Chapter 3

Quantum physics and information

In recent years there has been an increasing interest in questions concerning the relation between quantum physics and information theory. The present understanding is that the characteristic features of quantum physics that distinguishes it from classical physics, namely quantum interference in general and quantum entanglement in particular, creates the physical foundation for an approach to communication and to processing of information that is qualitatively different from the traditional one. At present there is only a partial understanding of this new approach, but the belief of many physicists is that a new type of *quantum information theory* should be developed as an alternative to classical information theory. This belief is supported by the discovery of algorithms that could speed up the computation of certain types of mathematical problems in a *quantum computer* and by the develpment of methods for secure and efficient communication by use of *entangled qubits*.

The development of this new approach to information and communication poses important challenges to the manipulation of quantum systems. This is so since *quantum coherence* is important for the methods to work, and in a system with many degrees of freedom *decoherence* will under normal conditions rapidly destroy the important quantum correlations. The very difficult challenge is to create a quantum system where, on one side, the quantum states are effectively protected from outside disturbances and, on the other side, the variables can rapidly be adressed and manipulated in a controlled way in order for the system to perform the task in question.

In this chapter we focus on some basic *theoretical* elements in this new approach to physics and information, while for the discussion of the present status of *implementations* of the ideas on physical systems we refer to several recent

books on the subject. We first focus on an example of how quantum physics admits the possibility of aquiring information in a radically new way through an *interaction-free measurement*. We then proceed to study how *qubits* can replace *bits* as the fundamental unit of information.

3.1 An interaction-free measurement

The usual picture of measurements performed on a quantum system is that they involve a non-negligible, minimal disturbance quantified by Planck's constant. If photons are used to examine a physical object, the minimal disturbance corresponds to letting a single photon interact with the system. The energy of the photon may be made small, but since this means making the corresponding frequency small, one will thereby loose resolution. Thus if a certain resolution is required, a minimal energy has to be carried by the photon and this gives rise to a finite perturbation of the object. The picture of measurements in classical theory is different. There the energy that is carried by light of a given frequency can be made arbitrarily small by reducing the amplitude, and therefore there is no lower limit to how much an (idealized) measurement will have to disturb the object studied.

However, this is not the complete picture. Quantum mechanics opens up the possibility for other types of more "intelligent" interactions than the direct "mechanical" interaction between the object and the measuring apparatus. With the use of quantum superposition (or interference) certain types of measurements can be performed which involve *no mechanical interaction* with the object. A particular example is discussed here.[1]

Let us assume that a measurement should be performed in order to examine whether or not an object is present within a small transparent box. If the object is not there the box is transparent to light, if it is there the box is not transparent since the object will absorb or scatter the photon. Let us further assume that measurements are performed with single photons.

A direct measurement would be to send a photon through the box and to register whether the photon is transmitted through the box or whether it is not transmitted. This would clearly give the information required. If the object is present, the information about this situation is achieved by a direct (mechanical) interaction between the photon and the object. Apparently this is the least interaction with the object that can be made in order detect its presence.

[1] This example is taken from A.C. Elitzur and L. Vaidman, Found. Phys **23** (1993) 987.

