NOTES ON QUANTUM COMPUTING AND RELATED TOPICS

D.A. Ross and A.J.G. Hey
Quantum Technology Group, University of Southampton, Southampton, SO17 1BJ

Abstract
These notes are intended as a simple introduction to the new field of quantum computing, quantum information theory and quantum cryptography. Undergraduate level quantum mechanics and mathematics is required for an understanding of these lectures. After an introduction to qubits and quantum registers, we introduce the key topics of entangled states and quantum logic gates. For two qubit states, we introduce the four Bell states as a change of basis. The essentials of quantum cryptography are then described, although this is just a straightforward application of quantum mechanics. The characters of Alice, Bob and Eve are first introduced here. Two qubit Bell states are used to demonstrate a novel 'dense coding' technique. Finally, in these communication applications, quantum teleportation is explained in detail, again making use of entangled Bell states. The technique of magnetic spin resonance is used as a familiar example to illustrate how qubit operations could in principle be realised. This leads on to the specification of quantum devices that can encode functions. All this is preparatory to a detailed discussion of two of the most significant quantum algorithms discovered to date, namely, Peter Shor's factorization algorithm and Lov Grover's quantum database search algorithm.

1. INTRODUCTION

The basic unit of a classical computer is a bit. This is a device that can be in one of two states. Usually this is a wire which is in the state $|1>$ if the wire carries a voltage and $|0>$ if it does not (more precisely the two states are distinguished by the electrode having a high or low voltage respectively). Thus such a bit can carry one binary digit, the two states representing the numbers 0 and 1. By assembling L such bits one can store numbers from 0 to $2^L - 1$. The memory of a modern computer contains of the order of 10^9 bits and the disk storage contains of the order of 10^{11} bits.

In early computers a memory device to store a bit consisted of a small toroid of ferromagnetic material with an electric coil wrapped around it. If the bit was "set" (i.e. in the state representing the number 1) then a current passed through the coil and the toroid produced a magnetic field. For the state representing 0 there was no current and consequently no magnetic field. Clearly the total number of such bits was limited by constraints of both size and cost and computer with more than 10^6 bits were rare.

Since then we have seen the revolution in semiconductor technology and a great deal of effort has been put into reducing the size and costs of these binary bits. Nowadays a flat microchip with a surface area of order 1 cm^2 can hold of the order of 10^8 bits. The small size of these memory chips has also had the effect of speeding up the rate at which computers can run; essentially this is because the electromagnetic signal has less distance to travel between components.

The original motivation for imagining a "quantum computer" was based on pushing these improvements in technology to their physical limit. The smallest device one can imagine, that can exist in two states, is a single electron which has the property of spin whose component in a given direction (usually taken to be the $z-$direction) can take one of two values, $\pm\frac{1}{2}\hbar$. We could take these two states to represent the two states of a binary bit. The spin of an electron can be flipped by the application of an oscillating magnetic field with the correct (resonant) frequency, and can in principle be measured by

applying a constant magnetic field in the z direction and observing the energy change. If this were a single outer electron of a molecule that represented one lattice point on the surface of a crystal, a surface area of order 1 cm^2 could hold of order 10^{16} such bits. The difficulty, of course, is that to store and read different numbers we would need to be able to apply or measure magnetic fields that differentiated between two neighbouring spins which were only 10^{-8} cm apart.

There is, however, an important qualitative difference between a classical bit, which is an electronic component, and a quantum bit, such as the spin of an electron. Whereas a classical bit can only be in one of two possible states (high or low voltage) and must be in one of these two states, a quantum bit need not be in one or other of the two allowed states but can in general be in any linear superposition of these states. The electron does not have to be in an eigenstate of the z component of spin, for which the value is definitely either $+\frac{1}{2}\hbar$ or $-\frac{1}{2}\hbar$, but in a linear superposition of these. For a register of L such quantum bits this gives us the opportunity of storing all possible numbers between 0 and $2^L - 1$, *simultaneously* and performing operations on these numbers and storing the result of applying such operations on all arguments simultaneously. The difficulty now arises of how to project from this linear superposition the particular value that we are interested in. This is where algorithms for quantum computing are used and there are cases in which these algorithms can significantly enhance the rate at which a computation can be performed. One particular example of this is a database search for which the time taken to carry out the search grows linearly with the size of the database if classical computational algorithms are used, but only as the square root of the size of the database if a quantum algorithm is used on an initial quantum state, which consists of a superposition of the entire database. The database in question must be a quantum version of the classical database.

The practical difficulties in constructing such quantum computers are enormous. So far the various algorithms have only been carried out on samples of at most two or three quantum bits. Nevertheless a theoretical study of the potential power of a quantum computers is a worthwhile enterprise, albeit in anticipation of significant improvement in the required engineering techniques.

2. DEFINITIONS ETC.

a. **qubit:**
A qubit is a quantum system which can be in one of two states. We shall think of these as spin-$\frac{1}{2}$ particles, the two states being two eigenstates of S_z, although it is likely that in practice a photon will be used, the two states being the state of polarization (horizontal or vertical) with respect to some chosen axis. The qubit can take 2-values - 0 or 1, which are associated with the two eigenstates as follows:

$$|1> \equiv \ |\uparrow>$$

$$|0> \equiv \ |\downarrow>$$

In general a qubit can be in a superposition of these two states with complex coefficients α and β,

$$\alpha|0> + \beta|1>, \quad (|\alpha|^2 + |\beta|^2 = 1)$$

and it is this property that distinguishes them from classical bits used in conventional computers. In mathematical terms, we say that since the general state of a qubit can be a superposition of the two pure states, with arbitrary complex coefficients, then the state a described as a vector in the two dimensional complex space $\mathcal{C}^2$.

b. **L-bit register:** A register is a set of L qubits. Such a register can be used to store an integer number, J, between 0 and $2^L - 1$. The state of the register is denoted by this number, e.g.

$$|J> \equiv \ |\uparrow\uparrow\downarrow\uparrow\downarrow \cdots \downarrow\downarrow> \ .$$

For example in the case of a 2-bit register

$$|0>\equiv\ |\downarrow\downarrow>$$
$$|1>\equiv\ |\downarrow\uparrow>$$
$$|2>\equiv\ |\uparrow\downarrow>$$
$$|3>\equiv\ |\uparrow\uparrow>$$

Once again, a register can be in a superposition of states

$$|\psi>\equiv\ \sum_{J=0}^{2^L-1} a_J|J>\ .$$

The interpretation of the (complex) coefficients a_J is that $|a_J|^2$ is the probability that a measurement of the state of the system will yield the value J. Clearly by conservation of probability we have

$$\sum_{J=0}^{2^L-1} |a_J|^2\ =\ 1.$$

Such states are also known as "coherent" states.
In mathematical terms, the state of an L qubit register is a vector in a space which is the outer product $\mathcal{C}^2\otimes\mathcal{C}^2\cdots\otimes\mathcal{C}^2$, one for each of the L qubits.

c. **Entangled pair:**
This is a pair of qubits which is in a superposition of eigenstates of S_z i.e. some superposition of the states $|0>,\ |1>,\ |2>,\ |3>$ defined above, in such a way that the state *cannot* be written as the product of states for each qubit.
Thus, for example the state

$$\frac{1}{2}\left(|0>+|1>+|2>+|3>\right)$$

is *not* an entangled pair, since it can be written as

$$\frac{1}{2}\left(|\downarrow>+|\uparrow>\right)\otimes\left(|\downarrow>+|\uparrow>\right),$$

whereas the state

$$\frac{1}{\sqrt{2}}\left(|0>+|3>\right)\ =\ \frac{1}{\sqrt{2}}\left(|\downarrow\downarrow>+|\uparrow\uparrow>\right)$$

is an example of an entangled pair. In general a superposition (with coefficients $a_i,\ i=0\cdots3$)

$$a_0|0>+a_1|1>+a_2|2>+a_3|3>$$

is an entangled state *unless*

$$\det\begin{vmatrix} a_0 & a_1 \\ a_2 & a_3 \end{vmatrix}\ =\ 0.$$

A specific example of entangled pairs occurs in the total spin of multi-electron atoms. In the case of He, for example, the two electrons can be in a total spin state $S=1$ with three allowed values for the $z-$component of spin, $S_z=-1,\ 0,\ 1$, or in a total spin state $S=0$. In terms of the individual spins of the two electrons these are given by

$$|\downarrow\downarrow>,\qquad S=1,\ S_z=-1$$
$$|\uparrow\uparrow>,\qquad S=1,\ S_z=1$$
$$\frac{1}{\sqrt{2}}\left(|\downarrow\uparrow>+|\uparrow\downarrow>\right),\qquad S=1,\ S_z=0$$
$$\frac{1}{\sqrt{2}}\left(|\downarrow\uparrow>-|\uparrow\downarrow>\right),\qquad S=0,\ S_z=0.$$

The two states $S = 1, S_z = 0$ and $S = 0, S_z = 0$ are examples of entangled states.
The concept of entangling can easily be extended to L qubits. The state is entangled *unless* it can be written as a product of states for each of the L qubits. Regarding the state as a vector in the space $\mathcal{C}^2 \otimes \mathcal{C}^2 \cdots \otimes \mathcal{C}^2$, a state is said to be entangled if it *cannot* be expressed as a single outer product of vectors in each $\mathcal{C}^2$ space, but only as a linear superposition of such outer products (known as a "tensor product").

d. **Unitary transformations:**
A Unitary transformation is a transformation which takes the superposition (coherent) state of L qubits

$$\sum_{J=0}^{2^L-1} a_J |J>$$

to

$$\sum_{J=0}^{2^L-1} a'_J |J>,$$

where

$$a'_J = \sum_{K=0}^{2^L-1} U_J^K a_K,$$

the matrix $\mathbf{U}$ being unitary

$$\mathbf{U}^\dagger \mathbf{U} \; = \; I.$$

From this unitarity property one can show that the new coefficients a'_J also obey the conservation of probability relation

$$\sum_{J=0}^{2^L-1} |a'_J|^2 = 1$$

and so the new state is also a superposition in which the probability of a measurement yielding the value J is $|a'_J|^2$. This is also a coherent state so the unitarity operator preserves the coherence.
A unitary transformation might only act on one qubit, leaving the other qubits in the register alone or alternatively it might act on two or more qubits simultaneously.

Examples of **U**:

The unitary transformations on a single qubit can be written in terms of four matrices, each depending on a single parameter, θ.

- $$\mathbf{u}_x(\theta) = \begin{pmatrix} \cos(\frac{\theta}{2}) & i\sin(\frac{\theta}{2}) \\ i\sin(\frac{\theta}{2}) & \cos(\frac{\theta}{2}) \end{pmatrix}.$$

  For a spin-$\frac{1}{2}$ particle, this corresponds to a rotation through angle θ about the $x-$ axis.

- $$\mathbf{u}_y(\theta) = \begin{pmatrix} \cos(\frac{\theta}{2}) & \sin(\frac{\theta}{2}) \\ -\sin(\frac{\theta}{2}) & \cos(\frac{\theta}{2}) \end{pmatrix}.$$

  For a spin-$\frac{1}{2}$ particle, this corresponds to a rotation through angle θ about the $y-$ axis.

