Quantum Computers

Index

Introduction

After the first Computer was created by Konrad Zuse in 1941, almost 70 years of very fast technological advancement have passed. Surprisingly, the high speed modern computers sitting in front of us, work on the same principles as their 30 ton ancestors. All of them are based on the manipulation and interpretation of binary information. This way of working with information is usually described by a mathematical model called Turing machine. Also, their hardware components store and manipulate data based on classical physics.

In this document, a new kind of computers will be introduced to you. Those computers are called quantum computers and have another way of processing information, which will be described by the mathematical model called the quantum Turing machine, and will have hardware components based on physics for microscopic elements which is called quantum physics.

Motivation

In 1985, Richard P. Feymann said "it seems that the laws of physics present no barrier to reducing the size of computers until bits are the size of atoms, and quantum behavior holds sway". According to [24] the end of the life of silicon-based transistor chip designs will be at 2012, which means we have to find a new technology to keep improving computers.

Quantum Computers could be a great alternative to nowadays computers since they would be faster (even exponentially faster) and could solve more problems than classical ones [10][6].

Quantum Physics

Quantum computers are based, as its name says, on a number of quantum physical properties. These will be explained next for a better understanding of the way quantum computers work. However, bear in mind that even when these properties have been proven experimentally and seem to work, quantum physics is nor a complete description of the reality nor a local theory [1].

The multiverse

The multiverse theory is a theory which is not proven, but helps to understand quantum physics.

In classical physics it is supposed that other universes do not affect our universe, however, in quantum physics every element in our universe has counterparts in a range of other universes. They are linked and so called quantum interference is generated, which can affect the state of the element in our universe. Every quantum world seems correlated with every other world precisely to the degree necessary to keep the universe consistent, and no more.

According to one of the most important scientists in quantum physic, David Deutsch, anything possible exists somewhere in the “multiverse”. If this is true, we can say that there are many universes (but a very tiny proportion of the multiverse) where you are a billion years old [7].

To understand the nature of multiverse interaction take this example: “When you go to a party, you usually meet people you've never met before, whose worlds you have never known. Some of those worlds can be quite something, too! In physics language, there is little correlation between your states. By the end of the evening (interaction), you have some shared party experiences - your states are more correlated than they were before. If you never meet again, the shared memories fade, and your worlds slowly return to almost their previous separateness (they decorrelate). You'll never be the same again, but you're still the same you” [14].

Superposition

The principle of superposition states that if the world can be in any configuration, any possible arrangement of particles or fields, and if the world could also be in another configuration, then the world can also be in a state which is a mixture of the two, where the amount of each configuration that is in the mixture is specified by a complex number.

For example, if a particle can be in position A and position B, it can also be in a state where it is an amount "3i/5" in position A and an amount "4/5" in position B. Usually this is written in the so called bra-ket notation:

$$|\psi\rangle = \frac{3}{5}i|A\rangle + \frac{4}{5}|B\rangle$$

In quantum physics, the state of a physical system is identified with a ray in a complex separable Hilbert space. Each vector in the ray is called a "ket" and written as $|\psi\rangle$, which would be read as "ket psi ". The “+” operation denotes superposition.

Decoherence

One of the biggest problems of quantum computers is the decoherence. This property states that if a coherent state (state with superposition) interacts with the environment, it will fall into a classical physics state without superposition.

This means that for a quantum computer to work with superpositioned states, it has to be completely isolated from the rest of the universe (no observing the state, no measuring it, ...).

Zeno effect

Related to the decoherence is the Zeno effect, which helps to keep particles in non coherent states. The Zeno effect states that an unstable particle, if constantly observed, will never decay into a superpositioned state.

Entanglement

Entanglement is the most important property in the field of quantum communication. It says that two or more particles can be linked, and if linked, you can change properties of one particle changing the linked one.