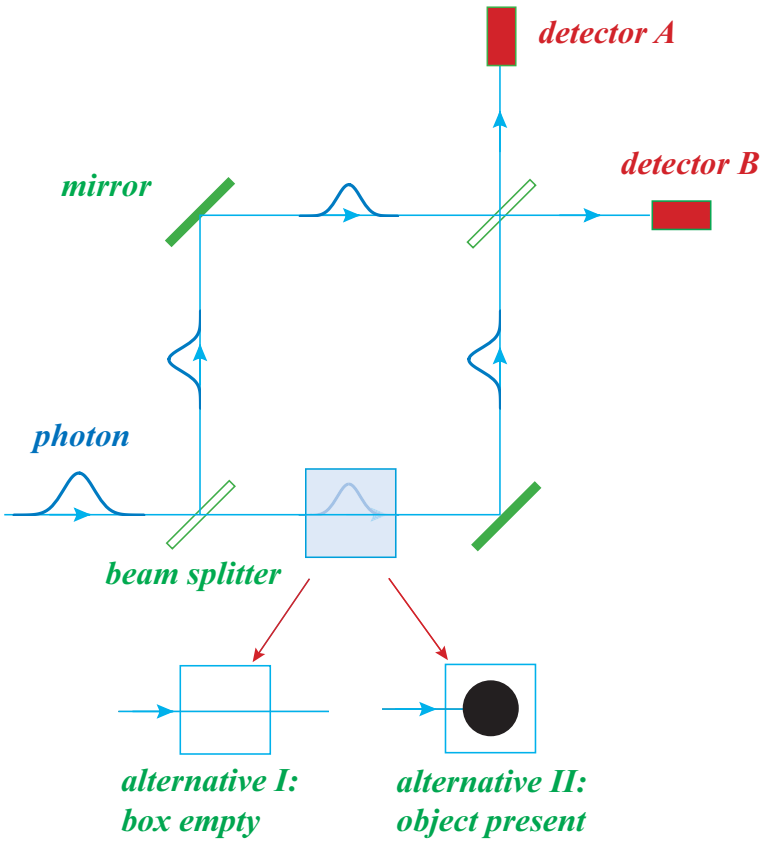

Figure 3.1: The set up of a single-photon measurement to detect the presence of an object in a transparent box by use of a Mach-Zender interferometer. A photon is sent through a beam splitter that directs it, in a superposition, either in the horizontal or vertical direction. On the lower path the box is placed. Therefore, if the object is present, the lower path is blocked, while if it is not there both paths are open. The two paths meet again at a second beam splitter and then the photon is directed towards one out of two possible detectors. The interferometer is arranged so that if both paths are open, destructive interference prevents the photon from reaching detector B. Thus, if the photon is registered by B this provides the information that the lower path is blocked and that the object is present in the box.

However, this is not the correct conclusion to draw, as is outlined in Fig.3.1. The figure shows a Mach-Zender interferometer where an incoming photon can follow two different paths and eventually be registered in of the two detectors. We first consider the case where both paths are open. The photon will first meet a beam splitter that with equal probability will direct the photon horizontally into the lower path or vertically into the upper part. On both paths the photon will meet a mirror that redirects it towards a second (50/50) beam splitter. Here the two components of the phoston wave functions will meet and form a superposition that can either direct it in the horizontal direction towards a detector A or vertically towards a detctor B.

If we neglect the coherence effect and assume an incoherent scattering of the photon by the beam splitters, with equal probability in the two directions, then we expect that the probability for detecting the photon by detector A to be 50%. With the same probability the photon will be detected by B. However, the quantum description of the transmission of the photon through the apparatus implies that the photon at intermediate times is not located (with a certain probability) on one of the paths, but is rather in a *superposition* of being on each of the two paths. This means that the two signals following the upper and lower paths will interfere when they meet at the second beam splitter. In the following we will assume the experimental setup to be adjusted to a situation where the interference acts constructively for a photon directed towards detector A and destructively for a photon directet towards detector B. Thus, the probability for detecting the photon by A is 1 and the probability for detecting the photon by B is 0. This will be the case as long as both paths are open. Clearly, if one of the paths are closed the photons that get through are instead detected with equal probability by A and B.

To describe the situation more formally let us denote the state of a photon moving in the horizontal direction by $|0\rangle$ and a photon moving in the vertical direction by $|1\rangle$. (With this notation we do not make any distinction between where in the apparatus the photon is.) The action of the beam splitters on a photon is described by the mapping

$$\begin{aligned} |0\rangle &\rightarrow \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle) \\ |1\rangle &\rightarrow \frac{1}{\sqrt{2}}(|1\rangle + i|0\rangle) \end{aligned} \tag{3.1}$$

while the action of the mirrors is given by

$$|0\rangle \rightarrow i|1\rangle\,, \quad (\text{lower mirror})$$

$$|1\rangle \;\rightarrow\; i|0\rangle\,, \;\; (\text{upper mirror}) \tag{3.2}$$

The lengths of the paths are assumed to be the same so the phase differences that are for photons on the two paths acquired are only due to phase changes at the mirrors and beam splitters. The photon is subject to a serie of transformations of the form (3.1) and (3.2) in the interferometer. Let us consider the mapping from the incoming state to the outgoing state (before detection) when only the upper path is open,

$$|0\rangle \rightarrow i|1\rangle \rightarrow -|0\rangle \rightarrow -\frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle) \rightarrow -\frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle) \tag{3.3}$$

Since we are interested in the state of a photon that exits from the last beam splitter, the intermediate states have been normalized, thus neglecting the probability that the photon is absorbed on the lower path. The interesting point to note that the final state is a superposition with equal probability for exit in the horizontal and vertical direction.

If both paths are open the mapping from the initial to the final state is instead

$$|0\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle) \rightarrow \frac{1}{\sqrt{2}}(-|0\rangle + i|1\rangle) \rightarrow -|0\rangle \tag{3.4}$$

and we note that only one component survives. The photon will exit (with probability 1) in the horizontal direction.

We will now turn to the original problem and consider the the situation where the box, which either is empty or not empty, is placed on one of the paths of the photon. The intention is to send one photon through the interferometer in order to investigate whether the box is empty or not. We note that if the box is empty we have the situation where both photon paths are open. If the box is not empty only one of the paths will be open.

