

Introduction to Quantum Computing for Folks

Joint Advanced Student School 2009

Ing. Javier Enciso
encisomo@in.tum.de

Technische Universität München

April 2, 2009

Table of Contents

- 1 Introduction
- 2 Quantum Mechanics
- 3 Quantum Bits
- 4 Quantum Gates
- 5 Quantum Computers
- 6 Quantum Algorithms
- 7 Conclusions

A (qu)bit of General Culture I



Figure 1: Sombrero vueltiao (Hat with laps)

A (qu)bit of General Culture II



Figure 2: Botero's Painting

Recommendations

- Forget the idea of common sense
- Einstein: “God does not play dice”
- Bohr: “Stop telling God what to do with his dice”
- Keep as skeptical as you can
- Find out the intended bugs

Table of Contents

- 1** Introduction
- 2 Quantum Mechanics
- 3 Quantum Bits
- 4 Quantum Gates
- 5 Quantum Computers
- 6 Quantum Algorithms
- 7 Conclusions

Introduction

- Certain quantum mechanical effects cannot be simulated efficiently on a classical computer [2]
- Building quantum computers proved tricky, and no one was sure how to use the quantum effects to speed up computation
- Applications of interest:
 - Quantum key distribution
 - Quantum teleportation
 - A three-bit quantum computer
- In quantum systems the amount of parallelism increases exponentially with the size of the system
- Physical implementation:
 - Ion traps
 - Nuclear Magnetic Resonance (NMR)
 - Optical and solid state techniques

Ion traps



Figure 3: 4 Magnets

Ion traps

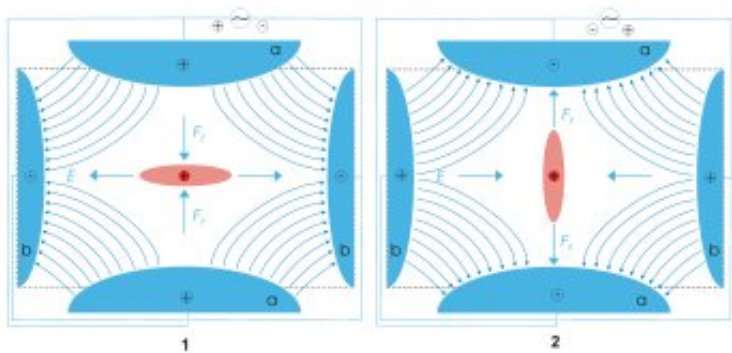


Figure 4: Paul trap

Table of Contents

- 1 Introduction
- 2 Quantum Mechanics**
- 3 Quantum Bits
- 4 Quantum Gates
- 5 Quantum Computers
- 6 Quantum Algorithms
- 7 Conclusions

Quantum Mechanics

- Quantum mechanics describes physical systems at the atomic level
- Quantum mechanical phenomena are difficult to understand since most of everyday experiences are not applicable
- By definition Quantum mechanics leads to several apparent paradoxes:
 - Compton effect: an action precedes its cause
 - Schrödinger's cat: the cat is simultaneously alive and dead
 - Einstein, Podolsky, and Rosen paradox: spooky action at a distance