Entanglement is very controversial among physicists, and there are two main theories:

- Two particles can be linked and change each other without interaction.
- The linked particles interact by so called "hidden variables". As an example for this you may imagine a 2D world. In the 2D world, a torus, if inserted, would look like two circles. When one of the circles is moved, the other would move too, in the 2D world it would seem they are not interacting, however they are interacting through the hidden third dimension.

Bits vs. Qubits

The basic element of information in classical computers is the bit. It has exactly two states which usually are represented by 1 or 0, but could also be represented by an up or a down arrow.

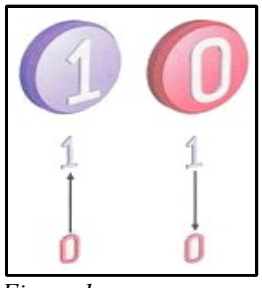

Figure 1: Representation of a bit

Quantum computers have, as their basic element of information, the quantum bit (qubit for short). While a bit can be represented as an arrow up or down, a qubit is represented by an arrow in a sphere where north is 1 and south is 0, and all other states are superpositions of these states. A qubit state is a unit vector in a two-dimensional complex vector space.

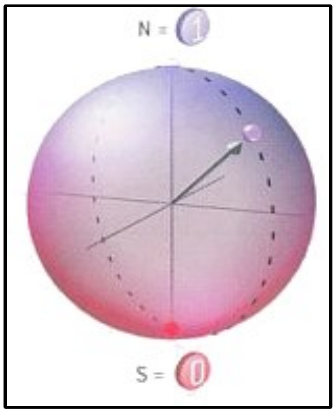

Figure 2: Representation of a qubit

It might seem that a qubit has an infinite amount of states, but when read, it can only be 0 or 1 because of the decoherence, however there is hidden quantum information, and this information grows exponentially. [12]

Quantum Gates

It appears that the laws of physics are completely reversible. That is, from any physical process we can always deduce the inputs from the outputs [9].

At first, it may seem as if classical computers do not follow this rule, however the lost information appears to be in the waste heat.

In quantum computers, we cannot allow this situation to occur. The radiation of the heat would depend on the state of the inputs to the quantum gate. Thus, in effect, the radiation of the heat would be a measurement on the inputs and decoherence would ensue. The universes would be so far apart as to be unable to interfere with each and the result, which depends upon the interference of these universes, would be invalid. Thus quantum gates must be reversible. Reversible gates must, by their very definition, have an equal number of inputs and outputs.[9]

Calculating with gates and qubits

To calculate with gates, in quantum computers, the transformation the gate performs is written in a Matrix. This matrix is multiplied by the input to get the result. As an example, it will be shown how to calculate with the NOT gate.

$$\neg x \equiv \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} x$$

Figure 3: Definition of the NOT gate operation as matrix

An input of a superposition of two states will be used: α |A> + β |B>, this will be written in a matrix as $\begin{pmatrix} \alpha \\ \beta \end{pmatrix}$ and the result by multiplying the gate transformation will be $\neg \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \beta \\ \alpha \end{pmatrix}$, which is exactly the negated probabilities β |A> + α |B>.

Universal Toffoli gate

Gates are called universal gates if they can be used to create any logic circuit. Also, as you can see in Figure 5, the Toffoli gate is reversible, which means it can be used for quantum computation. Due to this statements and the Zeno effect, we can conclude that every classical logic system can be simulated with a quantum computer.

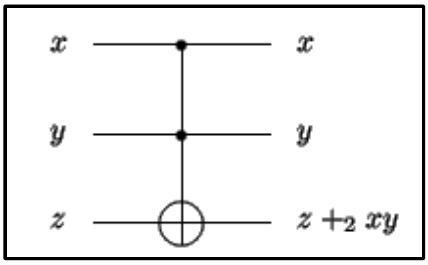

Figure 4: Diagrammatic representation of a Toffoli gate

Input 1	Input 2	Input 3	Output 1	Output 2	Output 3
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

Figure 5: Universal Toffoli gate's truth table

Square root of NOT

The square root of NOT is a pure quantum gate, which means that its behavior can not be simulated by a classical gate.

