QUANTUM INFORMATION PROCESSING

Jozef Gruska
Fakulta informatiky, Masarykova univerzita
Botanická 68a, 60200 Brno, Czech Republik[1]

Progress in science is often done by pessimists.
Progress in technology is always done by optimists.

ABSTRACT

All information processing that is currently performed, and even within such futuristic ideas as *DNA computing* and *molecular computing*, is actually done within the framework of classical physics. Information is stored, processed and transmitted using the elements, sources, processes, laws and limitations of the classical physics.

A new dimension to information processing and communication has appeared recently and it is currently very vigorously explored. The basic aim is to find out how to make use of elements, phenomena, resources, processes, laws and limitations of the quantum microworld to store, process and transmit information in a more efficient and more secure way as currently. Various methods and tools have been already found how to utilize laws and limitations of quantum Nature, and of the information processing that is going on in the quantum world, to make quantum computations and communications more efficient, (quantum) channels to have larger capacity, and (quantum) cryptography to be more secure than the classical one.

In the first part of the tutorial, the most basic properties of the classical and quantum information will be introduced and compared, and an introduction will be made into new concepts, principles and limitations on which quantum information processing and communication are based.

[1]Paper was written during the author stay with the Imai Quantum Computing Project, Tokyo and their support, as well as support of the grant GACR 201/01/041 is to be much acknowledged.

In the second, and the main part of the tutorial, several main outcomes of quantum information processing research will shortly be presented and discussed in several basic areas: quantum algorithms, quantum cryptography, quantum entanglement, quantum communication, quantum decoherence fighting and quantum processors. We will also discuss some very speculative directions of research that can be seen as the frontiers of the field.

For more detailed presentation of quantum computing see the book by Gruska (1999), and its regular updatings (more than 170 pages in August, 2002) on http://www.mcgraw-hill.co.uk/gruska, and by Chuang and Nielsen (2000), as well as the expository papers by Gruska (1999a, 2000) and Gruska et al. (2002),

1 Introduction

In the last ten years an enormous progress has been made in quantum information processing and communication.

Ten years ago only few very theoretical results were available with almost no indication that a rapid development and important outcomes for science and technology could follow soon. Landauer's thesis (*Information is physical*) was already known, but on a more specific level we had only Deutsch's (not yet fully satisfactory) model of the (universal) quantum Turing machine, a very simple Deutsch's quantum algorithm for a toy problem, a very simple cryptographic key-generation experiment and with hardly nobody who could imagine to have soon some (reliable) implementation of quantum gates.

After 10 years, we have a rapidly developing area in which about 350 papers are produced per month. An area with flourishing and increasingly broad theory already rich on deep, surprising, thoughts provoking and lasting results. We have a variety of techniques and technologies allowing already some elementary experiments to be performed (and very ambitious goals to put on the research and development agenda). We have quantum cryptography, aiming on unconditionally secure communication (with perfect detection of eavesdropping), approaching already a developing phase (recently, transmission of photons through optical fibers to distance 67 km has been reported by N. Gisin and through open air in night time to distance 23.4 km by H. Weinfurter). Projects of ground-satellite or plane-satellite cryptography communication are under way. NMR (Nuclear Magnetic Resonance) and quantum optics have been technologies used so far for most of the experiments, though future seems to be in solid-state technologies, where recently quite a few of ideas have been reported in developing various ways how to store, process and transform quantum information in a robust and reliable way. Shor's and Grover's algorithms made revolution in algorithmic design and threatened to break main current cryptosystems, provided quantum computers would be available. Moreover, in the last few years, the whole field of the quantum information processing and communication (QIPC) science and technology started to change (slowly) from the theory driven to the experiments driven field, what can be seen as a positive feature, especially from the point of view of developing new quantum information technologies.

There have been several other important impacts of the developments in QIPC. A fundamentally new view of physics started to be developed. Namely, that **physics is informational**. That is, that the investigation of information processing laws and limitations of Nature may be an important new (or even the key) way to understand Nature (and, perhaps, also to develop a theory of Nature that could be used to understand both physical and biological world).

In general, QIPC is a rapidly developing interdisciplinary research area that encompasses many disciplines such as physics, computer science, engineering, mathematics, chemistry and so on. It seems to have potential to revolutionize Information technology, to develop Quantum Information Technology and by that to have very broad impact on science, technology and society in large.

It is also interesting and useful to realize the following paradox:

- Quantum physics is extremely elaborated theory, full of paradoxes and mysteries. It takes any physicist years to develop a **proper feeling** for quantum mechanics.
- Some (theoretical) computer scientists/mathematicians, with almost no background in quantum physics, have been able to make **crucial** contributions to the theory of quantum information processing.

First moral out of that is that a proper mathematical simplification of reality may have enormous value and can allow to see laws and limitations of nature that can hardly be recognized when working with the full view of reality.

Second moral is that in order to understand and make significant contribution to quantum information processing, you do not need to go deep into quantum physics. Similarly, as to do significant contribution to classical information processing, you do not need to understand physics of transistors, memory and transmission channels.[2]

2 Quantum versus classical information

There are several fundamental differences between classical and quantum information and let us discuss them briefly even before we make clear what it is meant by the term *quantum information*[3].

[2]On a more technical and deeper level one should notice that in quantum information processing we (mostly) deal with discrete and finite dimensional systems. However, much of difficulties in learning deeply quantum mechanics is connected with the fact that it deals with continuous, infinite-state systems in 4-dimensional space-time. Moreover, the hardest part in learning quantum mechanics is to develop proper feeling how to relate quantum formalism to actual quantum phenomena (Mermin 2002).

[3]It is actually not easy to define what quantum information is. One of the views (Werner (2001)): *Quantum information is that kind of information which is carried by quantum systems*

The difference between classical and quantum information processing is mainly in the way information is represented and processed.

In **classical computers**, information is represented on **macroscopic level**, by **bits**, which can take on one of the two values

$$0 \qquad \text{or} \qquad 1$$

In **quantum computers**, information is represented on **microscopic level**, using the so called quantum bits, shortly **qubits** (or **qbits**), which can take on any from uncountable many values (states)

$$\alpha|0\rangle + \beta|1\rangle$$

where α, β are arbitrary complex numbers such that

$$|\alpha|^2 + |\beta|^2 = 1.$$

The expression (superposition) $\alpha|0\rangle + \beta|1\rangle$ should be understood as saying that, if measured, the qubit will be in the state 0 with probability $|\alpha|^2$ and in state 1 with probability $|\beta|^2$. (Or that it will be in state 0 with amplitude α and, simultaneously, in the state 1 with amplitude β.)

In addition, a classical n-bit register can be at any moment in one of 2^n states, but a quantum n-qubit register can be simultaneously in a superposition of 2^n of so called basis states $\{|x\rangle \,|\, x \in \{0,1\}^n\}$. This allows, for example, that 200 particles are simultaneously in a superposition of 2^n states what is the number larger than the number of particles in the universe. As a consequence, quantum computation exhibits massive parallelism unimaginable in the classical world.

2.1 Story of the classical information

Before discussing quantum information processing problems, results and potentials, as well as limitations, let us give at first a fresh look to the classical information.

There are several very specific aspects of the classical information. Some of them are well known, but community is, in general, not fully aware of them, others are almost unknown.

Transmission of classical information in time and space is (now) very easy. It took centuries, and many ingenious developments and discoveries

from the preparation device to the measuring apparatus in a quantum mechanical experiment. Observe, that in defining classical information we do not care about physical carriers of information. Actually, success of classical information theory is in that that it abstracts from both information carriers and 'meaning' and it concentrates on studying of laws and limitations of the efficient and faithful information transmition and storage using any classical physics carrier. Similarly, quantum information is investigated on an abstract level, abstracting from specific quantum information carriers.

(writing, book printing, photos, films, television, records, CD-disks, telegraph, telephone, satellites, computer networks, mobile telephones) and the idea of digitalization of all forms of information, to discover fully this property of information.

Making unlimited number of copies of the classical information is extremely easy. This is perhaps the most specific property of classical information and the one that creates headaches to modern information (software) and entertainment industries. A source of enormous potential for mass distribution of information, but also a source of problems related to the protection of intellectual properties.

Information has an information-less theory. Being old only 50 years, and due to Shannon, this is one of the most applied theory of 20th century, without which modern communication and modern methods of the storage of information would not be possible. It is interesting and important to observe that information theory is based on simple formal concepts, having actually nothing to do with the every-day interpretation of the term information. It is actually theory of efficient and secure transmition and storage of data.

Discovery that information is physical. An important step in the development of quantum information science was an observation of Rolf Landauer that **information is physical**. This means that any real information processing systems relies for its implementation upon systems whose behavior is completely described by the laws of physics. This implies that our understanding of the laws and potentials of the information processing power of Nature can change with the discovery of new and more powerful physical theories. Information can be represented in many different physical forms and can be (easily) converted from one representation to another. It exists, in a sense, independently of the devise used to represent it, but it requires at least one physical representation to be useful.

