POSSIBILITIES FOR QUANTUM INFORMATION PROCESSING

Štěpán Holub *

Abstract. This tutorial introduces quantum information science, a quickly developing area of multidisciplinary research. The basic idea of the field is to study physical systems obeying the laws of quantum mechanics to obtain promising possibilities for computation, image processing, data transfer and/or high precision detection.

Quantum information science is an intersection of mathematics, physics and informatics. We explain basic ingredients that contribute to the general picture. Although we mention also some up-to-date experimental results, the focus will be on the theoretical description of quantum data transfer and a possible quantum computer.

Key words: quantum mechanics, quantum information, quantum computer, Mach-Zehnder interferometer

Automatic processing of information is one of the most striking features of our present civilization. Origins of what we call "computer" date back to the first half of the twentieth century, when Alan Turing gave an ingenious mathematical description of a general algorithmic process (Turing, 1936). All our computers are in fact a kind of physical realization of the old fashioned device known as a *Turing machine*. From the mathematical point of view computers do not evolve, they are just faster and faster, due to enormous technological improvement, which obeys, since 1965, the famous prediction of Gordon Moore: the power of computer processing doubles every eighteen months.

There are, however, ultimate physical restrictions for classical computers, given by the speed of light (electromagnetic field) and the size of atoms. At the sub-atomic level, the laws of quantum physics begin to predominate, which profoundly challenges the classical approach to information. Quantum mechanics, on the other hand, is not only a thread. More importantly, it offers possibilities which give rise to a new and fascinating field of research called quantum information science .

The mathematical notion of information is usually based on symbols chosen from a finite alphabet, typically the famous zeros and ones. The physical part of the question is how to represent these symbols: which

* The work is a part of the research project MSM 0021620839 financed by MSMT.

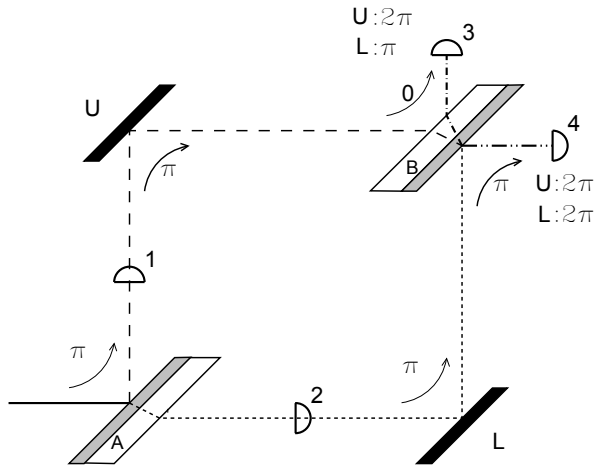


Figure 1. Mach-Zehnder interferometer.

states of which physical system should distinguish between them. If the information is "encoded" by a quantum system the situation seems to be quite analogous . The crucial difference, however, is the fact that quantum systems can exist in *superpositions* of basic states, a strange kind of mixture of them. Quantum information science is basically an attempt to take advantage of this property.

1. The difference between classical and quantum physics

1.1. MACH-ZEHNDER INTERFEROMETER

The difference between classical and quantum physics can be illustrated by a simple experiment called the Mach-Zehnder interferometer. The device is depicted in Figure 1.

A and B are half-silvered mirrors, which split a beam of light in two parts, hence called beamsplitters. Half of the beam goes through the mirror, the second half is reflected. U and L are just ordinary mirrors.

By the laws of optics, light changes its phase by π if reflected by a surface bounding an environment with higher refraction factor (i.e., lower speed of light). Therefore in our picture the only reflection not causing the phase shift is the reflection of the beam arriving from mirror U to mirror B, since the reflection occurs between glass (foreground) and air (background). (The phase shift caused by the transition through the glass is neglected in our description).

Numbers 1 - 4 refer to possible positions of detectors. If we measure at positions 1 and 2, the same energy is detected by each detector. Measurement by detectors 3 and 4 (with detectors 1 and 2 removed) shows that there is no signal on detector 3, only on 4.

The explanation is simple: the beam traveling to 3 through U is shifted by π with respect to the beam traveling through L. Therefore the destructive interference cancels the signal. On detector 4, on the other hand, the interference is constructive.

