3/2}$ state. (*d*) The two values of J_z for the $p_{1/2}$ state.

7.2.2 Performance of unitary transformations

- Closed quantum systems evolve unitarily as determined by their Hamiltonians
- To perform quantum computation one must be able to control the Hamiltonian to effect an ***arbitrary*** selection from a universal family of unitary transformations (See section 4.5)

Example Single spin might evolve under the Hamiltonian

$$H = P_x(t)X + P_y(t)Y$$

$P_{\{x,y\}}$ = classically controllable parameters

By manipulating P_x and P_y appropriately, one can perform ***arbitrary*** single spin rotations.

7.2.3 Preparation of fiducial initial states

- What can be used if numbers cannot be input?
- In classical machines one merely sets some switches in the desired configuration and that defines the input state.
- It is only necessary to be able to (repeatedly) produce one specific quantum state with high fidelity, since a unitary transform can turn it into ***any other desired*** input state.
- These quantum states are determined by suitable measurable physical parameters (spin, energy, frequency, etc.).

7.2.4 Measurement of output result

- The output from a good quantum algorithm is a superposition state which gives a useful answer with high probability when measured.

Example

A cubit state $a|0\rangle + b|1\rangle$

- Represented by the ground and excited states of a two-level atom
- Might be measured by pumping the excited state and looking for fluorescence
- If an electrometer indicates that fluorescence had been detected by a suitable device, then the qubit would collapse into the |1> state (this would happen with probability $|b|^2$)
- Otherwise the device would detect no charge, and the qubit would collapse into the |0> state

7.3 Harmonic oscillator computer

- A simple harmonic oscillator is a particle in a parabolic potential well

$$V(x) = m\omega^2 x^2/2$$

- The set of discrete energy eigenstates of a simple harmonic oscillator can be labeled as |n>

  n = 0, 1, …, ∞
- The relationship to quantum computation comes by taking a finite subset of these states to represent qubits. These qubits will have lifetimes determined by physicala parameters
- Unitary transforms can be applied by simply allowing the system to evolve in time.

7.3.2 The Hamiltonian

The ***Hamiltonian*** for a particle in a one-dimensional parabolic potential

$$H = \frac{p^2}{2m} + \frac{1}{2}m\omega^2 x^2$$

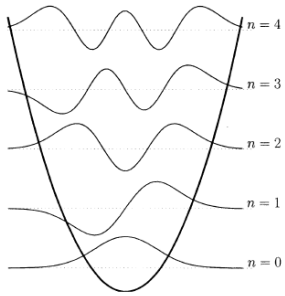
The solution using ***Schrödinger equation***

$$\frac{\hbar^2}{2m}\frac{d^2\psi_n(x)}{dx^2} + \frac{1}{2}m\omega^2\psi_n(x) = E\psi_n(x)$$

$$Ha^\dagger|\psi\rangle = \left([H, a^\dagger] + a^\dagger H\right)|\psi\rangle = (\hbar\omega + E)a^\dagger|\psi\rangle$$

$$a = \frac{1}{\sqrt{2m\hbar\omega}}\left(m\omega x + ip\right)$$

$$a^\dagger = \frac{1}{\sqrt{2m\hbar\omega}}\left(m\omega x - ip\right)$$



7.3.3 Quantum computation

$$\begin{aligned}
|00\rangle_L &\rightarrow |00\rangle_L \\
|01\rangle_L &\rightarrow |01\rangle_L \\
|10\rangle_L &\rightarrow |11\rangle_L \\
|11\rangle_L &\rightarrow |10\rangle_L
\end{aligned}$$

$$\begin{aligned}
|00\rangle_L &= |0\rangle \\
|01\rangle_L &= |2\rangle \\
|10\rangle_L &= (|4\rangle + |1\rangle)/\sqrt{2} \\
|11\rangle_L &= (|4\rangle - |1\rangle)/\sqrt{2}
\end{aligned}$$

Harmonic oscillator quantum computer *(Summary)*

Harmonic oscillator quantum computer

- **Qubit representation**: Energy levels $|0\rangle$, $|1\rangle$, . . ., $|2^n\rangle$ of a single quantum oscillator give n qubits.
- **Unitary evolution**: Arbitrary transforms U are realized by matching their eigenvalue spectrums to that given by the Hamiltonian $H = a^\dagger a$.
- **Initial state preparation**: Not considered.
- **Readout**: Not considered.
- **Drawbacks**: Not a digital representation! Also, matching eigenvalues to realize transformations is not feasible for arbitrary U, which generally have unknown eigenvalues.

7.4 Optical photon quantum computer

- The energy in an electromagnetic cavity is quantized in units of $\hbar\omega$. Each such quantum is called a ***photon***.
- Photons are chargeless particles, and do not interact very strongly with each other and most matter.
- In principle, photons can be made to interact with each other,using nonlinear optical media mediate interactions.
- Photons exhibit signature quantum phenomena, such as the interference produced in two-slit experiments.
- ***Thus a photon can be used to represent a quantum bit***.

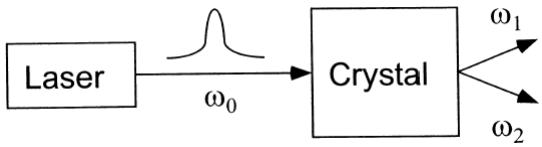
7.4.1. Physical apparatus

- ***How can photons represent qubits?***
  - Let's consider two cavities, whose total energy is $\hbar\omega$
  - Take the two states of a qubit as being whether the photon is in one cavity (**|01>**) or other (**|10>**).
  - The physical state of a superposition: $\mathbf{c_0|01> + c_1|10>}$ ***(dual-rail representation)***
  - Coherent laser output:

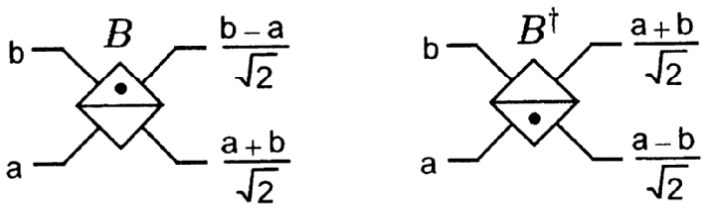
$$\left|\alpha\right\rangle = e^{-|\alpha|^2/2}\sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}\left|n\right\rangle$$

    |n> is an ***n***-photon energy eigenstate
  - Mean energy: $\mathbf{\langle\alpha|n|\alpha\rangle = |\alpha|^2}$

Parametric down-conversion scheme for generation of single photons



Optical beamsplitter



$$a_{out} = a_{in}\cos\theta + b_{in}\sin\theta$$

$$b_{out} = -a_{in}\sin\theta + b_{in}\cos\theta$$

7.4.2 Quantum computation

- Arbitrary unitary transforms can be applied to quantum information, encoded with single photons in the $\mathbf{c_0|01> + c_1|10>}$ dual-rail representation, using ***phase shifters***, ***beamsplitters***, and ***nonlinear optical Kerr media***.
- Cuantum mechanically modeled electromagnetic radiation
  - Vacuum state: |0>
  - Single photon state: $|1> = a^\dagger|0>$
  - n - photon state: $\left|n\right\rangle = \frac{a^{\uparrow n}}{\sqrt{n!}}\left|0\right\rangle$

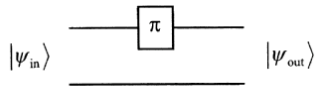
Phase shifter

- A phase shifter P acts just like normal time evolution, but at a different rate, and localized to only the modes going through it.
- The action of P on the vacuum state is to do nothing: $\mathbf{P|0> = |0>}$, but on a single photon state, one obtains $\mathbf{P|1> = e^{i\Delta}|1>}$