- $$\mathbf{u}_z(\theta) = \begin{pmatrix} e^{i\theta/2} & 0 \\ 0 & e^{-i\theta/2} \end{pmatrix}.$$

For a spin-$\frac{1}{2}$ particle, this corresponds to a rotation through angle θ about the $z-$ axis.

$$\mathbf{u}_0(\theta) = \begin{pmatrix} e^{i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{pmatrix}.$$

This corresponds to multiplication by an overall phase factor. The identity matrix, **I**, is $\mathbf{u}_0(4\pi)$. Spin representations of the rotation group are double-valued: a rotation by 2π generates an overall minus sign and 4π is required for the identity operation.

A general unitary 2×2 matrix can always be obtained from a product of these transformations.

Now consider 2 qubit states. The unitary matrices $\mathbf{U}$ are 4×4 matrices. For example

- $$\mathbf{U}_1 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

  This flips both qubits. It is a "NOT" gate, denoted by $\mathbf{U}_{NOT}$, i.e.

  $$\mathbf{U}_{NOT}|\uparrow\uparrow> = \mathbf{U}_1|3> = |0> = |\downarrow\downarrow> .$$

- $$\mathbf{U}_2 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

  This flips qubit 2 only, e.g.

  $$\mathbf{U}_2|\uparrow\uparrow> = \mathbf{U}_2|3> = |2> = |\uparrow\downarrow> .$$

- $$\mathbf{U}_3 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

  This flips qubit 2 if and only if qubit 1 is in the state $|1>$. This is a "controlled NOT gate", and is usually denoted as $\mathbf{C}_{NOT}$, e.g.

  $$\mathbf{C}_{NOT}|\uparrow\uparrow> = \mathbf{C}_{NOT}|3> = |2> = |\uparrow\downarrow>,$$

  but

  $$\mathbf{C}_{NOT}|\downarrow\uparrow> = \mathbf{C}_{NOT}|1> = |1> = |\downarrow\uparrow>,$$

- $$\mathbf{U}_4 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

  This flips qubit 1 if and only if qubit 2 is in the state $|1>$. It is also a controlled NOT gate and we denote it by $\mathbf{C}'_{NOT}$. Thus

  $$\mathbf{C}'_{NOT}|\uparrow\uparrow> = \mathbf{C}_{NOT}|3> = |1> = |\downarrow\uparrow>,$$

  but

  $$\mathbf{C}'_{NOT}|\uparrow\downarrow> = \mathbf{C}_{NOT}|2> = |2> = |\uparrow\downarrow>,$$

- $$\mathbf{U}_5 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

  This interchanges the two qubits and is denoted by $\mathbf{U}_{switch}$. This can be obtained from a combination (product) of $\mathbf{C}'_{NOT}$ and $\mathbf{C}'_{NOT}$, i.e.

$$\mathbf{U}_{switch} \;=\; \mathbf{C}_{NOT}\, C'_{NOT}\, C_{NOT}$$

Any L qubit unitary matrix can be constructed out of outer products of these single qubit unitary matrices (or their matrix products). However they will not in general be a single outer product of these 2×2 unitary matrices, but may be a sum of such outer products (this is known as a "tensor product").

In the above examples of 2 qubit unitary operators we have

$$\mathbf{U}_1 = \mathbf{u}_x(\pi) \otimes \mathbf{u}_x(-\pi)$$

$$\mathbf{U}_2 = \mathbf{I} \otimes (\mathbf{u}_0(\pi)\mathbf{u}_x(-\pi))$$

$$\mathbf{C}_{NOT} = \frac{1}{2}\left(\mathbf{I} \otimes \mathbf{I} - (\mathbf{u}_0(\pi)\mathbf{u}_z(-\pi)) \otimes \mathbf{I} + \mathbf{u}_0(\pi) \otimes \mathbf{u}_x(-\pi) + (\mathbf{u}_z(\pi)) \otimes \mathbf{u}_x(-\pi)\right).$$

The last is an example of such a tensor product.

A unitary matrix representing the transformation of an l qubit system is a matrix in the outer product space $\mathcal{C}^2 \otimes \mathcal{C}^2 \cdots \otimes \mathcal{C}^2$. If the transformation acts on each qubit separately then the matrix can be written as an outer product of a (2×2) matrix on each $\mathcal{C}^2$ space for each qubit. If, on the other hand, the transformation involves the interaction between qubits, as is the case for the controlled NOT gate, then the unitary matrix is not a single outer product of matrixes acting on each qubit, but a linear superposition of such outer products.

In general, a physical device can in principle be constructed that performs any of these unitary transformations. In the case of spin-$\frac{1}{2}$ particles we use the techniques of NMR (Nuclear Magnetic Resonance) to illustrate the construction of 'gedanken' devices, as is described later.

e. **Hadamard transformation:**

This is a unitary transformation which acts on each qubit with the matrix

$$\mathbf{u}_H \;=\; \frac{1}{\sqrt{2}} \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}$$

In terms of the fundamental single qubit transformations described above we have

$$\mathbf{u}_H \;=\; \mathbf{u}_0(\pi)\mathbf{u}_z(\pi)\mathbf{u}_y(-\pi/2).$$

The L qubit Hadamard transformation is represented by the outer product

$$\mathbf{U}_H \;=\; \mathbf{u}_H \otimes \mathbf{u}_H \otimes \mathbf{u}_H \cdots$$

It is often more convenient to use the pseudo-Hadamard transformation represented by the matrix

$$\mathbf{u}_{pH} \;=\; \mathbf{u}_y(-\pi/2) \;=\; \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}.$$

Either of these transformations has the effect that it transforms the lowest state $|0>$ into the sum of all states with equal coefficients,

$$\mathbf{U}_H|0> = \sum_{J=0}^{2^L-1} |J>$$

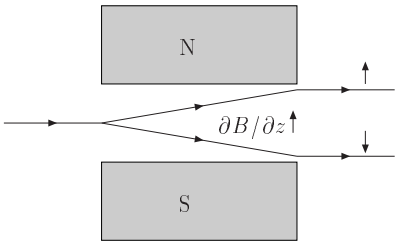


Fig. 1: Stern-Gerlach apparatus. A particle of spin-$\frac{1}{2}$ is passed between the poles of a magnet, which produces a non-uniform magnetic field in the $z-$direction. The particle is displaced upwards or downwards according to the $z-$compoent of its spin being $+\frac{1}{2}$ or $-\frac{1}{2}$ respectively. If the particle is initially in a superposition of these states then this apparatus forces it into one or other of the allowed states.

or

$$\mathbf{U}_{pH}|0>=\sum_{J=0}^{2^L-1}|J>\,.$$

The Hadamard gate is idempotent, i.e. it is equal to its own inverse, whereas this is not the case for the pseudo-Hadamard transformation. On the other hand a pseudo-Hadamard transformation can be achieved by a single rotation about the $y-$axis.

f. **Measurement:**
A measurement of a coherent state is an operation which "collapses" the state into a pure state. For a superposition (coherent state) we have for each value of K (0 to 2^L-1)

$$\sum_{J=0}^{2^L-1}a_J|J>\rightarrow\ |K>,$$

with probability $|a_K|^2$. This operation destroys the coherence of the state by collapsing it into one of the allowed pure states. The operation cannot be described by a simple matrix multiplication.
In the case of spin-$\frac{1}{2}$ particles such a collapse is effected by the simultaneous measurement of the $z-$component of spin of each of the particles. The $z-$component of spin of a single electron, S_z, may be measured using a "Stern-Gerlach" apparatus. The electron is passed through a region of non-uniform magnetic field in the $z-$direction. This causes a displacement of the path of the electron in one of two directions depending on the $z-$component of the spin of the electron (which is proportional to the $z-$component of the magnetic moment of the electron). From this displacement, the $z-$component of the spin can be deduced. If the electron was *not* in a pure eigenstate of S_z but a superposition of such eigenstates, then the operation of passing it through a Stern-Gerlach apparatus forces the electron into one of the two eigenstates of S_z.

g. **Bell states:**
These are four states for a 2 qubit system, which are specific examples of entangled pairs. They are labelled B_0, B_1, B_2, B_3 and may be defined as

$$|B_0>\equiv\ \frac{1}{\sqrt{2}}\left(|\uparrow\uparrow>+i|\downarrow\downarrow>\right)\ =\ \frac{1}{\sqrt{2}}\left(|3>+i|0>\right)$$

$$|B_1>\equiv\ \frac{1}{\sqrt{2}}\left(|\downarrow\downarrow>+i|\uparrow\uparrow>\right)\ =\ \frac{1}{\sqrt{2}}\left(|0>+i|3>\right)$$

$$|B_2>\equiv\ \frac{1}{\sqrt{2}}\left(|\downarrow\uparrow>-i|\uparrow\downarrow>\right)\ =\ \frac{1}{\sqrt{2}}\left(|1>-i|2>\right)$$

$$|B_3>\equiv\ \frac{1}{\sqrt{2}}\left(|\uparrow\downarrow>-i|\downarrow\uparrow>\right)\ =\ \frac{1}{\sqrt{2}}\left(|2>-i|1>\right)$$

These Bell states form an orthonormal set

$$< B_I|B_J >= \delta_{IJ},\ \ I,J = 0\cdots 3$$

so that any two qubit state can be expanded as a linear sum of Bell states.
They can be obtained by acting respectively on the pure state $|0>$, $|1>$, $|2>$, or $|3>$ with the unitary transformation

$$\mathbf{U}_{Bell} \ = \ \frac{1}{\sqrt{2}} \begin{pmatrix} 0 & 0 & i & 1 \\ 1 & -i & 0 & 0 \\ -i & 1 & 0 & 0 \\ 0 & 0 & 1 & i \end{pmatrix}$$

e.g.

$$|B_J> = \ \mathbf{U}_{Bell}|J>,\ \ J = 0,\cdots 3$$

It is useful to invert these Bell states, i.e to write the pure states as superpositions of Bell states. This gives

$$|0>=|\downarrow\downarrow>= \frac{1}{\sqrt{2}}\left(|B_1> -i|B_0>\right)$$

$$|1>=|\downarrow\uparrow>= \frac{1}{\sqrt{2}}\left(|B_2> +i|B_3>\right)$$

$$|2>=|\uparrow\downarrow>= \frac{1}{\sqrt{2}}\left(|B_3> +i|B_2>\right)$$

$$|3>=|\uparrow\uparrow>= \frac{1}{\sqrt{2}}\left(|B_0> -i|B_1>\right)$$

These may be written

$$|J> = \ \sum_{K=0}^{3} \left(U_{Bell}^{-1}\right)_J^K |B_K>$$

Thus a Bell state may be measured by passing it through a device which performs the inverse transformation of $\mathbf{U}_{Bell}$ and then measuring the $z-$components of spin of the two spin-$\frac{1}{2}$ particles. These Bell states have the remarkable property that they can be transformed into each other by transforming *only one* of the two qubits, i.e. the 4×4 transformation matrix which transforms $|B_I>$ into $|B_J>$ is of the form

$$\mathbf{I} \otimes \mathbf{v}_{IJ}.$$

for example

$$\mathbf{v}_{30} \ = \ \mathbf{u}_y(-\pi)$$

$$\mathbf{v}_{20} \ = \ \mathbf{u}_x(-\pi)$$

$$\mathbf{v}_{10} \ = \ \mathbf{u}_z(\pi)$$

$$\mathbf{v}_{00} \ = \ \mathbf{I}$$

This property of the Bell states is the crucial property on which applications such as quantum teleportation depend. Entanglement, as expressed in these Bell states, is the essence of the mystery of quantum mechanics. These states embody the non-local, 'faster-than-light' property of quantum mechanics, that Einstein so detested and which the EPR paradox was intended to highlight. Quantum algorithms make essential use of this non-local property to deliver their spectacular improvements over classical algorithms.