This is the classical description of the experiment. When the amount of light is diminished under certain *quantum*, the light starts to behave as a particle, the famous photon. This means that the whole photon is either reflected or passes through the mirror, it does not divide in two. The probability that the photon will be detected by detector 1 (2 resp.) is exactly one half. This is confirmed by the experiment.

A strange thing happens when we let the photon go through the mirror B without previous measurement. The classical probabilistic interpretation suggests that the probability will again be one half for both detectors 3 and 4. Indeed, with probability $1/4$ the photon will be reflected both by A and B, and similarly for the other three combinations. But the experimental result is the same as in the interference model: the signal is detected always at 4, never at 3. It is now the task for quantum mechanics to explain this kind of phenomena.

1.2. THE POSTULATES OF QUANTUM MECHANICS

Quantum mechanics is a mathematical tool for the description of quantum phenomena, and is based on three postulates.

Postulate 1 A quantum system with m possible observable values is described by the complex vector space $H_m = \mathbb{C}^m$ with inner product (called *Hilbert space*). A state of the system is a one-dimensional subspace of H_m. It is always represented by a unit vector u, traditionally written as $|u\rangle$.

From the point of view of quantum information science the basic quantum system is two-dimensional, and is called *qubit*, as an analog to the classical bit. To stress the analogy, basis vectors of H_2 are usually denoted by $|0\rangle$, and $|1\rangle$. Note that even if we restrict ourselves to a unit representation of the one-dimensional state subspace, it is not given uniquely. All vectors of the form $e^{\alpha i}|u\rangle$ are equivalent expressions of the same state. Note also that the arithmetic expression of basis vectors is the canonical

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

The basic difference between bit and qubit, already mentioned above, is the possibility of the system existing in a superposition of basis states, as for example the state

$$|u\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}.$$

Postulate 2 The time evolution of a quantum system is given by a unitary operator U. Therefore, if a system is in state $|u\rangle$ at time t_0, then it is in state $U|u\rangle$ at time t_1.

Obviously, the operator U depends on what happened to the system. It may be for example affected by an electromagnetic field of given intensity. In quantum information science we usually consider operators U as black boxes. This is again analogous to the classical approach to bits, when we for example speak about a NOT-gate, without examining its physical realization.

An operator is unitary, by definition, if it satisfies $U^*U = \mathrm{Id}$, where U^* is the adjoint operator of U. It is natural to work with the matrix representation of operators. Then U^* is the transposed complex conjugate matrix of U. An equivalent definition of unitary operator is that it preserves inner product, and therefore also the norm. This is a natural requirement on the time evolution of quantum systems, since then a unit vector evolves again to a unit vector. It is also important that unitary transformations are invertible, it is therefore always possible to reverse the process.

Probably the most useful unitary operator in quantum computing, as we shall see, is the *Hadamard* transform

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

Verifying that it is unitary is a simple exercise.

Postulate 3 Measurement of a quantum system is always related to a certain orthonormal basis. Consider a measurement of H_m in the orthonormal basis $|b_1\rangle, \ldots, |b_m\rangle$. After the measurement, the system collapses to one of the basis states $|b_i\rangle$, and the outcome will be a value λ_i corresponding to that state. It is the eigenvalue of $|b_i\rangle$ with respect to some operator related to the basis and called an *observable*. If the measured system is in the state

$$|u\rangle = \sum_{i=1}^{m} \alpha_i |b_i\rangle$$

then the eigenvalue of $|b_i\rangle$ will be obtained with probability $|\alpha_i|^2$. Note that the sum of probabilities of all outcomes is one, since $|u\rangle$ is a unit vector. The complex number α_i is called the *amplitude of probability*.

The measurement postulate is a very strange one. It claims that the result of a measurement is given only with certain probability. Quantum physics has no means to say more about the outcome; it claims that it is not the fault of the theory, it is nature, which is substantially random when it comes to measurements.

Moreover, the collapse of the system is in general not a unitary operation. Therefore measurements do not obey Postulate 2.

These facts have caused a lot of controversies. Albert Einstein, for example, insisted that the theory cannot be considered a complete description of physical reality (Einstein et al., 1935), and it seems that he never acquiesced to quantum mechanics. Nevertheless the point of view we are describing here, advocated for example by Niels Bohr (Bohr, 1935), became the mainstream.