$\mathbf{\Delta \equiv (n - n_0)L/c_0}$ is the difference between propagation times of light in vacuum and medium

$$|\psi_{out}\rangle = \begin{bmatrix} e^{i\pi} & 0 \\ 0 & 1 \end{bmatrix} |\psi_{in}\rangle ,$$

if we take the top wire to represent the $|01\rangle$ mode, and $|10\rangle$ the bottom mode, and the boxed π to represent a phase shift by π:



Beamsplitter

- Beamsplitter acts on two modes, which can be described by the creation (annihilation) operators ***a(a†)*** and ***b(b†)***
- The Hamiltonian

$$H_{bs} = i\theta \left(ab^\dagger - a^\dagger b\right)$$

- Unitary operation

$$B = \exp\left[\theta \left(a^\dagger b - ab^\dagger\right)\right]$$

- Transformations effected by ***B*** on ***a*** and ***b***

$$BaB^\dagger = a\cos\theta + b\sin\theta \qquad \text{and} \qquad BbB^\dagger = -a\sin\theta + b\cos\theta$$

Nonlinear Kerr media

- The most important effect of Kerr medium is the cross phase modulation it provides between two modes of light
- Hamiltonian: $H_{xpm} = -\chi a^\dagger a b^\dagger b$
- Unitary transform: $K = e^{i\chi L a^\dagger a b^\dagger b}$
- A controlled-NOT gate constructed for single photon states using Kerr media and beamsplitter combination

$$K|00\rangle = |00\rangle$$
$$K|01\rangle = |01\rangle$$
$$K|10\rangle = |10\rangle$$
$$K|11\rangle = e^{i\chi L}|11\rangle$$

Optical photon quantum computer
(Summary)

- **Qubit representation**: Location of single photon between two modes, $|01\rangle$ and $|10\rangle$, or polarization.
- **Unitary evolution**: Arbitrary transforms are constructed from phase shifters (R_z rotations), beamsplitters (R_y rotations), and nonlinear Kerr media, which allow two single photons to cross phase modulate, performing $\exp\left[i\chi L|11\rangle\langle 11|\right]$.
- **Initial state preparation**: Create single photon states (e.g. by attenuating laser light).
- **Readout**: Detect single photons (e.g. using a photomultipler tube).
- **Drawbacks**: Nonlinear Kerr media with large ratio of cross phase modulation strength to absorption loss are difficult to realize.

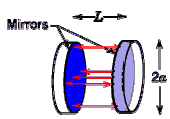
7.5 Optical cavity quantum electrodynamics

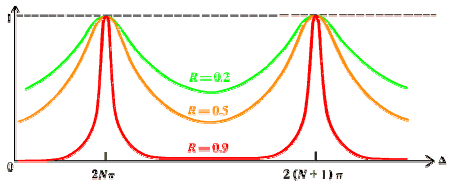
- Cavity quantum electrodynamics (QED) is a field of study which accesses an important regime involving coupling of single atoms to only a few optical modes.
- Experimentally, this is made possible by placing single atoms within optical cavities of very high Q (Quality factor); because only one or two electromagnetic modes exist within the the cavity, and each of these has a very high electric field strength, the dipole coupling between the atom and the field is very high
- Because of the high Q, photons within the cavity have an opportunity to interact many times with the atoms before escaping.

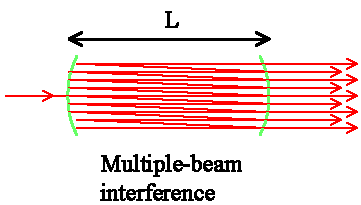
7.5.1 Physical apparatus

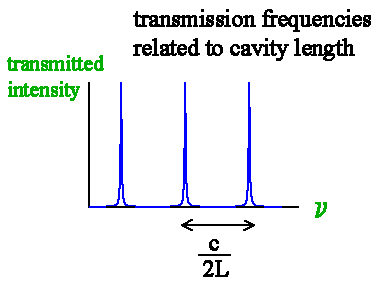
- The two main experimental components of a cavity QED system are the electromagnetic cavity and the atom.
- The main interaction involved in cavity QED is the dipolar interaction between an electric dipole moment and an electric field. One of the most important tools for realizing a very large electric field in a narrow band of frequencies and in a small volume of space, is the Fabry-Perot cavity.
- The electronic energy eigenstates of an atom as having only two states is an excellent approximation. This two-level atom approximation can be valid because we shall be concerned with the interaction with monochromatic light and, in this case the only relevant energy levels are those satisfying two conditions: their energy difference matches the energy of the incident photons, and symmetries ("selection rules") do not inhibit the transition.

The Fabry-Perot cavity (schematic view)









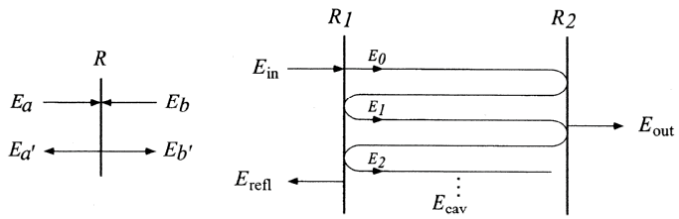
The Fabry-Perot cavity

- A basic component of a Fabry-Perot cavity is a partially silvered mirror, of which incident light Ea and Eb partially reflect and partially transmit, producing the output fields $E_{a'}$ and $E_{b'}$. These are related by the unitary transform

$$\begin{bmatrix} E_{a'} \\ E_{b'} \end{bmatrix} = \begin{bmatrix} \sqrt{R} & \sqrt{1-R} \\ \sqrt{1-R} & -\sqrt{R} \end{bmatrix} \begin{bmatrix} E_a \\ E_b \end{bmatrix}$$

R is the reflectivity of the mirror, and the location of the "-" sign is a convention chosen as given for convenience.

The Fabry-Perot cavity



$$E_{\text{cav}} = \sum_k E_k = \frac{\sqrt{1-R_1}E_{\text{in}}}{1 + e^{i\varphi}\sqrt{R_1 R_2}}$$

where $E_0 = \sqrt{1-R_1}E_{\text{in}}$, and $E_k = -e^{i\varphi}\sqrt{R_1 R_2}E_{k-1}$. Similarly, we find $E_{\text{out}} = e^{i\varphi/2}\sqrt{1-R_2}$, and $E_{\text{refl}} = \sqrt{R_1}E_{\text{in}} + \sqrt{1-R_1}\sqrt{R_2}e^{i\varphi}E_{\text{cav}}$.

The Fabry-Perot cavity

- One of the most important characteristics of a Fabry-Perot cavity is the power in the cavity internal field as a function of the input power and field frequency

$$\frac{P_{\text{cav}}}{P_{\text{in}}} = \left|\frac{E_{\text{cav}}}{E_{\text{in}}}\right|^2 = \frac{1 - R_1}{|1 + e^{i\varphi}\sqrt{R_1 R_2}|^2}$$

$\varphi = \omega d/c$, where d is the mirror separation.

