Introduction to Quantum Computing

Javier Enciso
encisomo@in.tum.de
Joint Advanced Student School 2009
Technische Universität München

April 22, 2009

Abstract

In this paper, a gentle introduction to Quantum Computing is presented. The main propouse is to enable the non-experienced reader with the basic concepts and notations related with Quantum Computing.

1 Introduction

There are certain quantum mechanical effects that cannot be simulated efficiently on the basis of the classical computation [1]. Moreover, building quantum computers is not a easy task, and indeed no one was sure how to use the quantum effects to speed up computation or solve the problems that are unsolvable with the technology available nowadays.

However, there are several applications of interest where quantum computing will exploid the quantum efects to produce surprising results, among the them it is possible to outline:

- Quantum key distribution: allows the encryption of information using the principles of quantum mechanics through insecure channels.
- Quantum teleportation: enables the transfer of information without its physical movement.
- Dense coding: gives the oportunity of sending two classical bits of information using only one quantum information bit.

In quantum systems the amount of parallelism increases exponentially with the size of the system [2].

In order to implement a physical quantum computer, it is needed to master some of the most prominent techniques which control the quantum states of the particules, say:

- Ion Traps: captures electrically charged particules, ions, within electric of magnetic fields.
- Nuclear Magnetic Resonance (NMR): controls the quantum states using a manegtic field at room temperature.
- Optical and solid state techniques: control photon's polarization or electron's spin.

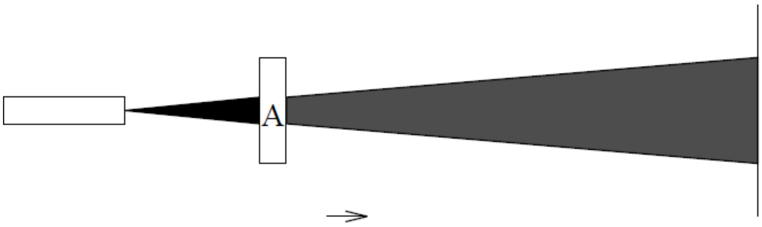

Figure 1: Photon Polarization Experiment I

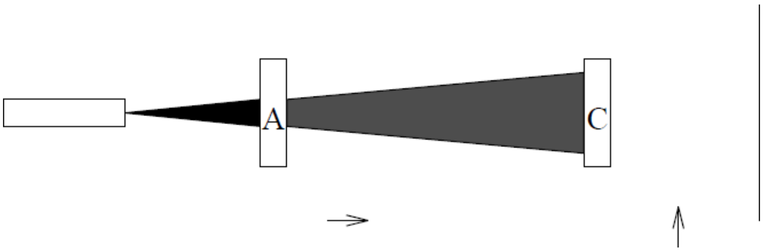

Figure 2: Photon Polarization Experiment II

2 Quantum Mechanics

Quantum Mechanics describes physical systems at the atomic level. In that context, Quantum Mechanical phenomena are difficult to understand since most of everyday experiences are not applicable[4]. What is more, by definition some of the ideas behind Quantum Mechanics lead 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.

2.1 Photon Polarization

In order to figure out the weirdness of the Quantum Mechanical efects, a photon system will be depicted. A photon's polarization state can be modelled by a unit vector pointing in the appropriate direction. Any arbitrary polarization can be expressed as a linear combination of the two basis vectors. Measurement of a state transforms the state into one of the measuring devices associated basis vectors.

Polarization of a photon can be described in the following way:

- $|\psi\rangle = a|\uparrow\rangle + b|\rightarrow\rangle$ where a and b are complex numbers
- $|\psi\rangle$ is a unit vector, $|a|^2 + |b|^2 = 1$

A polaroid, wich in principle could be the same as the one you would find in a photo shop, measures the quantum state of photons with respect to the basis:

- Filter A measures the photon polarization with respect to $|\rightarrow\rangle$

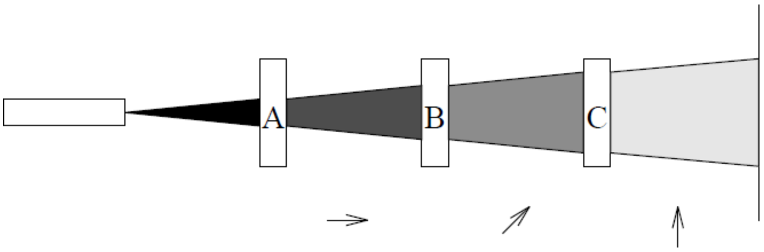

Figure 3: Photon Polarization Experiment III

- Filter C will measure these photons with respect to $|\uparrow\rangle$
- Filter B measures the quantum state with respect to

$$\{\frac{1}{\sqrt{2}}(|\uparrow\rangle + |\rightarrow\rangle), \frac{1}{\sqrt{2}}(|\uparrow\rangle - |\rightarrow\rangle)\}$$

Thus only one eighth of the original photons pass through the sequence of filters A, B, and C.