Experiment I

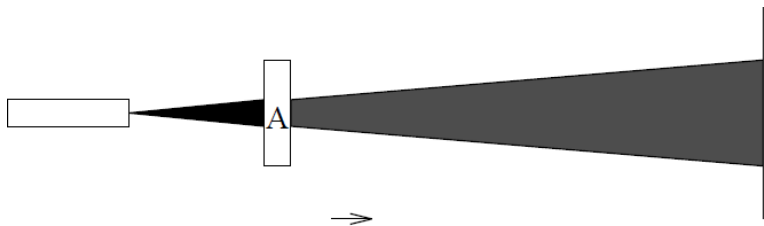


Figure 5: Photon Polarization Experiment

Experiment II

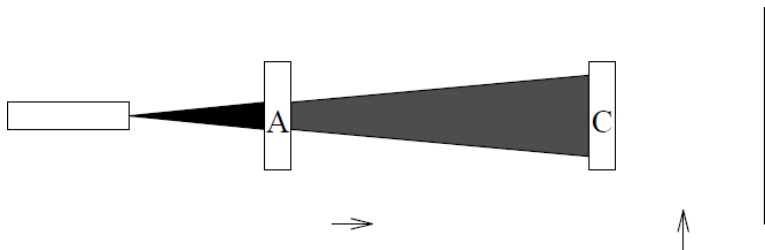


Figure 6: Photon Polarization Experiment

Experiment III

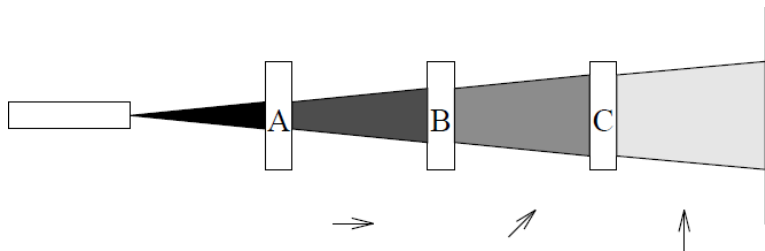


Figure 7: Photon Polarization Experiment

State Spaces and Bra/Ket Notation

- Ket $|x\rangle$ denotes column vectors and are typically used to describe quantum states
- Bra $\langle x|$ denotes the conjugate transpose of $|x\rangle$
- Combining $\langle x|$ and $|y\rangle$ as in $\langle x||y\rangle$, also written as $\langle x|y\rangle$
- Remarkable results:
 - Inner Product $\langle 0|0\rangle = 1$ (Normality)
 - $\langle 0|1\rangle = 0$ (Orthogonality)
 - $|0\rangle\langle 1||1\rangle = |0\rangle\langle 1|1\rangle = |0\rangle$
 - $|0\rangle\langle 1||0\rangle = |0\rangle\langle 1|0\rangle = 0|0\rangle = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$
 - Outer Product $|0\rangle\langle 1| = \begin{pmatrix} 1 \\ 0 \end{pmatrix} (0, 1) = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$

Table of Contents

- 1 Introduction
- 2 Quantum Mechanics
- 3 Quantum Bits**
- 4 Quantum Gates
- 5 Quantum Computers
- 6 Quantum Algorithms
- 7 Conclusions

Quantum Bits

- A qubit is a unit vector in a two dimensional complex vector space with fixed basis
- Orthonormal basis $|0\rangle$ and $|1\rangle$ may correspond to $|\uparrow\rangle$ and $|\rightarrow\rangle$
- The basis states $|0\rangle$ and $|1\rangle$ are taken to represent the classical bit values 0 and 1 respectively
- Qubits can be in a superposition of $|0\rangle$ and $|1\rangle$ such as $a|0\rangle + b|1\rangle$
- $|a|^2$ and $|b|^2$ are the probabilities that the measured value are $|0\rangle$ and $|1\rangle$ respectively

Quantum Key Distribution I

- Sequences of single qubits can be used to transmit private keys on insecure channels
- Classically, public key encryption techniques are used for key distribution
- For example, Alice and Bob want to agree on a secret key so that they can communicate privately. They are connected by an ordinary bi-directional open channel and a uni-directional quantum channel both of which can be observed by Eve, who wishes to eavesdrop on their conversation