A very important fact is that the same system can be measured in different bases of our choice. In other words, we can measure different observables. To obtain respective probabilities, it is then necessary to express the state in the chosen basis (or to use some other linear algebra tricks). Let us give an example. Measure the qubit

$$|u\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

in the canonical basis $|0\rangle$, $|1\rangle$, with eigenvalues 1, -1 respectively. Then the outcome will be plus or minus one with probability $1/2$, and the state of the system after the measurement will be $|0\rangle$ or $|1\rangle$. Note that the measurement is destructive. We will never be able to figure out which state has been measured.

If, on the other hand, one measures the same state in the basis

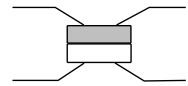
$$|b_1\rangle = |u\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \qquad |b_2\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}},$$

then one obtains the eigenvalue of $|b_1\rangle$ with probability one, and the state does not change.

1.3. MACH-ZEHNDER: THE SOLUTION OF THE RIDDLE

Let us now show how quantum mechanics explains the experimental results of the Mach-Zehnder interferometer. Observe that the interferometer consists of an experiment repeated twice in the same way, namely an interaction of a photon with a half-silvered mirror. The elementary experiment has two possible inputs: the photon arrives either from the glass-side, or from the silver-side of the mirror, and similarly two possible outputs: it leaves

the mirror on the glass side or on the silver side. (In Figure 1 only one possible input for the mirror A is shown.) Schematically the situation can be depicted as follows:



The detection of the photon on one of the two paths is an observable. Denote the basis for this observable by $|0\rangle$, $|1\rangle$. The photon is in state $|0\rangle$ if it travels along the upper path (mirror U in Figure 1) and in state $|1\rangle$ if traveling along the lower path (mirror L).

The key to the riddle is the **superposition**. The state of the photon can be a mixture of both basis states, and that's exactly what, according to quantum mechanics, happens after the interaction of the photon with the beamsplitter. The transformation is given by

$$|0\rangle \mapsto \frac{(|0\rangle + |1\rangle)}{\sqrt{2}}, \qquad |1\rangle \mapsto \frac{(|0\rangle - |1\rangle)}{\sqrt{2}}.$$

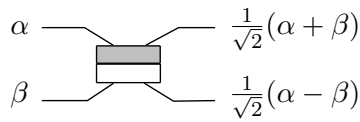
Recall that $|0\rangle$, $|1\rangle$ are vectors of $\mathbb{C}^2$:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

The matrix of the interaction is then

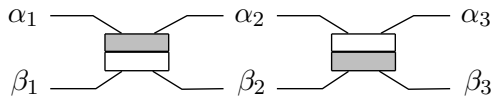
$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$

which is the above Hadamard transform. The action of the beamsplitter on a photon in a state $\alpha|0\rangle + \beta|1\rangle$ can be portrayed as:



In our description of the experiment in Figure 1 we suppose that the photon begins in state $|0\rangle$. Therefore after the interaction with the mirror A it will be in state $(|0\rangle+|1\rangle)/\sqrt{2}$, and, by Postulate 3, the probability that the photon will be detected by the detector 1 (2 resp.) is exactly one half. After detection the photon will be in a basis state corresponding to the detector by which it was detected.

An inspection of Figure 1 shows that the entire Mach-Zehnder interferometer can be schematized as:



The matrix of the second beamsplitter is

$$\sqrt{2}\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix},$$

and the overall effect of the apparatus is given by

$$\sqrt{2}\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \cdot \sqrt{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

which agrees with experimental results: the photon which enters along the upper path will be detected in the lower one (and vice versa).

2. Complexity and circuits

An algorithm is a method to solve a problem, which consists of many (typically infinitely many) instances. For example, an instance of the Traveling Salesman Problem (TSP) is a weighted graph, and the solution is the cheapest path through all nodes. An algorithmic solution of the problem must describe a **finite and uniform** procedure which solves all possible instances. It is not clear, a priori, which instructions should be accepted in an algorithm. One will surely not allow an instruction "find the cheapest path" in the algorithm for TSP, since instructions have to be clear and elementary. On the other hand, restricting the set of tools can result in too weak a concept of the algorithm.

During the 20th century the *Turing machine* (TM) was accepted as the correct expression of what we mean by algorithm. This general agreement is based on the fact that all alternative models are either weaker or equivalent to TM. Whence the Church-Turing thesis:

> Any problem, which can be algorithmically solved, can be solved by the Turing machine.

The thesis cannot be proved, of course, since it hinges on an intuitive notion of algorithmic solution. In fact, it is something between a claim and a definition.