A single square root of NOT gate produces a completely random output with equal probabilities of the output being 0 or 1. However two such gates linked sequentially produce an output that is the inverse of the input, and thus behave in the same way as the classical NOT gate.

This result is unparalleled in the classical world, one gate produces a random result while two gates linked sequentially produce a deterministic result.

$$|0\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$|1\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

Figure 6: Truth table of the square root of NOT gate

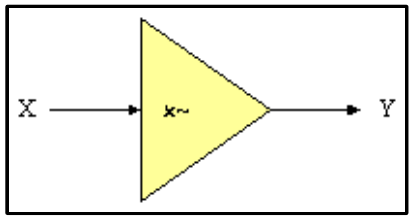

Figure 7: Diagrammatic representation of a square root of NOT gate

Other quantum gates

Rotation gates

A rotation gate is a general-purpose transformation that turns the unitary vector of the qubit by θ radians (with some other constant value Φ).

$$G_{\theta,\phi} = \begin{pmatrix} \cos(\theta) & \sin(\theta)e^{i\phi} \\ -\sin(\theta)e^{-i\phi} & \cos(\theta) \end{pmatrix}$$

Figure 8: Definition of a rotation gate's operation as matrix

Phase shift gates

The phase shift gates are another class of general purpose transformations. It shifts the phase of the qubit by Φ. This can be used to align the phases of qubits for superpositioning or to intentionally weigh certain qubits to interfere with other qubits.

$$\phi = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix}$$

Figure 9: Definition of a phase shift gate's operation as matrix

Walsh-Hadamard transformation gate

Arguably the most important gate in quantum computation is the Walsh-Hadamard transformation gate. Its function as a one-bit gate is to put the unsuperpositioned qubit into a superposition of the |1> and |0> states. As the quantum computer derives much of its power from superposition-based activities, this gate is crucial. [5]

The Hadamard gate generalizes to an arbitrary number of input qubits according to the following recursive definition (called the Walsh transformation W_n):

$W_1 = H$

$W_{n+1} = H \times W_n$

$$H = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}$$

Figure 10: Description of a Walsh-Hadamard transformation gate as matrix

Quantum Algorithms

The greatest differences between the classical and the quantum algorithms are these:

- Quantum algorithms can be faster than classical ones.
- Quantum algorithms can solve more problems than classical ones.
- A quantum algorithm can evaluate a function f(x) for many values of x simultaneously.

As an example I propose the algorithm in Figure 11. For two inputs, x and y, the algorithm calculates x and $y \oplus f(x)$. When using as input the values x=(|0> + |1>)/√2 and y=|0> an output of x=0, f(x)=0 is obtained, in case x=(|0> + |1>)/√2 is measured as x=0, and an output x=1, f(x)=1 otherwise. This outcome means that with just one input, we have the solution for both x=0, and x=1.