Quantum Key Distribution II



Figure 8: Alice

Quantum Key Distribution III



Figure 9: Bob

Quantum Key Distribution IV



Figure 10: Eve

Quantum Key Distribution V

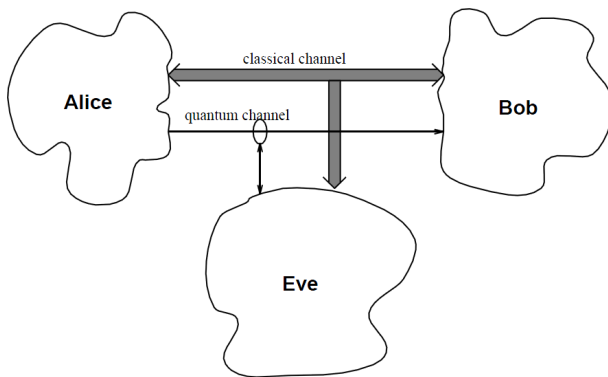


Figure 11: Key Distribution Scenario

Quantum Key Distribution VI

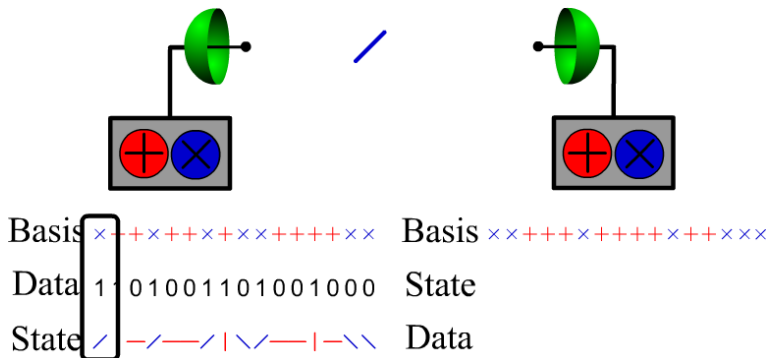
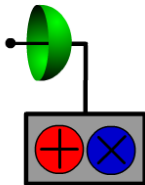
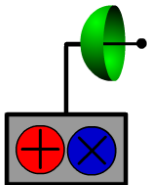


Figure 12: Transmission of the first state

Quantum Key Distribution VII



Basis $\times + + \times + + \times + \times + + + + \times \times$

Data 1101001101001000

State $\diagup | - \diagdown - \diagup | \diagdown - \diagup | - \diagdown$

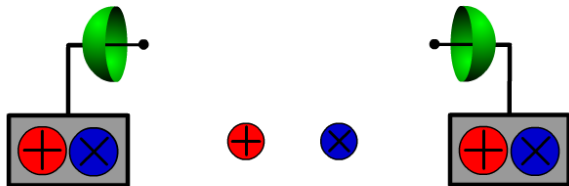
Basis $\times \times + + + \times + + + + \times + + \times \times \times$

State $\diagdown - \diagup | | | - \diagdown - \diagup | \diagdown$

Data 1000011110001100

Figure 13: Transmission of the last state

Quantum Key Distribution VIII



Basis $\times+++ \times+++ \times++ \times++++ \times\times$

Data 1101001101001000

State $\diagup | - \diagdown - \diagup | \diagdown - \diagup | - \diagdown$

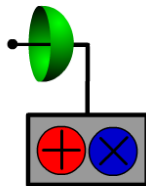
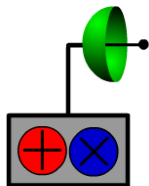
Basis $\times\times+++ \times++++ \times+++ \times++ \times\times$

State $\diagdown - \diagup | | - \diagdown | \diagup \diagdown$

Data 1000011110001100

Figure 14: Exchange of the basis

Quantum Key Distribution IX



Basis	x	+	+	+	++	xx	Basis	x	+	+	+	++	xx
Data	1	0	0	1	0	1	State	/	-	-		-	\
State	/	-	-		-	\	Data	1	0	0	1	0	1

Figure 15: Final agreement between Alice and Bob

Quantum Key Distribution X

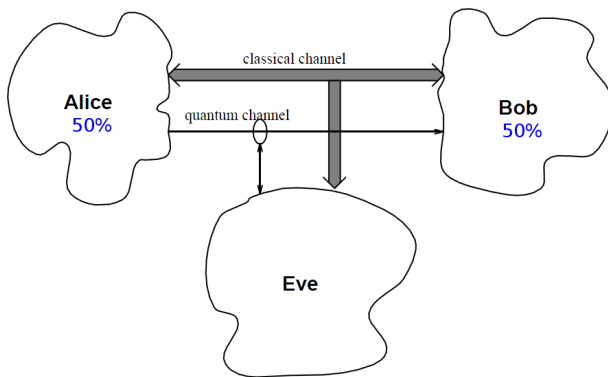


Figure 16: Agreement between Alice and Bob

Quantum Key Distribution XI

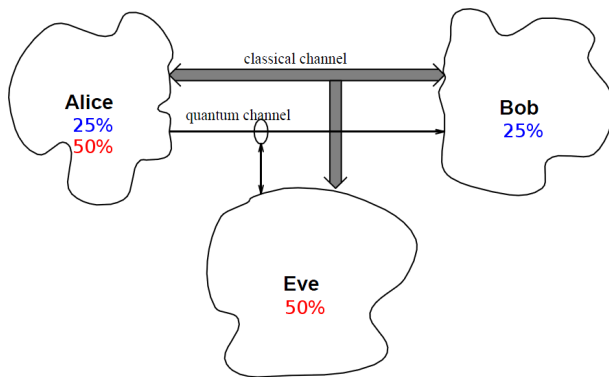


Figure 17: Agreement between Alice, Bob, and Eve

Multiple Qubits

- The state of a qubit can be represented by a vector in the two dimensional complex vector space spanned by $|0\rangle$ and $|1\rangle$
- The state space for two qubits, each with basis $\{|0\rangle, |1\rangle\}$, has basis $\{|0\rangle \otimes |0\rangle, |0\rangle \otimes |1\rangle, |1\rangle \otimes |0\rangle, |1\rangle \otimes |1\rangle\}$, briefly, $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$