A natural question arises: what about possible quantum computers? Could they do more than TM? The answer is negative. It is possible to simulate all quantum processes by the conventional computer, it just is very complicated and slow. Consequently, the right question is whether quantum computers can do something substantially faster than TM. The

answer to this question is not so simple. We first have to specify what is meant by "substantially faster", and therefore how the complexity of an algorithm should be measured.

The usual concept of algorithmic complexity deals with a function $f(n)$, which gives an upper bound for the number of elementary steps leading to the solution of any instance of length n. It turns out that given an algorithm, various kinds of classical computers do not differ too much in their ability to execute the algorithm. More precisely, if the complexity of an algorithm is given by a polynomial on the traditional TM, then it is given by a (smaller) polynomial also on our best contemporary computers. Somehow, since Turing, we have not invented *better* computers, we have only constructed faster Turing machines. It seems, therefore, that whether an algorithm is polynomial is independent of the machine we use.

In this respect (hypothetical) quantum computers can beat TM. As we shall see, there is a problem – although a bit artificial – which cannot be solved in polynomial time by TM, but is easy for a quantum computer. Even here, however, the situation is not so clear if we allow probabilistic Turing machines, i.e. algorithms which give the right answer with some required probability close to one. Of course, deterministic algorithms are always better, but if the error probability of a probabilistic TM is lower than the probability that your computer will be destroyed by a meteorite, it does not seem very reasonable to insist on deterministic algorithms. It is not known whether quantum probabilistic algorithms are stronger than classical probabilistic ones, and it seems unlikely that this could be proved in the near future, since the fact would imply extremely hard theoretical claims.

From the theoretical point of view, therefore, quantum computers are not convincingly better than classical ones. In practice, however, quantum algorithms have an ace in the hole: there is a practical probabilistic quantum algorithm which factors large numbers. The intractability assumption of such factorizations is the cornerstone of many presently used secure algorithms.

2.1. BOOLEAN AND QUANTUM CIRCUITS

Boolean circuits are a convenient way to describe an algorithm for a given input length, since each algorithm can be seen as a device computing a boolean function. The input is encoded as a sequence of 0s and 1s, and the output as well.

In the previous chapter we represented the beamsplitter in a way which recalls the schematic notation of logical gates. This was not by chance. We want to view quantum phenomena as building blocks for construction of

algorithms. There is, however, one important difference between classical logical gates and quantum ones: quantum processes are all reversible, while for example NAND, which is a universal boolean gate, is irreversible. It is impossible to find out whether the resulting 1 came from two zeros or from 0,1.

So far we have discussed the possibility that quantum computers are stronger than classical ones. Now it turns out that the possibilities of quantum gates may be limited since they have to be reversible. In reality, every classical circuit can be simulated in a reversible way, perhaps with some auxiliary inputs. There are universal reversible gates, for example the Toffoli gate $\mathcal{T}$, which has three input and three output bits. It is defined by

$$\mathcal{T} : (a, b, c) \mapsto (a, b, c \oplus ab),$$

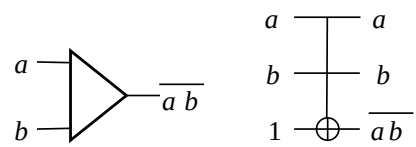
where $\oplus$ denotes the logical sum (i.e. XOR). The Toffoli gate is reversible, since $\mathcal{T} \circ \mathcal{T} = \mathrm{Id}$:

$$(a, b, c) \mapsto (a, b, c \oplus ab) \mapsto (a, b, c \oplus ab \oplus ab) = (a, b, c),$$

and it is universal, since

$$\mathrm{NAND}(a, b) = \mathcal{T}(a, b, 1).$$

In order to simulate boolean circuits by quantum circuits, it is therefore enough to construct a quantum Toffoli gate, which is in principle possible. Every quantum circuit will have a lot of auxiliary bits as is clear from the following comparison.



classical NAND reversible NAND

3. Quantum algortihms

So far three basic quantum algorithms which have better performance than classical algorithms are known:

– Deutch-Jozsa algorithm, which decides whether a given boolean function is constant or balanced;

– Quantum Fourier transform with several applications, the most important of which is Shor's factoring algorithm;
– Grover's algorithm for database search.

We have already noted that the most spectacular achievement of hypothetical quantum computers would be their ability to factor large integers. The Shor's algorithm is, from the quantum point of view, a direct application of the Fourier transform, which is a well known tool able to detect periodicity. It allows to find the order of a chosen element a in the cyclic group $\mathbb{Z}_N$, where N is the factored number, which allows, with a high probability, to find a factor.