3. QUANTUM CRYPTOGRAPHY

This is not really quantum computing but rather the use of quantum mechanics to transmit a key which is only known to the encoder (Alice) and the decoder (Bob). A better name than quantum cryptography would be quantum key distribution since quantum mechanics is used to create a method of cryptographic key distribution which can detect the presence of an eavesdropper (Eve) listening in.

A message N, which can be stored in an L-bit register is encoded with the use of a key K which is also a number between 0 and $2^L - 1$. The encoded message M is simply

$$M \ = \ N \oplus K$$

($\oplus$ means exclusive or - XOR).

The decoding is effected by again performing the XOR operation with K

$$M \oplus K \ = \ N \oplus K \oplus K \ = N \oplus 0 = N$$

The key is transmitted from encoder to decoder (or vice versa) by transmitting a large number of qubits (usually one will need at least 2L of these). The qubits are either in one of the two eigenstates of S_z *or* in one of the two eigenstates of S_x. These are chosen at random, but with equal probability by the encoder. For each qubit the encoder, Alice, records the eigenvalue of the qubit as well as the direction of spin (z or x) in which the qubit was an eigenstate. The decoder, Bob, measures either the z-component or the x-component of the spin of each qubit (at random, but with equal probability) and records the result as well as which direction of spin was measured.

In about half the cases Bob will have measured the spin in the same direction as Alice prepared it ("good" qubits). For such qubits Bob will obtain a result for the eigenvalue which is always equal to the eigenvalue corresponding to the eigenstate in which it was transmitted. In the remaining half, in which Bob measured the spin in a different direction from the direction in which they were prepared ("bad" qubits) the result will have equal probability of being equal or opposite to the eigenvalue of the prepared state. These "bad" bits must be discarded, but it is safe to build a key, K, from the remaining "good" qubits.

It is therefore sufficient for Bob to tell Alice (on an open line if necessary) in which direction the spin of each qubit was measured it but not the result. Alice can then tell Bob (again on an open line) which are the "good" qubits and which are the "bad" ones. Although this is public information, no third party can reconstruct the key, since the third party still does not know the eigenvalues of the "good" qubits.

One important feature of this technique is that the presence of an eavesdropper, Eve, can be detected. If Eve intercepts the signal from Alice, she does not know which setting, z or x, that Alice used. She must therefore choose a setting at random and then retransmit this result, using her setting, to Bob. Since Eve will not guess correctly every time, when Alice and Bob first make contact over the phone, they compare not only the settings but the results. If there is an eavesdropper then Alice and Bob will find that there are some "good qubits" on which they disagree. They then know that the security of the quantum channel is compromised. If they find perfect agreement, and can conclude there is no eavesdropper, they can then go ahead and exchange only setting information as described above.

Quantum key distribution, both over optical fibres and in free space, has been successfully demonstrated by a number of different groups.

4. DENSE CODING

This is a technique which can be used to send a message consisting of an integer between 0 and $2^{2L} - 1$, by transmitting L qubits only.

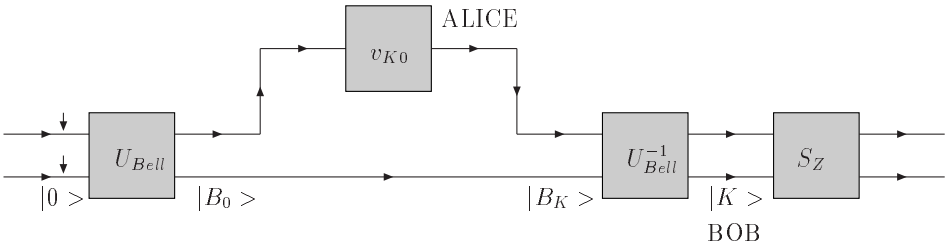


Fig. 2: Alice sends the number K ($K = 0 \cdots 3$) to Bob. Alice takes one particle from an entangled pair in Bell state $|B_0>$, performs the transformation $\mathbf{v}_{K0}$ on it, and sends it to Bob, who then measures the Bell state of the transformed entangled pair.

We consider just one qubit and use it to transfer a number, K, between 0 and 3.

The technique uses the fact that a transformation between Bell states can be effected by acting on one qubit only. Thus the sender, Alice, and receiver, Bob, each take one qubit from a state which is in a well defined Bell state, $|B_J>$. Alice then performs a transformation $\mathbf{v}_{JK}$ on her qubit and transmits it to Bob. Bob then measures the Bell state of the pair of qubits (the qubit that was sent plus the qubit from the original entangled pair) and deduces the value of K between 0 and 3.

As an example we assume that the sender and receiver both receive a qubit from an entangled pair which is in the state $|B_0>$.

The entangled pair starts in the state

$$|B_0> \equiv \frac{1}{\sqrt{2}}\left(|\uparrow\uparrow> + i|\downarrow\downarrow>\right)$$

Now Alice performs one of the following unitary transformations on her qubit

$$\mathbf{v}_{00} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

(no operation)

$$\mathbf{v}_{10} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$$

(rotation by π about the z-axis)

$$\mathbf{v}_{20} = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}$$

(rotation by $-\pi$ about the x-axis)

$$\mathbf{v}_{30} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

(rotation by -π about the y-axis).

The entangled pair is now in the state

$$|\psi_K> = \frac{1}{\sqrt{2}}\left(|\uparrow\ (\mathbf{v}_{K0}\uparrow)> + i|\downarrow\ (\mathbf{v}_{K0}\downarrow)>\right)$$

for some value of K between 0 and 3.

Now use

$$\mathbf{v}_{00}|\uparrow>=|\uparrow>$$
$$\mathbf{v}_{00}|\downarrow>=|\downarrow>$$
$$\mathbf{v}_{10}|\uparrow>=i|\uparrow>$$
$$\mathbf{v}_{10}|\downarrow>=-i|\downarrow>$$
$$\mathbf{v}_{20}|\uparrow>=-i|\downarrow>$$
$$\mathbf{v}_{20}|\downarrow>=-i|\uparrow>$$
$$\mathbf{v}_{30}|\uparrow>=|\downarrow>$$
$$\mathbf{v}_{30}|\downarrow>=-|\uparrow>$$

to see that $|\psi_K>$ are once again Bell states, i.e.

$$|\psi_0>=\frac{1}{\sqrt{2}}\left(|\uparrow\uparrow>+i|\downarrow\downarrow>\right)\;=\;|B_0>$$

$$|\psi_1>=\frac{1}{\sqrt{2}}\left(i|\uparrow\uparrow>+i(-i)|\downarrow\downarrow>\right)\;=\;|B_1>$$

$$|\psi_2>=\frac{1}{\sqrt{2}}\left(-i|\uparrow\downarrow>+i(-i)|\downarrow\uparrow>\right)\;=\;|B_2>$$

$$|\psi_3>=\frac{1}{\sqrt{2}}\left(|\uparrow\downarrow>-i|\downarrow\uparrow>\right)\;=\;|B_3>\,.$$

After performing one of these unitary operations on her electron, Alice sends the transformed electron to Bob. Bob now measures the new Bell state of the entangled pair and deduces the value of K from the result of that measurement.

5. QUANTUM TELEPORTATION

If a qubit is in a pure eigenstate then one can measure the z-component of spin and communicate the result of the measurement to a recipient. However, if the qubit is in some superposition

$$|\psi>=\;\alpha|\uparrow>+\beta|\downarrow>,$$

then any measurement of S_z will collapse the state into one of the two pure eigenstates. Thus a superposition state cannot be measured without destroying information about the original state. This result goes by the name of the 'Quantum No Cloning Theorem'.

The theorem is proved as follows:

Suppose that U_c is a unitary cloning operator, such that for any arbitrary quantum state $|\alpha>$,

$$U_c\,|\alpha>|0>=\;|\alpha>|\alpha>\,.$$

Likewise for a different quantum state $|\beta>$ we would have

$$U_c\,|\beta>|0>=\;|\beta>|\beta>\,.$$

Now let $|\psi>$ be another quantum state which is a linear superposition of $|\alpha>$ and $|\beta>$,

$$|\psi>=\;a\,|\alpha>\;+b\,|\beta>\,.$$

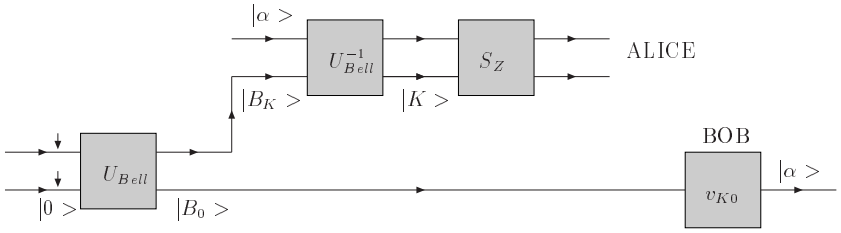


Fig. 3: Alice and Bob each take one qubit from an entangled pair in Bell state $|B_0>$. Alice then measures the Bell state of the entangled pair consisting of the qubit taken from the original Bell state pair and the unmeasured qubit she wishes to teleport to Bob, which is in the state $|\psi>$. She communicates the result of this measurement, K to Bob, who then performs the transformation $\mathbf{v}_{K0}$ on his qubit, thereby tranforming it into the state $|\psi>$

.

Operating on $|\psi>|0>$ with the cloning operator leads to

$$U_c\,|\psi>|0> = \; a\,|\alpha>|\alpha> \; + b\,|\beta>|\beta> .$$

This is *not* the state $|\psi>|\psi>$, which contradicts the postulate that the operator U_c clones *any* arbitrary quantum state.

Now, although, as we have seen, a quantum state (qubit) cannot be copied, we will now show that it can be transported from Alice to Bob, but only at the expense of destroying the original state. The method relies on the same properties of Bell states as the algorithm for dense coding. In the case of dense coding, Alice first performs a transformation on a single qubit of a two qubit Bell state, then sends the transformed qubit to Bob who finally measures the final Bell state of the resulting pair. For quantum teleportation, Alice and Bob again start with one qubit of an entangled Bell state pair. Alice measures the Bell state formed by her qubit and the unknown qubit and then tells Bob which transformation to make on his qubit to regenerate the original unmeasured qubit state.

It is necessary for both Alice and Bob each to take one of two qubits which have been prepared in some Bell state. Again we shall consider the state $|B_0>$ for convenience, although this can easily be generalized. Alice now has two qubits - the qubit in the state $|\psi>$ that she wishes to transport and the qubit obtained from the device that produced the entangled pair in Bell state $|B_0>$.

The three qubit state can therefore be written

$$|\phi> = |\psi> \otimes |B_0> = \; \frac{1}{\sqrt{2}}\,(\alpha|\uparrow\uparrow\uparrow> + i\alpha|\uparrow\downarrow\downarrow> + \beta|\downarrow\uparrow\uparrow> + i\beta|\downarrow\downarrow\downarrow>)$$

For convenience we shall write this as

$$|\phi> = \; \frac{1}{\sqrt{2}}\,(\alpha|\uparrow\uparrow> \otimes |\uparrow> + i\alpha|\uparrow\downarrow> \otimes |\downarrow> + \beta|\downarrow\uparrow> \otimes |\uparrow> + i\beta|\downarrow\downarrow> \otimes |\downarrow>)$$

where we have separated out the third qubit, which is the one taken from the Bell state $|B_0>$ by Bob. After Alice has measured the Bell state of her two qubits, Bob's qubit can be transformed into a 'copy' of the original qubit in the state $|\psi>$ by performing one of the four unitary transformations $\mathbf{v}_{K0},\ K = 0 \cdots 3$ used in the section above on dense coding. Which of the four unitary transformations needs to be used depends on the result of the Bell state measurement.