Example: Entangled States

The state $|00\rangle + |11\rangle$ cannot be described in terms of the state of each of its qubits separately. In other words, we cannot find a_1, a_2, b_1, b_2 such that $(a_1|0\rangle + b_1|1\rangle) \otimes (a_2|0\rangle + b_2|1\rangle) = |00\rangle + |11\rangle$ since

$$\begin{aligned}(a_1|0\rangle + b_1|1\rangle) \otimes (a_2|0\rangle + b_2|1\rangle) = \\ a_1a_2|00\rangle + a_1b_2|01\rangle + b_1a_2|10\rangle + b_1b_2|11\rangle\end{aligned}$$

and $a_1b_2 = 0$ implies that either $a_1a_2 = 0$ or $b_1b_2 = 0$

Measurement I

- The result of a measurement is probabilistic and the process of measurement changes the state to that measured

Example: Measurement of a 2-qubit system

- Any 2-qubit state can be expressed as $a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$. Where $a, b, c,$ and d are complex numbers such that $|a|^2 + |b|^2 + |c|^2 + |d|^2 = 1$
- Suppose we wish to measure the first qubit with respect $\{|0\rangle, |1\rangle\}$

$$\begin{aligned} a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle &= \\ |0\rangle \otimes (a|0\rangle + b|1\rangle) + |1\rangle \otimes (c|0\rangle + d|1\rangle) &= \\ u|0\rangle \otimes \left(\frac{a}{u}|0\rangle + \frac{b}{u}|1\rangle\right) + v|1\rangle \otimes \left(\frac{c}{v}|0\rangle + \frac{d}{v}|1\rangle\right) & \end{aligned}$$

- For quantum computation, multi-bit measurement can be treated as a series of single-bit measurements in the standard basis

Measurement II

- Particles are not entangled if the measurement of one has no effect on the other

Example: Measurement Entangled States

- The state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ is entangled since the probability that the first bit is measured to be $|0\rangle$ is $1/2$ if the second bit has not been measured
- The state $\frac{1}{\sqrt{2}}(|00\rangle + |01\rangle)$ is not entangled since:
$$\frac{1}{\sqrt{2}}(|00\rangle + |01\rangle) = |0\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

The EPR Paradox I

- Einstein, Podolsky, and Rosen proposed a gedanken experiment that seemed to violate fundamental principles relativity
- Imagine a source that generates two maximally entangled particles $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, called an EPR pair, and sends one to Alice and one Bob
- Suppose that Alice measures her particle and observes state $|0\rangle$
- Now Bob measures his particle he will also observe $|0\rangle$
- Similarly, if Alice measures $|1\rangle$, so will Bob

The EPR Paradox II

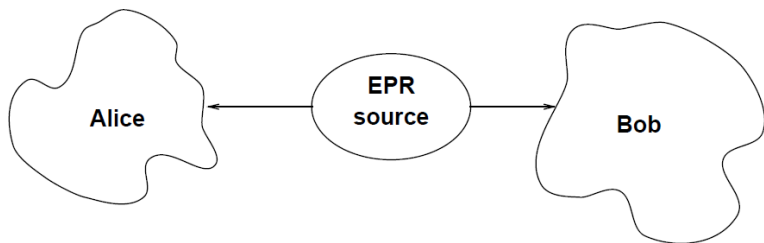


Figure 18: EPR Paradox Setup

Table of Contents

- 1 Introduction
- 2 Quantum Mechanics
- 3 Quantum Bits
- 4 Quantum Gates**
- 5 Quantum Computers
- 6 Quantum Algorithms
- 7 Conclusions

Quantum Gates

- Any linear transformation on a complex vector space can be described by a matrix
- One can think of unitary transformations as being rotations of a complex vector space

Simple Quantum Gates

- The transformations are specified by their effect on the basis vectors
- It can be verified that these gates are unitary. For example $YY^* = I$
- Transformations on basis vectors:

- Identity I :
$$\begin{array}{l} |0\rangle \rightarrow |0\rangle \\ |1\rangle \rightarrow |1\rangle \end{array} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

- Negation X :
$$\begin{array}{l} |0\rangle \rightarrow |1\rangle \\ |1\rangle \rightarrow |0\rangle \end{array} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

- Phase shift negation Y :
$$\begin{array}{l} |0\rangle \rightarrow -|1\rangle \\ |1\rangle \rightarrow |0\rangle \end{array} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

- Phase shift Z :
$$\begin{array}{l} |0\rangle \rightarrow |0\rangle \\ |1\rangle \rightarrow -|1\rangle \end{array} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

- Controlled-NOT C_{NOT} :
$$\begin{array}{l} |00\rangle \rightarrow |00\rangle \\ |01\rangle \rightarrow |01\rangle \\ |10\rangle \rightarrow |11\rangle \\ |11\rangle \rightarrow |10\rangle \end{array} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

- Walsh-Hadamard H :
$$\begin{array}{l} |0\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ |1\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{array} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Examples

- The use of simple quantum gates can be studied with two examples:
 - Dense coding
 - Teleportation
- The key to both dense coding and teleportation is the use of entangled particles

$$\psi_0 = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Dense Coding I

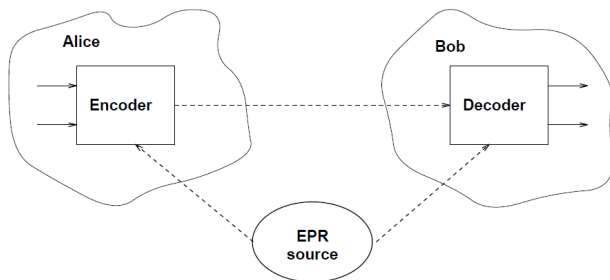


Figure 19: Dense Coding

- The idea is to send 2 bits of classical information using only 1 qubit
- Alice receives two classical bits, encoding the numbers 0 through 3

Dense Coding II

- Depending on this number Alice performs one of the transformations $\{I, X, Y, Z\}$

Value	Transformation	New State
0	$\psi_0 = (I \otimes I)\psi_0$	$\frac{1}{\sqrt{2}}(00\rangle + 11\rangle)$
1	$\psi_1 = (X \otimes I)\psi_0$	$\frac{1}{\sqrt{2}}(10\rangle + 01\rangle)$
2	$\psi_2 = (Y \otimes I)\psi_0$	$\frac{1}{\sqrt{2}}(- 10\rangle + 01\rangle)$
3	$\psi_3 = (Z \otimes I)\psi_0$	$\frac{1}{\sqrt{2}}(00\rangle - 11\rangle)$

Table 1: Resulting States Alice

- Bob applies a Controlled-NOT to the two qubits of the entangled pair
- He can measure the second qubit without disturbing the quantum state

Dense Coding III

Initial State	Controlled-NOT	bit 1	bit 2
$\psi_0 = \frac{1}{\sqrt{2}}(00\rangle + 11\rangle)$	$\frac{1}{\sqrt{2}}(00\rangle + 10\rangle)$	$\frac{1}{\sqrt{2}}(0\rangle + 1\rangle)$	$ 0\rangle$
$\psi_1 = \frac{1}{\sqrt{2}}(10\rangle + 01\rangle)$	$\frac{1}{\sqrt{2}}(11\rangle + 01\rangle)$	$\frac{1}{\sqrt{2}}(1\rangle + 0\rangle)$	$ 1\rangle$
$\psi_2 = \frac{1}{\sqrt{2}}(- 10\rangle + 01\rangle)$	$\frac{1}{\sqrt{2}}(- 11\rangle + 01\rangle)$	$\frac{1}{\sqrt{2}}(- 1\rangle + 0\rangle)$	$ 1\rangle$
$\psi_3 = \frac{1}{\sqrt{2}}(00\rangle - 11\rangle)$	$\frac{1}{\sqrt{2}}(00\rangle - 10\rangle)$	$\frac{1}{\sqrt{2}}(0\rangle - 1\rangle)$	$ 0\rangle$