Discovery that acquisition of information does not need energy but its removal does. Around 1970, Rolf Landauer discovered perhaps the most counter-intuitive principle concerning classical information. Namely, that information can be processed (acquired) without energy, and therefore, in principes, no-energy-computations are possible. However, erasure of information does require energy.

2.2 Story of quantum information

At the very beginning of the quantum information science story was the curiosity. What is the minimal amount of energy needed to perform computations? The question got of interest around 1970 after it was realized that the main problem at the design of supercomputers is how to get rid of the heat that information processing creates in them. Rolf Landauer discovered, as already mentioned, surprisingly, that information can be acquired without energy, and therefore, principally, theoretically no-energy computations is possible, but erasure of information does have a cost and generates heat.

The next big impulse came when the famous physicist Richard Feynman observed in 1982 that classical computers cannot simulate efficiently quantum processes. Soon afterwards, Turing machine model of quantum computers was developed (Deutsch (1985)) and 7-9 years later, see historical comments in Gruska (1999), it was shown that, for some theoretical problems, quantum computers could be much much faster than the classical ones.

The main killer up for quantum computing so far was the discovery, by computer scientist Peter Shor (1994), that there exist fast quantum algorithms to break modern cryptosystems on which security of our Internet communication is based. Soon after that it was shown that in order to start to design elements of quantum computers one does not have to wait until some extremely special technology, some *unobtainium*, will be discovered, but that basic experiments in quantum information processing can be performed with already developed technologies. For example, with nuclear magnetic resonance, so successfully already used in medicine and chemistry.

It is also interesting to observe that at the very beginning of the development of quantum information science there was a widespread scepticism among experts concerning the possibilities to build really powerful quantum computers, because of the effect called **decoherence** due to which an interaction of the environment with the computation process can very fast so much disrupt the computation processes that it becomes useless. Situation looked really hopeless. However, it was again Peter Shor who showed, in 1995, that there are techniques, called quantum error-correcting codes (QECC) and quantum fault-tolerant networks, that can sufficiently protect quantum system evolution against negative influences of the environment.

Error-correcting codes have been very successful to protect classical communication, but it seemed, from the physics point of view, that there cannot be successful quantum error correcting codes, for the reasons discussed later. Fortunately, it has been shown, once again, that physics itself is not sufficient to understand the laws and limitations of the physical world and that mathematics and informatics can help to turn seemingly impossible into possible.

The development of quantum information science brought later another discovery, formulated by the already mentioned principle that **physics is informational**. This means that information processing concepts, properties and processes of Nature are of the fundamental character and can bring new insights into the laws and limitations of Nature. Moreover, it seems more and more that by studying information processing properties of Nature we get a deeper insight into the laws of limitations of Nature than by studying energy creation and transformation processes.

2.3 Why quantum information processing?

There are four basic reasons why research in quantum information processing and communication (QIPC) is currently so much supported.

- Shor's algorithms, for integer factorization and discrete logarithm computation, showed that quantum computers can be of large importance for solving efficiently important practical problems. For example, for breaking main current public-key cryptosystems.
- Computer industry have realized a necessity to exploit microscopic and quantum phenomena in order to keep improving performance of computers according to the Moore law.
- Various important sciences and industries recognized big needs to increase our knowledge of the microworld and our techniques to manipulate individual particles, atoms and molecules.
- Security of communications and information systems has been recognized as being of the vital importance for the information society.

2.4 Moore law

It is nowadays accepted that information processing technology has been developing for the last 50 years according to the so-called Moore law. This law has now three forms.

Economic form: Computer power doubles, for constant cost, every two years or so.

Physical form: The number of atoms needed to represent one bit of information halves every two years or so.

Quantum form: For certain application, quantum computers need to increase in the size only by one qubit every two years or so in order to keep pace with the classical computers performance increase.

In this connection it is also interesting to observe that also the number of papers produced in quantum information processing, judging from their number at the Los Alamos quantum archive, is doubled every two years or so.

3 Basics concepts of QIP

There are two basic ways to see and to study quantum systems.

- As **closed (pure) quantum systems**, that are isolated from their environment and evolve under idealized rules (according to the Schrödinger equation). The key basic concepts of the closed quantum systems theory are that of *Hilbert space, pure state, unitary operators* and *projective measurements.*
- As **open quantum systems**, that are not isolated from their environment, and, due to their entanglement with the environment, their ideal evolution can be badly disturbed by the environment. The key basic concepts of open quantum systems theory are that of *mixed states, density matrices, superoperators (completely positive linear maps)* and *POVM measurements.*

3.0.1 Closed quantum systems

Closed quantum systems are well modeled by **Hilbert spaces**. A finitely dimensional Hilbert space, say n-dimensional, notation H_n, is a vector space of n-dimensional complex vectors, on which the **inner product**, $\langle x|y\rangle$, of two (column) vectors $x = (x_1, \ldots, x_n)^T$ and $y = (y_1, \ldots, y_n)^T$, is defined by $\langle x|y\rangle = \sum_{i=1}^n x_i^* y_i$.

The norm of a vector x is defined as $\sqrt{\langle x|x\rangle}$. Vectors of norm 1 correspond to the intuitive concept of quantum states. Vectors are usually written, using so called "bra-ket notation", as (column-vectors) "ket-vectors" $|x\rangle$. A "bra-vector" $\langle x|$, corresponding to $|x\rangle$, denotes the functional which to each ket-vector $|y\rangle$ associates the complex number $\langle x|y\rangle$. In other words, bra-vectors $\langle x|$ are row-vectors – row conjugate versions of the column-vectors corresponding to x.

Two quantum states are considered as orthogonal if their inner product is zero. Orthogonality of quantum states is a very important concept, because physically are perfectly distinguishable only orthogonal states.

Evolution of any closed quantum system is described by the Schrödinger equation

$$i\hbar \frac{\partial \psi(t)}{\partial t} = H(t)\psi(t),$$

where $i = \sqrt{-1}$, $\hbar$ is the Planck constant, $H(t)$ is a quantum analogue of the **Hamiltonian** of the classical system in time t, and $|\psi(t)\rangle$ is the state of the system in time t. From that it follows that evolution (computation) of a finite dimensional quantum system is performed by **unitary operators** and a step of such an evolution can be seen as a multiplication of a vector (state) $|\psi\rangle$ by a **unitary matrix**[4] A, i.e. as $A|\psi\rangle$. Unitary operators preserve norms and their eigenvalues have absolute value 1. (Unitary operators on qubits are actually rotations on Bloch sphere.)

Of special importance among unitary operators are the *Hadamard operator* and the *controlled not (CNOT) operator.* They are represented (in the standard basis)

[4] A matrix A is **unitary** if $A \cdot A^* = A^* \cdot A = I$, where A^* is a matrix obtained from A by the transposition and conjugation of its elements. The available set of unitary operations is usually restricted to those that can be composed out of products of simple unitary operators acting either on single qubits or on pairs of qubits.

by matrices H and CNOT defined as follows.

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad \mathrm{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Actually, the science and art of quantum programming, or of using quantum circuits, or processors, to solve a computational problem, is first to express the given computational task to be performed as a unitary matrix, and then to design a quantum circuit, composed of the elementary quantum gates realizable by an available technology, to perform the desirable computation as the multiplication of the input (vector), by the corresponding (unitary) matrix. Interesting enough, the XOR-gate and all unitary gates form a universal set of gates with which any unitary matrix multiplication can be implemented by a quantum circuit.

Remark *It is interesting/important to realize that if A is a unitary matrix, then so is $A^* = A^{-1}$. As a consequence, quantum evolution, represented by unitary matrices multiplication, is reversible.*

In general, we call an operation reversible, if from its outputs one can determine uniquely input arguments. Boolean logic operation NOT is reversible, but AND and OR are not. Interesting enough, so called Toffoli operation (gate) represented by the mapping $(x, y, z) \rightarrow (x, y, ((x \wedge y) \oplus z))$ is universal for designing of reversible Boolean functions.

Computational processes that are reversible seem to be a curiosity. It was therefore a very important step in developing the idea of quantum computing, when Bennet has shown, in 1973, very surprisingly, that any one-tape Turing machine can be simulated by a three-tape reversible Turing machine with only constant slowdown.

As already mentioned, in quantum computing the basic element is a quantum bit (**qubit**), that can take on infinitely many values of the form

$$\alpha|0\rangle + \beta|1\rangle, \quad |\alpha|^2 + |\beta|^2 = 1,$$

where α and β are complex numbers and $\{|0\rangle, |1\rangle\}$ are vectors of a (standard) basis in H_2. A qubit state can be seen as a unit-norm vector of the two-dimensional Hilbert space H_2.[5]

In addition to a *classical bit* (*cbit*), which takes on one of the two values 0 and 1, we can consider also a *probabilistic bit* (*pbit*) that can be seen as a convex combination

[5]To the basic theoretical realizations of qubits belong polarization states of photons, energy levels of electrons in hydrogen atoms, spins of particles, spins of electrons in quantum dots, and so on. (Currently, under exploration are such technologies as atoms trapped (and controlled) on integrated circuits; atoms, ions and photons trapped in microscopic cavities, excitations in semiconductor quantum dots and other nanostructures and coherent magnetic molecules and nanoparticles.) Various microtraps are a promising tool to implement quantum coherent interactions on atomic scale and can be seen as promising ingredients of potential quantum computers. The main task is to find out such implementations at which qubits couple weakly to environment, and have long decoherence time.

of 0, with probability p, and 1 with probability $1-p$. A quantum bit (*qbit* – *qubit*) can then be seen as taking on any values on so called Bloch sphere, at which any qubit of the form $\cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle$ can be represented as the point of the unit sphere with spherical coordinates ϕ and θ.

