QUANTUM COMPUTING

Course 10112
Advanced quantum mechanics

Ask Hjorth Larsen s021864
Kenneth Nielsen s021749
Pernille Voss Larsen s022005

DTU - Technical University of Denmark

6 October 2005

Table of contents

1 Introduction

The idea of quantum computing is rather new, but because of the technological perspectives it has experienced a fast growth in both theory and experimental fields.

While the physical limit of classical information storage is still far from reached, quantum mechanical, thermodynamical and material limitations will one day pose a serious problem. [3] One reason why this is not possible is that if the transistors get much smaller they will enter the quantum mechanical domain and the classical laws of physics that normally govern the computations will break down. And so if we are to build more powerful computers we will need to make the utilize the quantum mechanical laws rather than the classical ones. As it turns out, in doing so, a few extra advantages turn up, as the quantum computer will support entirely new algorithms which allow us to solve some specific problems extremely efficiently compared to the classical algorithms.

A quantum computer makes use of some distinct quantum mechanical phenomena like the possibility to superpose and entangle states. Thus the basic principle of quantum computation is that the quantum properties of particles can be used to represent and structure data and that devised quantum mechanisms can be used to perform operations with these data.

The following report attempts to describe some fundamental properties of quantum computing. First, the basic principles of quantum computing are described along with different approaches to the physical implementation of quantum computers. Afterwards some specifically quantum mechanical phenonema are dealt with. A brief description of problems that quantum computers might be able to solve efficiently is described. At last a resume of an article describing simulations of entaglement and quantum computing with electrons propagating in quantum wires is given.

2 Basic principles of quantum computing

2.1 The qubit

To explain the differences between classical computing and quantum computing, first, a classical bit, which is the fundamental unit of classical information, is considered.

A bit can be in one of two states, typically implemented as different fixed voltages, representing the two logical values *true* or *false*. Therefore an N-bit *register*, or a string of N classical bits, can be in one of the 2^N binary states from 000...0 to 111...1.

likewise, a two-state quantum system can be thought of as representing the two logical states true and false written as $|0\rangle$ and $|1\rangle$. Such a system is called a quantum bit or a *qubit* and is the fundamental unit of quantum information. The system can also be in a superposition of these two states and so will form a vector in the two-dimensional Hilbert space with orthonormal basis $\{|0\rangle, |1\rangle\}$, and thus the system can be in both states at the same time.

A qubit can now be written as a linear combination of the two states $|0\rangle$ and $|1\rangle$,

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,, \quad \alpha, \beta \in \mathbb{C}, \tag{1}$$

where α and β are complex amplitudes which obey the equation

$$|\alpha|^2 + |\beta|^2 = 1, \tag{2}$$

while the probability that the qubit will be measured in state $|0\rangle$ is $|\alpha|^2$ and the probability that it will be measured in state $|1\rangle$ is $|\beta|^2$. Thus the probability that the qubit will be measured in either state $|0\rangle$ or state $|1\rangle$ is 1.

It is evident that a qubit will behave as a classical bit if the states $|\psi\rangle = |0\rangle$ or $|\psi\rangle = |1\rangle$ are prepared, because these are orthonormal and can be distinguished perfectly.

Generalizing to an N qubit system, a state can be represented by a state vector in a 2^N-dimensional Hilbert space, with the eigenstates

$$\underbrace{\{|0\rangle, |1\rangle\} \otimes \{|0\rangle, |1\rangle\} \otimes ...}_{N} = \{|0\rangle, |1\rangle\}^{\otimes N} \tag{3}$$

as basis.

Now any N-qubit register in this space can be expanded as

$$|\psi_N\rangle = \sum_{x \in \{|0\rangle, |1\rangle\}^{\otimes N}} a_x\,|x\rangle\,, \qquad \sum_x |a_x|^2 = 1. \tag{4}$$

Then, if the state $|\psi_N\rangle$ is measured in the standard basis, the outcome $|\psi_N\rangle = |x\rangle$ will be obtained with probability $|a_x|^2$. [2] [1]

2.2 Quantum entanglement

A pair of qubits can exist in four states, namely $|00\rangle$, $|01\rangle$, $|10\rangle$ and $|11\rangle$, as well as in all superpositions of these states. A state said to be *entangled* if it cannot be fully expanded in a Kronecker product. Entanglement is a *non-local*, i.e. pertaining to sets of qubits instead of single qubits. This concept has no analogue in classical computing, and its importance will be explored later in the report.