7.5.2 The Hamiltonian

- The total Hamiltonian of the atom×electric field system in the cavity

$$H = H_{\text{atom}} + H_{\text{field}} + H_I$$

$$H_{\text{atom}} = \frac{\hbar\omega_0}{2} Z$$

where $\hbar\omega_0$ is the difference of the energies of the two levels, since the two states are energy eigenstates

$$H_I = g(\sigma_+ - \sigma_-)(a - a^\dagger)$$

7.5.2 The Hamiltonian

- Final solution for the total Hamiltonian

$$H = \frac{\hbar\omega_0}{2} Z + \hbar\omega a^\dagger a + g(a^\dagger \sigma_- + a\sigma_+)$$

$a^\dagger$ and a are raising and lowering operators on the single mode field, ω is the frequency of the field, ω_0 is the frequency of the atom, g is the coupling constant for the interaction between atom and field, σ_+ and σ_- are the Pauli raising and lowering operators

- For $N = a^\dagger a + Z/2$, $\delta = (\omega_0 - \omega)/2$ ***(detuning)*** and $[H,N] = 0$

$$H = \hbar\omega N + \delta Z + g(a^\dagger \sigma_- + a\sigma_+)$$

7.5.3 Single-photon single-atom absorption and refraction

- For single-photon single-atom interaction and

$$H = -\begin{bmatrix} \delta & 0 & 0 \\ 0 & \delta & g \\ 0 & g & -\delta \end{bmatrix}$$

- Since the basis states are |00>, |01>, |10>, for $U = e^{-iHt}$ time evolution $(\hbar \equiv 1)$

$$\begin{aligned} U = {} & e^{-i\delta t}|00\rangle\langle 00| \\ & + (\cos\Omega t + i\frac{\delta}{\Omega}\sin\Omega t)|01\rangle\langle 01| \\ & + (\cos\Omega t - i\frac{\delta}{\Omega}\sin\Omega t)|10\rangle\langle 10| \\ & - i\frac{g}{\Omega}\sin\Omega t\left(|01\rangle\langle 10| + |10\rangle\langle 01|\right) \end{aligned}$$

$\Omega = (g^2 + \delta^2)^{1/2}$ ***Rabi frequency***

Three level atom

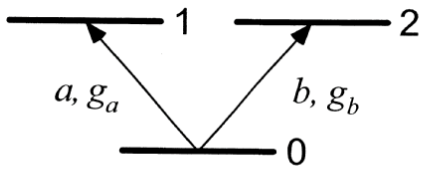


Figure 7.4. Three level atom (with levels 0, 1, and 2) interacting with two orthogonal polarizations of light, described by the operators a and b. The atom–photon couplings are respectively g_a and g_b. The energy differences between 0 and 1, and between 0 and 2 are assumed to be nearly equal.

Three level atom (Hamiltonian)

$$H = \begin{bmatrix} H_0 & 0 & 0 \\ 0 & H_1 & 0 \\ 0 & 0 & H_2 \end{bmatrix},$$

$$H_0 = -\delta$$

$$H_1 = \begin{bmatrix} -\delta & g_a & 0 & 0 \\ g_a & \delta & 0 & 0 \\ 0 & 0 & -\delta & g_b \\ 0 & 0 & g_b & \delta \end{bmatrix}$$

$$H_2 = \begin{bmatrix} -\delta & g_a & g_b \\ g_a & \delta & 0 \\ g_b & 0 & \delta \end{bmatrix}.$$

Three level atom (Kerr effect)

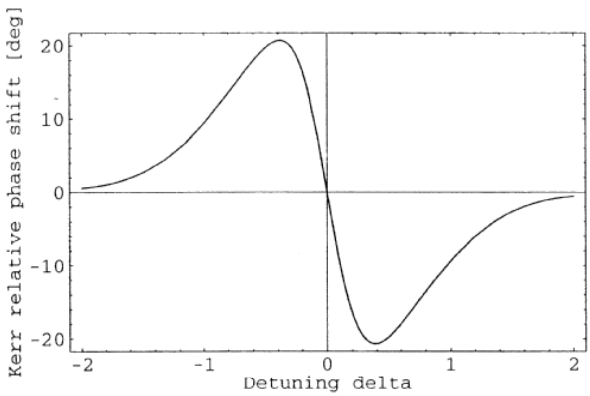


Figure 7.5. Kerr phase shift χ_3 in degrees, for $t = 0.98$ and $g_a = g_b = 1$, plotted as a function of the detuning δ, computed from (7.82) for single photons interacting with a single three-level atom.

7.5.4 Quantum computation

- QED can be used to perform quantum computation in a number of different ways, two of which are the following:
  - Quantum information can be represented by photon states, using cavities with atoms to provide nonlinear interactions between photons
  - Quantum information can be represented using atoms, using photons to communicate between the atoms
- Unitary transform ($\Delta = 16°$, single photons)

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & e^{i\varphi_a} & 0 & 0 \\ 0 & 0 & e^{i\varphi_b} & 0 \\ 0 & 0 & 0 & e^{i(\varphi_a+\varphi_b+\Delta)} \end{bmatrix}$$

7.5.4 Quantum computation

- Input state

$$|\psi_{\text{in}}\rangle = |\beta^+\rangle \left[\frac{|\alpha^+\rangle + |\alpha^-\rangle}{\sqrt{2}}\right]$$

- For approximation $|\alpha\rangle \approx |0\rangle + \alpha|1\rangle$

$$|\psi_{\text{in}}\rangle \approx \left[|0^+\rangle + \beta|1^+\rangle\right]\left[|0^+\rangle + \alpha|1^+\rangle + |0^-\rangle + \alpha|1^-\rangle\right]$$

$$\begin{aligned}|\psi_{\text{out}}\rangle &\approx |0^+\rangle\left[|0^+\rangle + \alpha e^{i\varphi_a}|1^+\rangle + |0^-\rangle + \alpha|1^-\rangle\right] \\ &\quad + e^{i\varphi_b}\beta|1^+\rangle\left[|0^+\rangle + \alpha e^{i(\varphi_a+\Delta)}|1^+\rangle + |0^-\rangle + \alpha|1^-\rangle\right] \\ &\approx |0^+\rangle|\alpha, \varphi_a/2\rangle + e^{i\varphi_b}\beta|1^+\rangle|\alpha, (\varphi_a + \Delta)/2\rangle\,,\end{aligned}$$

7.5.4 Quantum computation

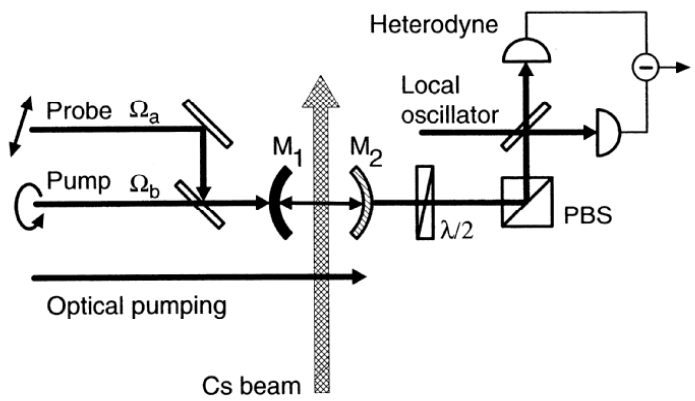


Figure 7.6. Schematic of an experimental apparatus used to demonstrate the possibility of using a single atom to provide cross phase modulation between single photons, as an elementary quantum logic gate. A linearly polarized weak probe beam of light Ω_a, and a stronger circularly polarized pump beam Ω_b are prepared and shone on an optical cavity with high reflectivity mirrors M_1 and M_2. Cesium atoms prepared in the electronic state $6S_{1/2}, F = 4, m = 4$ by optical pumping fall (the figure shows the atoms upside down) such that the average number of atoms in the cavity is around one. The light traverses the cavity, interacting with the atom; σ_+ polarized light causes strong transitions to the $6P_{3/2}, F' = 5, m' = 5$ state, and the orthogonal σ_- polarized light causes weak transitions to the $6P_{3/2}, F' = 5, m' = 3$ state. The polarization of the output light is then measured, using a half wave plate, a polarizing beamsplitter (PBS), and a sensitive balanced heterodyne detector (which selectively detects light at a specific frequency, as determined by the local oscillator). Figure courtesy of Q. Turchette.