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 $\langle x|y\rangle$.

Some fundamental results are:

- 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 $|0\rangle\langle 1| = \begin{pmatrix} 1 \\ 0 \end{pmatrix} (0, 1) = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$

3 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 $a|0\rangle + b|1\rangle$. Thus, $|a|^2$ and $|b|^2$ are the probabilities that the measured value are $|0\rangle$ and $|1\rangle$ respectively.

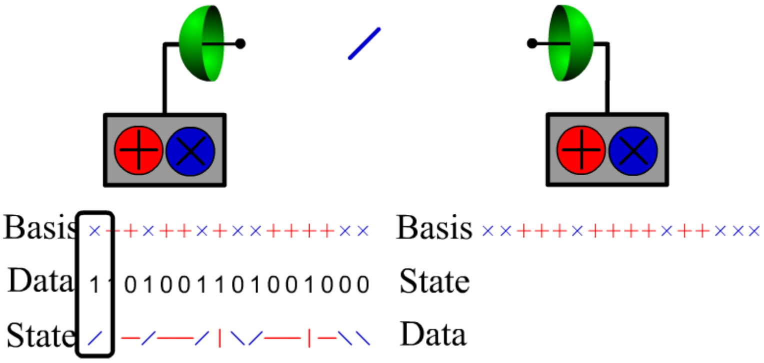
Basis × + + × + + × + × × + + + + × ×
Data 1 1 0 1 0 0 1 1 0 1 0 0 1 0 0 0
State / — / — / | \ / — | — \ \
Basis × × + + + × + + + + × + + × × ×
State
Data

Figure 4: Transmition of the first state

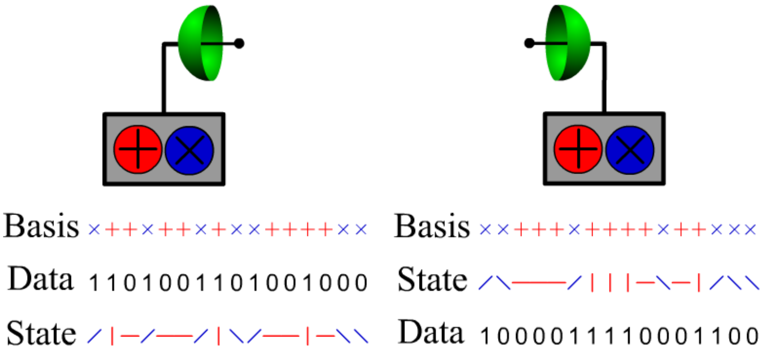
Basis × + + × + + × + × × + + + + × ×
Data 1 1 0 1 0 0 1 1 0 1 0 0 1 0 0 0
State / | — / — / | \ / — | — \ \
Basis × × + + + × + + + + × + + × × ×
State / \ — / | | | — \ — | / \ \
Data 1 0 0 0 0 1 1 1 1 0 0 0 1 1 0 0

Figure 5: Transmition of the last state

3.1 Quantum Key Distribution

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 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.

Alice sends a sequence of bits to Bob by encoding each bit in the quantum state of a photon. For each bit, Alice randomly uses one of the following two bases for encoding each bit:

$$\begin{array}{lcl} 0 \rightarrow |\uparrow\rangle & \text{or} & 0 \rightarrow |\nwarrow\rangle \\ 1 \rightarrow |\rightarrow\rangle & & 1 \rightarrow |\nearrow\rangle \end{array}$$

Bob measures the state of the photons he receives by randomly picking either basis. Bob and Alice communicate the basis they used for encoding and decoding of each bit over the open channel. On average, Alice and Bob will agree on 50% of all bits transmitted over the open channel[1]

Eve measures the state of the photons transmitted by Alice and resends new photons with the measured state. Eve will use the wrong basis approximately

[1] Animation at http://research.physics.illinois.edu/QI/Photonics/movies/bb84.swf