Another important difference between the classical and quantum systems is in the way systems are composed. A composition of two classical systems, S_1 and S_2, is the **Cartesian product**, $S_1 \times S_2$, of the two systems. Consequently, **any** state of the composed classical system is composed of the states of its subsystems. On the other hand, composition of two quantum systems, S_1 and S_2, is the **tensor product**, $S_1 \otimes S_2$, of the two systems. Consequently, **not any** state of the composed quantum system is composed of the states of subsystems. This apparently subtle difference between classical and quantum systems has surprisingly deep implications.

If a Hilbert space H_1 corresponds to a quantum system S_1 and a Hilbert space H_2 corresponds to a quantum system S_2, then the tensor product $H_1 \otimes H_2$ of H_1 and H_2 corresponds to the composed quantum $S_1 \otimes S_2$. (If the Hilbert space H_1 (H_2) has, as a vector space, basis $\{\alpha_i\}$ ($\{\beta_i\}$), then the tensor products of vectors[6] α_i and β_j form a basis of $H_1 \otimes H_2$.

Tensor product of n two-dimensional Hilbert spaces (qubits) is said to be an n-qubit quantum register.

A general state of an n-qubit register has, therefore, the form of a superposition

$$|\phi\rangle = \sum_{x\in\{0,1\}^n} \alpha_x|x\rangle, \qquad \sum_{x\in\{0,1\}^n} |\alpha_x|^2 = 1,$$

where $\{|x\rangle\}_{x\in\{0,1\}^n}$ represents a set of 2^n (standarad) basis states in H_{2^n} with $|x\rangle$ standing for $|x_1\rangle \otimes |x_2\rangle \otimes \ldots \otimes |x_n\rangle$ if $x = x_1x_2\ldots x_n \in \{0,1\}^n$. A multiplication by a $2^n \times 2^n$ matrix corresponds to a computation step on n qubit registers.

Power of quantum information processing is to large extend connected with **quantum superposition** and **quantum parallelism** - a possibility to perform, using quantum superposition, in a single quantum step, in a sense, many classical operations. For example, for any classical function

$$f : \{0,1,\ldots,2^n-1\} \to \{0,1,\ldots,2^n-1\}$$

there exists a unitary operator U_f such that for any $x \in \{0,1\}^n$,[7]

$$U_f(|x\rangle|0^{(n)}\rangle) = |x\rangle|f(x)\rangle.$$

[6]Tensor product of two vectors $x = (x_1,\ldots,x_n)$ and $y = (y_1,\ldots,y_m)$ is the mn-dimensional vector $x \otimes y$ with components $(x_1y_1,\ldots,x_1y_m,x_2y_1,\ldots,x_ny_m)$. Tensor product of two matrices, $A = \{a_{ij}\}$ of dimension n and $B = \{b_{ij}\}$ of dimension m is the matrix C, of dimension mn, composed of matrices $c_{ij} = a_{ij}B$.

[7]This time we take x simultaneously as a string and as a representation of an integer in the range $\{0,\ldots,2^n-1\}$.

Moreover, in a single quantum step, using the tensor product H_n of n Hadamard operators H, that is with only a linear amount of physical resources, we can get from the state $|0^{(n)}\rangle|0^{(n)}\rangle$ to the state

$$|\phi\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle|f(x)\rangle, \tag{1}$$

and therefore all 2^n values of f are "computed" in a single step. (The catch is that by any measurement of $|\phi\rangle$ we can get only one out of all values of f. However, for some applications, this does not cause a problem and leads indeed to a significant speed-up — comparing with the classical computations.)

Another key concept of pure quantum systems is that of quantum **(projection) measurement** or **von Neumann measurement**. If a state $|\phi\rangle$ is measured with respect to an **observable** represented by an orthonormal basis $\{|\beta_i\rangle\}$, then, on the quantum level, as the result of the measurement, a *collapse* of $|\phi\rangle$ to one of the basis states, say $|\beta_i\rangle$, happens, and, on the classical level, information is obtained to which of the states $|\beta_i\rangle$ the collapse happened. $|\langle\phi|\beta_i\rangle|^2$ is then the probability that $|\phi\rangle$ collapses into the state $|\beta_i\rangle$ (so called the *Born rule*). In its most general form, an observable (a measuring device) is represented by a Hermitian operator A (that is such an operator A that $A^* = A$).[8]

One can also measure particular bits or parts of a quantum register. For example, if, in the state (1), the last register is measured, then the classical outcome of such a measurement is a specific y in the range of function f, and the overall state collapses to the state

$$\frac{1}{\sqrt{k}} \sum_{\{x\,|\,f(x)=y\}} |x\rangle|y\rangle,$$

where $k = |\{x\,|\,f(x) = y\}|$.

Quantum measurement is actually a way how to get classical information, that is the one people work with, from quantum information.

3.0.2 Open quantum systems

In open quantum systems, in which there is an interaction of the system with the environment, the very basic concepts are that of **mixed states** and of **density matrices**.

A mixed state is a probability distribution on pure states – what correspond to the case that a source produces various pure states, each with a fixed probability.

A density matrix ρ is defined by $\rho = \sum_{i=1}^{k} \lambda_i|\phi_i\rangle\langle\phi_i|$, where $|\phi_i\rangle$ are pure states and $\sum_{i=1}^{k} \lambda_i = 1$, with all $\lambda_i > 0$. Such a density matrix is said to correspond to the mixed state at which the pure state $|\phi_i\rangle$ is produced with the probability λ_i.

[8] Observe that in the classical computing measurement plays so trivial role (one just reads (or displays, or prints out) the outcome) that it is mostly not recognized as an important part of the computation process.

Of importance is the fact that two mixed states with the same density matrix are physically non-distinguishable. Therefore, the concepts of mixed states and density matrices are often used as synonyms.

Two operations on (density) matrices are of key importance for open quantum systems theory.

Trace of a matrix A, notation $Tr(A)$, is the sum of diagonal elements of A. One physical meaning of the trace operation is that the average value of the measurement of a mixed state ρ with respect to an observable A is given by $Tr(A\rho)$.

Tracing out a quantum system B from a density matrix ρ of a bipartite quantum system $A \otimes B$, notation $\rho_A = Tr_B(\rho)$, is a density matrix that shows how the state ρ is seen from an observer that see only the quantum system A.[9]

Superoperators are the most general physical operators that can be performed on open systems. Formally, they are completely positive (trace preserving) linear operators on density matrices. Less formally, superoperators are combinations of the following physical operators: (a) composition of a given quantum system with a new (auxiliary) quantum system, called usually an **ancilla**, and creation in that way of an extended quantum system; (b) unitary operators performed on the extended quantum system; (c) projection measurement on the extended quantum system; (d) deletion of the ancilla.

On open quantum systems one can also perform so called **POVM-measurements** - positive operator valued measure measurements. They can be seen as the projection measurements performed on extended quantum systems, created using some auxiliary ancilla, followed by the deletion of the ancilla.

4 Basic quantum limitations

Quantum mechanics imposes on quantum information processing several very special and severe limitations. This is a bad news. A good news is that there is a way to utilize these limitations in important positive ways.

Heisenberg's uncertainty principle. For some pairs of physical quantities, for example for position and momentum, there is no way to measure simultaneously both of them with an arbitrary precision.

No-cloning principle. Quantum information cannot be copied faithfully. (This is an extremely severe limitation, that has far reaching impacts and we will discuss them later.)

Non-demolition measurement principle. There is, in general, no way to measure quantum states without perturbing them.

[9] Technically, if dimension of A (B) is n (m), then ρ_A is obtained from ρ, if, in the decomposition of ρ into submatrices of dimension m, each submatrix is replaced by its trace, that is by a single number.

Holevo's principle. There is no way to store more than n bits in an n-qubit register in such a way that one can read out all of them faithfully.

5 Quantum entanglement

Informally, entanglement is a feature of quantum objects that allows particles to exhibit much closer correlations than classical objects exhibit. For example, due to quantum entanglement a measurement of one particle of an entangled system determines instantaneously a property of the related entangled particles, even if they are far away.

Quantum entanglement is arguably the most inherently quantum feature of quantum information, computation and communication – a feature that is at heart of quantum physics. Quantum entanglement is also increasingly often considered as an important physical resource that is, to a very large extent, behind new and surprising power quantum computations and communications exhibit – comparing to the classical computation and communication.