Table 2: Resulting States Bob

- Now, Bob applies H to the first qubit

Dense Coding IV

State	First bit	H (First bit)
ψ_0	$\frac{1}{\sqrt{2}}(0\rangle + 1\rangle)$	$\frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}(0\rangle + 1\rangle) + \frac{1}{\sqrt{2}}(0\rangle - 1\rangle)\right) = 0\rangle$
ψ_1	$\frac{1}{\sqrt{2}}(1\rangle + 0\rangle)$	$\frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}(0\rangle - 1\rangle) + \frac{1}{\sqrt{2}}(0\rangle + 1\rangle)\right) = 0\rangle$
ψ_2	$\frac{1}{\sqrt{2}}(- 1\rangle + 0\rangle)$	$\frac{1}{\sqrt{2}}\left(-\frac{1}{\sqrt{2}}(0\rangle - 1\rangle) + \frac{1}{\sqrt{2}}(0\rangle + 1\rangle)\right) = 1\rangle$
ψ_3	$\frac{1}{\sqrt{2}}(0\rangle - 1\rangle)$	$\frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}(0\rangle + 1\rangle) - \frac{1}{\sqrt{2}}(0\rangle - 1\rangle)\right) = 1\rangle$

Table 3: Applying H to the first bit

- Finally, Bob measures the resulting bit which allows him to distinguish between 0 and 3, and 1 and 2

Teleportation I



Figure 20: Evidence of Teleportation in the Past

Teleportation II

- The objective is to transmit the quantum state of a particle using classical bits and reconstruct the exact quantum state at the receiver
- **Since quantum state cannot be copied, the quantum state of the given particle will necessarily be destroyed**

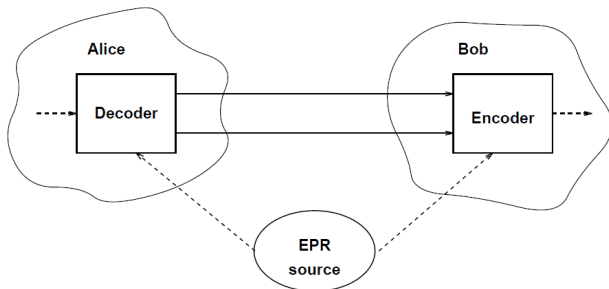


Figure 21: Teleportation

Teleportation III

- Alice has a qubit whose state she doesn't know. She wants to send the state of this qubit

$$\phi = a|0\rangle + b|1\rangle$$

to Bob through classical channels. As with dense coding, Alice and Bob each possess one qubit of an entangled pair

$$\psi_0 = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Teleportation IV

- Alice applies the decoding step of dense coding to the qubit ϕ to be transmitted and her half of the entangled pair

$$\begin{aligned}\psi \otimes \psi_0 &= \\ & \frac{1}{\sqrt{2}}(a|0\rangle \otimes (|00\rangle + |11\rangle) + b|1\rangle \otimes (|00\rangle + |11\rangle)) \\ & \frac{1}{\sqrt{2}}(a|000\rangle + a|011\rangle + b|100\rangle + b|111\rangle)\end{aligned}$$

of which Alice controls the first two bits and Bob controls the last one

Teleportation V

- Alice now applies $C_{\text{NOT}} \otimes I$ and $H \otimes I \otimes I$ to this state:

$$\begin{aligned}
 & (H \otimes I \otimes I)(C_{\text{NOT}} \otimes I)(\psi \otimes \psi_0) = \\
 & (H \otimes I \otimes I)(C_{\text{NOT}} \otimes I) \frac{1}{\sqrt{2}}(a|000\rangle + a|011\rangle + b|100\rangle + b|111\rangle) \\
 & (H \otimes I \otimes I) \frac{1}{\sqrt{2}}(a|000\rangle + a|011\rangle + b|110\rangle + b|101\rangle) \\
 & \frac{1}{2}(a(|000\rangle + |011\rangle + |100\rangle + |111\rangle) \\
 & \quad + b(|010\rangle + |001\rangle - |110\rangle - |101\rangle)) \\
 & \frac{1}{2}(|00\rangle(a|0\rangle + b|1\rangle) + |01\rangle(a|1\rangle + b|0\rangle) \\
 & \quad + |10\rangle(a|0\rangle - b|1\rangle) + |11\rangle(a|1\rangle - b|0\rangle))
 \end{aligned}$$

- Alice measures the first two qubits to get one of $|00\rangle$, $|01\rangle$, $|10\rangle$, or $|11\rangle$ with equal probability