Let us consider the possible outcomes of the experiment where a photon is sent through the interferometer:

1. The photon does not get through.
   We conclude that the object is present, the photon has interacted with the object.

2. The photon is registered by detector A.
   The result is inconclusive. Whether the object is there or not there is always a chance for the photon to be detected by A. The experiment has to be repeated.

3. The photon is registered by detector B.
   We conclude that the object is present, since the probability of detecting the photon by B with both paths open is 0.

Of the possible outcomes we focus on 3., which is the interesting one. In this case the presence of the object has been detected without any interaction with it. This is so since the *detection* of the photon implies that no interaction has taken place. A natural explanation seems to be that the photon has followed the upper (open) path, but that the detection of the photon provides information about the lower path (that it is closed). This result depends crucially on the possibility of quantum superposition. In a classical theory this would not happen. Note however, the curious fact that when the object blocks the path, in reality no superposition takes place. The result of the measurement will be the same as in a classical theory with a certain probability for the photon to follow the upper path. It is *our knowledge* of the possible outcomes when both paths are open that allows us to draw the conclusion that one path is closed.

In conclusion this thought experiment shows that a direct interaction in a measurement is not always needed. But there has to be a *possibility* for the interaction to take place. A superposition between two states where one of them interacts (when the object is there) and the other does not is an important ingredience in the set up.

The example discussed here shows that alternative ways to collect information with quantum mechanical methods is a possibility. Quantum coherence or superposition is important for such methods to work. Also the importance of using ”intelligent ways” to address the measuring problem, instead of a (naive) direct measurement is emphasized.

3.2 From bits to qubits

In the classical information theory developed by Shannon information is quantified in terms of discrete *units of information*. Thus, the elementary information unit is a *bit*, and this is viewed as a function which can take two possible values, normally the numerical values 0 and 1. The information lies in specifying which of the two values to asign to the bit. The idea is that a general message, to an arbitrary good precision, can be expressed in terms of a finite sequence of bits.

The idea of *quantizing information* creates the basis for the general theory of information. But as we all know it also creates the basis for a practical approach

to information and communication in the form of digital signals. Whereas communication (by telephone, radio or TV) used to be in the form of *analog signals*, presently the use of digital signals are preferred because this admits a more precise determination (and correction) of the information content of the signal.

Information theory can be viewed (and is normally so) as a mathematical discipline. However, from a physics point of view, it is natural to focus on the implementation of the theoretical ideas in terms of physical signals. Thus the information will normally be coded into signals that are created and manipulated in physical (electronic) devices. They are transmitted by physical mediators (electromagnetic waves or electric signals) and are again manipulated and decoded in (electronic) receivers.

A message consisting of a certain number of bits can be viewed as a *state* of a physical system. With N bits there are 2^N states, which represent all the different messages that can be encoded in the N bits. In this picture the factorization of the message into single bits corresponds to a separation of the physical system into N two-state subsystems. Thus, the information unit *bit* corresponds to the *two-state system* as a physical unit. Such a system can be realized in many ways, as a physical system that can easily be switched between two stable states, as an electric signal with only two allowed values (”on” or ”off”) etc.

The important point to note is that the two-state system considered in this way is a *classical* system. And the interesting question which has been addressed in recent years is whether quantum physics should introduce a new picture of the (physical) unit of information. The classical two-state system has its counterpart in the quantum two-state or two-level system, and for the quantum system a new feature is that *coherent superpositions* between states are possible. In the same way as the classical two-state system is associated with a bit of information, the quantum two-level system is associated with a new information unit, a *qubit*. While the possible values of a bit is restricted to 0 and 1, the qubit takes values in a two-dimensional Hilbert space spanned by two vectors $|0\rangle$ and $|1\rangle$. Thus a general qubit state is

$$|q\rangle = \alpha|0\rangle + \beta|1\rangle \tag{3.5}$$

with α and β as complex coefficients.

Let us therefore assume that a message in this new picture is encoded not in a classical state of a system, but in a quantum state of a finite-dimensional Hilbert space. Such a Hilbert space is unitarily equivalent to a tensor product of N two-level systems, provided we restrict the dimension of the Hilbert space to

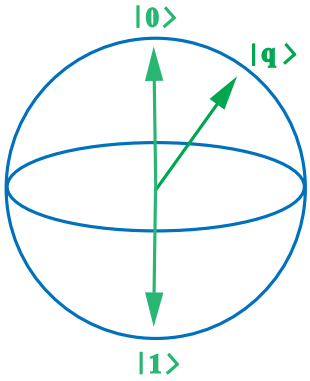

Figure 3.2: The physical states of a qubit can be viewed as points on a sphere. The poles of the sphere correspond to the two classical one-bit states 0 and 1

$M = 2^N$. In this sense we can view the qubit as the elementary building block of information. Note however that the general state is not a product state of the qubits, since also superpositions should be included. This means that the general state involves *entanglement* between the qubits.