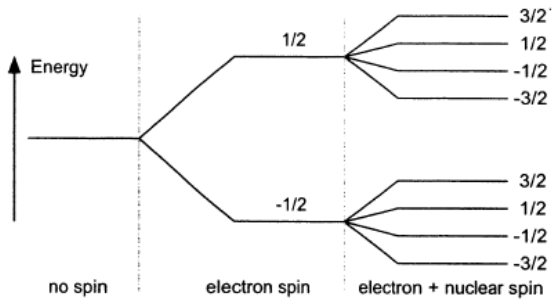
Optical cavity quantum electrodynamics (Summary)

Optical cavity quantum electrodynamics

- **Qubit representation**: Location of single photon between two modes, $|01\rangle$ and $|10\rangle$, or polarization.
- **Unitary evolution**: Arbitrary transforms are constructed from phase shifters (R_z rotations), beamsplitters (R_y rotations), and a cavity QED system, comprised of a Fabry–Perot cavity containing a few atoms, to which the optical field is coupled.
- **Initial state preparation**: Create single photon states (e.g. by attenuating laser light).
- **Readout**: Detect single photons (e.g. using a photomultipler tube).
- **Drawbacks**: The coupling of two photons is mediated by an atom, and thus it is desirable to increase the atom–field coupling. However, coupling the photon into and out of the cavity then becomes difficult, and limits cascadibility.

7.6 Ion traps

- As we saw in previous sections spins provide potentially good representations for qubits. But energy difference between different spin states is typically very small compared with other energy scales (such as the kinetic energy of typical atoms at room temperature).



Ion traps

- However it's possible to increase the accuracy by insulating and trapping small numbers of charged atoms in electromagnetic traps, then cooling the atoms until their kinetic energy is much lower than the spin energy contribution.

Exercise 7.24

The energy of a nuclear in a magnetic field B = 10 Tesla: $\approx 5 \times 10^{-26}$J

Thermal energy of one particle at room temperature: $\approx 2 \times 10^{-31}$J

Trap geometry and lasers

- Hamiltonian governing the motion of the N ions in the trap

$$H = \sum_{i=1}^{N} \frac{M}{2}\left(\omega_x^2 x_i^2 + \omega_y^2 y_i^2 + \omega_z^2 z_i^2 + \frac{|\vec{p}_i|^2}{M^2}\right) + \sum_{i=1}^{N}\sum_{j>i} \frac{e^2}{4\pi\epsilon_0 |\vec{r}_i - \vec{r}_j|}$$

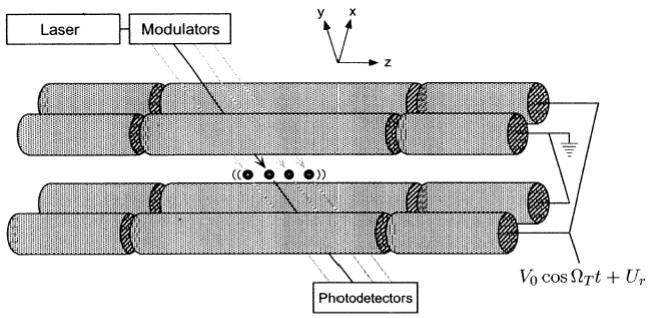


Figure 7.7. Schematic drawing (not to scale) of an ion trap quantum computer, depicting four ions trapped in the center of a potential created by four cylindrical electrodes. The apparatus is typically contained in a high vacuum ($\approx 10^{-8}$ Pa), and the ions are loaded from a nearby oven. Modulated laser light incident on the ions through windows in vacuum chamber perform operations on and are used to readout the atomic states.

Sideband cooling method

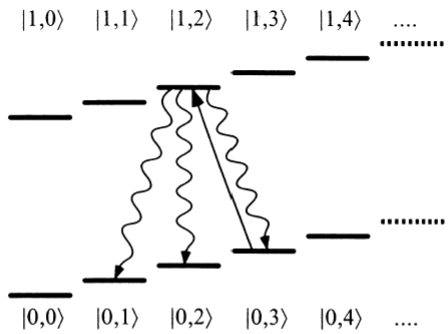


Figure 7.8. Sideband cooling method, showing transitions between $|0, n\rangle$ and $|1, m\rangle$, where 0 and 1 are two electronic levels, and n and m are phonon levels representing motional states of the ion. Laser light is tuned to have energy one phonon less than the electronic transition, such that, for example, the $|0, 3\rangle$ state transitions to the $|1, 2\rangle$ state, as shown. The atom then spontaneously decays into the lower energy 0 state (wiggly lines), randomly going to either $|0, 1\rangle$, $|0, 2\rangle$, or $|0, 3\rangle$ (with nearly equal probabilities). Note that the laser light actually causes all possible transitions between $|0, n\rangle$ and $|1, n-1\rangle$, since these all have the same energy. However, this process does not touch the $|0, 0\rangle$ state, and eventually that is the state in which the atom will be left.

Atomic structure

- There are numerous possible sources of angular momenta in atom: orbital, electron spin, and nuclear spin. Consequently total angular momentum becomes a uniquely defined property of the state.

Example: Two spin-1/2 spins.

The computational basis for this two qubit space is |00>, |01>, |10>, |11>

Using eigenstates of the total momentum operator, defined by $j_x = (X_1 + X_2)/2$, $j_y = (Y_1 + Y_2)/2$, $j_z = (Z_1 + Z_2)/2$, and $J^2 = j_x^2 + j_y^2 + j_z^2$

The states $|j, m_j\rangle_J$ are eigenstates of J^2 with eigenvalue $j(j+1)$, and simultaneously eigenstates og j_z, with eigenvalue m_j.

$$
\begin{aligned}
|0,0\rangle_J &= \frac{|01\rangle - |10\rangle}{\sqrt{2}} \\
|1,-1\rangle_J &= |00\rangle \\
|1,0\rangle_J &= \frac{|01\rangle + |10\rangle}{\sqrt{2}} \\
|1,1\rangle_J &= |11\rangle .
\end{aligned}
$$

7.6.2 The Hamiltonian

$$
\begin{aligned}
H_I &= -\vec{\mu}\cdot\vec{B} \\
&\approx \left[\frac{\hbar\Omega}{2}\left(S_+ e^{i(\varphi-\omega t)} + S_- e^{-i(\varphi-\omega t)}\right)\right] \\
&\quad + \left[i\frac{\eta\hbar\Omega}{2}\left\{S_+ a + S_- a^\dagger + S_+ a^\dagger + S_- a\right\}\left(e^{i(\varphi-\omega t)} - e^{-i(\varphi-\omega t)}\right)\right]
\end{aligned}
$$

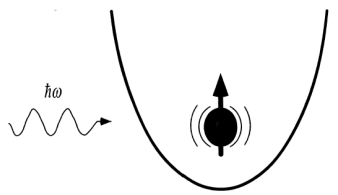


Figure 7.9. Toy model of a trapped ion: a single particle in a harmonic potential with two internal states, interacting with electromagnetic radiation.

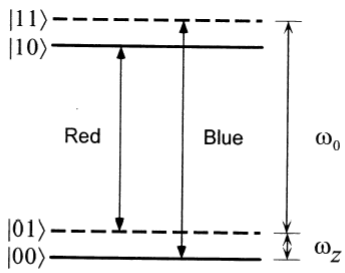


Figure 7.10. Energy levels of the toy model trapped ion showing the red and blue motional sideband transitions, which correspond to creation or annihilation of a single phonon. There is an infinite ladder of additional motional states, which are usually not involved. The states are labeled as $|n, m\rangle$ where n represents the spin state, and m the number of phonons.