Teleportation VI

- Depending on the result of the measurement, the quantum state of Bob's qubit is projected to $a|0\rangle + b|1\rangle$, $a|1\rangle + b|0\rangle$, $a|0\rangle - b|1\rangle$, $a|1\rangle - b|0\rangle$ respectively
- When Bob receives the two classical bits from Alice he knows how the state of his half of the entangled pair compares to the original state of Alice's qubit

Bits recieved	State	Decoding
00	$a 0\rangle + b 1\rangle$	I
01	$a 1\rangle + b 0\rangle$	X
10	$a 0\rangle - b 1\rangle$	Z
11	$a 1\rangle - b 0\rangle$	Y

Table 4: Decoding Transformation

Teleportation VII

- Bob can reconstruct the original state of Alice's qubit, ϕ , by applying the appropriate decoding transformation to his part of the entangled pair

Table of Contents

- 1 Introduction
- 2 Quantum Mechanics
- 3 Quantum Bits
- 4 Quantum Gates
- 5 Quantum Computers**
- 6 Quantum Algorithms
- 7 Conclusions

Quantum Computers

- Quantum mechanics can be used to perform computations
- Computations done via quantum mechanics are qualitatively different from those performed by a conventional computer
- All quantum state transformations have to be reversible

Quantum Gate Arrays

- The Toffoli gate T can be used to construct complete set of boolean connectives

$$T|1, 1, x\rangle = |1, 1, \neg x\rangle \text{ (NOT)}$$

$$T|x, y, 0\rangle = |x, y, x \wedge y\rangle \text{ (AND)}$$

- Complex Unitary Operations:

- Controlled-NOT $C_{\text{NOT}} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X$

- Toffoli $T = |0\rangle\langle 0| \otimes I \otimes I + |1\rangle\langle 1| \otimes C_{\text{NOT}}$

- Fredkin "Controlled Swap" $F = |0\rangle\langle 0| \otimes I \otimes I + |1\rangle\langle 1| \otimes S$ where S is the swap operation $S = |00\rangle\langle 00| + |01\rangle\langle 10| + |10\rangle\langle 01| + |11\rangle\langle 11|$

Table of Contents

- 1 Introduction
- 2 Quantum Mechanics
- 3 Quantum Bits
- 4 Quantum Gates
- 5 Quantum Computers
- 6 Quantum Algorithms**
- 7 Conclusions

Shor's Algorithm

- In 1994 Peter Shor found a bounded probability polynomial time algorithm for factoring n -digit numbers on a quantum computer
- The most efficient classical algorithm known today is exponential in the size of the input
- Shor's Algorithm uses a standard reduction of the factoring problem to the problem of finding the period of a function

The Quantum Fourier Transform I

- Fourier transforms in general map from the time domain to the frequency domain
- Discrete Fourier transform (DFT) operates on N equally spaced samples in the interval $[0, 2\pi)$
- The fast Fourier transform (FFT) is a version of DFT where N is a power of 2
- The quantum Fourier transform (QFT) is a variant of the DFT which uses powers of 2. The QFT operates on the amplitude of the quantum state, by sending

$$\sum_x g(x)|x\rangle \rightarrow \sum_c G(c)|c\rangle$$

where $G(c)$ is the DFT of $g(x)$, and $|x\rangle$ and $|c\rangle$ both range over the binary representations for the integers between 0 and $N - 1$

The Quantum Fourier Transform II

- The QFT U_{QFT} with base $N = 2^m$ is defined by:

$$U_{QFT} : |x\rangle \rightarrow \frac{1}{\sqrt{2^m}} \sum_{c=0}^{2^m-1} e^{\frac{2\pi icx}{2^m}} |c\rangle$$

Outline of Shor's Algorithm

Shor's Algorithm

- 1 Quantum parallelism
- 2 State whose amplitude has the same period as f
- 3 Applying a QFT
- 4 Extracting the period
- 5 Finding a factor of M
- 6 Repeating the algorithm, if necessary

Search Problems

- A large class of problems can be specified as search problems of the form “find some x in a set of possible solutions such that statement $P(x)$ is true.”
- Such problems range from database search to sorting to graph coloring
- An unstructured search problem is one where nothing is known about the structure of the solution space and the statement P . For example, determining $P(x_0)$ provides no information about the possible value of $P(x_1)$ for $x_0 \neq x_1$
- A structured search problem is one where information about the search space and statement P can be exploited. For instance, searching an alphabetized list