To understand quantum entanglement, a two-qubit system which can be divided into two parts, A and B, is considered. The Hilbert space of this biparticle system is the Kronecker product $H_A \otimes H_B$, where H_A and H_B are the Hilbert spaces of the two systems A and B, respectively.

The simplest examples of entangled states of a two-qubit system are

$$\left|\phi^{\pm}\right\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle) \tag{5}$$

$$\left|\psi^{\pm}\right\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle) \tag{6}$$

It is now possible to look at the implications of entanglement. It is assumed that a state $|\phi^+\rangle$ is prepared, and that two observers P and Q each have access to only one of the two qubits A and B. If P now measures a qubit A in the standard basis, he will obtain the result $|0\rangle_A$ with probability $\frac{1}{2}$ and $|1\rangle_A$ with probability $\frac{1}{2}$. If P result is $|0\rangle_A$ then it means that the system is in the state $|00\rangle$, and thus the value of the second qubit can be inferred immediately. In other words, the measurement by observer P influences the future measurement by observer Q. In principle this would occur even if the two qubits comprising the state were at two totally different locations. Furthermore, these non-local correlations can only be created locally, and thus the two systems have to interact initially in order to become entangled.

Qubits for a quantum computer can for instance be implemented using particles with two spin-$\frac{1}{2}$ states, spin-up and spin-down, identifying $|0\rangle = \binom{1}{0}$ for spin up and $|1\rangle = \binom{0}{1}$ for spin down. But in fact any system, possessing an observable quantity, which is conserved under time evolution such that it has at least two discrete and sufficiently spaced consecutive eigenvalues, is a suitable candidate for implementing a qubit. [2]

3 Data representation and logical operations in quantum computers

As explained in the previous sections, quantum computers will operate on and store data represented by qubits. Like classical computers, quantum computers rely on logical gates to operate on data, only certain differences arise as a consequence of the laws of quantum mechanics. Formally, a quantum mechanical gate is any device which can perform a unitary transformation on an input *state*. Logical operations on these states can be represented by unitary matrices.

A fundamental property which stems from the unitarity, is that the gate operation returns not only one boolean value as in the classical case. Instead the output state must belong to the same space as the input state, i.e contain the same number of qubits as the input state. This implies that it is not possible to recreate all classical gates - for example, generally, it is not possible from the single-bit result of a logical AND operation to infer the value of each input bit, meaning that the logical AND cannot be represented as a unitary transformation.

To clarify the notion of "input" and "output", consider a string of n qubits, i.e. $|b_1 b_2..b_n\rangle$. This sequence is one *state* and can be written [1, eq.(2)],

$$|\psi\rangle = \sum_{x=00..0}^{11..1} c_x |x\rangle \,, \tag{7}$$

where the sum of the square amplitudes of the coefficients c_x equals 1.

The simplest possible gates are unary operators. Using the kets in the above expressions as a basis, all states and operators (regardless of the number of qubits) can be written in matrix form. A single qubit is any superposition $\alpha|0\rangle + \beta|1\rangle$, meaning that its coordinate matrix has dimension 2×1. Consequently, a unary operator must be 2×2, i.e.

$$\underline{\underline{U}} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} . \tag{8}$$

Binary quantum gates are somewhat more complicated, taking as input a state on the form

$$|\psi\rangle = c_{00}|00\rangle + c_{01}|01\rangle + c_{10}|10\rangle + c_{11}|11\rangle \,. \tag{9}$$

In the example with two qubits, the state vector will reside in a four-dimensional space, and thus all binary operators are represented by the unitary 4×4 matrices.

As an example, consider a quantum mechanical equivalent of the XOR gate, frequently called a *controlled-not* or CNOT gate. It takes two qubits as input; if the first qubit is $|0\rangle$, both qubits remain untouched. If it is $|1\rangle$, the second qubit is negated. In other words, the $|10\rangle$ and $|11\rangle$ states are interchanged whereas $|00\rangle$ and $|01\rangle$ are unmodified. This uniquely determines the matrix representation

$$\underline{\underline{\mathrm{CNOT}}} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} . \tag{10}$$

On a side note, while unary and binary operators may seem incompatible since their arguments have different dimensions, any unary operator can be expressed as a binary operator which performs no operation using its second argument. This is done simply by applying a Kronecker product with unity to the operator.