Quantum entanglement used to be seen, practically till 1996, especially due to the accompanying non-locality impacts, as being behind various mysteriously looking and weird phenomena of quantum world, and of interest mainly only to the philosophers of science. Since then, our perception of entanglement has changed significantly. Currently, quantum entanglement is increasingly believed to be a resource that can be exploited to implement various quantum information processing tasks, at spatially separated locations, and to be behind new **gold mine for science and technology** to which the outcomes of the research in quantum information science and quantum information technology seem to pave the road.

Quantum entanglement is considered to be of large importance for theory and practice of quantum information processing because it allows:

- to perform tasks that are not possible otherwise;
- to speed-up some computations;
- to economize (even exponentially) communications;
- to increase capacity of (quantum) communication channels;
- to implement perfectly secure communications;
- to develop more general and more powerful theories of computations and communications than the framework of classical physics allows;
- to develop a new and better understanding of the key quantum phenomena and, by that, a deeper, information processing based, understanding of Nature.

5.1 Formal definitions

The definition of entanglement of pure bipartite states is simple and quite natural.

A pure state $|\phi\rangle$ of a bipartite quantum system $A \otimes B$ is **entangled** if $|\phi\rangle$ is not a tensor product of a pure state from A and a pure state from B. An example of such a state is the so called *EPR state*

$$|\mathrm{EPR}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

of the quantum system $H_2 \otimes H_2$.

In general, two qubit state

$$a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$$

is not entangled if and only if $ad - bc = 0$.

The case of entanglement of mixed states of bipartite systems seems to be slightly less natural. A mixed state ρ is **entangled** if ρ cannot be written as a convex combination of the tensor products of mixed states

$$\rho = \sum_{i=1}^{k} p_i \rho_{A,i} \otimes \rho_{B,i},$$

where $\rho_{A,i}$ ($\rho_{B,i}$) are mixed states of the quantum system A (B).

Actually, in both definitions there is the same idea behind: a state is entangled if it cannot be created by two parties provided they perform quantum operations only on their subsystems and, in addition, they communicate only classically. In other words, a state is entangled if it is correlated not only classically.

Both definitions generalize naturally to the case of multipartite systems. However, it has turned out that it is useful to consider many different types of multipartite entanglement. An entangled state of an m-partite quantum system $S_1 \otimes S_2 \otimes \ldots \otimes S_m$ is called $(\mathcal{M}_1 : \mathcal{M}_2 : \ldots : \mathcal{M}_k)$-separable, where $\mathcal{M}_1, \mathcal{M}_2, \ldots, \mathcal{M}_k$ is a partition of the set $\{1, 2, \ldots, m\}$, if it is separable with respect to the tensor product of the quantum system $S_{\mathcal{M}_i}$ that are themselves tensor products of quantum systems $\{S_j \mid j \in \mathcal{M}_i\}$.

Example The so-called Smolin (2000) state

$$\rho_s = \frac{1}{4}\sum_{i=1}^{4} |\Phi_i\rangle\langle\Phi_i| \otimes |\Phi_i\rangle\langle\Phi_i|,$$

where $\{|\Phi_i\rangle \mid i \in \{1, 2, 3, 4\}\}$ are all Bell states (to be defined on page 19), is entangled in the Hilbert space $A \otimes B \otimes C \otimes D$, where A, B, C, D are two dimensional Hilbert spaces, but it is $\{A, B\} : \{C, D\}$-separable, $\{A, C\} : \{B, D\}$-separable and also $\{A, D\} : \{B, C\}$-separable.

An important fact is that if a pure state of n qubits is entangled, then particular qubits may not be in any pure state. However, they are in a mixed state that can be obtained from the pure state by tracing out the remaining qubits. For example, if two particles are in the EPR-state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, then none of particles is in a pure state, but each of them is in the following mixed state: $|0\rangle$ with probability $1/2$ and $|1\rangle$ with the same probability, represented by the density matrix $\frac{1}{2}I$, where I is the unit matrix.

Now we can summarize in the following table (adopted from Mermin (2002)) main differences between classical bits and qubits.

Bits versus qubits	bits	qubits
States of n bits	$x, 0 \leq x \leq 2^n$	$\sum \alpha_x \|x\rangle$
Subsets of n bits	always have states	generally have no states
Reversible operations	permutation	unitary operations
Can the state be learnt?	yes	no
How to get information	just look	measure
Information obtained	x	x with prob. $\|\alpha_x\|^2$
State after infor. is obtained	the same x	different $\|x\rangle$

5.2 Power of entanglement

There are several ways power of entanglement has already been demonstrated.

5.2.1 Speeding-up quantum computations

It is intuitively clear that entanglement plays an important role in many quantum algorithms that exhibit much better performance than known classical algorithms for the same tasks. It is less clear how to demonstrate such intuition formally and convincingly.

In case of pure states, it is already clear that without possibility to have states with increasingly growing multipartite entanglement we cannot have an exponential speed up comparing to the classical case. This follows from the results of Jozsa and Linden (2002) presented bellow.

Definition For a given integer p a pure state of n qubits is said to be p-blocked if no its $p+1$ qubits are entangled (after tracing out the remaining qubits).

Theorem Consider any quantum computational process on **pure** states (with increasing input size n). Suppose there is an p such that states produced during the computation of the algorithm are p-blocked at every stage. Then the computation can be classically simulated in polynomial time.

Corollary Increasing multipartite entanglement is necessary for exponential quantum speed-up (on pure states).

However, it is not clear whether a necessity of increasingly growing entanglement can be demonstrated also in the case of computations with mixed states.

Let us now mention some of the main success in the design of efficient quantum algorithms

1. Deutsch (1985) showed that it is sufficient to use one quantum query to determine whether a function
$$f : \{0,1\} \rightarrow \{0,1\},$$
given as a black-box, is constant or not, Classically, two queries are needed.

2. Deutsch and Jozsa (1992) showed that it is sufficient to use one quantum query to decide whether a function
$$f : \{0,1,\ldots,2^n - 1\} \rightarrow \{0,1\},$$
given as a black-box, is constant or not, given a promise that f is either constant or balanced. Classically, up to $2^{n-1}+1$ queries may be needed for any deterministic algorithm (though polynomial time randomized algorithm does exist to solve the problem).

3. Simon (1994) showed polynomial time quantum algorithm to determine for any function $f : \{0,1,\ldots,2^n - 1\} \rightarrow \{0,1,\ldots,2^n - 1\}$, given as a black-box, such an s that $f(x) = f(y)$ iff $x = y \oplus s$, given a promise that such a single s exists. Classically, no polynomial time randomized algorithm for this problem exists.

4. Shor (1994) designed polynomial time quantum algorithm to factorize integers — what would allow to break the RSA cryptosystem – no classical polynomial time algorithm for factorization is known. (Shor and other showed that quantum computers could break also other well known public-key cryptosystems.)

5. Grover (1996) showed that quantum search in an unordered database of n elements can be done with $\sqrt{n}$ queries — that would allow to break the DSA cryptosystem – while classically n queries may be needed.

6. For several other computational and simulation problems, for which no classical polynomial time algorithm is known, polynomial time quantum algorithms (simulation of quantum systems, sampling wavelet transforms). For example, for solving so called Pell equation.

5.3 Entanglement as a computation primitive and (super)catalyst

There are several other ways entanglement is of importance for quantum information processing.

- Gottesman and Chuang (1999) have shown that entanglement is a computational primitive because it is possible to realize any quantum computation by starting with some GHZ states ($\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$ and then to perform one-qubit operations and Bell measurements.

  Rausschendorf and Briegel (2000) have shown that universal quantum computation is possible by starting with a proper multipartite entangled state (a sort of a *computational substrate*) and then performing only one-qubit measurements.

- Entanglement can also serve as a catalyst – it can allow to perform quantum processes that are otherwise impossible, and in such a way that entanglement used at the process, as a *catalyst*, is not consumed by the process itself and, therefore, it can be "returned back", after the process terminates.

  Indeed, Jonathan and Plenio (1999) have shown that there are pairs of pure states $(|\phi_1\rangle, |\phi_2\rangle)$ such that using local quantum operations and classical communications (LOCC) one cannot transform $|\phi_1\rangle$ into $|\phi_2\rangle$, but with the assistance of an appropriate entangled state $|\psi\rangle$, as a catalyst, one can transfer $|\phi_1\rangle$ into $|\phi_2\rangle$, using LOCC, in such a way that the state $|\psi\rangle$ is not changed in the process.

  Moreover, as shown by Bandyopadhyay and Roychwdhury (2001), entanglement can serve as a **super-catalyst** that not only allows to perform operations otherwise impossible, but that during such a process the catalyst can even increase its entanglement.

5.3.1 Making communication more efficient

There are six basic ways entanglement can bring new quality to communication. Three of them will now be discussed shortly. The other three: quantum teleportation, quantum cryptography and quantum error-correcting codes will be discussed in more details later.

Decreasing communication complexity For some communication complexity tasks quantum communication can be much more efficient than the classical ones.