Apparently there is much more than one bit of information contained in each qubit, since the qubit states form a continuum that interpolate between the "classical" states $|0\rangle$ and $|1\rangle$. However, one should be aware of the fact that even if more information is contained in the *specification* of the qubit state, this information cannot be read out by making a measurement on the qubit. This is due to the probabilistic interpretation of the state. One may compare this to a situation with a (classical) probability distribution over the two states 0 and 1. Since the probability distribution depends on a continuous parameter, much more than one bit of information is needed to specify the value of this parameter. However, since each classical two-state system can only be in the states 0 or 1, an ensemble of these systems is needed to provide the information about the probability distribution.

In the case of qubits the situation is somewhat similar, but not completely so. Unlike a classical probability distribution the superposition of states is a resource that can be used for some types of information processing. This has been demonstrated by specific examples.

3.3 Communication with qubits

New possibilities open up in communication when we can exploit quantum interference and quantum entanglement. We show here a simple example of *dense coding* of information with the help of entangled qubits.

Let us assume that a sender A (often referred to as *Alice*) wants to send a two-bit message to a receiver B (referred to as *Bob*). The question that is posed is whether this can be done by transmitting a single qubit, since the claim is that a qubit carries more information than a bit. The apparent answer is no: If Alice prepares the the qubit in a pure state and send it to Bob, he can read out the information by a measuring the state in a given basis (corresponding to measuring the spin component in some direction). The result is 0 or 1, where the probability for getting these two results is determined by the decomposition of the prepared state on the the two basis states $|0\rangle$ and $|1\rangle$. It seems that the best they can do in order to send the meassage is to agree on what basis to use. Then Alice can choose between two possible states $|0\rangle$ and $|1\rangle$ and Bob can determine which of the states is chosen by making a measurement in the same basis as used by Alice. But in this way a qubit can communicate only one bit of information.

However, a more intelligent way to do it exists. Let us assume that Alice and Bob in advance have shared a pair of qubits with maximum entanglement. They may for example be in the state

$$|c,+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{3.6}$$

We assume the qubits are kept in a safe way so that the entanglemet is kept unchanged until the qubits are used for communicating the message.

The four two-bit messages can be associated with a set of four states, denoted 00, 01, 10 and 11, by assigning one of the states to each of the messages. Alice now encodes the chosen message to her (entangled) qubit by making a transformation on it. The transformation is determined by the message in the following way,

$$\begin{aligned}
00 &\rightarrow \quad \mathbf{1}\otimes\mathbf{1}\,|c,+\rangle = \;\; |c,+\rangle \\
01 &\rightarrow \quad i\sigma_z\otimes\mathbf{1}\,|c,+\rangle = i\,|c,-\rangle \\
10 &\rightarrow \quad i\sigma_x\otimes\mathbf{1}\,|c,+\rangle = i\,|a,+\rangle \\
11 &\rightarrow \quad i\sigma_y\otimes\mathbf{1}\,|c,+\rangle = \;\; |a,+\rangle
\end{aligned} \tag{3.7}$$

In the first case no change is made to her qubit, in the second case a rotation of π around the z-axis is performed, in the subsequent cases rotations around the y-

axis and z-axis are performed. (We here envisage the qubit states as spin states.) We note that in all cases no change is done to the B-qubit, and in all cases the maximal entanglement is kept by transforming the original state into another Bell state.

Alice now transmits her qubit to Bob who is free to make measurements on both entangled qubits. We note that the four different (two-bit) messages are incoded in the four orthogonal Bell states. Bob can determine which one is chosen by Alice by measuring the (eigen)value of an observable which has the Bell states as eigenstates (assuming different eigenvalues for the four states). If Bob in advance has been informed about the key to decode the message from the Bell states, then he will obtain the full two-bit message from the measurement.

In this way Alice has managed to transfer the two-bit message to Bob by encoding the message into a single qubit which is afterwards transmitted to Bob. The second qubit, belonging to Bob is not affected by the manipulations performed by Alice. Also note that the original entangled state contains no information about the message. Nevertheless, the message is read out by making a measurement on both qubits.