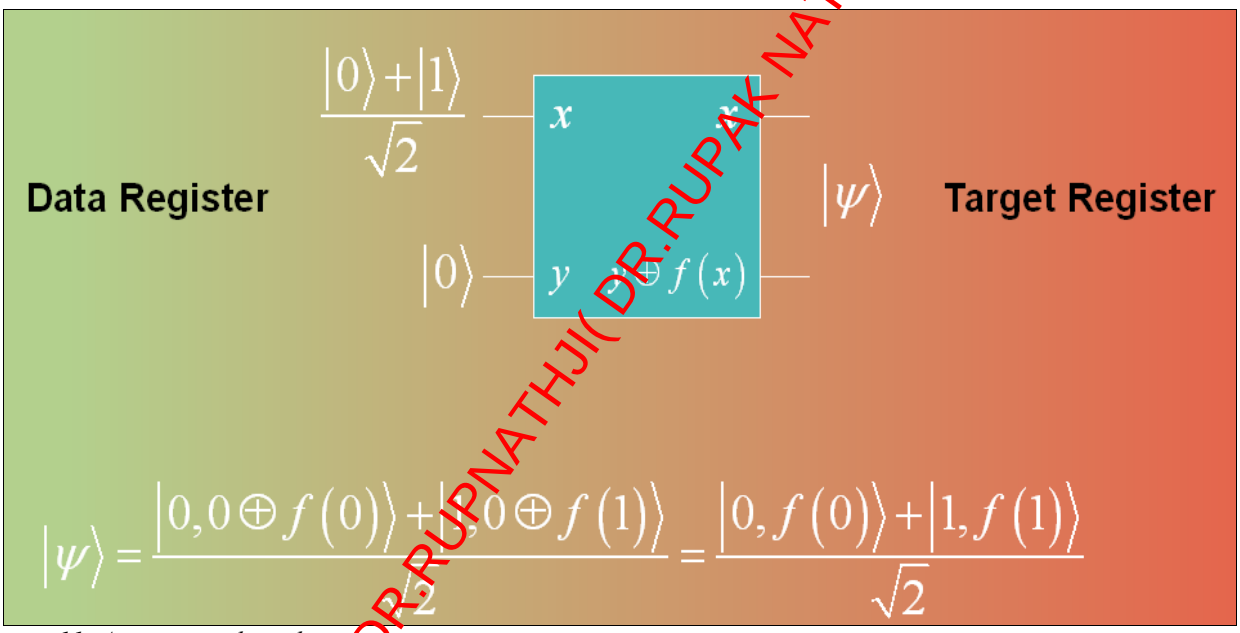

Figure 11: A quantum algorithm

A very important example of the power of quantum algorithms is Shor's algorithm.

Shor's algorithm

By the early nineties it was known that a quantum computer could be faster than any classical computer for certain problems. Nonetheless, these observations were largely driven by academic curiosity.

This changed in 1994 when Peter Shor, a scientist working for Bell Labs, devised a polynomial time algorithm for factoring large numbers on a quantum computer. This discovery drew great attention to the field of quantum computing. [6]

The algorithm was seen as important since the difficulty of factorization is the base of most of nowadays cryptographic systems.

The fastest algorithm publicly available for factorizing a large number runs in exponential time while Shor's algorithm runs in $O((\log n)^2 \cdot \log \log n)$ on a quantum computer, and must perform $O(\log n)$ steps of post processing on a classical computer.[6]

The world's first quantum computer?

In 2007, a computer called Orion was presented by D-Wave.

The technology in D-Wave's quantum computer, called "adiabatic quantum computing", is based on superconducting electronics. Superconductors can be used to build large structures that behave according to the rules of quantum mechanics. D-Wave specialists say these structures naturally shield themselves from external noise, creating a safe haven for quantum effects. The system operates with thermal noise, generated by the thermal agitation of the electrons inside the electrical conductor. According to Geordie Rose, D-Wave's founder and CEO, this makes decoherence time irrelevant.