Interestingly, the CNOT gate can be used to entangle qubits. Consider the unentangled state

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle . \tag{11}$$

CNOT operates on $|\psi\rangle$ as follows (normalization omitted)

$$\mathrm{CNOT}(|00\rangle + |10\rangle) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = |00\rangle + |11\rangle \tag{12}$$

Obviously, the resulting state cannot be written as a Kronecker product, which implies that the state is entangled. Thus the operation can produce an entangled state from an unentangled state. The state listed here, specifically, is an Einstein-Podolsky-Rosen pair. It is readily seen that the CNOT operation is its own inverse, which curiously implies that the states can be unentangled by another CNOT gate. It will later become clear exactly why entanglement is useful to quantum computing.

Since the classical logical operations, as mentioned before, are not necessarily expressible in terms of quantum computational operators, many classical operations cannot be directly implemented using quantum gates. Indeed, the XOR gate described above, suitably combined with unary operators, may provably be used to construct any unitary transformation of n-qubits [2, p.8], whereas it would be insufficient to construct all classical logical gates. The gates mentioned in this section, i.e. all unary unitary transformations plus CNOT, are therefore the only necessary gates in the construction of a quantum computer.

4 Peculiarities of quantum information processing

The *no-cloning theorem* of quantum mechanics states that it is not possible to construct a device capable of creating a copy of an arbitrary unknown state. This is a severe limitation compared to classical computing where the ability to copy arbitrary data is fundamental. Suppose we want to "copy" a single qubit, i.e. a superposition of $|0\rangle$ and $|1\rangle$. The problem can be partially circumvented by using entanglement: while the state cannot simply be recreated, it can still be mapped unitarily to the highly entangled state $\alpha\,|00..0\rangle + \beta\,|11..1\rangle$ containing arbitrarily many qubits [1, p.250], where the coefficients are in accordance with the original superposition.

5 Quantum decoherence and error correction

Classically, data can be corrupted during any data transfer involving sufficiently noisy connections. Such corruption can be detected by sending the data twice (or more) and making a bitwise comparison of the data. If an error should be detected, it can also be corrected, provided that the data has been sent thrice: if one bit is wrong, then the two remaining bits, which agree, are very probably correct.

In quantum computers, likewise, corruption of data is a problem since interaction and entanglement of data with the surroundings might introduce errors. The simple "majority vote" of classical computing relies on the copying of data. Using the procedure stated above, the information for the quantum mechanical case can be arrayed using entanglement. If one qubit should become entangled with an outside source, a majority vote will securely accomplish the reconstruction of damaged data. One complication is that the entanglement probably disturbs both terms in the above superposition, meaning that three qubits may not be enough to reliably perform the reconstruction. Instead, five qubits would be necessary to deal with this duplicate error in a 3-to-2 vote. In practice, several different errors may occur, and methods involving additional qubits may be used to deal with these. For example, there exists a method (*Steane code*) which will correct one phase shift error and one bit flip error using seven qubits. The method is described in detail in [8]. In a quantum computer, information may randomly become entangled with elements of the surroundings over time. This phenomenon is known as decoherence, and its treatment likewise requires error correction.

6 Problems that quantum computers could solve efficiently

Quantum information technology can be used to solve a number of problems. A few examples are quantum prime factorization, application of quantum teleportation and quantum cryptography, which will be described below.

6.1 Quantum factorization

One of the strengths of quantum computing is the ability to solve huge factorization problems. For a classical computer it is easy to multiply two big prime numbers by each other, but it might be very complicated to find the prime factorizations of huge numbers, because classical computers more or less have to try all numbers from an end. This also explains why the difficulty of factoring large numbers is responsible for the strengths of most cryptographic systems. As an example, for a classical computer being able to test for 10^{10} different numbers per second, which is actually more than any computer built today can handle, the average time to find the factors of a 60-digit long number would exceed the age of the universe.

Using quantum computers, on the other hand, factorization problems might be solved much faster than with classical computers. One algorithm which can be used for factorization of large numbers using quantum computers is the so-called emphShor's algorithm, and will be described below. Like all quantum computer algorithms, Shor's algorithm is probabilistic, meaning that it gives the a correct answer with high probability, and the probability of failure can be decreased by repeating the algorithm.