For example, for the following **dating problem**: Alice and Bob have diaries for next n days specifying for each evening whether they are free (1) or busy (0) that evening. How many bits they need to exchange in order to find out a day in which they could spent evening together?

Communicating only classically, Alice and Bob need to exchange n bits in the worst case. When communicating quantumly, $\mathcal{O}(\sqrt{n}\lg n)$ bits are sufficient to solve the dating problem (Buhrman et al. (1998)).

In some other cases, less natural so far, as shown by Raz (2000), exponential speed-up can be obtained using quantum communication.

Increasing capacity of quantum channels: If two communicating parties share some entangled states, then communication capacity of their channel can be increased and there is no upper bound how big increase can be (Bennett et al. (1999)). Surprisingly, from several capacities that have been defined for channels with quantum inputs and outputs, entanglement assisted capacity is the only one that we already know how to compute.

5.3.2 Making strategies in quantum games more powerful

Quantum entanglement has turned out to be of importance also in the case of mathematical games. In the case players are allowed to share entangled states their quantum strategies (that is their moves realized by performing quantum operations) can be more powerful than classical strategies. This seems to be the case especially for multi-players games. This has been illustrated, for example, on the *minority game*,[10] by Hayden et al. (2001). Recently, there have appeared many papers studying quantumization of particular games, such as *Battle of sexes*, *Prisoner dilemma* and so on. A more general approach to quantum games has already been worked out and several quantum versions of the main theorems of the classical game theory have been presented by Lee and Johnson (2002).

5.4 From the classical to quantum teleportation

Discovery of quantum teleportation has been so far one of the major results that demonstrated power of entanglement as of an information transmission resource.

5.4.1 Classical teleportation

The so called **No-teleportation theorem**, one of the fundamental laws of quantum mechanics, says that **(classical) teleportation** is impossible. This means that there is no way to use classical channels to transmit faithfully quantum information.

In more technical terms, there is no possibility to measure, in general, a single copy of quantum state in such a way that the classical outcomes of the measurement would be sufficiently to reconstruct faithfully the state.

Indeed, the classical teleportation would imply that **quantum cloning is possible** and this would imply that *super-luminal communication* is possible.

5.4.2 Quantum teleportation

In contrast to the classical no-teleportation theorem, quantum teleportation is possible, as theoretically demonstrated by Bennett et al. (1996).

[10] In the minority game each party can choose 0 or 1. In case minority of parties choose 0, all of them get 1 point, otherwise nobody gets a point.

Indeed, let us assume that two parties, called in quantum computing usually Alice and Bob, share two particles, P_A and P_B, in the EPR state

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle$$

and Alice gets a new particle P_u, in an unknown state $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$, to teleport. The total state of the system of three particles P_A, P_B and P_u, is then, after a proper rearrangement of terms,

$$\begin{aligned}|\phi\rangle|EPR\rangle &= \frac{1}{2}|\Phi^+\rangle(\alpha|0\rangle + \beta|1\rangle) + \frac{1}{2}|\Psi^+\rangle(\beta|1\rangle + \alpha|0\rangle) \\ &\quad + \frac{1}{2}|\Phi^-\rangle(\alpha|0\rangle - \beta|1\rangle) + \frac{1}{2}|\Psi^-\rangle(-\beta|0\rangle + \alpha|1\rangle),\end{aligned}$$

where

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \qquad |\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle),$$
$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \qquad |\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle).$$

are so-called Bell states (that form a (Bell) basis in H_4). If now Alice performs a measurement of her two particles, with respect to the Bell basis, then Bob's particle state collapses, with equal probability, to one of the states

$$\alpha|0\rangle + \beta|1\rangle, \quad \alpha|1\rangle + \beta|0\rangle, \quad \alpha|0\rangle - \beta|1\rangle, \quad -\alpha|1\rangle + \beta|0\rangle$$

and Alice gets information, 2 bits, which of the four potential outcomes of the measurement has happened. If Alice then sends these two bits, using a public classical channel, to Bob, then he can achieve that his particle gets into the state that was teleported by just performing on his particle, depending on two bits received, one of the following Pauli operators[11]

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \sigma_y = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Comments on teleportation

- Alice can be seen as dividing information contained in $|\phi\rangle$ into quantum information - transmitted through the EPR channel — and the classical information - transmitted through a classical channel.

[11]Pauli operator σ_x (σ_z) actually stands for a bit (sign) error on a qubit. The fact that quantum errors can actually be decomposed to bit and sign errors is behind the fact that powerful quantum error correcting codes do exist.

- In a quantum teleportation, an unknown quantum state $|\phi\rangle$ can be disambled into, and later reconstructed from, two classical-bit-states and a maximally entangled pure quantum state.

- Using quantum teleportation, an unknown quantum state can be *teleported* from one place to another by a sender who does not need to know — for teleportation itself — neither the state to be teleported nor the location of the receiver.

- The teleportation procedure cannot be used to transmit information faster than light, but it can be argued that quantum information presented in unknown state is transmitted instantaneously (except the two random bits to be transmitted at the speed of light, at most).

- EPR channel is irreversibly used up during the teleportation process.

- At the end of teleportation, the particle P_u is in a mixed state that corresponds to a random bit and therefore Alice has nothing. In some sense, the state that is teleported is deleted from Alice's particle and imposed on Bob's particle.

A process inverse to teleportation, in which one qubit is used to send two bits, is called **superdense quantum coding**.

For teleportation we assume that parties share pure maximally entangled states. This is practice very difficult to achieve. However, a variety of techniques has been developed how to concentrate entanglement (that is to get from many pure and less entangled states few maximally entangled states) and how to purify mixed entangled states – the ones one usually has in practice – (that is how to get from many mixed entangled states as many as possible pure maximally entangled states) – see Gruska (1999-2002) for a description of such techniques.

The first experimental verification of a possibility of quantum teleportation was done in Zeilinger's group, see Bouwmester et al. (1997). However, the experimental status in this area is still far from being satisfactory. Reliability is still very low. Quantum teleportation therefore remains to be a big experimental challenge.

6 Quantum algorithms

As already mentioned the main successes in the area of designing quantum algorithms have been algorithms of Shor and Grover. Let us discuss them in more details in order to illustrate techniques used.

6.1 Shor's factorization algorithm

Shor's polynomial time algorithm for factorization, to be discussed in this section, is a highly nontrivial algorithm that uses a new technique, that of Quantum Fourier Transform.

The fastest classical algorithm to factor m bit numbers requires time $\mathcal{O}(e^{cm^{1/3}(\lg m)^{2/3}})$. Shor's factorization algorithm requires $\mathcal{O}(m^2 \lg^2 m \lg\lg m)$ time on a quantum computer and polynomial time on a classical computer.

Correctness and efficiency of Shor's algorithm is based on several simple results from number theory.

Lemma If there is a polynomial time quantum algorithm to find a *nontrivial solution* (different from ± 1) of the modular quadratic equations

$$a^2 \equiv 1 \pmod n,$$

then there is a polynomial time quantum algorithm to factorize integers.

Proof. Let $a \neq \pm 1$ be such that $a^2 \equiv 1 \pmod n$. Since

$$a^2 - 1 = (a+1)(a-1),$$

if n is not prime, then a prime factor of n has to be a prime factor of either $a+1$ or $a-1$. By using Euclid's algorithm to compute

$$gcd(a+1, n) \quad \text{and} \quad gcd(a-1, n)$$

we can find, in $\mathcal{O}(\lg n)$ steps, a prime factor of n.

The second key concept is that of the **period**, or **order**, of the functions $f_{n,x}(k) = x^k \bmod n$. It is the smallest integer r such that $f_{n,x}(k+r) = f_{n,x}(k)$ for any k, i.e. the smallest r such that $x^r \equiv 1 \pmod n$.

Now we can present an algorithm to solve modular quadratic equation:

1. Choose randomly $1 < y < n$.
2. Compute $gcd(y, n)$. If $gcd(y, n) \neq 1$ we have a factor.
3. Find period r of function $y^k \bmod n$.
4. If r is odd or $y^{r/2} \equiv \pm 1 \pmod n$, then go to step 1; otherwise stop.

If this algorithm stops, and there is a non-zero probability that it does, then $y^{r/2}$ is a non-trivial solution of the equation $x^2 \equiv 1 \pmod n$, and so we can factor n.

A general scheme for factorization has now the form shown in Figure 3:

The main contribution of Shor was to show that one can use quantum version of Fourier transform to compute efficiently period of the function $f_{n,x}(k) = x^k \bmod n$, and then consequently to factorize efficiently integers.[12]

A generalization of the technique used to perform factorization, so called "**phase estimation**" is one of the major techniques to design efficient quantum algorithms.