To see this, we expand the above expression for $|\phi>$ into a sum of Bell states for the first two qubits, using the expressions for the inversions of the Bell states given below the definition of the Bell states. After collecting terms this gives

$$|\phi> \quad = \quad \frac{1}{2}\left(|B_0>\otimes(\alpha|\uparrow>+\beta|\downarrow>)+|B_1>\otimes(-i\alpha|\uparrow>+i\beta|\downarrow>)\right.$$
$$\left.+|B_2>\otimes(-\alpha|\downarrow>+\beta|\uparrow>)+|B_3>\otimes(i\alpha|\downarrow>+i\beta|\uparrow>)\right)$$

Applying the inverses of the operators $\mathbf{v}_{K0},\ K=0\cdots 3$ to the state $|\psi>$, which we wish to teleport, we can see that this may be written

$$|\phi> \quad = \quad \frac{1}{2}\Big(|B_0>\otimes(\mathbf{v}_{00})^{-1}|\psi>+|B_1>\otimes(\mathbf{v}_{10})^{-1}|\psi>$$
$$+|B_2>\otimes(\mathbf{v}_{30})^{-1}|\psi>+|B_3>\otimes(\mathbf{v}_{20})^{-1}|\psi>\Big)$$

A measurement of the Bell state by Alice collapses the wavefunction into one of these components. In particular, it forces the qubit taken by Bob into the state $\mathbf{v}_{K0}^{-1}|\alpha>$ [1]. The result of the measurement tells Alice into which component the wavefunction has collapsed. She then communicates this information to Bob who performs the relevant unitary transformation on his qubit which is then transformed into the required state $|\psi>$.

Note that although the wavefunction collapses immediately upon the measurement of the Bell state by Alice - so that the Bob's qubit is also instantaneously collapsed, the information required to reproduce the initial state $|\psi>$ has to be communicated from the sender to the recipient at a velocity less than or equal to the velocity of light.

6. A 'GEDANKEN REALISATION: MAGNETIC RESONANCE

We start by showing how magnetic resonance can be used to effect the transformations $\mathbf{u}_x,\ \mathbf{u}_y,\ \mathbf{u}_z$ on a single qubit, which is taken to be the spin part of the wavefunction of a spin-$\frac{1}{2}$ particle.

We take the example of $\mathbf{u}_y$ and work (for convenience) in a system of units where $\hbar=1$.

First we imagine the spin-$\frac{1}{2}$ placed in a uniform magnetic field of magnitude B_0 in the $z-$ direction.

The part of the Hamiltonian that depends on the spin is then given by

$$H=\mu B_0\mathbf{S}_z,$$

where for a particle of charge e and mass m, and gyromagnetic ratio g (=2 for an electron), the magnetic moment (vector) is given by

$$\underline{\mu}=g\frac{e}{2m}\underline{S},$$

the operators for the components of $\underline{S}$ being represented by the 2×2 matrices

$$\mathbf{S}_x=\frac{1}{2}\begin{pmatrix}0&1\\1&0\end{pmatrix},\ \mathbf{S}_y=\frac{1}{2}\begin{pmatrix}0&-i\\i&0\end{pmatrix},\ \mathbf{S}_z=\frac{1}{2}\begin{pmatrix}1&0\\0&-1\end{pmatrix}$$

This leads to a ("Zeeman") energy splitting between the two pure states ($S_z=\pm\frac{1}{2}$) with energy difference $\omega_0=\mu B_0$.

Now we apply an oscillating magnetic field with angular frequency ω_0 and amplitude $B',(\ B'\ll B)$ in the *negative* y-direction, so that the (spin dependent part of the) Hamiltonian becomes

$$H=\mu B\mathbf{S}_z-\mu B'\cos(\omega_0 t)\mathbf{S}_y.$$

[1] This collapse of the state of Bob's qubit due to a measurement performed by Alice is an example of the Einstein-Podolsky-Rosen (EPR) paradox.

We write the time dependent spin-part of the wavefunction as

$$\begin{pmatrix} a(t)e^{-i\omega_0 t/2} \\ b(t)e^{i\omega_0 t/2} \end{pmatrix},$$

where we have displayed explicitly the time dependence of the two states in the absence of the applied oscillating magnetic field. Defining $\omega' = \frac{1}{2}\mu B'$ the Schroedinger equation is

$$i\frac{\partial}{\partial t}\begin{pmatrix} a(t)e^{-i\omega_0 t/2} \\ b(t)e^{i\omega_0 t/2} \end{pmatrix} = \omega_0 \mathbf{S}_z \begin{pmatrix} a(t)e^{-i\omega_0 t/2} \\ b(t)e^{i\omega_0 t/2} \end{pmatrix} - 2\omega' \cos(\omega_0 t)\mathbf{S}_y \begin{pmatrix} a(t)e^{-i\omega_0 t/2} \\ b(t)e^{i\omega_0 t/2} \end{pmatrix},$$

which upon writing $\cos(\omega_0 t) = \frac{1}{2}\left(e^{i\omega_0 t} + e^{-i\omega_0 t}\right)$ and a little algebra simplifies to

$$i\frac{\partial}{\partial t}\begin{pmatrix} a(t) \\ b(t) \end{pmatrix} = -\omega' \mathbf{S}_y \begin{pmatrix} a(t) \\ b(t) \end{pmatrix} - \omega' \mathbf{S}_y \begin{pmatrix} a(t)e^{-2i\omega_0 t} \\ b(t)e^{2i\omega_0 t} \end{pmatrix}.$$

Now we make the approximation that since we shall apply the oscillating field for a time which is large compared with $1/\omega_0$, the last term in the above equation oscillates very rapidly and averages out to a very small quantity over this time interval and may therefore be neglected. We thus end up with

$$i\frac{\partial}{\partial t}\begin{pmatrix} a(t) \\ b(t) \end{pmatrix} = -\omega' \mathbf{S}_y \begin{pmatrix} a(t) \\ b(t) \end{pmatrix}.$$

This is a pair of first order differential equations whose solution is

$$\begin{pmatrix} a(t) \\ b(t) \end{pmatrix} = \begin{pmatrix} \cos\left(\frac{1}{2}\omega' t\right) & \sin\left(\frac{1}{2}\omega' t\right) \\ -\sin\left(\frac{1}{2}\omega' t\right) & \cos\left(\frac{1}{2}\omega' t\right) \end{pmatrix} \begin{pmatrix} a_0 \\ b_0 \end{pmatrix},$$

where $a_0,\ b_0$ are the initial values of $a(t)$ and $b(t)$. Thus we see that if we set $\theta = \omega' t\ (= \frac{1}{2}\mu B' t)$ then this pulse of oscillating magnetic field in the (negative) $y-$ direction effects the transformation represented by the matrix $\mathbf{u}_y(\theta)$. The transformations $\mathbf{u}_x(\theta)$ and $\mathbf{u}_z(\theta)$ are similarly effected by applying the oscillating magnetic fields in the negative $x-$ and $z-$ directions respectively.

In most cases the spin-$\frac{1}{2}$ particle is a nucleus and this method is known as "Nuclear Magnetic Resonance" (NMR).

When there is more than one spin-$\frac{1}{2}$ particle present, they will interact with each other through the magnetic moments associated with their spins. Now, in addition to the energy shifts produced by the applied uniform magnetic field in the $z-$direction, there is a shift which depends in general on the mutual orientation of the various spins in the system, e.g for a two qubit system there will be a contribution to the energy whose sign depends on whether the spins are of the same sign or of opposite sign. It is this contribution to the energy which is used to construct devices which effect transformations on system consisting of more than one qubit and which are not single outer products of transformations on each bit (such as a controlled NOT gate).

Now consider NMR devices which operate on a two qubit system.

Notation:

$\phi_w^{(l)}$ means a pulse which rotates the spin state of qubit l through an angle ϕ about the w-axis. The inverse of this operation is written $\phi_{-w}^{(l)}$. Thus $\phi_w^{(l)}$ is a pulse which performs the transformation $\mathbf{u}_w(\phi)$ on qubit l. Note that in usual NMR notation the angle ϕ is usually quoted in *degrees*.

If $w = z$ then these operators effect a phase change through angle $\phi/2$ with sign depending on the spin of the qubit.

A further operator which effects a phase change is written $\phi^{(12)}$. This is just a time delay in which the state of the two qubits evolves under the influence of the coupling of the mutual spins, which may be written $\lambda S_z^{(1)} S_z^{(2)}$. The time delay occurs for a period $2\phi/\lambda$ such that the phase change of the state is $+\phi/2$ if both the spins have the same z-component and $-\phi/2$ if the two spins have opposite z-component.

In terms of 4×4 matrices for a 2 qubit (bit 1 is the most significant bit and bit 2 is the least significant bit) system these pulses may be represented as

$$\phi_y^{(2)} = \begin{pmatrix} \cos\left(\frac{\phi}{2}\right) & \sin\left(\frac{\phi}{2}\right) & 0 & 0 \\ -\sin\left(\frac{\phi}{2}\right) & \cos\left(\frac{\phi}{2}\right) & 0 & 0 \\ 0 & 0 & \cos\left(\frac{\phi}{2}\right) & \sin\left(\frac{\phi}{2}\right) \\ 0 & 0 & -\sin\left(\frac{\phi}{2}\right) & \cos\left(\frac{\phi}{2}\right) \end{pmatrix}$$

$$\phi_y^{(1)} = \begin{pmatrix} \cos\left(\frac{\phi}{2}\right) & 0 & \sin\left(\frac{\phi}{2}\right) & 0 \\ 0 & \cos\left(\frac{\phi}{2}\right) & 0 & \sin\left(\frac{\phi}{2}\right) \\ -\sin\left(\frac{\phi}{2}\right) & 0 & \cos\left(\frac{\phi}{2}\right) & 0 \\ 0 & -\sin\left(\frac{\phi}{2}\right) & 0 & \cos\left(\frac{\phi}{2}\right) \end{pmatrix}$$

$$\phi_x^{(2)} = \begin{pmatrix} \cos\left(\frac{\phi}{2}\right) & i\sin\left(\frac{\phi}{2}\right) & 0 & 0 \\ i\sin\left(\frac{\phi}{2}\right) & \cos\left(\frac{\phi}{2}\right) & 0 & 0 \\ 0 & 0 & \cos\left(\frac{\phi}{2}\right) & i\sin\left(\frac{\phi}{2}\right) \\ 0 & 0 & i\sin\left(\frac{\phi}{2}\right) & \cos\left(\frac{\phi}{2}\right) \end{pmatrix}$$

$$\phi_x^{(1)} = \begin{pmatrix} \cos\left(\frac{\phi}{2}\right) & 0 & i\sin\left(\frac{\phi}{2}\right) & 0 \\ 0 & \cos\left(\frac{\phi}{2}\right) & 0 & i\sin\left(\frac{\phi}{2}\right) \\ i\sin\left(\frac{\phi}{2}\right) & 0 & \cos\left(\frac{\phi}{2}\right) & 0 \\ 0 & i\sin\left(\frac{\phi}{2}\right) & 0 & \cos\left(\frac{\phi}{2}\right) \end{pmatrix}$$

$$\phi_z^{(2)} = \begin{pmatrix} e^{i\phi/2} & & & \\ & e^{-i\phi/2} & & \\ & & e^{i\phi/2} & \\ & & & e^{-i\phi/2} \end{pmatrix}$$

$$\phi_z^{(1)} = \begin{pmatrix} e^{i\phi/2} & & & \\ & e^{i\phi/2} & & \\ & & e^{-i\phi/2} & \\ & & & e^{-i\phi/2} \end{pmatrix}$$

and

$$\phi^{(12)} = \begin{pmatrix} e^{i\phi/2} & & & \\ & e^{-i\phi/2} & & \\ & & e^{-i\phi/2} & \\ & & & e^{i\phi/2} \end{pmatrix}$$