7.6.2 The Hamiltonian

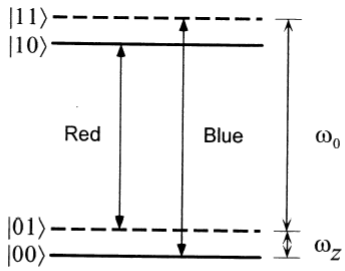


Figure 7.10. Energy levels of the toy model trapped ion showing the red and blue motional sideband transitions, which correspond to creation or annihilation of a single phonon. There is an infinite ladder of additional motional states, which are usually not involved. The states are labeled as $|n, m\rangle$ where n represents the spin state, and m the number of phonons.

$$H_0 = \hbar\omega_0 S_z + \hbar\omega_z a^\dagger a$$

$$S_+(t) = S_+ e^{i\omega_0 t} \qquad S_-(t) = S_- e^{-i\omega_0 t}$$
$$a^\dagger(t) = a^\dagger e^{i\omega_z t} \qquad a(t) = a e^{-i\omega_z t}.$$

$$H_I' = \begin{cases} i\frac{\eta\hbar\Omega}{2}\left(S_+ a^\dagger e^{i\varphi} - S_- a e^{-i\varphi}\right) & \omega = \omega_0 + \omega_z \\ i\frac{\eta\hbar\Omega}{2}\left(S_+ a e^{i\varphi} - S_- a^\dagger e^{-i\varphi}\right) & \omega = \omega_0 - \omega_z \end{cases}$$

Single qubit operations

- Applying an electromagnetic field tuned to frequency ω_0 turns on the internal Hamiltonian term

$$H_I^{\text{internal}} = (\hbar\Omega/2)(S_+ e^{i\varphi} + S_- e^{-i\varphi})$$

- By choosing φ and the duration of the interaction appropriately, this allows us to perform operations $\boldsymbol{R_x(\theta) = exp(-i\theta S_x)}$ and $\boldsymbol{R_y(\theta) = exp(-i\theta S_y)}$, which by Theorem 4.1 thereby allow us to perform any single qubit operation on the spin state.
  - ***Theorem 4.1:*** ***Suppose U is a unitary operation on a single qubit. Then there exist real numbers a, b, g and d such that***

$$\boldsymbol{U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta)}$$

Controlled phase-flip gate

- If one qubit is stored in the atom's internal spin state, and another qubit is stored using the |0> and |1> phonon states, it a controlled phase-flip gate can be perform with the unitary transform

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$$

Controlled phase-flip gate

- For an atom that has a third energy level and laser tuning to the frequency $\omega_{aux} + \omega_z$, to cause transitions between the |20> and |11> states:

$$H_{aux} = i(\eta\hbar\Omega`/2)(S_+e^{i\varphi} + S_-e^{-i\varphi})$$

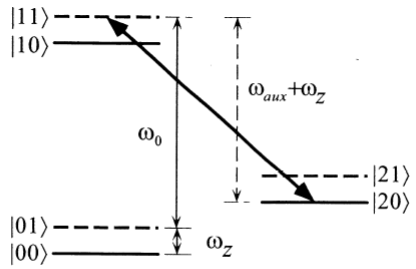


Figure 7.11. Energy levels of a three-level atom in an ion trap, with two phonon states each. The labels $|n, m\rangle$ indicate the atom's state n and the phonon state m. The $|20\rangle \leftrightarrow |11\rangle$ transition is used to perform a controlled phase-flip gate.

Swap gate

- Swapping qubits between the atom's internal spin state and the phonon state can be done by tuning a laser to the frequency w0 – wz, and arranging the unitary transform

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

- If the initial state is a|00> + b|10> (that is, the phonon is initially |0>), then the state after the swap is a|00> + b|01>, so this accomplishes the desired swap operation.

7.6.4 Experiment and summary

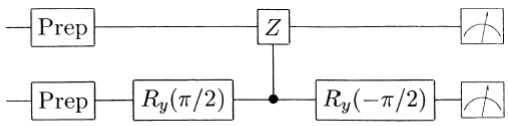


Figure 7.14. Quantum circuit modeling the ion trap controlled-NOT experiment. The top wire represents the phonon state, and the bottom, the ion's internal hyperfine state.

Ion trap quantum computer

- **Qubit representation**: Hyperfine (nuclear spin) state of an atom, and lowest level vibrational modes (phonons) of trapped atoms.
- **Unitary evolution**: Arbitrary transforms are constructed from application of laser pulses which externally manipulate the atomic state, via the Jaynes–Cummings interaction. Qubits interact via a shared phonon state.
- **Initial state preparation**: Cool the atoms (by trapping and using optical pumping) into their motional ground state, and hyperfine ground state.
- **Readout**: Measure population of hyperfine states.
- **Drawbacks**: Phonon lifetimes are short, and ions are difficult to prepare in their motional ground states.

Nuclear magnetic resonance (NMR)

- NMR is a phenomenon which occurs when the nuclei of certain atoms are immersed in a static magnetic field and exposed to a second oscillating magnetic field.

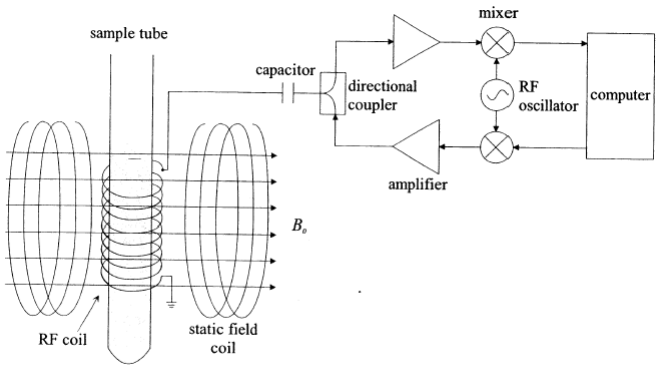


Figure 7.16. Schematic diagram of an NMR apparatus.

Single spin dynamics

- The Hamiltonian

$$H = (\omega_0/2)Z + g(X\cos\omega t + Y\sin\omega t)$$

- Schrödinger equation

$$i\partial_t|\chi(t)\rangle = H|\chi(t)\rangle$$

- Solution

$$|\vec{n}| = t\sqrt{\left(\frac{\omega_0 - \omega}{2}\right)^2 + g^2}$$

- A single qubit rotation about the axis

$$\hat{n} = \frac{\hat{z} + \frac{2g}{\omega_0 - \omega}\hat{x}}{\sqrt{1 + \left(\frac{2g}{\omega_0 - \omega}\right)^2}}$$

By an angle

$$|\varphi(t)\rangle = e^{i\left[\frac{\omega_0 - \omega}{2}Z + gX\right]t}|\varphi(0)\rangle$$

Decoherence

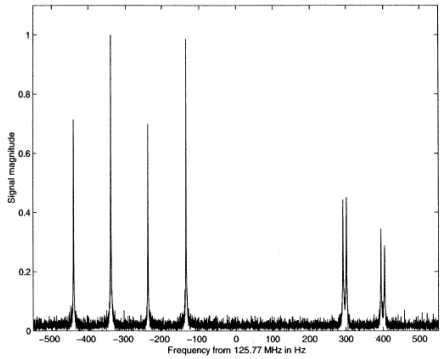


Figure 7.17. Carbon spectrum of ^{13}C labeled trichloroethylene. The four lines on the left come from the carbon nucleus directly bound to the proton; four lines appear because of couplings to the proton and to the second carbon nucleus, whose own signal gives the closely spaced four lines on the right. The second carbon nucleus is further away from the proton than the first, and thus has a much smaller coupling to it.