[12] The **Quantum Fourier Transform** is a quantum variant of the **Discrete Fourier Transform** (DFT). DFT maps a discrete function to another discrete one with equally distant points as

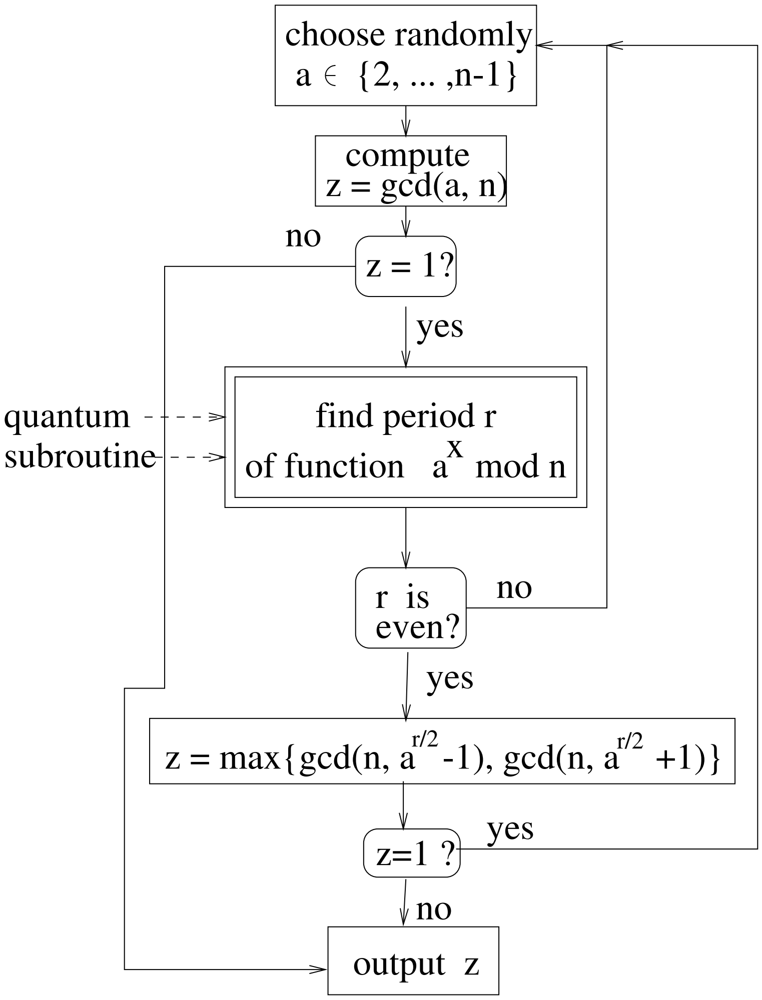

Figure 1: A general scheme of the Shor's factorization algorithm

its domain. For example it maps a q-dimensional complex vector

$$\{f(0), f(1), \ldots, f(q-1)\} \text{ into } \{\bar{f}(0), \bar{f}(1), \ldots, \bar{f}(q-1)\},$$

where for $c \in \{0, \ldots, q-1\}$

$$\bar{f}(c) = \frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} e^{2\pi iac/q} f(a), \tag{2}$$

for $c \in \{0, \ldots, q-1\}$.

The quantum version of DFT (QFT) is the unitary transformation

$$\mathrm{QFT}_q : |a\rangle \to \frac{1}{\sqrt{q}} \sum_{c=0}^{q-1} e^{2\pi iac/q} |c\rangle \tag{3}$$

6.2 Grover's algorithm

Grover's method seems to apply to problems for which it is hard to find a solution, but it is easy to check a to-be-solution.

> **Problem of unsorted database search:** In an unsorted database of N items there is one, x_0, satisfying an easy to verify condition P. Find x_0.

Classical algorithms need in average $\frac{N}{2}$ checks.
Quantum algorithms exist that need only $\mathcal{O}(\sqrt{N})$ steps.

The basic idea of Grover's algorithm is depicted in the Figure 2: At the very beginning, a state is created that is an equally weighted superposition of all basis states. Then, in each iteration step of the algorithm, at first the amplitude is negated at the basis states ($|x_0\rangle$) that corresponds to the searched-for solution (x_0). After that, using a unitary operation of the "inversion about the average", it is achieved that the absolute value of the amplitude at the basis state ($|x_0\rangle$), corresponding to the searched-for solution, is increased and the amplitudes at all other basis states decrease (in the absolute value). After a proper number of steps, the only non-zero amplitude is at the basis state that corresponds to the searched-for solution ($|x_0\rangle$). In case a measurement is performed at that time, we get, with the probability 1, the solution we are searching for, see Figure 2.

We shall deal now with a more general problem. Namely, that there is more than one solution and that the number $t = |\{x \mid f(x) = 1\}|$ of solutions is known.

Grover's search algorithm has now the following form:

Start in the state

$$|\phi\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle$$

---

for $0 \leq a < q$, with the unitary matrix

$$F_q = \frac{1}{\sqrt{q}} \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \omega & \omega^2 & \dots & \omega^{(q-1)} \\ 1 & \omega^2 & \omega^4 & \dots & \omega^{2(q-1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \omega^{(q-1)} & \omega^{2(q-1)} & \dots & \omega^{(q-1)^2} \end{pmatrix},$$

where $\omega = e^{2\pi i/q}$ is the *qth root of unity.*

If applied to a quantum superposition, QFT_q performs as follows;

$$\mathrm{QFT}_q : \sum_{a=0}^{q-1} f(a)|a\rangle \rightarrow \sum_{c=0}^{q-1} \bar{f}(c)|c\rangle,$$

where $\bar{f}(c)$ is defined by (2).

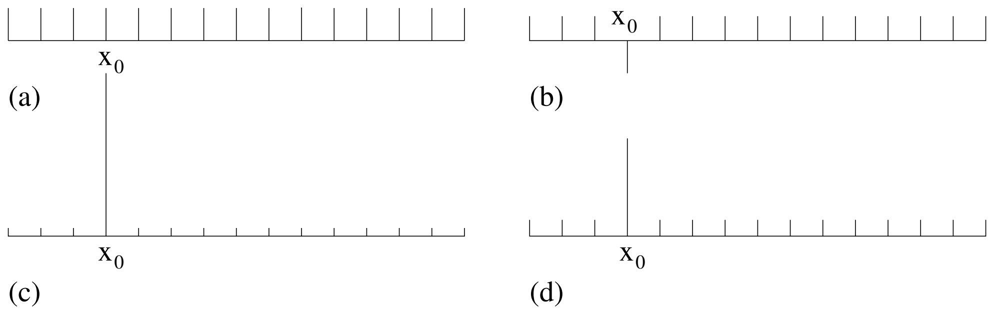

Figure 2: "Cooking" the solution with Grover's algorithm

and iterate $\lfloor\frac{\pi}{4}\sqrt{2^n}\rfloor$ times the transformation

$$-\underbrace{H_n V_0^n H_n V_f}_{\text{Grover's iterate}}|\phi\rangle \rightarrow |\phi\rangle.$$

where $H_n = \bigotimes_{i=1}^n H$ is the Hadamard transformation on n qubits, V_0 is the unitary mapping such that $V_0(|0\rangle) = -|0\rangle$ and $V_0(|x\rangle) = |x\rangle$ for $x \neq 0$ and $V_f(|x\rangle) = (-1)^{f(x)}|x\rangle$.

Finally, measure the register to get x_0 and check whether $f(x_0) = 1$. If not, repeat the procedure.

It has been shown that the above algorithm is optimal for finding the solution with probability $> \frac{1}{2}$.

In the case that there are t solutions, repeat the above iteration $\left\lfloor\frac{\pi}{4}\sqrt{\frac{2^n}{t}}\right\rfloor$ times.

6.2.1 Analysis of Grover's algorithm

Denote

$$X_1 = \{x \mid f(x) = 1\}, \qquad X_0 = \{x \mid f(x) = 0\},$$

and denote the state after jth iteration of Grover's iterate $-H_n V_0^n H_N V_f$ as

$$|\phi_j\rangle = k_j \sum_{x \in X_1} |x\rangle + l_j \sum_{x \in X_0} |x\rangle,$$

with $k_0 = \frac{1}{\sqrt{2^n}} = l_0$. Since

$$|\phi_{j+1} = -H_n V_0^n H_n V_f |\phi_j\rangle,$$

it holds

$$k_{j+1} = \frac{2^n - 2t}{2^n} k_j + \frac{2(2^n - t)}{2^n} l_j$$

$$l_{j+1} = \frac{2^n - 2t}{2^n} l_j - \frac{2t}{2^n} k_j$$

what yields

$$k_j = \frac{1}{\sqrt{t}} \sin((2j+1)\theta)$$

$$l_j = \frac{1}{\sqrt{2^n - t}} \cos((2j+1)\theta)$$

where $\sin^2\theta = \frac{t}{2^n}$.

The aim now is to find such an j which maximizes k_j and minimizes l_j. This is easy. Take j such that $\cos((2j+1)\theta) = 0$, that is $(2j+1)\theta = (2m+1)\frac{\pi}{2}$. Hence $j = \frac{\pi}{4\theta} - \frac{1}{2} + \frac{m\pi}{2\theta}$, what yields $j_0 = \lceil \frac{\pi}{4\theta} \rceil$, and because $\sin^2\theta = \frac{t}{2^n}$, we have

$$0 \leq \sin\theta \leq \sqrt{\frac{t}{2^n}}$$

and therefore

$$j_0 = \mathcal{O}\left(\sqrt{\frac{2^n}{t}}\right).$$

There has been a lot of explorations and developments in connection with the above two algorithms.