Thus for example a series of pulses which flips the sign of the state $|3>$ but leaves the others unchanged is given (up to an irrelevant overall phase) by

$$90_z^{(2)}\, 90_z^{(1)}\, 90^{(12)} \;=\; e^{-i\pi/4} \begin{pmatrix} e^{i\pi} & & & \\ & 1 & & \\ & & 1 & \\ & & & 1 \end{pmatrix}$$

A controlled NOT gate, which flips the spin of the least significant qubit if and only if the most significant qubit is set

$$|j> \otimes |k> \rightarrow |j> \otimes |j \oplus k>$$

$$|0> \rightarrow |0>, \quad |1> \rightarrow |1>, \quad |2> \rightarrow |3>, \quad |3> \rightarrow |2>$$

This has a 4×4 matrix representation

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Up to an overall phase, this may be reproduced by the series of pulses (sequence obtained by reading from right to left)

$$C_{NOT} \;=\; 90_{-y}^{(2)}\, 90_z^{(2)}\, 90_{-z}^{(1)}\, 90^{(12)}\, 90_y^{(2)}$$

To see this we first consider the three middle terms

$$\begin{aligned} 90_z^{(2)}\, 90_{-z}^{(1)}\, 90^{(12)} \quad &= \quad \begin{pmatrix} e^{i\left(-\frac{\pi}{4}+\frac{\pi}{4}+\frac{\pi}{4}\right)} & & & \\ & e^{i\left(-\frac{\pi}{4}-\frac{\pi}{4}-\frac{\pi}{4}\right)} & & \\ & & e^{i\left(+\frac{\pi}{4}+\frac{\pi}{4}-\frac{\pi}{4}\right)} & \\ & & & e^{i\left(+\frac{\pi}{4}-\frac{\pi}{4}+\frac{\pi}{4}\right)} \end{pmatrix} \\ &= \quad e^{i\left(\frac{\pi}{4}\right)} \begin{pmatrix} 1 & & & \\ & -1 & & \\ & & 1 & \\ & & & 1 \end{pmatrix} \end{aligned}$$

and

$$\begin{aligned} 90_{-y}^{(2)} \begin{pmatrix} 1 & & & \\ & -1 & & \\ & & 1 & \\ & & & 1 \end{pmatrix} 90_y^{(2)} \quad &= \quad \frac{1}{2} \begin{pmatrix} 1 & -1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & & & \\ & -1 & & \\ & & 1 & \\ & & & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & -1 & 1 \end{pmatrix} \\ &= \quad \frac{1}{2} \begin{pmatrix} 1 & -1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & -1 & 1 \end{pmatrix} \\ &= \quad \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \end{aligned}$$

Thus we see that $C_{NOT} = 90^{(2)}_{-y}\, 90^{(2)}_{z}\, 90^{(1)}_{-z}\, 90^{(12)}\, 90^{(2)}_{y}$ reproduces the required controlled NOT gate up to an overall phase.

Likewise $C'_{NOT} = 90^{(1)}_{-y}\, 90^{(2)}_{-z}\, 90^{(1)}_{z}\, 90^{(12)}\, 90^{(1)}_{y}$ reproduces the other type of controlled NOT in which the most significant bit is flipped if and only if the least significant bit is "set".

Therefore the following combination of pulses will interchange the two qubits

$$U_{switch} = 90^{(2)}_{-y}\, 90^{(2)}_{z}\, 90^{(1)}_{-z}\, 90^{(12)}\, 90^{(2)}_{y} 90^{(1)}_{-y}\, 90^{(2)}_{-z}\, 90^{(1)}_{z}\, 90^{(12)}\, 90^{(1)}_{y} 90^{(2)}_{-y}\, 90^{(2)}_{z}\, 90^{(1)}_{-z}\, 90^{(12)}\, 90^{(2)}_{y}$$

Consider the following combination of pulses

$$U_{Bell} \;\equiv\; C'_{NOT} 90^{(1)}_{z} 90^{(2)}_{z} 90^{(12)} 90^{(2)}_{-x} 90^{(2)}_{z} 90^{(1)}_{-z} 90^{(12)}$$

This has a matrix representation

$$\begin{aligned}
\mathbf{U}_{Bell} &= \frac{1}{\sqrt{2}} \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} -1 & & & \\ & 1 & & \\ & & 1 & \\ & & & 1 \end{pmatrix} \begin{pmatrix} 1 & -i & 0 & 0 \\ -i & 1 & 0 & 0 \\ 0 & 0 & 1 & -i \\ 0 & 0 & -i & 1 \end{pmatrix} \begin{pmatrix} 1 & & & \\ & -1 & & \\ & & 1 & \\ & & & 1 \end{pmatrix}, \\
&= \frac{-i}{\sqrt{2}} \begin{pmatrix} 0 & 0 & i & 1 \\ 1 & -i & 0 & 0 \\ -i & 1 & 0 & 0 \\ 0 & 0 & 1 & i \end{pmatrix}
\end{aligned}$$

which is the matrix (up to an overall phase) that converts pure states into Bell entangled states.

A two qubit Hadamard gate (a device that performs a two qubit Hadamard transformation) can be constructed (up to an overall phase) as

$$H \;=\; 90^{(1)}_{y} 90^{(2)}_{y} 180^{(12)}.$$

In terms of the matrix representation

$$\mathbf{H} \;=\; \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ -1 & 1 & -1 & 1 \\ -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \begin{pmatrix} i & & & \\ & -i & & \\ & & -i & \\ & & & i \end{pmatrix} = \frac{i}{2} \begin{pmatrix} 1 & -1 & -1 & 1 \\ -1 & -1 & 1 & 1 \\ -1 & 1 & -1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}$$

7. QUANTUM LOGIC GATES USING MAGNETIC RESONANCE

We consider a two qubit system. A Controlled NOT gate (exclusive or - XOR) is a device into which one sends a pair of qubits in the state

$$|j> \otimes |k>, \quad (j,k = 0,1)$$

and the output state is

$$|j> \otimes |k \oplus j>$$

In general the input states could be superpositions

$$|\psi> = \sum_{j=0}^{1} a_j |j>$$

$$|\phi>=\sum_{k=0}^{1} b_k|k>$$

In this case the device performs the operation

$$|\psi>\otimes|\phi>\rightarrow \sum_{j,k=0}^{1} a_j b_k|j>\otimes|j\oplus k>$$

Such a device could consist of a proton (or other nucleus) trapped at some site in a semiconductor (a "quantum dot") in spin state j with magnetic moment $g_I\mu_N$, and an electron in spin state k trapped at some other site in the semiconductor (or a nucleus with a very much larger magnetic moment). The magnetic moment of the electron is $2\mu_B$, which is much larger than that of the proton by a factor of the ratio of the proton to electron mass. A constant magnetic field B_0 is applied in the z-direction. The proton is the first qubit and the electron is the second qubit There is a mutual interaction between the two magnetic moments, which depends on the distance between the two qubits and the relative orientation of their spins.

The Hamiltonian for the system has a part which is proportional to the applied magnetic field, which we may write as

$$H_{mag} \;=\; B_0\left(g_I\mu_N(j-1/2)+2\mu_B(k-1/2)+(-1)^{(j+k)}\,\lambda\right)$$

Where λ encodes the mutual interaction and is multiplied by a sign which is positive if the spins are aligned and negative otherwise. The energy levels between the two allowed states for the electron differ by

$$B_0\left(2\mu_B+2\lambda\right) \;\equiv\; \omega_0+\Delta\omega,$$

if $j=1$, and

$$B_0\left(2\mu_B-2\lambda\right)) \;\equiv \omega_0-\Delta\omega,$$

if $j=0$.

By applying an oscillating magnetic field in the $y-$direction with frequency $\omega_0+\Delta\omega$ and amplitude B' one can induce oscillations in the spin state of the electron *provided the proton is in the state* $j=1$. If the proton is *not* in this state then the probability for inducing transitions is negligibly small. Likewise the probability for inducing transitions in the proton is negligibly small. If this oscillating magnetic field is applied for a time

$$t=\frac{\pi}{\mu_B B'},$$

then the electron will (almost) always flip its spin state.

Thus we have constructed a device which performs the following operations

$$|0>\otimes|0>\rightarrow |0>\otimes|0>$$
$$|0>\otimes|1>\rightarrow |0>\otimes|1>$$
$$|1>\otimes|0>\rightarrow |1>\otimes|1>$$
$$|1>\otimes|1>\rightarrow |1>\otimes|0>$$

We see that the second output qubit contains the exclusive XOR of the two input qubits. Note that this is just a Controlled NOT gate, (C_{NOT}).

Very simply we can construct a NOR gate which performs

$$|j>\otimes|k>\rightarrow\; |j>\otimes|*j\oplus k>,$$

simply by changing the frequency of the oscillating magnetic field to $\omega_0-\Delta\omega$

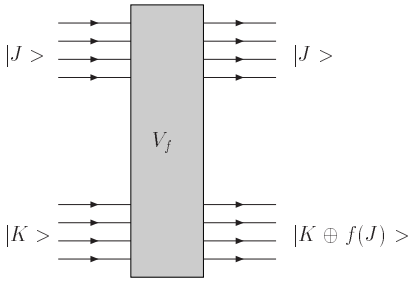


Fig. 4: V_f is a function device which performs the transformation $|J> \otimes |K> \rightarrow |J> \otimes |K \oplus f(J)>$.

8. FUNCTIONS

The device described above can easily be used to produce quantum states that encode functions. In the case of a function $f(j)$ which maps a single qubit onto a single qubit ($j = 0, 1,\ f(j) = 0, 1$) then the applied magnetic field in this device should be set to

$$B' \sum_{j=0}^{1} f(j) e^{i\omega(j)t} \theta(\pi - B'\mu_B t)$$

where

$$\omega_j = \omega_0 - (-1)^j \Delta\omega.$$

This then performs the operation

$$|j> \otimes |k> \rightarrow\ |j> \otimes |k \oplus f(j)> .$$

If k is taken to be 0, then the second bit just contains $f(j)$ at output.

This device is easily extended to a function which maps an integer between 0 and $2^L - 1$ onto a single bit. The first qubit is replaced by an L qubit register known as the "control register". This consists of L protons trapped at different sites on the semiconductor. Now each proton will have a different mutual interaction term with the electron because the distance between the magnetic dipoles is different for each of the protons. The magnetic part of the Hamiltonian now becomes

$$H_{mag} \ = \ B_0 \left(\sum_{l=1}^{L} g_I \mu_N (j_l - 1/2) + 2\mu_B (k - 1/2) + \sum_{l=1}^{L} (-1)^{(j_l + k)} \lambda_l \right)$$

and the energy difference between the two electron states is

$$\omega(J) \ = \ B_0 \left(2\mu_B - \sum_{l=1}^{L} 2\,(-1)^{j_l} \lambda_l \right) \ \equiv \ \omega_0 + \sum_{l=1}^{L} \Delta\omega_J,$$

The input register (the protons) is in the state $|J>$ where

$$J = \sum_{l=1}^{L} j_j 2^{l-1}.$$

Now by applying an oscillating magnetic field

$$B' \sum_{J=0}^{2^L - 1} f(J) e^{i\omega(J)t} \theta(\pi - B'\mu_B t)$$

the device will perform the transformation

$$|J> \otimes |k> \rightarrow\ |J> \otimes |k \oplus f(J)> .$$

Again if we set $k = 0$ initially then the device will return $f(J)$ in the electron qubit ("target qubit").