Grover's Algorithm I

Grover's Algorithm

- 1 Prepare a register containing a superposition of all possible values $x_i \in [0, \dots, 2^n - 1]$
- 2 Compute $P(x_i)$ on this register
- 3 Change amplitude a_j to $-a_j$ for x_j such that $P(x_j) = 1$
- 4 Apply inversion about the average to increase amplitude of x_j with $P(x_j) = 1$
- 5 Repeat steps 2 through 4 $4 \frac{\pi}{4} \sqrt{2^n}$ -times
- 6 Read the result

Grover's Algorithm II

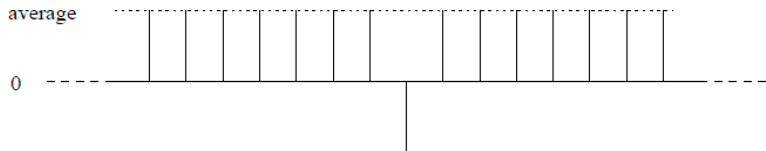


Figure 22: Amplitudes after Step 3

Grover's Algorithm III

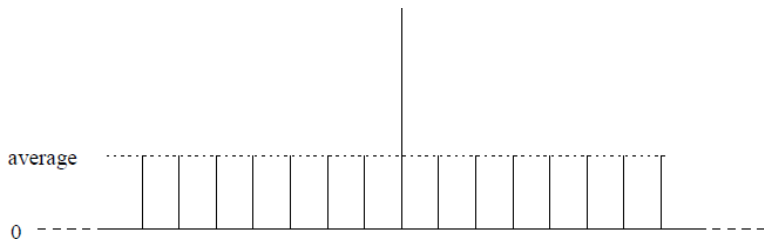


Figure 23: The resulting amplitudes

Quantum Error Correction

- One fundamental problem in building quantum computers is the need to isolate the quantum state
- An interaction of particles representing qubits with the external environment disturbs the quantum state, and causes it to decohere, or transform in an unintended and often non-unitary fashion
- Quantum error correction must reconstruct the exact encoded quantum state
- Reconstruction appears harder than in the classical case since the impossibility of cloning or copying the quantum state

Characterization of Errors

- The possible errors for each single qubit considered are linear combinations of no errors I , bit flip errors X , phase errors Z , and bit flip phase errors Y

$$|\psi\rangle \rightarrow (e_1 I + e_2 X + e_3 Y + e_4 Z)|\psi\rangle = \sum_i e_i E_i |\psi\rangle$$

Table of Contents

- 1 Introduction
- 2 Quantum Mechanics
- 3 Quantum Bits
- 4 Quantum Gates
- 5 Quantum Computers
- 6 Quantum Algorithms
- 7 Conclusions**

Conclusions

- Quantum computations must be linear and reversible, any classical algorithm can be implemented on a quantum computer
- Given a practical quantum computer, Shor's algorithm would make many present cryptographic methods obsolete
- Grover's search algorithm proves that quantum computers are strictly more powerful than classical ones
- It is an open question whether we can find quantum algorithms that provide exponential speed-up for other problems
- A big breakthrough for dealing with decoherence came from the development of quantum error correction techniques

Further Reading

- Andrew Steane's Quantum computing [3]
- Richard Feynman's Lectures on Computation [1]
- Williams and Clearwater's book Explorations in Quantum Computing [5]
- SIAM Journal of Computing issue of October 1997
- Leonard Susskind's lecture on Modern Physics: Quantum Mechanics [4]

References I



Richard Phillips Feynman.

Feynman Lectures on Computation.

Perseus Books, Cambridge, MA, USA, 2000.



Eleanor G. Rieffel and Wolfgang Polak.

An introduction to quantum computing for non-physicists.

ACM Comput. Surv., 32(3):300–335, 2000.



Andrew Steane.

Quantum Computing.

Rept. Prog. Phys., 61:117–173, 1998.



Leonard Susskind.

Modern physics: Quantum mechanics, 2008.

[Online; accessed 31-March-2009].

References II



Colin P. Williams.

Explorations in Quantum Computing.

Springer Publishing Company, Incorporated, 2008.

Acknowledgement

- Prof. Slavyanov, for his outstanding commitment and good will
- Prof. Huckle, for his clever advice and recommendation on the selection of the literature
- Csaba Vigh, for 10 days of “Hard Fun”
- Distinguish members of the JASS09, for their kindness and attention during the talks

Questions

Please, do not hesitate in asking academic stuff, or contact me through encisomo@in.tum.de