For example, it has been shown that integer factorization problem is a special case of so called Hidden subgroup problem[13] for Abelian groups and that for all such problems there are polynomial time quantum algorithms. This implies, for example, that quite a few of major public-key cryptosystems could be broken would we have powerful quantum computers. On the other hand, it is one of the major open problems in the area of quantum algorithms whether there are efficient algorithms also for Hidden subgroup problems for non-Abelian groups. Positive answer to that would imply, for example, that the graph isomorphism problem[14] can be solved in quantum polynomial time.

A lot of applications have been found for Grover's method. In principle, Grover's idea can be used to improve efficiency with which unstructured search problems can be solved. That implies that quantum computers could allow to solve various important optimization problems, such as scheduling and traveling salesman problem, for much larger inputs as so far. The method itself has been generalized to so called **amplitude amplification methodology** to speed-up quantum algorithms.

[13] The hidden subgroup problem is defined as follows: Given is an (efficiently computable) function $f : G \to R$, where G is a group and R is a finite set. Given is also a promise that there exists a subgroup $G_0 \leq G$ such that f is constant and distinct on the cosets of G_0. The task is to find a generating set for G_0 (in polynomial time (in $\lg|G|$) number of calls to the oracle for f and in the overall polynomial time).

[14] Graph isomorphism problem has a special position in complexity theory. It is in **NP**, no polynomial algorithm to solve it is known and it is also not known that it would be an **NP**-complete problem.

7 Quantum cryptography

There has been for several years a large interest in quantum cryptography. The main reason for that is that real-life applications seem to be feasible with current technology. (What does not seem to be case with other potential applications of quantum information processing research.) Actually, to perform unconditionally secure classical key distribution using quantum means one does not need a sophisticated quantum processors or long-term quantum memory. Very good sources and detectors of photons are sufficient.

In the classical information processing, security of the data storage and transition is getting rapidly of large, even crucial, importance, both from the practical and theoretical point of view. In connection with that, cryptography tasks, concepts, methods and tools, in a broad sense, are of growing importance.

Of large practical importance are methods for secure encryption, digital signatures, authentication, secret sharing. On a more general level the main task of modern cryptography is "to construct schemes which are robust against malicious attempts to make these schemes to deviate from their prescribed functionality" see Goldreich (1999).

It has turned out to be very nontrivial to develop properly very fundamental concepts related to the security of classical cryptography. Moreover, it has turned out that once these concepts are properly developed they are of fundamental importance for theory of computation. For example such concepts as *secure encryption*, *one-way function (with trapdoor)*, *zero-knowledge proof systems*, *bit commitment*, (cryptographically perfect) *random-number generators*, and so on.

From the practical point of view, one can say that most of the secret-key cryptographic methods are so secure how secure is the key generation.

One of the first successes of quantum cryptography was the development of methods that allow to have so called *unconditionally secure* classical key generation, where security is guaranteed by the laws of quantum physics and not by unproven complexity assumptions, as in the case of classical cryptography. More exactly, there are quantum protocols for classical key generation such that the probability that the key generation parties do not share, at the end of the protocol, the same key, or that an eavesdropper learns something about the key being generated, goes very fast to zero — depending on a security parameter.

In short, the underlying principle of unconditionally secure quantum key generation is that Nature prohibits gaining information on the state of a quantum system without disturbing it.

The first, and perhaps still the best such method is known as BB84 protocol, due to Bennett and Brassard. It is based on the fact that there is no way to distinguish perfectly by measurement two un-orthogonal states and that perfect quantum cloning is impossible.

BB84 is one of so called "prepare-and-measure" protocols – Alice sends photons with carefully and randomly chosen polarization and Bob measures them. No quantum processor is needed.

In order to generate an n-bit binary key between Alice and Bob, Alice first generates a random $m > n$ binary string and then sends its bits, one by one, using polarized photons, in the following way. To send 0 (1) Alice sends each photon in a randomly chosen state $|0\rangle$ or $|0'\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ (($|1\rangle$ or $|1'\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$)). Bob measures incoming photons, using each time randomly either the standard basis $\{|0\rangle, |1\rangle\}$ or the dual basis $\{|0'\rangle, |1'\rangle\}$, and keep secret results of measurements.

After all transmissions, Bob tells Alice, using a public communication channel, the sequence of bases he has chosen for measurements (but not their outcomes) and Alice tells him, again using a public communication channel, in which cases he used for his measurement the same basis as she did for encoding. The corresponding bits of their sequences then form so called *raw keys*. These keys of Alice and Bob should be the same in case there was no eavesdropping and channel was noiseless. To check for eavesdropping, Alice and Bob agree, by public communication, which subset of bits from their keys to make public. If they do that, they can see whether there was some eavesdropping or that the probability of eavesdropping is negligible.[15] In case an eavesdropping is detected, key generation process has to be repeated. Otherwise, the remaining parts of the raw keys should be with large probability the same. Finally, *error-correction techniques* can be used to make sure that Alice and Bob share indeed the same key and so-called *privacy amplification technique* can be used to make sure that knowledge of the potential eavesdropper about the generated key is negligible.

Concerning "real-life application, it has been shown that BB84 protocol is secure at a bit error rate of about 19%, insecure at a bit error rate 25%. A modification of BB84 that uses 6 states is secure at a bit error rate about 27%.

In the classical cryptography there is a perfectly secure encryption method, so-called ONE-TIME PAD (Verner) cryptosystem. Disadvantage of this method is that if two parties wants to send securely n bits, they need to share an n-bit random binary string as the key, and that secret key can be used only once. This is sometimes formulated as follows:

Shannon theorem n bits are sufficient and necessary to hide perfectly n classical bits.

How about "hiding", or sending with perfect security, qubits? This seems to be much more complex task, because just to specify fully one qubit one may need (infinitely) many classical bits. However, surprisingly, the following holds (Mosca et al. (2000)).

Quantum Shannon theorem $2n$ bits are sufficient and necessary to hide perfectly n qubits.

[15] In the case of eavesdropping there is a non-zero probability that result of Bob's measurement is different from the bit Alice sent even in the case both of them used the same basis – Alice for encoding and Bob for measurement.

Actually, there is a simple way how to use 2 bits to hide one qubit and this leads actually to the quantum version of ONE-TIME PAD cryptosystem (Leung (2000)).

If both parties share two bits b_1b_2, then encoding of a qubit $|\phi\rangle$ is done as

$$\sigma_x^{b_1}\sigma_z^{b_2}|\phi\rangle = |\psi\rangle$$

and decoding of the received state $|\psi\rangle$ is done by the operation

$$\sigma_z^{b_2}\sigma_x^{b_1}|\psi\rangle = |\phi\rangle.$$

This method is perfectly secure because the overall density matrix of the transmitted state is, in the case of one qubit, the density matrix $\frac{1}{2}I$ – the matrix corresponding to the random bit.

In case both parties share $2n$ EPR pairs, they can perform perfect encryption without sharing a secret classical key. Indeed, EPR pairs are just used to generate the shared secret key of $2n$ bits. For that it is sufficient that parties measure their particles in the standard basis – and it does not matter in which order they measure their particles.

In a similar way, as in the case of classical cryptography, various techniques are being developed for quantum digital signature, quantum authentication, quantum secret sharing, quantum secret multiparty distributed computing and so on.

Moreover, similarly as in the classical case, theoretical concepts related to the security of cryptographic tasks are one of the main driving forces of the research in quantum information processing.

On the more practical level, quantum cryptography is approaching a developing stage and even some byproducts are getting to market. Remarkable successes, as already mentioned, have been achieved in long-distance transmissions of photons. Large effort is currently devoted to finding reliable sources and detectors of photons and a big task is to make progress in implementations of so called *quantum repeaters*.

8 Decoherence fighting

Untill 1995, there has been strong scepticism (and this is not to say that it is completely over) whether some meaningful quantum information processing will be possible at al. There have been two reasons for such scepticism:

- No real quantum system can be isolated completely from its environment and it gets very soon entangled with the environment. As a consequence, subtle quantum superpositions, so vital for quantum information processing, start to deteriorate very fast. This phenomenon is known as *quantum decoherence* and it is well-known that decoherence grows exponentially with time. For some technologies faster, for other slower, but in any case to such an extend very fast that, in general, theoretically perfect processing of quantum states can be performed without errors only for very tiny time.

- Since the number of quantum errors seemed to be infinite and quantum information cannot be copied and, in addition, quantum measurement in general destroys irreversibly quantum states, it has been believed that quantum error-correcting codes cannot function as well as in the classical case.

Fortunately, it has been soon discovered that under very reasonable assumptions we have only two basic types of quantum errors: **bit errors**, represented by the Pauli matrix σ_x, and **sign errors** represented by the Pauli matrix σ_z. Any other error can be decomposed into those errors in such a way that if we learn to correct these two basic errors, then we can correct any error.