Generalizing this to a function which maps an integer between 0 and $2^L - 1$ to an integer in the range 0 to $2^{L'} - 1$ presents severe practical difficulties. Now as well as L protons at different sites in the semiconductor we need L' electrons at different sites and we need to be able to access each of these with a different frequency oscillating field.

Writing a function $f(J)$ as

$$f(J) \equiv \sum_{l'=1}^{L'} f_{l'}(J) 2^{l'-1},$$

the oscillating magnetic field applied to the l' electron must be

$$B' \sum_{J=0}^{2^L-1} f_{l'}(J) e^{i\omega(J)t} \theta(\pi - B'\mu_B t).$$

If the "target register" (the L' electrons) are initially in the state K then this device performs the operation

$$|J> \otimes |K> \rightarrow |J> \otimes |K \oplus f(J)> .$$

Setting $K = 0$ thus generates $f(J)$ in the target register.

Note that this is an example of a "reversible gate", i.e. if we pass the output through the apparatus we recover the input.

$$|J> \otimes |K \oplus f(J)> \rightarrow |J> \otimes |K> .$$

This quantum device can produce a quantum state which is a superposition of functions of several inputs. In particular, if we set all the L qubits (protons) of the "control" register to be eigenstates of S_x with eigenvalue $+\frac{1}{2}$, i.e. each in the state

$$\frac{1}{\sqrt{2}} \left(|\uparrow> + |\downarrow> \right),$$

then the register is in the superposition [2]

$$\frac{1}{\sqrt{2^L}} \left(|0> + |1> + |2> + \cdots \right) = \sum_{J=0}^{2^L-1} |J> .$$

If the target (electrons) register was initially in the state 0 (i.e. all electrons in the state $|\downarrow>$) then upon exit the target register is would the state

$$\sum_{J=0}^{2^L-1} |f(J)> .$$

We thus have a state which contains all of the possible values of $f(J)$ simultaneously. However, once a measurement is made on the spin in the z-direction of spins of all the electrons the state collapses into one of the allowed values of J for the protons and the corresponding $f(J)$ for the electrons. There is equal probability for obtaining each value of the pair $(J, f(J))$.

An "oracle" is a device which reverses the sign of a wavefunction of the register is in some particular (marked) state $|J_0>$. This can be achieved by constructing a function device in which the target

[2] This is equivalent to the state obtained by operating on the state $|0>$ with a Hadamard transformation.

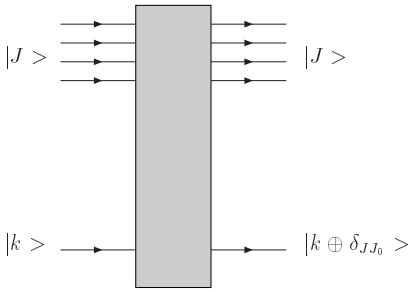


Fig. 5: The oracle operating on a control register and a single qubit target register performs the transformation $|J> \otimes |k> \rightarrow |J> \otimes |k \oplus \delta_{JJ_0}>$.

register is a single qubit ($L' = 1$) which is flipped if and only if the control register is in the state $|J_0>$, i.e.

$$|J> \otimes |k> \rightarrow \ |J> \otimes |k \oplus \delta_{JJ_0}> .$$

If $|k>$ is initially in the state

$$|k>= \frac{1}{\sqrt{2}} \left(|0> - |1> \right),$$

then

$$|k \oplus \delta_{JJ_0}> = \ (-1)^{\delta_{JJ_0}} \frac{1}{\sqrt{2}} \left(|0> - |1> \right),$$

so that the device flips the sign of the wavefunction (for the entire system) if and only if the control register is in the state $|J_0>$.

9. DISCRETE FOURIER TRANSFORMS

We consider the example of taking the Fourier transform of a 2 qubit quantum system, which is in the state

$$|\psi>= \sum_{J=0}^{3} a_J |J> .$$

The Fourier transform state is

$$|\phi>= \sum_{K=0}^{3} b_K |K>,$$

where

$$b_K = \sum_{J=0}^{3} e^{i\pi JK/2} a_J.$$

For this we need the following quantum devices which can perform unitary operators.

a. The first is a unary operator which acts on one qubit only

$$\mathbf{u}_y \left(\frac{\pi}{2} \right) \ = \ \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix},$$

which corresponds to a rotation through $\pi/2$ about the y-axis.

$$\mathbf{u}_y \left(\frac{\pi}{2} \right) | \uparrow> = \frac{1}{\sqrt{2}} \left(| \uparrow> - | \downarrow> \right)$$

$$\mathbf{u}_y \left(\frac{\pi}{2} \right) | \downarrow> = \frac{1}{\sqrt{2}} \left(| \downarrow> + | \uparrow> \right)$$

This can act on *either* of the two qubits so we will write these as $\mathbf{U}^A_{(1)}$ and $\mathbf{U}^A_{(2)}$. Thus acting on the two qubit system represented by the bases vectors $|0>$ to $|3>$, these operators may be written as the 4×4 matrices

$$\mathbf{U}^A_{(1)} \;=\; \mathbf{u}_y\left(\frac{\pi}{2}\right) \otimes \mathbf{I} \;=\; \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ -1 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 \end{pmatrix}$$

$$\mathbf{U}^A_{(2)} \;=\; \mathbf{I} \otimes \mathbf{u}_y\left(\frac{\pi}{2}\right) \;= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & -1 & 1 \end{pmatrix}$$

b. A binary operator, $\mathbf{U}^B(\phi)$, which acts on a two qubit system, leaving all states alone except that the state $|1> \equiv \;|\downarrow\uparrow>$ is multiplied by a phase $e^{i\phi}$.
In 4×4 matrix notation, therefore

$$\mathbf{U}^B(\phi) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & e^{i\phi} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

c. The binary operator, $\mathbf{U}_{NOT}$ which flips both qubits

$$\mathbf{U}_{NOT} \;=\; \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

d. The binary operator that interchanges the two qubits

$$\mathbf{U}_{switch} \;=\; \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Now the operation of the Fourier transform consists of the sequential application of the following operations:

a. Applicaton of the operator $\mathbf{U}_{NOT}$
b. Application of operator $\mathbf{u}_y(\pi/2)$ on qubit (1), $(\mathbf{U}^A_{(1)})$
c. Application of $\mathbf{U}^B(\pi/2)$
d. Application of operator $\mathbf{u}_y(\pi/2)$ on qubit (2), $(\mathbf{U}^A_{(2)})$
e. Application of the operator $\mathbf{U}_{switch}$.
In other words

$$\begin{aligned} \mathbf{F}_T \;\; &\equiv \;\; \mathbf{U}_{switch}\mathbf{U}^A_{(2)}U^B(\pi/2)\mathbf{U}^A_{(1)}\mathbf{U}_{NOT} \\ &= \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & -1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & i & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ -1 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \\ &= \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix} \end{aligned}$$

Thus we see that

$$\mathbf{F}_T|J> = \frac{1}{2}\sum_{K=0}^{3} e^{i(JK\pi/2)}|K>,$$

as required.

This can be generalized to an L-bit system, using appropriate combinations of $\mathbf{U}^A_{(j)}$ and $\mathbf{U}^B_{jk}(\pi/2^n)$, $(i,j,k,n = 0\cdots(2^L-1))$.

10. FACTORIZATION

Factorization algorithm:
To factorize the number N, we can use an algorithm known as "Shor's algorithm".

Let a be coprime with N (no common factors).

The function defined by

$$f_{a,N}(J) \equiv (a^J, \text{ MOD } N)$$

has a period, P.

Provided P is even and $(a^{P/2}, \text{ MOD } N) \neq N-1$, then the greatest common divisors of the pairs

$$(a^{P/2}+1,\ N) \text{ and } (a^{P/2}-1,\ N)$$

are factors of N.

Example:

$$N = 21,\ \ a = 2$$

$$(2, \text{ MOD } 21),\ (2^2, \text{ MOD } 21)\ (2^3, \text{ MOD } 21)\ (2^4, \text{ MOD } 21)\ (2^5, \text{ MOD } 21)$$

$$(2^6, \text{ MOD } 21)\ (2^7, \text{ MOD } 21)\ (2^8, \text{ MOD } 21)\ (2^9, \text{ MOD } 21)\ \cdots$$

$$= 2,\ 4,\ 8,\ 16,\ 11,\ 1,\ 2,\ 4,\ 8,\ \cdots$$

The period of the function $P = 6$, so that $2^{6/2} = 8$.

The greatest common divisor of 9 and 21 is 3.
The greatest common divisor of 7 and 21 is 7.
Thus the factors of 21 are 7 and 3.

Now finding the greatest common divisor of two numbers can be achieved by a very fast algorithm (due to Euclid). The difficulty is finding the period, P, of the function $f_{a,N}(J)$. By classical computers this is the same level of complexity as any other factorization algorithm.

However by quantum encoding the function $f_{a,N}(J)$ the period can be found relatively rapidly.

First we construct a device that performs the operation

$$|J>\otimes|K> \rightarrow |J>\otimes|K \oplus f_{a,N}(J)>,$$

using the magnetic resonance method described above. Then (by polarizing the spins of all the qubits in the control register in the $x-$direction, with eigenvalue $+\frac{1}{2}$), we consider the input

$$\sum_{J=0}^{2^L-1} \frac{1}{\sqrt{2^L}}|J>\otimes|0>$$

and obtain upon output

$$\sum_{J=0}^{2^L-1} \frac{1}{\sqrt{2^L}} |J> \otimes |f_{a,N}(J)> .$$

Next we make a measurement of the spin state (in the $z-$direction of the target register . This returns $f_{a,N}^q,\ q = 0, \cdots (P-1)$, which is one of the P allowed values of the function $f_{a,N}(J)$.

This immediately collapses the control register into a superposition (unnormalized)

$$\sum_r |rP + q>,$$

where r runs from zero to the integer below $2^L/P$. The problem is that q can take any non-negative integer value up to $P-1$. However if we take the Fourier transform of this state this effect is 'washed away'. In more detail the Fourier transform of the above function (again unnormalized) is

$$\sum_{K=0}^{2^L-1} \sum_r e^{i(K(rP+q)\pi/2^L)} |K> .$$

If P is an integer divisor of 2^L then the factor

$$\sum_{r=0}^{2^L/P} e^{i(KrP\pi/2^L)}$$

vanishes unless K is an integer multiple of $2^L/P$. This means that any subsequent measurement of the z-component of the spin of the control register will yield a result which is an integer multiple of $2^L/P$. Thus after a few such measurements the value of P can be determined with high confidence.

In the more realistic case where P is *not* an integer divisor of 2^L the result of the Fourier transform is a superposition which is very highly peaked around integer multiples of $2^L/P$. Thus several measurements of the spin state of the Fourier transformed control register have to be taken. However once again the value of P can be deduced with a high level of confidence after a number of measurements which is far fewer than the number of operations required to factorize a number using classical computers.