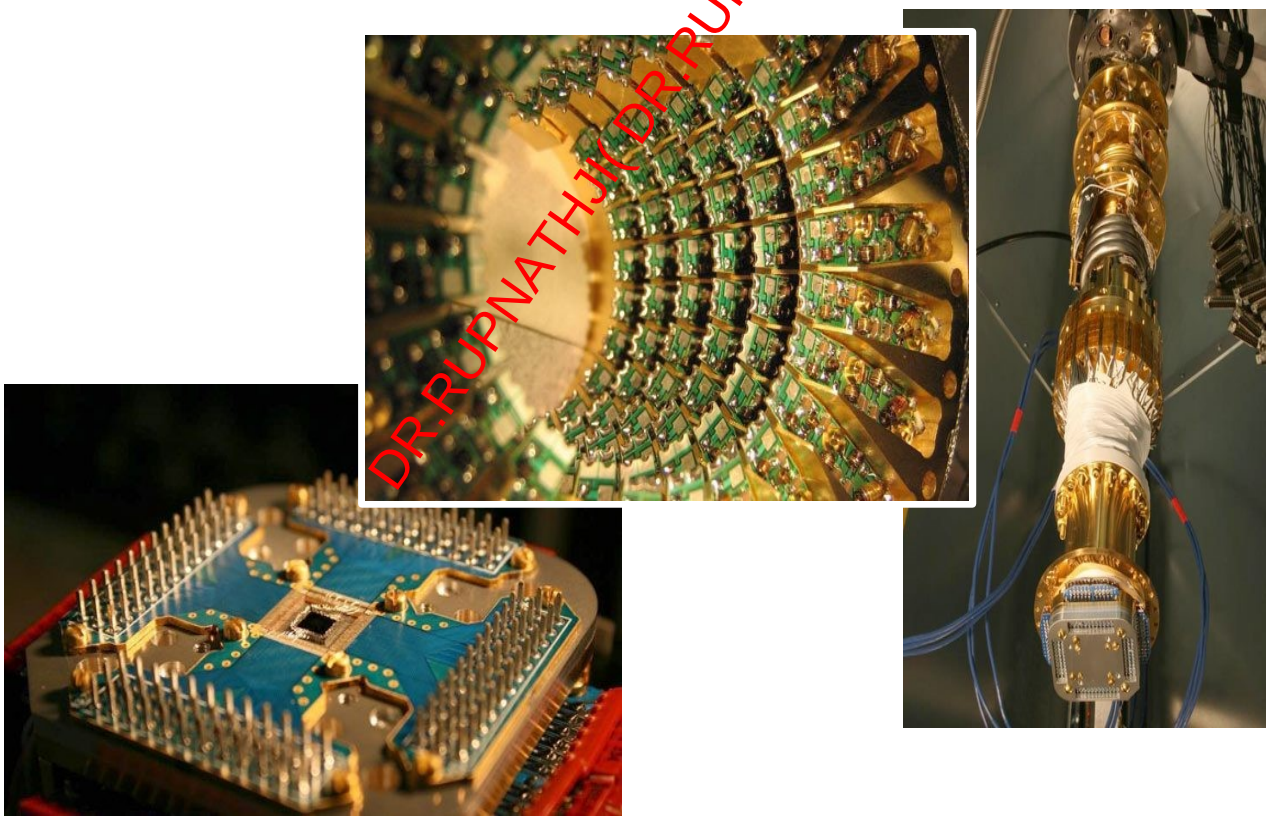

Figure 12: Some components of Orion (D-Wave's quantum computer)

[Left] A 16-qubit processor mounted in its sample holder

[Up] One of its noise filtering stages

[Right] A picture of the Orion chip's sample holder attached to one of the dilution fridges, ready to begin a cooldown. It works at 0.005°C above absolute zero (-273°C) (about 500 times colder than interstellar space)

This computer was very controversial for a time, since D-Wave was not publishing any papers on the subject, and neither were they giving any detailed information about the architecture of Orion. This brought D-Wave's Chief Executive Herb Martin to explain that the machine is not a true quantum computer and is instead a kind of special-purpose machine that uses some quantum mechanics to solve problems.

Review

Quantum computers seem to be a good technology to succeed classical computers. However, there still are a lot of problems which have to be solved first. Some of the biggest are the decoherence, data storage, the need of a noise free environment and the question which is the best hardware scheme for quantum computers. But there already are some ideas to solve some of them, such as read quantum information out of nuclear “spins”[20], diamond-based quantum computing for noise free environments within room temperature [19] or silicon chips for optical quantum computing [21].