The entanglement is essential for being able to transmit the full message by a single qubit. In fact, if we consider Alice's qubit separately, it is all the time in the same state, described by the reduced density matrix

$$\hat{\rho}_A = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|) \tag{3.8}$$

This means that *all the information is contained in the entanglement between the two qubits*, since no information lies in the reduced states of the two qubits. From this we also note the important point: The message can only be read by the receiver who has the second qubit of the entangled pair. In this way the message is protected from others than Bob. This principle of protecting information by encoding the information into entangled pairs of qubits is the basis for *quantum cryptography*, which is a field of research that has been rapidly developed in recent years.

3.4 Principles for a quantum computer

The probably most interesting suggestion for application of quantum physics to information technology is in the form of *quantum computers*. The idea is that a

computer build on quantum principles will manipulate information in a qualitatively different way than a classical computer and thereby solve certain types of problems much more efficiently.

A type of problem that is most interesting for physicists is *simulation of quantum systems*. Today numerical solutions of physics problems are important for research in almost any field of physics, but the capacity of present day computers gives a clear limitation to the size of the problem that can be solved. Thus, a quantum system with N degrees of freedom has a Hilbert space with dimension m^N, if each degree of freedom is described by an m-dimensional space. This means that m^N complex parameters are needed to specify a Hilbert space vector, and the number of variables to handle therfore grows exponentially with N.

The idea is that a quantum computer *works as a quantum mechanical system*, with the computation performed by unitary transformation on superposition of qubit states. For the simulation of quantum systems there is an obvious gain, since the number of qubits needed to represent the wave function grows linearly with the number of degrees of freedom N rather than exponentially. In addition to the simulation of quantum systems there are also certain other types of mathematical problems that can be solved more efficiently with the use of quantum superposition. Two algorithms that have gained much interest are the *Shor algorithm* for factorizing large numbers and the *Grover algorithm* for making efficient serch through data bases.

The typical feature of a quantum computer is to work with superpositions of (qubit) states. From a computational point of view this can be seen as new type of *quantum parallel computing*. In the picture of path integrals we may view a classical computation as a (classical) path, where each logical operation corresponds to making a (new) direction for the path. Parallel processing in this picture corresponds to working simultaneously with several paths in the ”space of logical operations”. In the quantum computer many paths are, in a natural way, involved at the same time in the form of a superposition of states, and the final result is obtained by quantum mechanical interference between contributions from all the (classical) paths. Clearly, if a problem should be solved much more efficiently on a quantum computer than on a classical computer, superposition of states has to be used extensively in the computation. This means that the qubits will be highly entangled during the computation. The serious challenge for constructing a quantum computer is therefore to be able to preserve and operate on such highly entangled states.

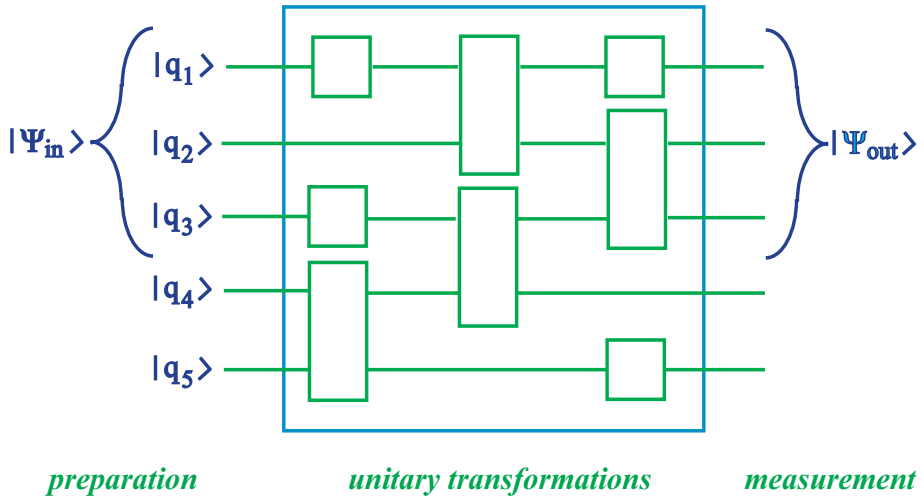

Figure 3.3: A schematic picture of a universal quantum computer. An input state is prepared as a quantum state of a set of qubits. A network of logical gates, that perform one-qubit and two-qubit transformations, operates on the input qubits (and a set of additional work qubits) to produce an output state. The result of the computation is read out by measuring the state of each output qubit. In the diagram the horisontal lines represent the qubits and the boxes represent the gates or logical operations performed on the qubits.

3.4.1 A universal quantum computer

The idea of a universal quantum computer is similar to that of a universal classical computer. Thus, a universal quantum computer is designed to solve general types of problems by reducing the computation to elementary qubit operations. This means that the input wave function is encoded in a set of (input) qubits, and the computational program acts on these by performing *logical operations* in the form of unitary transformations on the qubits. A standard set of unitary *one-qubit* and *two-qubit* operations are used, where each operation is performed at a logical gate. Together the logical gates form a *computational network* of gates.