If P turns out to be one of the forbidden values, the the process must be repeated using a different value of a (a separate function device). However the probability of P being allowed is greater than 50%.

11. GROVER'S ALGORITHM

The objective is to force a register which is a superposition of all allowed states (with equal coefficient) into a particular "marked state". The state is marked by passing the system through an "oracle", which reverses the sign of the wavefunction if and only if the register is in the marked state. With a classical computer one must systematically compare all the states with the marked state, a process which grows as the maximum allowed marked number (i.e. as 2^L for an L bit register), whereas using Grover's algorithm this process only grows as the square root of the maximum allowed number (i.e. as $2^{L/2}$ for an L bit register).

First an example using two qubits:

Initially the qubits are in the state $|0>$. We apply a (pseudo-) Hadamard transformation, **H**, which performs the operation

$$|0> \rightarrow \ \mathbf{H}|0> = \ \frac{1}{2}\left(|0> + |1> + |2> + |3>\right)$$

$\mathbf{U}_J$ is a matrix which flips the sign of the state $|J>$, but leaves all other states alone, i.e.

$$\mathbf{U}_J|\Psi> = |\Psi> -2<J|\Psi>|J> .$$

The device which performs such an operation is the oracle.

Now consider the sequence of operators $\mathbf{H}\,U_0H^{-1}\mathbf{U}_JH$ acting on $|0>$

$$\begin{aligned}\mathbf{H}\,U_0H^{-1}\mathbf{U}_JH|0> &= \sum_{K=0}^{3}\frac{1}{2}\mathbf{H}\,U_0H^{-1}\mathbf{U}_J|K> \\ &= \sum_{K=0}^{3}\frac{1}{2}\mathbf{H}\,U_0H^{-1}|K> -\mathbf{H}\,U_0H^{-1}|0> \\ = \sum_{K=0}^{3}\frac{1}{2}\mathbf{H}\,H^{-1}|K> - \sum_{K=0}^{3}&<0|\mathbf{H}^{-1}|K>\mathbf{H}|0> -\mathbf{H}\,H^{-1}|J> +2<0|\mathbf{H}^{-1}|J>\mathbf{H}|0>\end{aligned}$$

Now

$$\sum_{K=0}^{3}\frac{1}{2}\mathbf{H}\,H^{-1}|K> = \mathbf{H}|0>$$

and

$$<0|\mathbf{H}^{-1}|K> = \frac{1}{2} \text{ for all K}$$

This leaves

$$\mathbf{H}\,U_0H^{-1}\mathbf{U}_JH|0> = -|J> .$$

This device forces the state $|0>$ into the state $|J>$ (up to a sign) after a single pass.

This has been achieved experimentally by Jones using a solution of the base cytosine in D_2O. This results in a molecule with two unpaired protons forming a two spin system. Selective NMR pulses can be applied to each proton.

Now consider L bits.
Again a Hadamard transformation is applied to the state $|0>$,

$$\mathbf{H}|0> = \frac{1}{\sqrt{2^L}}\sum_{K=0}^{2^L-1}|K> .$$

The oracle flips the sign of the state $|J>$, but leaves all other states unchanged

$$\mathbf{U}_J|\Psi> = |\Psi> -2<J|\Psi>|J>$$

$$<0|\mathbf{H}^{-1}|K> = \frac{1}{\sqrt{2^L}}, \text{ for all } K$$

Let $|\Psi> \equiv \mathbf{H}|0>$.

Now consider the operator $\mathbf{H}\,U_0H^{-1}\mathbf{U}_J$ acting on the state $|\Psi>$

$$\begin{aligned}\mathbf{H}\,U_0H^{-1}\mathbf{U}_J|\Psi> &= \sum_{K=0}^{2^L-1}\frac{1}{\sqrt{2^L}}\mathbf{H}\,U_0H^{-1}|K> -\frac{2}{\sqrt{2^L}}\mathbf{H}\,U_0H^{-1}|J> \\ = \sum_{K=0}^{2^L-1}\frac{1}{\sqrt{2^L}}|K> -2\sum_{K=0}^{2^L-1}&\frac{1}{\sqrt{2^L}}<0|\mathbf{H}^{-1}|K>\mathbf{H}|0> -\frac{2}{\sqrt{2^L}}\mathbf{H}\,U_0H^{-1}|J> +\frac{4}{\sqrt{2^L}}<0|\mathbf{H}^{-1}|J>\mathbf{H}|0> \\ &= \mathbf{H}|0> -\frac{2}{2^L}2^L\mathbf{H}|0> +\frac{4}{2^L}\mathbf{H}|0> -\frac{2}{\sqrt{2^L}}|J> \\ &= -\left(1-\frac{4}{2^L}\right)|\Psi> -\frac{2}{\sqrt{2^L}}|J>\end{aligned}$$

Now consider the operator $\mathbf{H}\,U_0 H^{-1}\mathbf{U}_J$ acting on the state $|J>$

$$\begin{aligned}\mathbf{H}\,U_0 H^{-1}\mathbf{U}_J|J> &= -\mathbf{H}\,\mathbf{U}_0 H^{-1}\mathbf{U}_J|J> \\ &= -|J> +2<0|\mathbf{H}^{-1}|J>\mathbf{H}|0> \\ &= -|J> +\frac{2}{\sqrt{2^L}}|\Psi>\end{aligned}$$

Consider the space of the two (non-orthogonal) states $|\Psi>$ and $|J>$. In this subspace the operator $\mathbf{H}\,U_0 H^{-1}\mathbf{U}_J$ has the matrix representation

$$-\begin{pmatrix} \left(1-\frac{4}{2^L}\right) & \frac{2}{\sqrt{2^L}} \\ -\frac{2}{\sqrt{2^L}} & 1 \end{pmatrix}$$

For large L we may approximate this by

$$-\begin{pmatrix} \cos(\alpha/2) & \sin(\alpha/2) \\ -\sin(\alpha/2) & \cos(\alpha/2) \end{pmatrix}$$

where

$$\alpha = \frac{4}{\sqrt{2^L}}.$$

If we perform this operation N times where N is the nearest integer to

$$\pi\frac{\sqrt{2^L}}{4}$$

then we get (approximately) the matrix

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

In other words the state is converted from pure $|\Psi>$ which we obtain by passing $|0>$ through a Hadamard gate, to the required state $|J>$ in less than $\sqrt{2^L}$ passes.

$$\left(\mathbf{H}U_0 H^{-1}\mathbf{U}_J\right)^N \mathbf{H}|0> \approx |J> .$$

The error in this approximation is of order $1/\sqrt{2^L}$.

It may be more convenient to use orthogonal states. We therefore define the state $|\Phi>$ which is orthogonal to $|J>$ by

$$|\Phi> = \sqrt{\frac{2^L}{2^L-1}}\left(|\Psi> -\frac{1}{\sqrt{2^L}}|J>\right) \;=\; \frac{1}{\sqrt{2^L-1}}\sum_{K\neq J}|K>$$

so that

$$|\Psi> = \sqrt{\frac{2^L-1}{2^L}}|\Phi> +\frac{1}{\sqrt{2^L}}|J> = \cos\beta|\Phi> +\sin\beta|J>,$$

where $\sin\beta = 1/\sqrt{2^L}$, i.e.

$$<0|\mathbf{H}|\Phi> = \cos\beta$$

$$<0|\mathbf{H}|J> = \sin\beta$$

The operator $\mathbf{U}_0$ may be expressed as

$$\mathbf{U}_0 \;=\; \mathbf{I} - 2|0><0|,$$

where $\mathbf{I}$ is the identity operator, so that

$$\mathbf{H}\,U_0 H^{-1} \;=\; \mathbf{I} - 2\mathbf{H}|0><0|\mathbf{H}^{-1}$$

Now the operator $\mathbf{O} \;\equiv \mathbf{H}\,U_0 H^{-1}\mathbf{U}_J$ acts on the orthogonal $|\Phi>,\ |J>$ subspace as follows.

$$\begin{aligned}
\mathbf{O}|J> &= -\mathbf{H}\,U_0 H^{-1}|J> = \;-|J> + 2\mathbf{H}|0><0|\mathbf{H}^{-1}|J> \\
&= -|J> + 2\sin\beta\,\cos\beta|\Phi> + 2\sin^2\beta|J> \\
&= -\left(\cos(2\beta)|J> - \sin(2\beta)|\Phi>\right)
\end{aligned}$$

$$\begin{aligned}
\mathbf{O}|\Phi> &= \mathbf{H}\,U_0 H^{-1}|\Phi> = \;|\Phi> - 2\mathbf{H}|0><0|\mathbf{H}^{-1}|\Phi> \\
&= |\Phi> - 2\cos^2\beta|\Phi> - 2\sin\beta\,\cos\beta|J> \\
&= -\left(\cos(2\beta)|\Phi> + \sin(2\beta)|J>\right)
\end{aligned}$$

Thus in this subspace the operator $\mathbf{O}$ has the (unitary) representation

$$\mathbf{O} \;=\; -\begin{pmatrix} \cos(2\beta) & \sin(2\beta) \\ -\sin(2\beta) & \cos(2\beta) \end{pmatrix}$$

The precise number of times one need to apply the operator O in order to obtain a pure state $|J>$ is given by

$$(2N+1)\beta = \frac{\pi}{2}$$

$$N = \frac{\pi}{4\sin^{-1}\left(\frac{1}{\sqrt{2^L}}\right)} - \frac{1}{2}$$

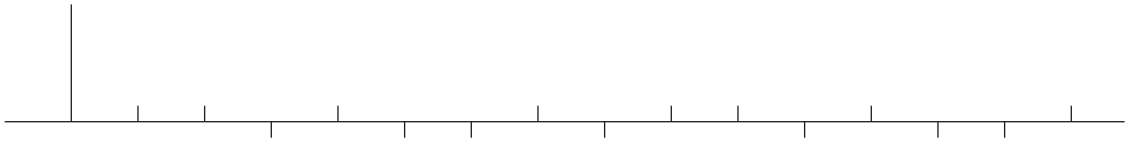
Note that for $L = 2$, the exact solution is $N = 1$.

In the following example we take the case of four qubits, so that the register store a number between 0 and 15. We assume that the marked state is the number 7. We begin by taking the state $|0>$ and performing a Hadamard transformation so that we have a superposition of all states with equal coefficients. Now we pass the state four times, though the series of transformations $\mathbf{U}_7,\ H,\ U_0$, and $\mathbf{H}$. Note that after three iterations the state is almost purely in the state $|7>$, as required. In fact the coefficient of the component $|7>$ is 0.96 rather than unity and there is still a small component from the other states. Recalling that the probability to find the system in a given state is the square (modulus) of the coefficient, we see that there is a 99.8% probability to find the system in the required state after three iterations. We note also that upon application of a fourth iteration the purity of the state is lost - the components of the other states has increased considerably.