- For a single qubit state, these effects may be phenomenologically characterized with a density matrix transformation model

$$\begin{bmatrix} a & b \\ b^* & 1-a \end{bmatrix} \rightarrow \begin{bmatrix} (a-a_0)e^{-t/T_1}+a_0 & be^{-t/2T_2} \\ b^*e^{-t/2T_2} & (a_0-a)e^{-t/T_1}+1-a_0 \end{bmatrix}$$

Multiple spin Hamiltonian

- For an ***n*** spin coupled system:

$$H = \sum_k \omega_k Z_k + \sum_{j,k} H^J_{j,k} + H^{\mathrm{RF}} + \sum_{j,k} H^{\mathrm{D}}_{j,k} + H^{\mathrm{env}}$$

- Simple two spin Hamiltonian

$$H = H^{sys} + N^{RF}$$

$$H^{sys} = aZ_1 + bZ_2 + cZ_1Z_2$$

$$e^{-iH^{sys}t/\hbar}R^2_{x1}e^{-iH^{sys}t/\hbar}R^2_{x1} = e^{-2ibZ_1t/\hbar}$$

- Realization of a controlled-NOT gate is simple using refocusing pulses and single qubit pulses. Unitary transform:

$$U_{CZ} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$$

$$\sqrt{i}\,e^{iZ_1Z_2\pi/4}e^{-iZ_1\pi/4}e^{-iZ_2\pi/4} = U_{CZ}$$

7.7.4 Experiment

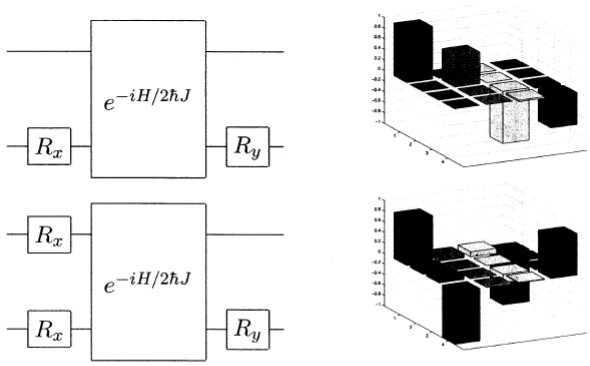


Figure 7.19. Quantum circuits implemented with NMR and the real part of the experimentally measured output deviation density matrices. In these circuits, R_x and R_y denote single qubit gates which perform 90° rotations about $\hat{x}$ and $\hat{y}$, implemented with RF pulses about 10 microseconds long, and the two qubit box with $e^{-iH/2\hbar J}$ is a free evolution period of time $1/2J \approx 2.3$ milliseconds. (top) Controlled-NOT circuit, and the output measured for a thermal state input, showing the exchange of the $|10\rangle$ and $|11\rangle$ diagonal elements, as expected from the classical truth table for the CNOT gate. (bottom) Circuit for creating the Bell state $(|00\rangle - |11\rangle)/\sqrt{2}$, and its output, when a $|00\rangle$ effective pure state is prepared as an input.

Quantum algorithm

- Three required operators for a problem size of four elements (n=2 qubits):
  - oracle operator O (which performs a phase flip based on the f(x)
    - x = {0,1,2,3}; f(x) = 0 except at one value x_0, where $f(x_0) = 1$

$$O = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$$

  - the Hadamard operator on two qubits $H^{\otimes 2}$
  - the conditional phase shift operator P

$$P = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$$

NMR quantum computer (Summary)

NMR quantum computer

- **Qubit representation**: Spin of an atomic nucleus.
- **Unitary evolution**: Arbitrary transforms are constructed from magnetic field pulses applied to spins in a strong magnetic field. Couplings between spins are provided by chemical bonds between neighboring atoms.
- **Initial state preparation**: Polarize the spins by placing them in a strong magnetic field, then use 'effective pure state' preparation techniques.
- **Readout**: Measure voltage signal induced by precessing magnetic moment.
- **Drawbacks**: Effective pure state preparation schemes reduce the signal exponentially in the number of qubits, unless the initial polarization is sufficiently high.

Quantum Computational Intelligence

Outline

- Overview
- Quantum search (revisited)
  - Extensions:
    - Search over arbitrary initial amplitude distributions
    - Quantum Associative Memory (QuAM)
- Beyond Phase Amplification
  - QuAM - Upgraded
  - Competitive Learning
- Conclusions

Quantum Computational Intelligence

Computational intelligence

- Seeks to produce algorithms that solve problems which are intractable using traditional methods of computation.

Quantum Computational intelligence

- Extension of the field into the domain of quantum computing.

Current Research

- Quantum Artificial Neural Networks
- Structured Search
- Quantum inspired Genetic Algorithm
- Decision Tree evaluation using quantum computation.
- Quantum algorithm for learning DNF formulas
- Quantum Bayesian Networks

Quantum Artificial Neural Networks

- Quantum Associative Memory
- Competitive Learning
- ANN implementation using quantum dots

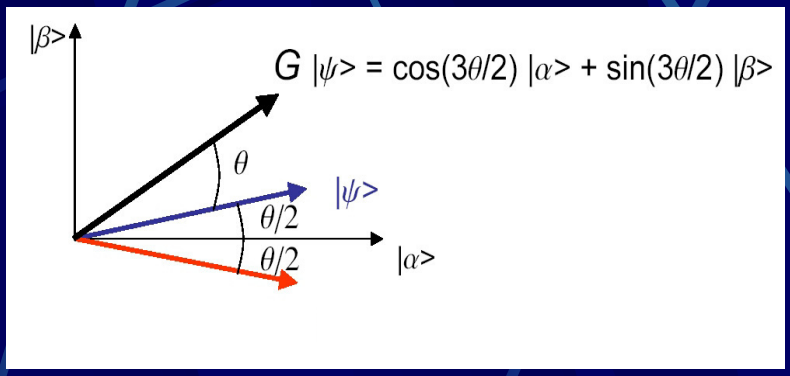
‘Classical’ problems with ANNs

- Repetition of training examples
  - humans do not undergo the prolonged and repeated exposure to information that ANNs require to learn training patterns.
- Memoryless learning / Catastrophic forgetting
  - humans remember and recall information that is provided to them as a part of learning.
  - For ANNs, training examples are used for the changing of the weights and are immediately forgotten.
  - new information forces a neural network to forget older information. (ICNN´97, Menneer and Narayanan, 1998).

Quantum Based ANN's

- Pros:
  - Exponential Memory Capacity
  - Fast (Linear/Polynomial) training times
  - Closer resemblance to human cognitive processing (???)
- Cons
  - Input collapses the quantum wave function
    - I.e.. The superposition of stored patterns is collapsed to a single pattern.
    - So the QuANN needs to be retrained constantly

Grover's Search Revisited



$$\hat{I}_\phi = \text{the identity matrix except for } \phi\phi = -1$$

$$\hat{G} = -H^{\otimes n}\hat{I}_0 H^{\otimes n}$$

Notation

$$|\tau\rangle = |101\rangle$$

$$= 0|000\rangle + 0|001\rangle + 0|010\rangle + 0|011\rangle + 0|100\rangle + 1|101\rangle + 0|110\rangle + 0|111\rangle$$

$$= (0, 0, 0, 0, 0, 1, 0, 0)$$

Example

$$|\psi\rangle = |000\rangle = (1, 0, 0, 0, 0, 0, 0, 0)$$

$$|\psi\rangle \mapsto |\psi'\rangle = \frac{1}{2\sqrt{2}}(1, 1, 1, 1, 1, 1, 1, 1)$$

Apply Grover Iteration:

$$\frac{\pi}{4}\sqrt{N} = \frac{\pi}{4}\sqrt{8} = 2.22 \approx 2$$

Example (cont)

- Iteration 1

$\hat{I}_\phi$ $|\psi^{'}\rangle \mapsto |\psi^{''}\rangle = \frac{1}{2\sqrt{2}}(1,1,1,1,1,-1,1,1)$

$\hat{G}$ $|\psi^{''}\rangle \mapsto |\psi^{'''}\rangle = \frac{1}{4\sqrt{2}}(1,1,1,1,1,5,1,1)$

- Iteration 2

$\hat{I}_\phi$ $|\psi^{'''}\rangle \mapsto |\psi^{''''}\rangle = \frac{1}{4\sqrt{2}}(1,1,1,1,1,-5,1,1)$

$\hat{G}$ $|\psi^{''''}\rangle \mapsto |\psi^{'''''}\rangle = \frac{1}{16\sqrt{2}}(-2,-2,-2,-2,-2,-21,-2,-2)$

- Measure

$(\frac{21}{16\sqrt{2}})^2 = 86.13\%$

Arbitrary Initial distribution Example

- Pass

$|\psi\rangle = \frac{1}{2}(1,0,0,1,1,1,0,0)$

$\hat{I}_\phi$ $|\psi\rangle \mapsto |\psi^{'}\rangle = \frac{1}{2}(1,0,0,1,1,-1,0,0)$