In Fig. 3.4.1 a schematic picture of a universal quantum computer is shown. The input data is encoded by preparation of an input quantum state. The computer program acts on the input state and by a unitary transformation produces an output state where the result of the computation is read out by a quantum measurement. The computational task is specified partly by the transformation performed on the

state and partly on how the measurement is performed.

This picture of a quantum computer is quite analogous to that of a classical computer, where bits of information are processed at logical gates that together form a logical network. The main difference is that in the quantum computer the information is processed as quantum superposition between states. And the computation is *reversible* since the unitary transformations are all invertible. This is different from a (standard) classical computer where some of the standard logical operations are irreversible in the sense that the mapping between the input state and the output state is not one-to-one.

A universal set of logical gates

The idea of a universal quantum computer is based on possibility of factorizing any unitary transformation that acts on the quantum states of an N qubit system in terms of a small number of standard one-qubit and two-qubit transformations. We will here only outline how such a factorization is shown. It involves the following steps,

1. A unitary transformation acting on a finitedimensional Hilbert space can be factorized in terms of two-level unitary transformations. These transformations act on two-level subsystems spanned by orthonormalized vectors of a common basis in the full Hilbert space,

$$\hat{U} = \prod_n \hat{U}(i_n, j_n) \tag{3.9}$$

   where i_n and j_n denotes the basis states affected by the nth transformation

2. A two-level unitary transformation acting between basis states of the N-qubit Hilbert space can be factorized in terms of a set of one-qubit and two-qubit operations. If the number of terms in the factorization is finite, a general unitary transformation can only be represented in an approximate form. Thus, the continuous parameters of the unitary transformation is replaced by a set of finite values.

The following one-qubit and two-qubit transformation gives an example of a universal set of qubit operations,

1. *The Hadamard transformation.*
   This is a single-qubit transformation defined by the operations on the qubit

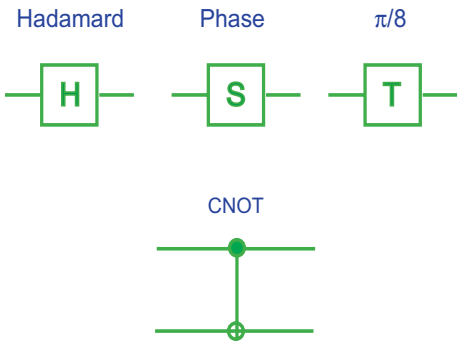

Figure 3.4: Symbolic representation of logical gates. In the representation of the CNOT gate the upper line corresponds to the control qubit and the lower line to the target qubit

states in the following way,

$$\begin{aligned} \hat{H}\,|0\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ \hat{H}\,|1\rangle &= \frac{1}{\sqrt{2}}(\,|0\rangle - |1\rangle) \end{aligned} \tag{3.10}$$

In matrix form this is,

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix} \tag{3.11}$$

2. *The Phase transformation.*
   This is also a single-qubit transformation, defined by

$$\begin{aligned} \hat{S}\,|0\rangle &= |0\rangle \\ \hat{S}\,|1\rangle &= i\,|1\rangle \end{aligned} \tag{3.12}$$

   which in matrix form is

$$S = \begin{pmatrix} i & 0 \\ 0 & 1 \end{pmatrix} \tag{3.13}$$

3. *The $\pi/8$ transformation.*
   This is the third single-qubit transformation. It is defined by

$$\begin{aligned} \hat{T}\,|0\rangle &= |0\rangle \\ \hat{T}\,|1\rangle &= e^{i\pi/4}|1\rangle \end{aligned} \tag{3.14}$$

with the matrix form

$$T = \begin{pmatrix} e^{i\pi/4} & 0 \\ 0 & 1 \end{pmatrix} \tag{3.15}$$

4. *The $CNOT$ transformation.*
This is a two-qubit transformation, which is a quantum version of a *controlled not* operation. It is defined by

$$\begin{aligned} \hat{C}_{NOT}\,|0\rangle \otimes |0\rangle &= |0\rangle \otimes |0\rangle \\ \hat{C}_{NOT}\,|0\rangle \otimes |1\rangle &= |0\rangle \otimes |1\rangle \\ \hat{C}_{NOT}\,|1\rangle \otimes |0\rangle &= |1\rangle \otimes |1\rangle \\ \hat{C}_{NOT}\,|1\rangle \otimes |1\rangle &= |1\rangle \otimes |0\rangle \end{aligned} \tag{3.16}$$