The key capability of quantum computers is therefore fast computation of the Fourier transform. While the classical Fast Fourier Transform works in time $O(N \log N)$, the Quantum Fourier Transform is polynomial in $\log N$, which means an exponential speedup.

Here we explain in detail a simple version of Deutch-Jozsa algorithm. Although it has limited importance for practical problems, the algorithm makes clear why the quantum approach can have advantages over the classical one. First we need some more theory regarding composite systems.

3.1. COMPOSITE SYSTEMS

Consider a quantum system made up of n smaller systems. Then we have the following additional

Postulate 4 The system V consisting of systems $V_1, V_2, \ldots, V_n$ is the tensor product

$$V = V_1 \otimes V_2 \otimes \cdots \otimes V_n.$$

This means that it is a $\Pi_1^n d_i$ dimensional system, where d_i is the dimension of V_i, and the basis of V is the set

$$\{|v_{j_1}\rangle \otimes \cdots \otimes |v_{j_n}\rangle \mid j_i = 1, \ldots, d_i,\ i = 1, \ldots, n\}.$$

We usually consider only systems composed of several qubits. They have dimension 2^n, where n is the number of qubits. The notation of basis vectors

$$|k_1\rangle \otimes \cdots \otimes |k_n\rangle,$$

where $k_i \in \{0, 1\}$ is often simplified into $|k_1 \ldots k_n\rangle$. This is a very clever notation, since if sequences $k_1 \ldots k_n$ are understood as binary numbers, one obtains the basis

$$\{|0\rangle, |1\rangle, |2\rangle, \ldots, |2^n - 1\rangle\}$$

of the composite system. For example the basis of the four dimensional system is $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$, which indicates its possible decomposition

into two qubits. It is important to note that, although the composite system is a tensor product of smaller systems, it also contains states which cannot be written as tensor product of vectors from those systems; it cannot be decomposed. For instance, the state

$$|w\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

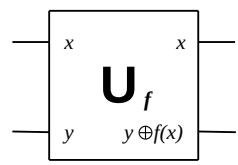
of the four dimensional system is not a product of two qubits, as is easy to verify. The two qubits are said to be *entangled*.

Note that if two qubits are in the state $|w\rangle$, they will with probability $1/2$ have both values corresponding to $|0\rangle$, or both values corresponding to $|1\rangle$. This implies a very strange fact, which challenges basic intuitions of classical physics. It is experimentally possible to prepare entangled qubits (photons, for instance), which can be then separated to a distance of many kilometers. If one of the qubits is measured, the outcome will immediately determine the outcome of the measurement of the distant entangled qubit. In other words, quantum mechanics allows *non-local* effects, which was one of the motives for Einstein's disconcertion.

3.2. DEUTSCH'S ALGORITHM

Deutsch's problem is linked to origins of quantum algorithms. We are given a black box function $f : \{0,1\}^2 \mapsto \{0,1\}$, and have to decide whether it is constant or not. In the classical setting it is obvious that we need to make two queries, i.e. to learn both values of f, in order to decide the question. On the other hand, the question asks for just one bit of information: constant yes, or no? Unfortunately there is no way to ask **just this** question. But that is exactly what a quantum computer can do. Deutch's algorithm shows how to decide the question by a single query.

First it is important to clarify how a quantum black box function is given. The function f is in general not injective, therefore irreversible, and we have seen that all quantum circuits have to be reversible. The standard way to represent such functions is the following gate, with an auxiliary input and output:



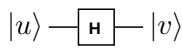
The U_f transform acts on the two qubit system and is defined on the basis vectors $|x\rangle \otimes |y\rangle$ by

$$|x\rangle \otimes |y\rangle \overset{U_f}{\longmapsto} |x\rangle \otimes |y \oplus f(x)\rangle.$$

It is easy to see that it just permutes the basis vectors $|00\rangle, |01\rangle, |10\rangle, |11\rangle$. Note that $U_f \circ U_f = \mathrm{Id}$, therefore the transform is unitary.