$\hat{G}$ $|\psi^{'}\rangle \mapsto |\psi^{''}\rangle = \frac{1}{4}(-1,1,1,-1,-1,3,1,1)$

$\hat{I}_\phi$ $|\psi^{''}\rangle \mapsto |\psi^{'''}\rangle = \frac{1}{4}(-1,1,1,-1,-1,-3,1,1)$

$\hat{G}$ $|\psi^{'''}\rangle \mapsto |\psi^{''''}\rangle = \frac{1}{8}(1,-3,-3,1,1,5,-3,-3)$

39.06%

Arbitrary Initial distribution (cont)

- Need to create a new operator which synchronizes the phase of non-solution states.
- Define an operator which performs a phase shift on set P containing all states with non-zero amplitudes. $\hat{I}_P$

Example 3

$$|\psi\rangle = \frac{1}{2}(1,0,0,1,1,1,0,0)$$

$\hat{I}_\phi$ $|\psi\rangle \mapsto |\psi'\rangle = \frac{1}{2}(1,0,0,1,1,-1,0,0)$

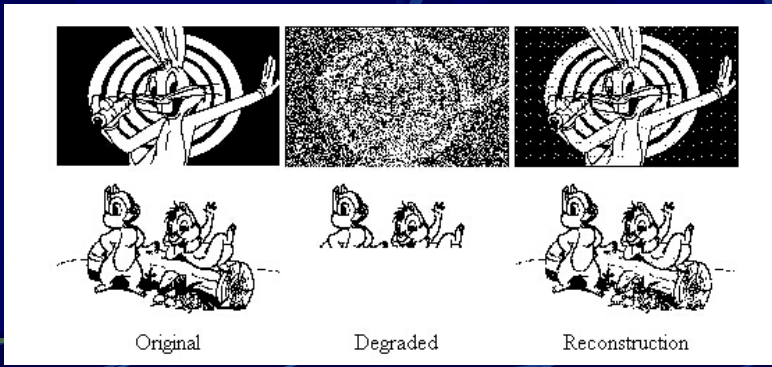
$\hat{G}$ $|\psi'\rangle \mapsto |\psi''\rangle = \frac{1}{4}(-1,1,1,-1,-1,3,1,1)$

$\hat{I}_P$ $|\psi'\rangle \mapsto |\psi''\rangle = \frac{1}{4}(1,1,1,1,1,-3,1,1)$

$\hat{G}$ $|\psi''\rangle \mapsto |\psi'''\rangle = (0,0,0,0,0,1,0,0)$

Associative Memory (AM)

- Performs pattern completion
  - Learning a set (P) of ***complete*** prototypical patterns
  - Output a complete pattern upon presentation of an incomplete or noisy input pattern



Quantum Associative Memory

- Initial pattern memorization / Learning (not covered)
- Can be performed in O(nm) number of steps using 2n+1 qubits where
  - n – pattern length
  - m – number of patterns

Quantum Associative Memory (I)

- Pattern completion
  - Can be done using the modified search algorithm presented previously.

$$|\psi^{'}\rangle = \hat{G}\hat{I}_P\hat{G}\hat{I}_\tau|\psi\rangle$$

  - Repeat T times (T≈≈√N)

$$|\psi^{''}\rangle = \hat{G}\hat{I}_\tau|\psi^{'}\rangle$$

Example 4

$$|\psi\rangle = \frac{1}{2}(1,0,0,1,1,1,0,0)$$

but now the pattern we search for is $\tau = |00?\rangle$. Then:

$$|\psi\rangle \longmapsto^{\hat{I}_\tau} |\psi^{'}\rangle = \frac{1}{4}(-1,0,0,1,1,1,0,0)$$

$$|\psi^{'}\rangle \longmapsto^{\hat{G}} |\psi^{''}\rangle = \frac{1}{4}(3,1,1,-1,-1,-1,1,1)$$

$$|\psi^{''}\rangle \longmapsto^{\hat{I}_P} |\psi^{'''}\rangle = \frac{1}{4}(-3,-1,1,1,1,1,1,1)$$

$$|\psi^{'''}\rangle \longmapsto^{\hat{G}} |\psi^{''''}\rangle = \frac{1}{8}(7,3,-1,-1,-1,-1,-1,-1)$$

Thus the probability of obtaining the correct answer is $(\frac{7}{8})^2 = 76.6\%$

QuAM summary

- Need to create a pattern DB represented as a superposition of states
- At the same time need to create the operator $\hat{I}_P$
- To query the system need to create the operator $\hat{I}_\phi$, where ϕ is(are) the target pattern(s)

Classical vs Quantum Associative Memory

- Classical Case (Hopfield Network)
  - Can store approx. 0.15n patterns, where n is the number of nodes
- QuAM
  - Stores 2^n patterns, where n is the number of qubits.
  - Quantum search is quite slow for pattern recall.

Beyond Phase Amplification

- Question:

  Are Unitary Operators Nessesary ??

  - **For DB initialization -> Yes**
    - **To create a coherent superposition of basis states reversible operators must be used.**
  - **For query Processing -> NO**
    - **The superposition is collapsed anyways**

Non-Unitary Operators

- Ex: Observation of a system is not unitary nor evolutionary
- Since pattern recall requires decoherance and collapse of the quantum system into one basis state, pattern recall is a non-evolutionnary and non-unitary operation.

Non-Unitary Operators

- Given a string *q* over the alphabet *{ 0,1,? }*, define a new (non-unitary) operator $\hat{R}^q$

$$r_{\phi\chi} = \begin{cases} 1 & \text{if } \phi \equiv \chi \text{ and } h(\phi, q) \geq 1 \\ -1 & \text{if } h(\phi, q) > h(\chi, q) \geq 1 \\ 0 & \text{otherwise} \end{cases}$$

  - Where h(a,b) is the hamming distance
  - The '1's entries allow states with non-zero hamming disnace the possibility of being chosen.
  - The '-1' perform destructictive interference to allow the state with maximal hamming distance to be chosen.

Example 5a

- Consider a 2 qubit system

$$|\psi\rangle = 1/\sqrt{2}\,|01\rangle + 1/\sqrt{2}\,|11\rangle$$

- And a query string q = '11'

$$\hat{R}^{11} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$\hat{R}^{11}|\psi\rangle = |11\rangle$$

Example 5b

- Consider a 2 qubit system
- And a query $|\psi\rangle = 1/\sqrt{2}\,|00\rangle + 1/\sqrt{2}\,|10\rangle$

$$\hat{R}^{11} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$\hat{R}^{11}|\psi\rangle = |10\rangle$$

Competitive Learning

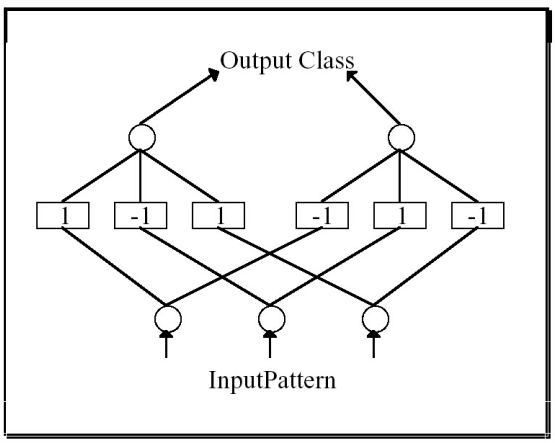


Figure 1. Classical Hamming net storing two patterns

Conclusions

- QuAM offers exponential increase instorage capasity
- Using phase ampliphication offers polynomial(quadratic) speedup in pattern retreval over 1-nearest neighbour alg.
- Using non-unitary operators offers an exponential speedup for pattern retreval.

Conclusions

- QuAM is the most practical application of Quantum Computing
  - A 30 qubit system can store over a billion patterns
  - Shor's factoring technique will only be practical if we can factor very large numbers (> 512 bits) requiring a large number of qubits.