We note that the state of the first qubit is left unchanged. It acts as a *control qubit* on the second qubit: If the first qubit is in the state $|0\rangle$ the second qubit is left unchanged. If the first qubit is in the state $|1\rangle$ the second qubit switches state $|0\rangle \leftrightarrow |1\rangle$. With the basis vectors of the product space written in matrix form,

$$\begin{aligned} |0\rangle \otimes |0\rangle \rightarrow \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \;,\;\; |0\rangle \otimes |1\rangle \rightarrow \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \\ |1\rangle \otimes |0\rangle \rightarrow \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \;,\;\; |1\rangle \otimes |1\rangle \rightarrow \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \end{aligned} \tag{3.17}$$

the $CNOT$ operation corresponds to the following 4×4 matrix,

$$C_{NOT} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{3.18}$$

The definitions above give the action of qubit operations on a set of basis vectors for the single-qubit and-two qubit spaces. With specification of the qubits involved, the action of these operators on a complete set of basis vectors for the full N- qubit space is determined, and thereby the action of the operators on any state vector, by the principle of linear superposition.

3.4.2 A simple algorithm for a quantum computation

As already mentioned, certain algorithms have been designed for solving mathematical problems more efficiently on a quantum computer than can be done on a classical computer. A famous example is *Shor's algorithm*, that adresses the question of how to factorize large numbers. This is a hard problem on a classical computer, since the computational time used to factorize large nubers will in general increase exponentially with the number of digits. (This fact is the basis for making use of factorization of large numbers as keys in crytographic schemes.) The demonstration by P. Shor that the factorization can be done more efficiently on a quantum computer is one of the reasons for the boost of interest for quantum computing over the last decade.

In this section we will focus on a simpler algorithm introduced by D. Deutsch some time ago. The intention is to use this algorith as a simple demonstration of how superposition makes it possible to adress certain types of problems more efficiently.

The problem adressed is to study *one-bit functions*. Such a function gives a mapping

$$f(x):\ \{0,1\} \to \{0,1\} \tag{3.19}$$

We will need to add these functions, and note that addition between one-bit numbers can be defined from ordinary addition if the result is defined *modulo 2*. Thus, the explicit addition rule is

$$0+0=0\ ,\ \ 0+1=1+0=1\ ,\ \ 1+1=0 \tag{3.20}$$

We also note that there exist four different one-bit functions (3.19),

$$\begin{aligned} &f_a:\{0,1\}\to\{0,1\}\ ,\ \ f_b:\{0,1\}\to\{1,0\} \\ &f_c:\{0,1\}\to\{0,0\}\ ,\ \ f_d:\{0,1\}\to\{1,1\} \end{aligned} \tag{3.21}$$

where the sets of input values and output values are here considered as *ordered sets*. Let us assume that a function $f(x)$ is known only *operationally, i.e.,* by assigning the input variable x the two possible values 0 and 1, the two output values $f(0)$ and $f(1)$ are produced. (We may think of the function as a *black box* that produce the output result from a given input.) Initially the function is not known and instead of determining the function in the way indicated we examine the function by use of a simple quantum computation.

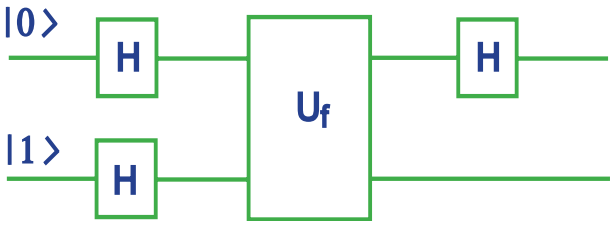

Figure 3.5: Schematic representation of qubit transformations for Deutsch's algorithm. The first qubit is prepared in the $|0\rangle$ state and the second qubit in the $|1\rangle$ state. They are both transformed by a *Hadamard* operation before a two-qubit operation is performed. This operation, U_f, is determined by the (unknown) one-bit function $f(x)$. Finally a second *Hadamard* transformation is performed on the first qubit before a measurement is performed.

We then assume that the function can be implemented on qubit states in the following way

$$T_f : |q\rangle = \alpha|0\rangle + \beta|1\rangle \rightarrow \alpha|f(0)\rangle + \beta|(f(1)\rangle \tag{3.22}$$

This is considered as a single (qubit) operation even if both results $f(0)$ and $f(1)$ are present in the output state. We wish to define the operation as a *unitary transformation*, but note that (3.22) will not be unitary for all the four functions (3.21). The mapping between input and output states is therefore modified to operate as a *two-qubit transformation* in the following way,

$$U_f : |x\rangle \otimes |y\rangle \rightarrow |x\rangle \otimes |y + f(x)\rangle \tag{3.23}$$

where $|x\rangle$ and $|y\rangle$ denote standard qubit basis states ($|0\rangle$ and $|1\rangle$). We note that the first qubit ($|x\rangle$) is left unchanged by the transformation; it acts as a control qubit on the second qubit. Thus, if $f(x) = 0$ the state of the second qubit is left unchanged, if $f(x) = 1$ the state of the second qubit is flipped ($0 \leftrightarrow 1$). It is straight forward to check that (3.23) defines a unitary transformation.