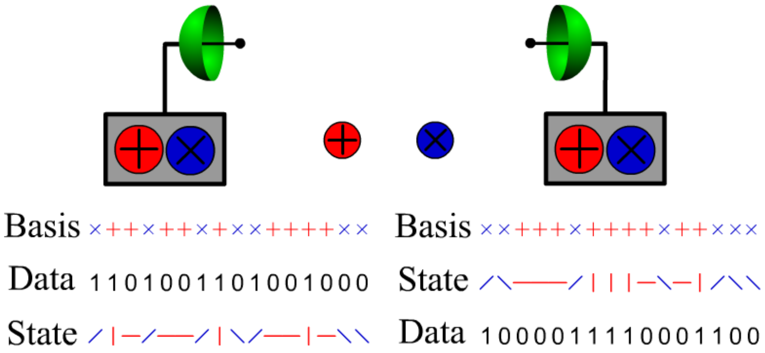
Basis × + + × + + × + × × + + + + × ×
Data 1101001101001000
State
Basis × × + + + × + + + + × + + × × ×
State
Data 1000011110001100

Figure 6: Exchange of the basis

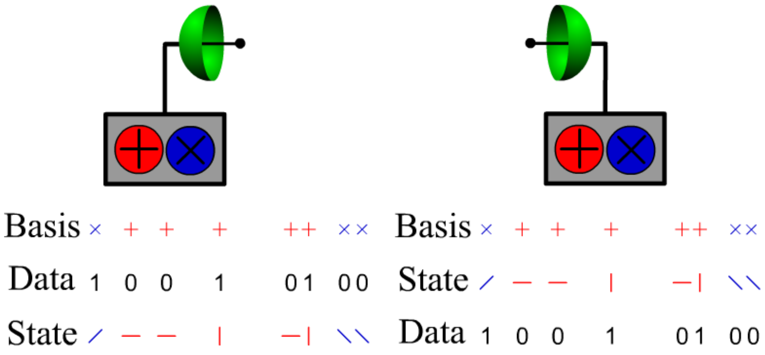

Figure 7: Final agreement between Alice and Bob

50% of the time and will resend the bit with the wrong basis. When Bob measures a resent qubit with the correct basis there will be a 25% probability that he measures the wrong values. Thus any eavesdropper on the quantum channel is bound to introduce a high error rate that Alice and Bob can detect by communicating a sufficient number of parity bits of their keys over the open channel.

3.2 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, $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$.

As an example, consider the following. 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

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

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

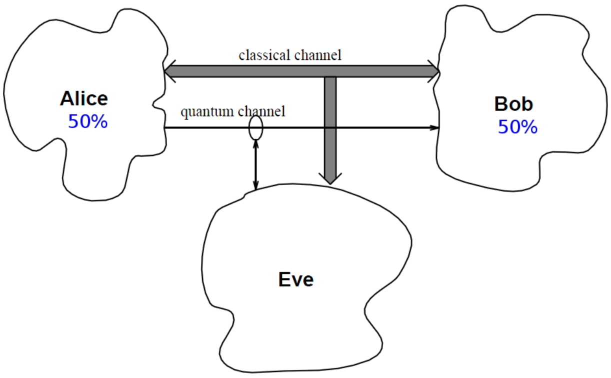

Figure 8: Agreement between Alice and Bob

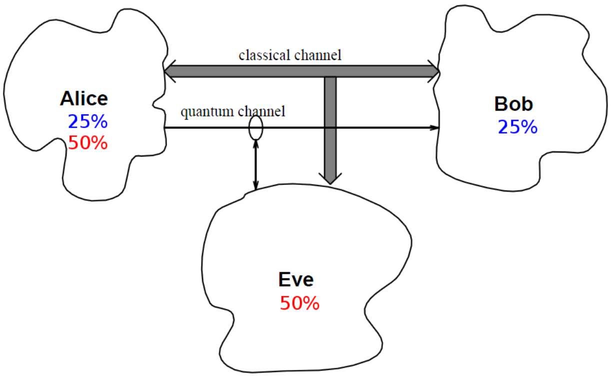

Figure 9: Agreement between Alice, Bob, and Eve

3.3 Measurement

The result of a measurement is probabilistic and the process of measurement changes the state to that measured. In order to measure 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 $\{|0\rangle, |1\rangle\}$

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

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

Let's consider the measurement of entangled[2] states. The state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ is entangled since the probability that the first bit is measured to be $|0\rangle$

[2] Particles are entangled if the measurement of one has effect on the other.