The fastest algorithm used for factorizing of a large number, n, whose representation has $\log_2(n)$ bits, on a classical computers runs in exponential time, as $e^{c(\log(n))^{1/3}\cdot(\log\log(n)))^{2/3}}$, where c is a constant. In contrast, Shor's algorithm does not run in exponential time, but as $(\log(n))^2 \cdot \log(\log(n))$, and this fact distinguishes quantum computers from classical computers. This difference derives from the fact, with a classical computer, only one division may be performed at a time, whereas for a quantum computer several calculations can be performed parallel, because of the way states are superposed.

The algorithm is composed of two parts. The first part of the algorithm turns the factorization problem into the problem of finding the period of a function, and may be implemented classically. The second part of the algorithm finds the period using a quantum Fourier transform and is responsible for the quantum speedup.

To perform Shor's algorithm, a function $F(a) = x^a \pmod{n}$ is considered, where a is the superposition of states. When the greatest common divisor of the two numbers x and n is 1, they are said to be coprime. The function is periodic with period r when x is an integer coprime to n, where n is the number that has to be factorized. On a classical computer it will take exponential long time to calculate the function $F(a)$ for an exponential number of a's. In contrast, Shor's algorithm utilizes quantum parallelism to perform the exponential number of operations in one step.

Knowing that $F(a)$ is a periodic function with period r, it can be calculated that

$F(0) = x^0 \pmod{n} = 1$ because $x^0 = 1$ and therefore $F(r) = x^r \pmod{n} = 1$ and $F(2r) = x^{2r} \pmod{n} = 1$ and so on.

Shor's algorithm tries to find the period r for the function $F(a)$. To perform this, the algorithm creates a quantum memory register with two parts. In the first part of the register the algorithm places a superposition of the all integers a which are desired for evaluation of the function $F(a)$. The desired values for the a's are chosen to be the integers from 0 to q^{-1}, where q is the power of 2 such that $n^2 \leq q \leq 2n^2$. Then the algorithm calculates $F(a)$ and places the result in the second part of the quantum memory register.

As described, the number n is represented by a $\log_2(n)$ bit string. Thus $F(a)$ must be calculated an exponential number of times with respect to the length of the encoded input to the algorithm.

Afterwards, the algorithm measures the state of the second register which now contains the superpositions of all possible outcomes of $F(a)$. Measuring this register has the effect on the state that it will collapse into some observed value, k. Furthermore, it has the side effect of projecting the first part of the quantum register into a state consistent with the value measured in the second part. Thus measurement of the second part results in exactly one value, thereby causing the other partition to collapse into a superposition of the basis states consistent with the value observed in the second part.

After the measurement, the second part of the register will contain the observed value k, and the first part of the register will contain a superposition of the basis states whose evaluation in $F(a)$ produces k.

Recall that $F(a)$ is a periodic function and thus the first part of the register might contain the values c, $c{+}r$, $c{+}2r$, where c is the lowest possible integer that satisfies the equation $x^c \pmod{n} = k$.

Performing a Fourier transformation on the contents of the first part of the register will yield the amplitudes of the register at integer multiples of the quantity $\frac{q}{r}$.

Now measuring the first part of the quantum register will yield an integer multiple of the inverse of the period with high probability. Once this number is found from the quantum memory register, a classical computer will be able to analyze it making a guess to find the actual value of r and from this guess compute the possible factors of n. Thus the number n has become factored. [6] [7]

6.2 Quantum cryptography

Traditional cryptographic solutions rely upon computationally intensive mathematical algorithms whereby information can be encrypted. Classical protocols exist, but these are not informationally secure and could be broken by a quantum computer. Therefore it might be interesting to get a technology by which secure information can be protected by use of quantum cryptography. To explain this technology, it is necessary to look at *quantum key distribution*.

The goal of quantum key distribution is to share a secret random bit string, called a cryptographic key between two persons, Alice and Bob, who have an insecure secret quantum channel and a public classical channel at their disposal. To be useful and to provide security, the key must be absolutely random, and it must be kept completely secret from anyone but the two communicating persons.

Now, in quantum key distribution, an eavesdropper is allowed to interact with the quantum information carriers that might be sent from Alice to Bob, at the risk of disturbing them. Furthermore the eavesdropper can passively listen to all classical information between the two persons. But it is not possible for the eavesdropper to alter or suppress the classical information.