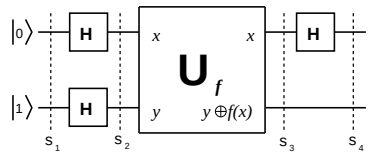
This is the first two-qubit gate we see here. It should not be confused with the beamsplitter gate, which is one-qubit, and in this context should be depicted as

where $|v\rangle = H|u\rangle$, or even better as



to indicate that we do not care about whether the Hadamard gate is physically realised by the beamsplitter or otherwise.

The quantum circuit solving Deutsch's problem is quite simple. It consists, apart from the black box, of three Hadamard gates:



We have indicated the four stages of the algorithm by vertical lines. In the initial stage, the two qubit are in the state

$$s_1 = |01\rangle.$$

In the second stage we obtain

$$s_2 = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

What happens in the black box depends, of course, on the function f. The simplest case is $f(0) = f(1) = 0$, when U_f is the identity. Therefore

$$s_3 = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} \qquad \text{for } f(0) = f(1) = 0.$$

If $f(0) = f(1) = 1$, the action of U_f is given by

$$|00\rangle \mapsto |01\rangle \qquad |01\rangle \mapsto |00\rangle \qquad |10\rangle \mapsto |11\rangle \qquad |11\rangle \mapsto |10\rangle.$$

Then

$$s_3 = \frac{1}{2} U_f(|00\rangle - |01\rangle + |10\rangle - |11\rangle) = \frac{1}{2}(|01\rangle - |00\rangle + |01\rangle - |10\rangle) =$$
$$= -\frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

Similarly we can proceed with the other two possibilities to obtain altogether

$$s_3 = \begin{cases} \pm\frac{|0\rangle+|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle-|1\rangle}{\sqrt{2}} & \text{if } f(0) = f(1), \\ \pm\frac{|0\rangle-|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle-|1\rangle}{\sqrt{2}} & \text{if } f(0) \neq f(1). \end{cases}$$

Finally,

$$s_4 = \begin{cases} \pm|0\rangle \otimes \frac{|0\rangle-|1\rangle}{\sqrt{2}} & \text{if } f(0) = f(1), \\ \pm|1\rangle \otimes \frac{|0\rangle-|1\rangle}{\sqrt{2}} & \text{if } f(0) \neq f(1). \end{cases}$$

Now it suffices to measure the first qubit. The eigenvalue of $|0\rangle$ will disclose that f is constant, the eigenvalue of $|1\rangle$ the opposite.

Deutch's algorithm shows the basic idea of all quantum algorithms: the superposition of states allows, in a sense, to compute many values at the same time. Note that after the Hadamard transforms, a combination of all basis vectors enters the gate U_f.

On the other hand, this alone does not mean that after the evaluation of the combination we have a direct approach to any value we wish to know, since there is no obvious way to extract the desired information from the result. For example, if we measured the first qubit of the state s_3, we would get both eigenvalues with the same probability regardless of f.

4. Quantum information

Information science is not limited to algorithms and solving problems. An equally important task is sending information over a channel, and doing so **efficiently** and often also **secretly**, which gives rise to classical coding theory and cryptology. What happens if we consider a channel which has quantum-mechanical properties, instead of the classical one? Quantum mechanics suggest that quantum systems contain much more information than classical bits. Superposition of states allows parallel transmission of a lot of information. Suppose for example that we want to transmit four bits b_i, $i = 0, \ldots, 3$ of classical information. We can prepare a two qubit system in superposition

$$\frac{1}{2}\sum_{i=0}^{3}(-1)^{b_i}|i\rangle \quad = (-1)^{b_0}\frac{|00\rangle}{2} + (-1)^{b_1}\frac{|01\rangle}{2} + (-1)^{b_2}\frac{|10\rangle}{2} + (-1)^{b_3}\frac{|11\rangle}{2},$$

which contains four bits of information encoded as signs of the basis states. This is a promising idea, but alas, it does not work. The irreparable reason is that it is impossible to gain the information from the system. There is

no way to distinguish reliably between the sixteen possible states suggested above. By a measurement we obtain again just two bits of information, and maybe not even that, if the measurement is not reasoned: we have already seen that to measure the state

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

yields no information at all, since the outcome is a completely random bit. The problem is that each measurement, by Postulate 3, is destructive. Some information is always lost as soon as we measure a superposition of basis states.

4.1. NO-CLONING THEOREM

One may think of the following solution. Make many copies of the received state, and then by many different experiments, for example by repeated measurements in different bases, learn what the original state was like. Unfortunately, this idea does not help either. Quantum mechanics prohibits copying states! More precisely, it allows to make a copy only of basis states, which corresponds to the classical copying of information, and hence does not yield an advantage. The result is known as the No-cloning theorem, and we are going to prove it.