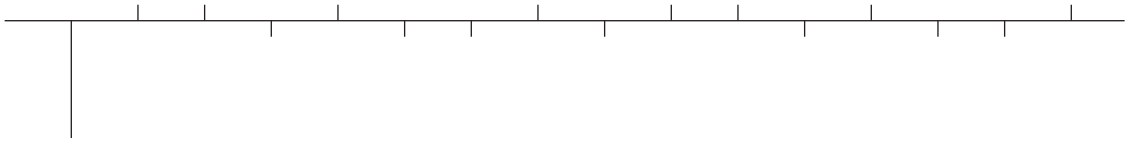
Iteration 1

U_7

H



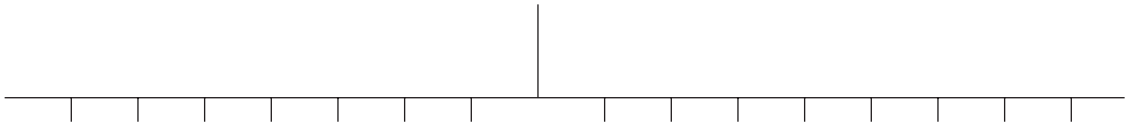
U_0



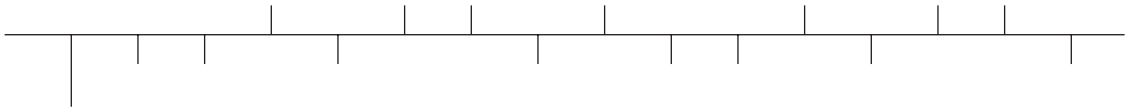
H

Iteration 2

U_7

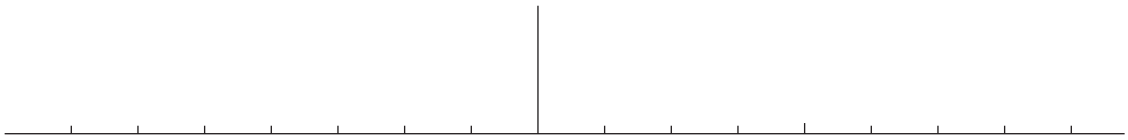


H



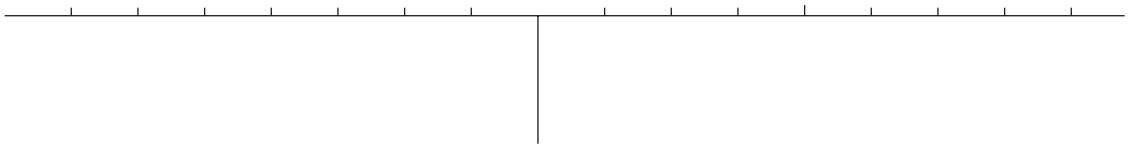
U_0

H



Iteration 3

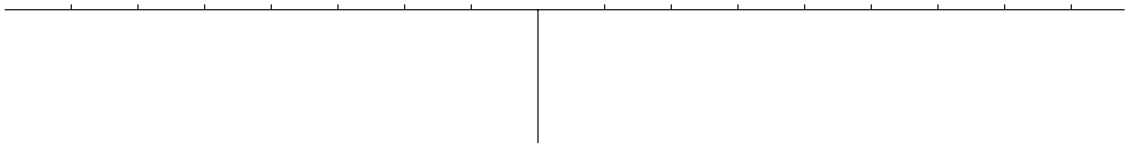
U_7



H

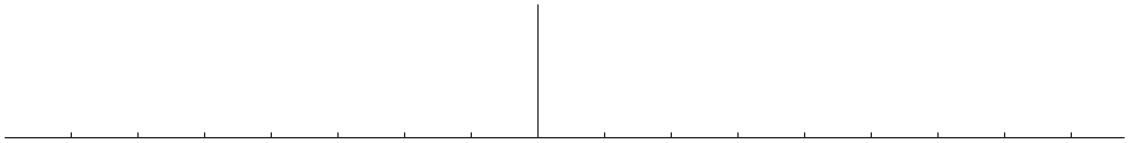
U_0

H



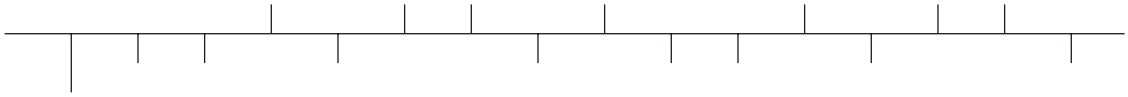
Iteration 4

U_7

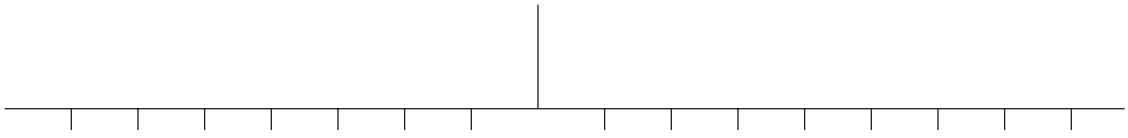


H

U_0



H



11.1 Using Grover's Algorithm to Search a Database

Consider a function $f(J)$ which maps an integer J to an integer $F = f(J)$. For simplicity assume that the map is one-to-one. The objective is to force a state into the state $|J> \otimes |F>$, given knowledge of F but not J. Once again we need an oracle which reverses the sign of the wavefunction for a state if the second (target) register is in the state $|F>$, but otherwise leaves the state unchanged.

Using a sequence of NMR pulses we can construct a device which performs the operation V_f, such that

$$|J> \otimes |K> \rightarrow \ \mathbf{V}_f |J> \otimes |K> \equiv \ |J> \otimes |K \oplus f(J)> .$$

The first register is the "control" register and the second register is the "target register". Since we assume that the map is one-to-one we are assuming that these registers both contain L qubits.

Note that V_f is an idempotent operator, i.e. the device is reversible. In particular,

$$\mathbf{V}_f |J> \otimes |0> = \ |J> \otimes |f(J)>$$

$$\mathbf{V}_f |J> \otimes |f(J)> = \ |J> \otimes |0>$$

Now define an device W which is a Hadamard gate acting on the control register *only* followed by the device V_f, with the matrix representation

$$\mathbf{W} \ \equiv \ \mathbf{V}_f H$$

$$\mathbf{W}^{-1} \ = \ \mathbf{V}_f \, H^{-1}$$

where H is a Hadamard gate acting on the control register only. Thus

$$\mathbf{W}|0> \otimes |0> = \ \frac{1}{\sqrt{2^L}} \sum_{K=0}^{2^L-1} \mathbf{V}_f |K> \otimes |0> = \frac{1}{\sqrt{2^L}} \sum_{K=0}^{2^L-1} |K> \otimes |f(K)>$$

Since the map is one-to-one we can rewrite this last expression as

$$\frac{1}{\sqrt{2^L}} \sum_{F=0}^{2^L-1} |f^{-1}(F)> \otimes |F> .$$

Now let U_F be a device which flips the sign of the quantum state if and only if the target register is in the state $|F>$. From the above discussion on Grover's algorithm for L qubits it follows that

$$\left(\mathbf{W} U_0 W^{-1} \mathbf{U}_F \right)^N \mathbf{W}|0> \otimes |0> \approx |f^{-1}(F)> \otimes |F>,$$

where N is the nearest integer to $\sqrt{2^L}\pi/4$.

12. DEUTSCH'S ALGORITHM

Consider a one bit function ("true" or "false"), $f(I)$, where I is an integer between 0 and $2^L - 1$, but $f(I)$ can only take the values 0 or 1. If $f(I) = 0$ for all values of I or $f(I) = 1$ for all values of I, then the function is said to be "even". If $f(I) = 1$ for $2^L/2$ values of I and $f(I) = 0$ for the remaining $2^L/2$ values then the function is said to be "balanced".

For a classical computer, if we want to establish whether a function is even or balanced (or neither) we would need to sample the function for all values of the argument, I. Using Deutsche's algorithm we can construct a state which is a function of a superposition of all possible arguments and with a single

enquiry we can establish either that the function is not balanced or (exclusive) that the function is not even.

Single qubit:

Let U_f be a quantum logic gate which perform the operation on a single control bit and a single target bit

$$|j>\otimes|k>\rightarrow\ \mathbf{U}_f|j>\otimes|k>=\ |j>\otimes|k\oplus f(j)>,$$

where $f(j)$ is a single bit function of the single bit j, e.g.

$$\mathbf{U}_f|j>\otimes|0>=\ |j>\otimes|f(j)>$$

Now let $|k>$ be

$$|k>=\ \frac{1}{\sqrt{2}}\left(|\downarrow>-|\uparrow>\right)\ =\ \frac{1}{\sqrt{2}}\left(|0>-|1>\right)$$

such that

$$\mathbf{U}_f|j>\otimes|k>=\ \frac{1}{\sqrt{2}}\left(|j>\otimes|f(j)>-|j>\otimes|0>\right),\ \text{ if } f(j)=1,$$

and

$$\mathbf{U}_f|i>\otimes|j>=\ \frac{1}{\sqrt{2}}\left(|j>\otimes|f(j)>-|j>\otimes|1>\right),\ \text{ if } f(j)=0.$$

In other words

$$\mathbf{U}_f|j>\otimes|k>=\ \frac{1}{\sqrt{2}}(-1)^{f(j)}|j>\otimes|k>$$

Now let $|j>$ be

$$|j>=\ \frac{1}{\sqrt{2}}\left(|\uparrow>+|\downarrow>\right)\ =\ \frac{1}{\sqrt{2}}\left(|1>+|0>\right)$$

$$\begin{aligned}\mathbf{U}_f|j>\otimes|k> &= \frac{1}{\sqrt{2}}\left((-1)^{f(0)}|0>+(-1)^{f(1)}|1>\right)\otimes|k> \\ &= (-1)^{f(0)}|\left(|0>+(-1)^{(f(1)+f(0))}|1>\right)\otimes|k>.\end{aligned}$$

Now the control bit is in an eigenstate of S_x with eigenvalue $-\frac{1}{2}$ if $f(0)\oplus f(1)=1$ (balanced) and $+\frac{1}{2}$ if $f(0)\oplus f(1)=0$ (constant).

Extension to L bits for the control register:

U_f is a device that performs the operation

$$|J>\otimes|k>\rightarrow\ \mathbf{U}_f|J>\otimes|k>=\ |J>\otimes|k\oplus f(J)>.$$

Here $f(J)$ is a single bit function of the integer J.

We start with the control register in the state

$$\mathbf{H}|0>=\frac{1}{\sqrt{2^L}}\sum_{K=0}^{2^L-1}|K>$$

and the target bit in the state $(|0>-|1>)/\sqrt{2}$, as before.

Upon output from the device the control register is in the state

$$\frac{1}{\sqrt{2^L}} \sum_{K=0}^{2^L-1} (-1)^{f(K)} |K> .$$

If f is balanced then this state is orthogonal to $\mathbf{H}|0>$, i.e the overlap

$$\frac{1}{\sqrt{2^L}} \sum_{K=0}^{2^L-1} (-1)^{f(K)} < 0|\mathbf{H}|K >$$

is zero. On the other hand if the function is constant then the overlap has modulus unity.

Thus we pass the sample through a Stern-Gerlach apparatus that only allows the particle to pass if $S_x = L/2$. From this measurement we can deduce the following with absolute certainty

- If the sample passes through then the function is NOT balanced (the overlap is not zero).
- If the sample does not pass though then the function is NOT constant (the modulus of the overlap is not unity).

FURTHER READING

The following references contain full references to the literature and alternative presentations to the topics discussed in these notes:-

1. "The Feynman Lectures on Computation" by Richard P. Feynman, edited by Anthony J.G. Hey and Robin W. Allen, (Perseus Books, 1996; Penguin Books 1999).
2. "Explorations in Quantum Computing" by Colin P. Williams and Scott H. Clearwater (TELOS, Springer-Verlag, 1997).
3. "Introductions to Quantum Computation", edited by Hoi-Kwong Lo, Sandu Popescu and Tim Spills (World Scientific, 1998).
4. "Feynman and Computation: Exploring the Limits of Computes", edited by Anthony J.G. Hey (Perseus, 1999).