If the eavesdropper then interacts with the quantum signal, Alice and Bob will detect it and abort their message. In other words, it is not possible for the eavesdropper to remain undetected and obtain significant information on the cryptographic key at the same time, and thus only Alice and Bob can obtain the secure information. [1]

The important consequence of the Heisenberg Principle is that any attempt for an eavesdropper to tamper with the transmission of a secret signal will result in an alternation of the signal states that cannot be prevented. This ”fingerprint” manifests itself as an overall error rate that can be detected by the authorized communicators. [4]

7 Quantum teleportation

Quantum teleportation is interesting because it is a phenomenon that makes it possible to transform a lot of information very fast.
Quantum teleportation has no classical counterparts. It involves an initial state, in which a pair of particles in a maximally entangled state, for instance the state $\sqrt{\frac{1}{2}}(|00\rangle + |11\rangle)$, is shared between two parties. This is followed by a second state in which the shared entangled state is used. The pair of particles is used to achieve transmission of a qubit via two classical bits or transmission of two classical bits via one qubit, respectively.

Quantum teleportation illustrates the fact that in order to achieve transmission of intact quantum states, two qualitatively different resources are required, a quantum resource that cannot be copied and a directed resource that cannot travel faster than light. For quantum teleportation, the first function is provided by the entangled state shared by the two particles, while the second function is performed by two classical bits. Thus quantum information theory involves two species of information, classical information and entanglement, and three primitives, transmission of a bit, transmission of a qubit and sharing of a pair of entangled states. [1]

8 Physical implementation of quantum computers

Realizing a quantum computer is not an easy task, and indeed only very limited actual quantum computers have been made. This section discusses possible approaches to physically constructing quantum computers.

As written previously, a quantum computer draws the advantages through the concept of entangled states of qubits and the manipulation of these, which is also what makes it difficult to realize quantum computers. First one has to create a qubit, i.e. to make a physical system that can contain the information required. Second one has to make sure that the system can maintain this information. This means that one have to minimize e.g. the entanglement with the environment, also known as decoherence, resulting in loss of information. Decoherence can be avoided by proper amplication and error correction of data, as described in section 5. And third it must be possible to perform a unitary operation on the system to implement the appropriate algorithms.

Ideas for many different kinds of solutions have been conceived, and in the following we will go through the basic principles of some of these systems.

8.1 Ion trap

A single atom with a ground state and a long lived exited state is an example of a system with two quantum mechanical states. If it is possible to form superpositions of these states in a controlled manner, it can be utilized as a qubit. In such a system the ground state, $|g\rangle$, is used as the $|0\rangle$ state, the exited state, $|e\rangle$, is used as the $|1\rangle$ state, and superpositions are formed by rotation.

Such systems are formed by trapping atoms in an electric field with high vacuum. For an actual system a string of ions is created. Here single atom modes of vibration are initialized with laser pulses, and these interact with the neighbouring atoms through Coulomb interaction to create a collective vibration. These normal mode vibrations can both be created and removed by laser pulses and thus it is possible to transfer information along the string.

One of major setbacks of this method is that noise control requires very low temperatures, in the order of μK.

In these systems single qubit operations have been performed but realizing a quantum gate i.e. a two qubit operation have not yet been accomplished. [2]

8.2 Nuclear Magnetic Resonance

Nuclear magnetic resonance (NMR) is a physical phenomenon based upon the magnetic property of the nucleus of a atom.

In systems where NMR is used to realize quantum computers the two qubit states $|0\rangle$ and $|1\rangle$ is represented by the two spin states of a spin-$\frac{1}{2}$ particle.

A molecule is placed in a strong magnetic field, and thus it is possible to manipulate the spin states by applying oscillating magnetic fields in pulses of a certain duration. However, it is difficult to measure the state of only a single molecule, and thus a relatively large number, about 10^{23}, of molecules in a liquid is used simultaneously.

So far, NMR has been the most successful technique for realizing qubits, but unfortunately it is not as likely to scale well as some of the solid state based solutions. [2]

9 Entanglement and quantum computing with ballistic electrons

The following section describes an article, *Entanglement and quantum computing with ballistic electrons* by Andrea Bertoni and Susanna Reggiani. The article considers a specific approach to implement a solid-state quantum computer, including the implementation of qubits as a selection of a universal set of quantum gates. Subsequently, for a model system numerical simulations of electron propagation in quantum wires are performed.