We now consider the computation is performed that is shown in diagrammatic form in Fig. 3.4.2. It corresponds to the following sequence of unitary transformations

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

$$
\begin{aligned}
&\rightarrow \quad \frac{1}{\sqrt{2}}((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\
&\rightarrow \quad \frac{1}{2\sqrt{2}}\Big[((-1)^{f(0)} + (-1)^{f(1)})|0\rangle \\
&\qquad\qquad +((-1)^{f(0)} - (-1)^{f(1)})|1\rangle\Big] \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\
&\equiv \quad |q_1\rangle \otimes |q_2\rangle
\end{aligned}
\tag{3.24}
$$

We note that the for the first qubit there are two possible final states depending on whether $f(0)$ and $f(1)$ are equal or different. Thus,

$$
\begin{aligned}
f(0) + f(1) &= 0 \;\Rightarrow\; |q_1\rangle = (-1)^{f(0)}|1\rangle \\
f(0) + f(1) &= 1 \;\Rightarrow\; |q_1\rangle = (-1)^{f(0)}|0\rangle
\end{aligned}
\tag{3.25}
$$

This implies that by making a measurement on this qubit which projects it either to the state $|0\rangle$ or $|1\rangle$ we can decide the value of $f(0) + f(1)$. This does not fully determine the function $f(x)$, it only distinguishes between the invertible functions f_a, f_b and the non-invertible functions f_c, f_d. However, what is interesting is that this information should normally only be available after two operations with the function, while here only one operation with the function on a superposition of states is needed.

This demonstrates the point that the use of quantum superpositions makes it possible to perform in one operation what would normally correspond to two classical computations. This is what we have referred to as *quantum parallel processing*. There is a close relation between the evaluation discussed here of quantum states that contain information about both functional values $f(0)$ and $f(1)$ and the interaction-free measurement discussed earlier, where the state vector contains information about both the paths that the photon may follow.

The example given by Deutsch's algorithm may be too simple to convincingly justify the claim that the quantum computation is more efficient than the classical computation. Obviously the unitary transformation U_f corresponding to the function $f(x)$ has to be supplemented by other qubit operations and this does not make it completely clear that there is a net gain. The important point to make is that only one evaluation which involves $f(x)$ has been done rather than two. For the other algorithms mentioned one can demonstrate more explicitly the gain by showing that the number of qubit operations scales in a different way than the number of operations in a classical computer. This makes it clear that quantum parallelism may indeed speed up certain types of calculations.

3.4.3 Can a quantum computer be constructed?

The considerations on how a quantum computer may more efficiently solve certain types of problems makes it a very interesting idea. But is it feasable that this idea can be implimented in the form of a real physical computer? The difficulties to overcome are extremely demanding. At present qubit operations with a small number of qubits may be performed, but the idea that thousands and thousands of qubits work coherently together at the quantum level is at this stage an attractive dream. Some people working in the field are rather pessimistic that the necessary control of the quantum states can in reality be made. In particular the problem of *decoherence* is extremely demanding, although algorithms for correcting quantum states that are modified due to decoherence have been suggested.

But other workers in the field remain optimistic, and at the level of making controlled quantum operations on a few qubits there has been an impressive progress. There is in fact a competition between different types of realizations of physical qubits. In the context of electronic systems interesting developments are based on the use of electronic spin as the two-level variable. In the context of quantum optics the use of trapped two-level atoms or ions has been extensively studied. One particularly interesting application is in the form of *optical lattices*, where a collection of laser beems are used to trap atoms in a periodic potential, where the lasers are used to adress the atoms in the form of one-qubit operations and where where they are used to let the atoms interact in the form of two-qubit operations.

One should note that even if the construction of a *universal* quantum computer at this stage may be far away in time, there may be partial goals that can be more readily achieved. Ideas of quantum cryptography have already been implemented, and in the field of computation a *quantum simulator* may be a much closer goal than a universal computer. Recent developments suggests that the use of optical lattices may give a realistic approach towards this goal, and the simulation of quantum spin lattices in this way may be a possibility in a not too distant future.

3.5 Problems

(To be completed.)