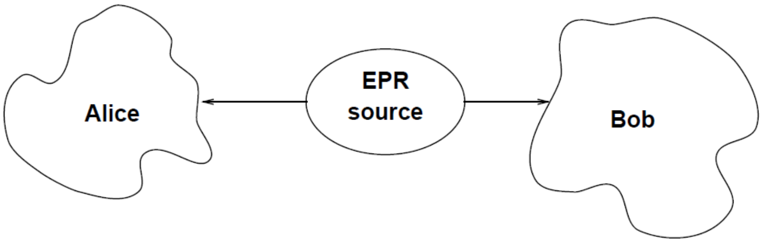

Figure 10: EPR Paradox Setup

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: $\frac{1}{\sqrt{2}}(|00\rangle + |01\rangle) = |0\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$.

3.4 The EPR Paradox

Einstein, Podolsky, and Rosen proposed a thought experiment that seemed to violate fundamental principles relativity. In fact, they proposed that, according with the principles of Quantum Mechanics, information could travel faster than speed of light, leading to the so called EPR paradox.

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. Then, 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.

4 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.

4.1 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 include the following:

- Identity I : $\begin{array}{lcl} |0\rangle & \to & |0\rangle \\ |1\rangle & \to & |1\rangle \end{array} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
- Negation X : $\begin{array}{lcl} |0\rangle & \to & |1\rangle \\ |1\rangle & \to & |0\rangle \end{array} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
- Phase shift negation Y : $\begin{array}{lcr} |0\rangle & \to & -|1\rangle \\ |1\rangle & \to & |0\rangle \end{array} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$
- Phase shift Z : $\begin{array}{lcr} |0\rangle & \to & |0\rangle \\ |1\rangle & \to & -|1\rangle \end{array} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

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

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

4.2 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.

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

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

4.2.2 Teleportation

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.

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

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

Alice applies the decoding step of dense coding to the qubit ϕ to be transmitted and her half of the entangled pair of which Alice controls the first two bits and Bob controls the last one.

Alice measures the first two qubits to get one of $|00\rangle$, $|01\rangle$, $|10\rangle$, or $|11\rangle$ with equal probability. 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. Bob can reconstruct the original state of Alice's qubit, ϕ, by applying the appropriate decoding transformation to his part of the entangled pair.

5 Quantum Computers

Quantum mechanics can be used to perform classical computations [3]. Computations done via Quantum Mechanics are qualitatively different from those performed by a conventional computer. However, all quantum state transformations have to be reversible.

Quantum Gate Arrays

For two arbitrary unitary transformations U_1 and U_2, the transformation $|0\rangle\langle 0| \otimes U_1 + |1\rangle\langle 1| \otimes U_2$ is also unitary. The Toffoli gate T can be used to construct complete set of boolean connectives:

$$\begin{aligned} T|1, 1, x\rangle &= |1, 1, \neg x\rangle \text{ (NOT)} \\ T|x, y, 0\rangle &= |x, y, x \wedge y\rangle \text{ (AND)} \end{aligned}$$

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 “Controled Swap” $F = |0\rangle\langle 0| \otimes I \otimes I + |1\rangle\langle 1| \otimes S$ where S is the swap operation $S = |00\rangle\langle 00| + |01\rangle\langle 10| + |10\rangle\langle 01| + |11\rangle\langle 11|$

6 Quantum Algorithms

6.1 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.

Outline of Shor’s Algorithm[5]:

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

Grover's Search Algorithm

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.

Outline of Grover's Algorithm[5]:

1. Prepare a register containing a superposition of all possible values $x_i \in [0, \ldots, 2^n - 1]$
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 $\frac{\pi}{4}\sqrt{2^n}$-times
6. Read the result

6.2 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.

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:

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

7 Conclusions

The challenge for computer scientists and others is to develop new programming techniques appropriate for quantum computers. 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.

References

[1] Richard Phillips Feynman. *Feynman Lectures on Computation.* Perseus Books, Cambridge, MA, USA, 2000.

[2] Eleanor G. Rieffel and Wolfgang Polak. An introduction to quantum computing for non-physicists. *ACM Comput. Surv.*, 32(3):300–335, 2000.

[3] Andrew Steane. Quantum Computing. *Rept. Prog. Phys.*, 61:117–173, 1998.

[4] Leonard Susskind. Modern physics: Quantum mechanics, 2008. [Online; accessed 31-March-2009].

[5] Colin P. Williams. *Explorations in Quantum Computing.* Springer Publishing Company, Incorporated, 2008.