9.1 Implementation of a qubit and quantum wires

A quantum wire is proposed by preparing a GaAs/AlGaAs or a Si/SiO_2 system in such a way that two parallel conductive lines are surrounded by nonconductive matter. A qubit here is represented by an electron, which would be able to travel along either wire. The qubit states $|0\rangle$ and $|1\rangle$ correspond to the electron being on the left or right wire, respectively. In other words, it is the location of the expectation value of x, the position transversal to the wires, which distinguishes the two states.

9.2 Implementation of gates

The article considers three different gate implementations: two unary gates and a binary gate. The first type of unary gates is created by letting the two conductive wires run closely along each other for a certain distance, (the *coupling region*), such that the electron may "jump" from one wire to the other. When the two wires are close together, the Fermi-Dirac principle makes the two formerly symmetrical states split into one with high energy and one with low energy. Now the wavefunction of a propagating electron, when it is crossing the coupling region, will oscillate between the two wires with a period, $\tau = \frac{\Delta E}{h}$. When the electron reaches the end of the coupling region, the oscillation process terminates and the wave function will continue propagating with new components along either wire. This transformation can be represented by a 2×2 rotation matrix.

A second kind of single-qubit transformation was also obtained by introduction of a potential barrier on one of the two wires. If the barrier is small enough, the component of the qubit residing on this wire will penetrate the barrier, yet be delayed by a certain amount compared to the component on the other wire. The operation therefore represents a mutual phase shift.

In order to implement a two-qubit gate, two couples of wires were modelled such that the wire corresponding to the state $|1\rangle$ for the first qubit and the wire corresponding to the state $|0\rangle$ for the second qubit got closer to each other as shown in figure 1. This allows the two qubits to become entangled. Effectively, the component introduces a phase shift to the $|01\rangle$ state of the system.

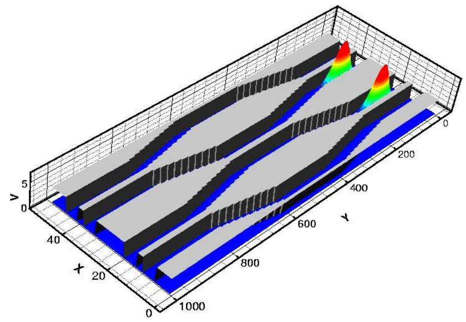

Figure 1: *Schematic potential profile of the two-qubit gate*

9.3 Propagation of qubits inside quantum wires

Until now, no description has been provided of how qubits would actually move in the quantum wires. The method used relies on *surface acoustic waves*. Basically, a sinusoidal acoustic wave of very high frequency (order of 3 GHz) is made to propagate through the material using a transducer. The acoustic wave can generate a moving, sinusoidal potential along the axis of propagation in the material, such that an electron trapped inside a potential well will be forced to propagate at the same speed as the wave. The article notes that this method, importantly, will not interfere with the gate implementations described above.

9.4 Measurements of entanglement by numerical simulations

In order to check for the feasibility of the gates under investigation, a realistic profile of a conducting band inside a doped two-dimensional electron gas was simulated, where the two coupled wires were formed inside a GaAs/AlGaAs structure as shown i figure 2. Then, to inject single electrons into the system, the region containing the electron gas was connected to the wire region.

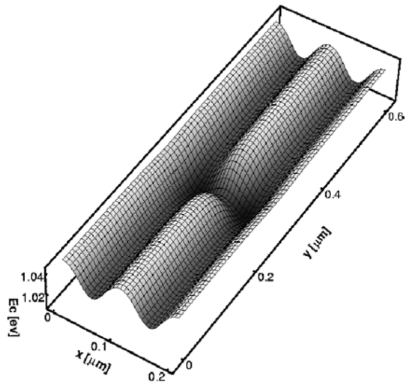

Figure 2: *A two-qubit gate formed of thwo quantum wires.*

As expected, for the simulations it was found that the binary gate was able the entangle the two qubits by introduction of a phase factor to the $|01\rangle$ state.

On the other hand, another major effect was observed. The two electrons evidently interact electrostatically, resulting in entanglement with respect to their y-variables, i.e. the location along the wire axis. To study why the two electrons were entangled in their y-position, simulations were performed where two electrons propagated either in the same direction or in opposite directions along two parallel wires realized by Si/SiO_2. For this model the "amount" of entanglement was calculated as a function of time by means of the *von Neumann entropy* of the reduced density matrix calculated for the system.