References

- http://www.cic.unb.br/docentes/weigang/qc/aci.html
- http://www.cs.ualberta.ca/~ilya/courses/c605-QC/Refs.pdf

Final Thoughts

- **Prof. Sham:** Well, we factored number 15 into 3 times 5. It was a thorny problem, but, by Jove, we did it. We started building our NMR computer in 1997 with a 5-million-dollar grant from DARPA. So it took 5 years, a few million dollars, and much hard work to build our room sized computer. But just think how powerful it is! And according to theory, NMR computers have tremendous growth potential. They can have as many as 10 qubits!
- **Reporter:** Could you please tell us something about your future plans?
- **Prof. Sham:** Well. I plan to continue publishing in Nature Magazine. Another exciting development is that I plan to add one more qubit to NMR computers in the next few years. We've won another 3-million-dollar grant from DARPA to continue our work. Isn't our government just great! We can't wait to start factoring number 18.

Archive/Links

[Home]
[Members]
[Schedule]
[Overview]
[Sponsors]
[Archive/Links]
[Contact]

Mar 8, 2002 QC Seminar (Winter'01) materials are still available here:
http://www.cs.ualberta.ca/~bulitko/qc/qc2001

Mar 8, 2002 University of Waterloo QC slides for the textbook are here:
http://cacr.math.uwaterloo.ca/~mmosca/quantumcoursef00.htm

May 2, 2002 Here is a link for the Quantum Computation and Quantum Information book:
http://squint.org/qci/
The website contains: Errata, Sample from Chapter 1, and Changes from 1st to 2nd printing

May 2, 2002 The following is a link to a page containing a quantum computer emulator:
http://rugth30.phys.rug.nl/compphys0/qce.htm
in case someone is interested.

May 13, 2002 Quantum mechanics postulate 3 (p. 84 of the text) discussion is here.

May 14, 2002 UofT Summer School in Quantum Information Processing (May 14-18, 2001) :
http://www.fields.utoronto.ca/programs/scientific/00-01/quantum_computing/abstracts.html

May 21, 2002 From Vahid Rezania on the garbage bits: I think the problem is raised because the
function g(x) remains unknown. If there is no information about g(x) and
you cannot erase it, probably you cannot reverse the process. Further in
quantum case this qubit will interfer with output qubit, and again since
there is no information about g(x), you cannot get the exact result.

May 22, 2002 From Dan Tzur on why garbage bits are bad : Well, I don't know yet, but I found this webpage that could lead to an answer:

http://arxiv.org/PS_cache/quant-ph/pdf/9806/9806084.pdf

and this:

http://qso.lanl.gov/~zalka/QC/QC.html

Home | Members | Schedule | Overview | Sponsors | Archive/Links | Contact

For problems or questions regarding this web contact V.Bulitko.
Last updated: 03/08/02.

Contact

[Home]
[Members]
[Schedule]
[Overview]
[Sponsors]
[Archive/Links]
[Contact]

Name Prof. Vadim Bulitko
(summer school chair)

Mailing Address Department of Computing Science
University of Alberta
Edmonton, Alberta, T6G 2H1
CANADA

Fax (780) 492-1071

WWW http://www.cs.ualberta.ca/~bulitko

E-Mail bulitko@ualberta.ca

Home | Members | Schedule | Overview | Sponsors | Archive/Links | Contact

For problems or questions regarding this web contact V.Bulitko.
Last updated: 03/08/02.

Overview

[Home]
[Members]
[Schedule]
[Overview]
[Sponsors]
[Archive/Links]
[Contact]

Summer School Title	Introduction to Quantum Computing (*the Computing Science Perspective*)
Short-term objectives	Introduce Quantum Computing basics to the interested parties around UofA
Long-term objectives	Engage into AI/CS/Math research projects benefiting from Quantum Computing
Format	Seminar-type meetings, tentatively 1-1.5 hours twice a week
Prerequisitives	No background in quantum mechanics or linear algebra is required. General computing science/math background would be beneficial
Target audiences	CS/Math/Physics grad students & faculty but open to all interested parties
Textbook	Nielsen, M., Chuang, L., (2000). *Quantum Computation and Quantum Information*. Cambridge University Press.
	(the numbers correspond to the sections in the text -- as a summer school/seminar we will have a certain flexibility in the topic selection and will be able to take audience feedback into account): 1 Introduction and overview 1 1.1 Global perspectives 1 1.1.1 History of quantum computation and quantum information 2 1.1.2 Future directions 12 1.2 Quantum bits 13 1.2.1 Multiple qubits 16 1.3 Quantum computation 17 1.3.1 Single qubit gates 17 1.3.2 Multiple qubit gates 20 1.3.3 Measurements in bases other than the

Tentative topics	computational basis 22 1.3.4 Quantum circuits 22 1.3.5 Qubit copying circuit? 24 1.3.6 Example: Bell states 25 1.3.7 Example: quantum teleportation 26 1.4 Quantum algorithms 28 1.4.1 Classical computations on a quantum computer 29 1.4.2 Quantum parallelism 30 1.4.3 Deutsch's algorithm 32 1.4.4 The Deutsch--Jozsa algorithm 34 1.4.5 Quantum algorithms summarized 36 1.5 Experimental quantum information processing 42 1.5.1 The Stern--Gerlach experiment 43 1.5.2 Prospects for practical quantum information processing 46 1.6 Quantum information 50 1.6.1 Quantum information theory: example problems 52 1.6.2 Quantum information in a wider context 58 2 Introduction to quantum mechanics 60 2.1 Linear algebra 61 2.2 The postulates of quantum mechanics 80 2.3 Application: superdense coding 97 2.4 The density operator 98 2.4.1 Ensembles of quantum states 99 2.4.2 General properties of the density operator 101 2.4.3 The reduced density operator 105 2.5 The Schmidt decomposition and purifications 109 2.6 EPR and the Bell inequality 111 3 Introduction to computer science 120 3.1 Models for computation 122 3.2 The analysis of computational problems 135 3.3 Perspectives on computer science 161 4 Quantum circuits 171 4.1 Quantum algorithms 172 4.2 Single qubit operations 174 4.3 Controlled operations 177

	4.4 Measurement 185 4.5 Universal quantum gates 188 4.6 Summary of the quantum circuit model of computation 202 4.7 Simulation of quantum systems 204 5 The quantum Fourier transform and its applications 216 5.1 The quantum Fourier transform 217 5.2 Phase estimation 221 5.3 Applications: order-finding and factoring 226 5.4 General applications of the quantum Fourier transform 234 6 Quantum search algorithms 248 6.1 The quantum search algorithm 248 6.2 Quantum search as a quantum simulation 255 6.3 Quantum counting 261 6.4 Speeding up the solution of NP-complete problems 263 6.5 Quantum search of an unstructured database 265 6.6 Optimality of the search algorithm 269 6.7 Black box algorithm limits 271 7 Quantum computers: physical realization 277 7.1 Guiding principles 277 7.2 Conditions for quantum computation 279 7.2.1 Representation of quantum information 279 7.2.2 Performance of unitary transformations 281 7.2.3 Preparation of fiducial initial states 281 7.2.4 Measurement of output result 282 7.3 Harmonic oscillator quantum computer 283 7.3.1 Physical apparatus 283
Presenters	Prof. Vadim Bulitko & TBA
Tentative time-line	May - June 2002
Class participation	Due to the volume of the material and limited lecture time an active off-line reading of the text and working through the exercises will be necessary for the participants. Guest presentations will be welcome.

Registration	No official UofA registration is required. Simply e-mail to the school chair if you are [seriously] interested in attending and/or presenting/teaching.

Home | Members | Schedule | Overview | Sponsors | Archive/Links | Contact

For problems or questions regarding this web contact V.Bulitko.
Last updated: 03/08/02.