References

Papers

[1] A. Einstein, B. Podolsky, and N. Rosen, "Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?" (1935) (http://prola.aps.org/pagegif/PR/v47/i10/p777_1/p777)

[2] A. Barenco (Oxford), C. H. Bennett (IBM), R. Cleve (Calgary), D. P. DiVincenzo (IBM), N. Margolus (MIT), P. Shor (AT&T), T. Sleator (NYU), J. Smolin (UCLA), H. Weinfurter (Innsbruck), "Elementary gates for quantum computation" (Physical Review A, March 22, 1995 (AC5710))

[3] James Higgo, "Does the 'many-worlds' interpretation of quantum mechanics imply immortality?" (http://www.higgo.com/quantum/qti.htm)

[4] Lev Vaidman, Zion Mitrani, "Qubit versus bit for measuring an integral of a classical field" (School of Physics and Astronomy, Raymond and Beverly Sackler Faculty of Exact Sciences, Tel-Aviv University, Tel-Aviv 69978, Israel, 16/5/2004)

[5] Brian Patterson, "Quantum Gates, A Closer Look" (http://www.cs.iastate.edu/~patterbj/cs/quantum/fp/index.htm)

[6] Matthew Hayward, "Quantum Computing and Shor's Algorithm" (http://alumni.imsa.edu/~matth/quant/299/paper/)

[7] David Deutsch, "It from Qubit" (Centre for Quantum Computation, The Clarendon Laboratory, University of Oxford, September 2002)

[8] Mark Oskin, Frederic T. Chong, Isaac Chuang., "A Practical Architecture for Reliable Quantum Computers" (IEEE Computer, Jan. 2002) (http://www.cs.washington.edu/homes/oskin/Oskin-A-Practical-Architecture-for-Reliable-Quantum-Computers.pdf)

Internet pages

[9] "Quantum Gates" (http://www.themilkyway.com/quantum/FinalReport/QuantumGates.html)

[10] "The Quantum Computer" (http://www.cs.caltech.edu/~westside/quantum-intro.html)

[11] Simon Bone, Matias Castro, "A Brief History of Quantum Computing" (http://www.doc.ic.ac.uk/~nd/surprise_97/journal/vol4/spb3/#1.1%20Quantum%20computer%20basics)

[12] Zdzislaw Meglicki, "Introduction to Quantum Computing" (http://beige.ucs.indiana.edu/M743/M743.html)

[13] Josh Clark, "How Quantum Suicide Works" (http://science.howstuffworks.com/quantum-suicide.htm)

[14] John Sankey, "The Many Worlds of Quantum Mechanics" (http://www.sankey.ws/qm.html)

University and technology press

[15] "Turning 'Funky' Quantum Mysteries Into Computing Reality" (Massachusetts Institute of Technology, 2008, February 21) (http://www.sciencedaily.com/releases/2008/02/080216095718.htm)

[16] "Physicists Modify Double-Slit Experiment to Confirm Einstein's Belief" (March 12, 2007) (http://www.physorg.com/news92937814.html)

[17] "Adiabatic quantum computing" (February 12, 2007) (http://arstechnica.com/journals/science.ars/2007/2/12/7008)

[18] D-Wave Quantum Computer photo gallery (http://dwave.wordpress.com/2007/01/)

[19] David Baron, "Single spinning nuclei in diamond offer a stable quantum computing building block" (May 31, 2007) (http://www.news.harvard.edu/gazette/2007/06.07/99-quantumcomputing.html)

[20] "A Quantum (Computer) Step" (November 19, 2006) (http://unews.utah.edu/p/?r=111406-1)

[21] "Silicon chips for optical quantum technologies" (March 27, 2008) (http://www.eurekalert.org/pub_releases/2008-03/uob-scf032608.php)

[22] "Quantum computer solves problem, without running" (February 22, 2006) (http://www.news.uiuc.edu/news/06/0222quantum.html)

[23] "D-Wave Demonstrates 28-Qubit Quantum Computer" (November 15, 2007) (http://www.tfot.info/news/1048/d-wave-demonstrates-28-qubit-quantum-computer.html)

[24] "Bell Labs Extends Lifetime of Transistor Chip Design", Computergram International (June 25, 1999) (http://findarticles.com/p/articles/mi_m0CGN/is_3690/ai_54997676)