First we have to formulate the claim properly. Suppose we have an unknown state $|u\rangle$ and want to copy it. This means we want to implement the transformation

$$|u\rangle \otimes |0\rangle \quad \overset{U}{\longmapsto} \quad |u\rangle \otimes |u\rangle.$$

The choice of $|0\rangle$ as the "blank state" is arbitrary, but it has to be firm. We do not know anything about u, and therefore cannot choose the blank state to somehow fit the copied one.

By Postulate 2, the transformation has to be unitary. The No-cloning theorem now claims that if U is a unitary transformation then the desired copying equality holds only for two states $|a\rangle$, $|b\rangle$.

To prove the theorem let

$$\begin{aligned} U(|a\rangle \otimes |0\rangle) &= |a\rangle \otimes |a\rangle, \\ U(|b\rangle \otimes |0\rangle) &= |b\rangle \otimes |b\rangle. \end{aligned}$$

Consider now a general state $\alpha|a\rangle + \beta|b\rangle$. Since U is a linear operator, we have

$$\begin{aligned} U((\alpha|a\rangle + \beta|b\rangle) \otimes |0\rangle) &= \alpha \cdot U(|a\rangle \otimes |0\rangle) + \beta \cdot U(|b\rangle \otimes |0\rangle) \\ &= \alpha \cdot |a\rangle \otimes |a\rangle + \beta \cdot |b\rangle \otimes |b\rangle. \end{aligned}$$

Suppose that U copies $\alpha|a\rangle + \beta|b\rangle$. Then also

$$\begin{aligned} U(\alpha|a\rangle + \beta|b\rangle) \otimes |0\rangle &= (\alpha|a\rangle + \beta|b\rangle) \otimes (\alpha|a\rangle + \beta|b\rangle) \\ &= \alpha^2 \cdot |a\rangle \otimes |a\rangle + \alpha\beta|a\rangle \otimes |b\rangle + \beta\alpha|b\rangle \otimes |a\rangle + \beta^2 \cdot |b\rangle \otimes |b\rangle. \end{aligned}$$

Comparing the two expressions it is obvious that either α or β is zero, which completes the proof.

4.2. QUANTUM CRYPTOGRAPHY

So far we have spoken about drawbacks of quantum information, which essentially follow from the destructive nature of the measurement. That very feature, however, turns out to be very useful from the security point of view. In short, if an eavesdropper intercepts a quantum channel he or she cannot escape unnoticed.

We describe the cryptography protocol BB84, which exploits this basic idea. The name of the protocol comes from the fact that it was published by C. H. Bennett and G. Brassard in 1984 (Bennett and Brassard, 1984). The aim of the protocol is to exchange a secret key over a public quantum channel. The key can be subsequently used for other cryptography tasks.

Suppose $\mathcal{A}$ and $\mathcal{B}$ want to exchange a secret key of length n. Then $\mathcal{A}$ generates two sequences $b_1, \ldots, b_m$ and $c_1, \ldots, c_m$ of $m = \delta n$ random bits. The number δ has the following significance: during the protocol many transmitted qubits will be discarded. Therefore δ is chosen so that at least n usable bits remain with required high probability.

$\mathcal{A}$ then encodes each bit by a qubit in the following way. Denote

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \qquad\qquad |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

There are now two possibilities to encode each bit b_i by a qubit $|u_i\rangle$:

$$\begin{array}{ll} 0 \mapsto |0\rangle & \\ 1 \mapsto |1\rangle & \end{array} \quad \text{or} \quad \begin{array}{ll} 0 \mapsto |+\rangle & \\ 1 \mapsto |-\rangle & \end{array}.$$

$\mathcal{A}$ choses the encoding according to the values of c_i. If $c_i = 0$, the bit b_i is encoded by $|0\rangle$ or $|1\rangle$, if $c_i = 1$, by $|+\rangle$ or $|-\rangle$. All qubits are now transmitted through a public channel to $\mathcal{B}$, which measures $|u_i\rangle$ in a randomly chosen basis d_i.

If $d_i \neq c_i$, the outcome is a useless random number. If, on the other hand, $d_i = c_i$, the output is equal to the input. After the measurement, both $\mathcal{A}$ and $\mathcal{B}$ make their sequences of basis choices c_i and d_i public. It is

now clear which bits are usable for the shared secret. Suppose there are at least $2n$ of them (which happens with high probability depending on δ).