Numerical results obtained for simulations of two electrons propagating in the same direction along two parallel wires is shown in figure 3. Because of the Coulomb interaction the entanglement increases very quickly and reaches a maximal value, then slightly decreasing, as shown to the left in the figure, where the entanglement is plotted as function of the time. The maximum entanglement is plotted as a function of the distance between the wires to the right in the figure. The graph shows that the obtained maximum entanglement decreases with increasing distance between the wires. In constrast, if two electrons are moving in opposite directions along the two parallel wires,

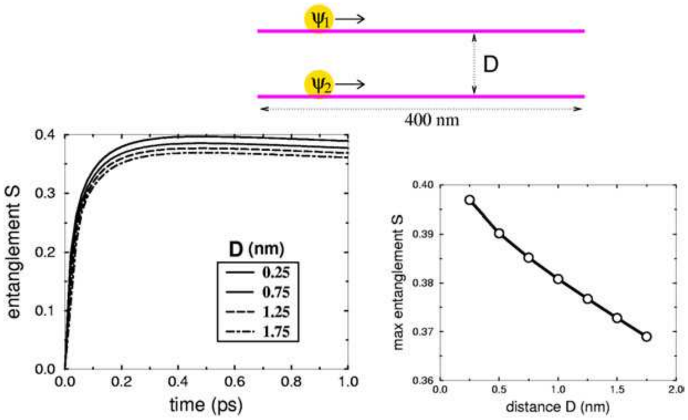

Figure 3: *Results obtanined for simutions of two electrons moving in the same direction.*

the obtained results are very different from the previous results as shown in figure 4. As shown to the left in the figure the entanglement increases as the electrons are approching each other, while it decreases as they move away from each other again. The entanglement reaches a finally reaches a constant value. The dependency of this final value on wire distance is plotted to the right in figure 4, and the final entanglement has a maximum when the distance between the wires is about 1 nm as shown to the right in the figure. [9]

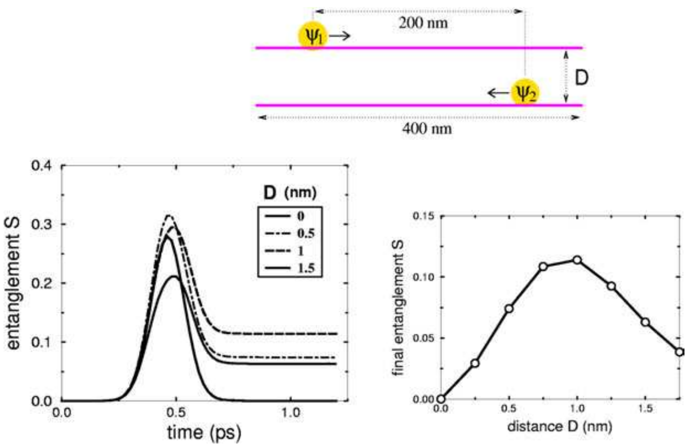

Figure 4: *Results obtained for simulations of two electrons moving in opposit directions.*

References

[1] Quantum Information and Computation, Charles H. Benneth and David P. DiVincerro, Macmillan Magazine Ltd, 2000

[2] Fighting Entanglement with Entanglement, Søren Stenild Huhl and Sune Lehmann, University of Copenhagen, 2000

[3] Limits on Silicon Nanoelectronics for Terascale Integration, James D. Meindl et al., Science, September 2001

[4] Pushing the Frontier Sce: Quantum Crypthography Research at MITRE, Gerals Gilbert, http://www.mitre.org/news/the_edge/january_02/gilbert2.html

[5] Fysik, Morten kringelbach, http://www.kringelbach.dk/Inf_TeleportationEnRealitet.html

[6] Quantum Computing and Shor's Algoritm, Hetthew Hayward, http://alumni.imsa.edu/ matth/quant/299/paper/

[7] Wikipedia, "Shor's algorithm", http://en.wikipedia.org/wiki/Shor's_algorithm

[8] Calderbank-Shor-Steane Codes, http://beige.ovpit.indiana.edu/B679/node120.html

[9] Entanglement and Quantum Computing with Ballistic Electrons, Andrea Bertoni and Sasanna Reggiani, Semiconductor Science and Technology, 2004