In the control stage $\mathcal{A}$ and $\mathcal{B}$ randomly choose half of the usable bits to check publicly, seeing whether the values agree. They should agree, and if they do not the channel was intercepted (or is otherwise unreliable). Therefore, if a disagreement in some chosen number t of control bits appears, the exchange is discarded.

The eavesdropper $\mathcal{E}$ is successful on the j-th bit only if $c_i = d_i = e_i$, where e_i is the basis in which $\mathcal{E}$ measured $|u_i\rangle$, and only if the bit was not chosen for the control. Since the basis in which the bit is encoded is random and is disclosed only after the transmission, the interception by $\mathcal{E}$ will, with high probability, cause a detectable disturbance of the transmitted signal.

Note that the No-cloning theorem plays an important role here. Even if the transmission of the signal is public, an eavesdropper cannot make a copy of it for further inspection.

4.3. PRACTICAL REALIZATIONS

Although the theory of quantum information is very nice, there is an obvious question: How much of the theory can be implemented? The effort to build quantum computers by such research giants as IBM, the U.S. Department of Defense and the NEC Electronic Corporation is extremely intense. The opinions on the practicality of quantum computers differ from scientist to scientist, and the situation is changing very quickly.

The difficulties encountered are enormous, and it is hard to say whether they are substantial, or whether everything is just a question of technology development. The theoretical results described in this chapter are experimentally verifiable. The main problem is that quantum systems are very unstable. Quantum mechanics works for *closed* quantum systems and it is difficult to avoid an interaction of the system with the environment, and to keep the system under control. For reasonably large systems this is impossible so far. In 2001 IBM announced an experimental realization of 7 qubit computation which implemented Shor's algorithm to verify that $15 = 3 \cdot 5$. At the moment, however, it seems that the approach used in this experiment cannot be extended beyond 10 qubits.

The approach is called *Nuclear magnetic resonance* (NMR), which handles large number of molecules (about 10^8), which produce a macroscopically detectable signal. An alternative approach is called *ion trap*, and deals with single atoms cooled to a very low temperature. This approach seems to be more promising at the moment. In December 2005 researchers from the University of Michigan announced that they constructed an ion trap using a technology similar to classical chips (Stick et al., 2006).

In the area of quantum communication the situation is much more optimistic. The first computer network in which communication is secured with quantum cryptography was unveiled in 2004 in Cambridge, Massachusetts. It is based on optic fibers and covers a distance of about 10 km. Quantum key distribution described in this chapter was experimentally demonstrated in 1993 for a distance of several tens of kilometers. However, at the present time the maximum is about 50 km due to weakening of the signal.

References

Bennett, C. H. and Brassard, G. (1984) Quantum cryptography: Public key distribution and coin tossing, In *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, pp. 175–179.

Bohr, N. (1935) Can Quantum-Mechanical Description of Physical Reality be Considered Complete?, *Phys. Rev.* **48**, 696–702.

Cleve, R., Ekert, A., Macchiavello, C., and Mosca, M. (1998) Quantum algorithms revisited, *R. Soc. Lond. Proc. Ser. A* **454**, 339–354.

Deutsch, D. and Jozsa, R. (1992) Rapid solution of problems by quantum computation, *Proc. Roy. Soc. London Ser. A* **439**, 553–558.

Einstein, A., Podolsky, B., and Rosen, N. (1935) Can Quantum-Mechanical Description of Physical Reality be Considered Complete?, *Phys. Rev.* **47**, 777–780.

Gruska, J. (1999) *Quantum computing*, Advanced Topics in Computer Science Series, McGraw-Hill International (UK) Limited, London.

Hirvensalo, M. (2001) *Quantum computing*, Natural Computing Series, Berlin, Springer-Verlag.

Nielsen, M. A. and Chuang, I. L. (2000) *Quantum computation and quantum information*, Cambridge, Cambridge University Press.

Stick, D., Hensinger, W. K., Olmschenk, S., Madsen, M. J., Schwab, K., and Monroe, C. (2006) Ion trap in a semiconductor chip, *Nature Phys.* **2**, 36–39.

Turing, A. M. (1936) On computable numbers, with an application to the entscheidungs problem, *Proc. Lond. Math. Soc.* **43(2)**, 230–265.