The main discovery was done by Shor (1995, 1996). He showed that effective quantum error-correcting codes do exists. The main idea is that we can encode qubits into entangled states and in such a way we can use entanglement to fight, in polynomial time, exponentially fast growing decoherence – due to entanglement.

An example of good quantum code is the following so called LMPZ code at which one qubit is encoded using five qubits:

$$|0\rangle \rightarrow \frac{1}{\sqrt{6}}(|00000\rangle+|11100\rangle-|10011\rangle-|01111\rangle+|11010\rangle+|00110\rangle+|01001\rangle+|10101\rangle)$$

$$|1\rangle \rightarrow \frac{1}{\sqrt{6}}(|11111\rangle-|00011\rangle-|10000\rangle+|01100\rangle+|11001\rangle-|00101\rangle-|01010\rangle+|10110\rangle)$$

Remark*In the classical computing, if one bit b is encoded using three bits, that is as bbb, then, at the majority voting decoding, the probability of error decreases from ε to ε^2. In the quantum case, by encoding one qubit through five qubits, as above, one can also decrease error from ε to ε^2.*

In addition, Shor has shown that not only quantum error correcting codes do exist, but we can perform quantum computation in fault-tolerant way. Finally, it has been shown that using so called *concatenated codes* we can transfer quantum information securely and unlimitedly in time and space provided quantum elements used, gates and channels, meet certain threshold limits concerning their reliability. In total, this implies that reliable quantum information processing is, in principle, possible.

One of the main tasks at using quantum error correcting codes is to make encoding in such a way that we can detect any error without disturbing the erroneous state. Since any error is a quantum operation, we can then undo the error by performing another quantum operation.

The following simple example illustrates well the whole process of quantum error correction process.

Example of a qubit communication process through a noisy channel using a 3-qubit bit-error correcting code.

Alice's encoding. Alice encodes the qubit $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$ by a network of two XOR gates and two additional qubits in the ancilla state $|00\rangle$ into the entangled state $\alpha|000\rangle + \beta|111\rangle$, see Figure 3.

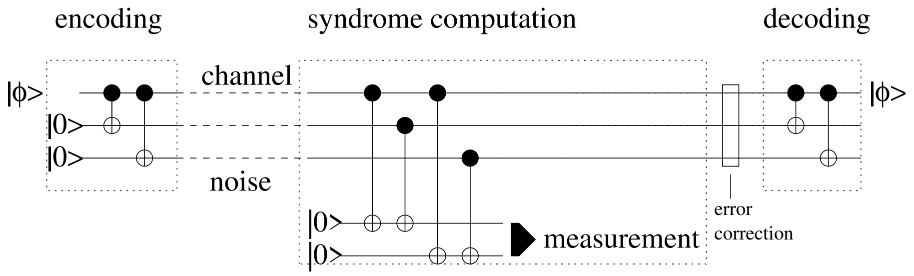

Figure 3. Circuit for encoding, syndrom computation, error correction and decoding

Noisy channel. Let us assume that a bit error occurs with the probability $p > \frac{1}{2}$ on any qubit and results in one of the states shown bellow:

state	probability
$\alpha\|000\rangle + \beta\|111\rangle$	$(1-p)^3$
$\alpha\|100\rangle + \beta\|011\rangle$	$p(1-p)^2$
$\alpha\|010\rangle + \beta\|101\rangle$	$p(1-p)^2$
$\alpha\|001\rangle + \beta\|110\rangle$	$p(1-p)^2$
$\alpha\|110\rangle + \beta\|001\rangle$	$p^2(1-p)$
$\alpha\|101\rangle + \beta\|010\rangle$	$p^2(1-p)$
$\alpha\|011\rangle + \beta\|100\rangle$	$p^2(1-p)$
$\alpha\|111\rangle + \beta\|000\rangle$	p^3

Syndrome computation process: By using two additional ancilla qubits in state $|00\rangle$ and four XOR operations, see Figure 3, syndromes of errors can be computed as shown in the following table

state	syndrome
$(\alpha\|000\rangle + \beta\|111\rangle)$	$\|00\rangle$
$(\alpha\|100\rangle + \beta\|011\rangle)$	$\|11\rangle$
$(\alpha\|010\rangle + \beta\|101\rangle)$	$\|10\rangle$
$(\alpha\|001\rangle + \beta\|110\rangle)$	$\|01\rangle$
$(\alpha\|110\rangle + \beta\|001\rangle)$	$\|01\rangle$
$(\alpha\|101\rangle + \beta\|010\rangle)$	$\|10\rangle$
$(\alpha\|011\rangle + \beta\|100\rangle)$	$\|11\rangle$
$(\alpha\|111\rangle + \beta\|000\rangle)$	$\|00\rangle$

Error correction. Bob does nothing if syndrome is 00 and performs σ_x operation

on third qubit if syndrome is 01
on second qubit if syndrome is 10
on first qubit if syndrome is 11

The resulting state is $\alpha|000\rangle + \beta|111\rangle$. The final decoding provides the state $\alpha|0\rangle + \beta|1\rangle$.

9 Quantum processors

Design of quantum processors and even of more powerful quantum gates, such as, for example, the XOR-gate, is still technologically a formidable task.

There have been experimental runnings of several quantum algorithms and even error-correcting processes on 5-qubit or even 7-qubit processors. In spite of all that progress, a design of 20-30 qubit processors, that could already be used to simulate interesting quantum processes, seems still to be not the question of the next days.

So far most of the experiments have been done using various forms of NMR technology with various types of molecules. NMR technology has been around already for quite a while and used extensively in medicine and chemistry. This way a lot of expertise has been obtained what could then be used also for performing some rudimentary quantum information processing. Views differ on how much this technology scales, but in general they are not very optimistic. Estimates of the upper bounds go from 20 to 100 qubits.

Two other technologies that have been explored for quite a while, are trapped ions or atoms and cavity QE.

There have been also very interesting suggestions to perform quantum information processing using linear optics elements.[16]

However, it is widely believed that in order to make some significant progress in designing effective quantum processors some solid-state technology has to be used. There have been many suggestions along these lines, but this seems to be a long process to overcome all obstacles. *Quantum dots* are one of the most perspective solid-state idea.

10 Frontiers

So far we have been discussing mainly "traditional" areas of quantum information processing and communication research.

[16]For example, Knill et al. (2001) describe a way to implement efficient and scalable quantum computing using only passive linear optics, photo-detectors, and single photon sources.

Step by step, as understanding grows that QIPC research is aiming to get insights into the most basic problems of science, various new areas are being explored, sometimes yet on a (very) speculative level. Let us list few of such areas that represent current frontiers of QIPC.

- Can we extend the usual concept of computability? Current concept of computability has been established using only logical arguments. Is it not necessary that also such concepts as computability are based on physical laws? For example, Kieu (2002) claims that there is no physical laws that would contradict his new concept of computability at which the halting problem for Turing machines is computable, but "classically" undecidable problems with higher degree of undecidability remain undecidable.

  In general, the question whether we can get "beyond Turing" is getting to be more and more on the current research agenda.

- What is the power of more specific physical information processing modes? For example, what is the power of fermionic, bosonic and anyonic information processing?

- What is information processing power of more powerful physical theories? For example, of quantum relativistic theory, field theory and so on? Can we have different results concerning information processing power for such theories? Yes, indeed. For example, unconditionally secure bit commitment is possible in the relativistic setting (Kent (2000)), but impossible in the non-relativistic setting, (see Gruska (1999-2002) for an overview of the interesting story of quantum bit commitment).

- Can we develop a really new information processing interpretation of quantum physics and by that a brand new quantum information processing foundation of physical world? (See Fuchs (2002) for such considerations.)

- Which role plays quantum information processing in brain activities. There is a lot of speculations on this subject, but not yet enough hard-core results.

11 Conclusions

In spite of the enormous progress in the recent time in the area of quantum information processing and communication theory, and also in the experimental area, the whole field is clearly at its very beginnings.

It is also too early to say in which areas we can expect soon, or main, impacts of new discoveries.

As mentioned by Braunstein, we even do not know, to say it in a popular way, whether "we will have sooner quantum computers or quantum telephones".

However, one can say, practically for sure, that something very important will come out of all this effort.

One can also point out several specific areas concentration on which is much needed in the near future.

- To develop new methodologies to design efficient quantum algorithms.
- To show for other practically important computation problems that quantum algorithms can be more efficient than classical ones.
- To explore in depth different types and different measures of entanglement for multipartite states.
- To explore to what extend such basic quantum phenomena as superposition and entanglement can be witness also at the macroscopic objects.[17]

Actually, to develop quantum information processing science can and should be seen as the main goal of theoretical informatics at all. This is related to the following our view, long time ago developed, of informatics as science.

> The scientific goal of physics is to discover and explore the laws and limitations of the physical world.
>
> The scientific goal of informatics, as fundamental science, is to discover and explore the laws and limitations of the quantum information processing world.

Time will show which of these two words are more basic, if any.

References

[1] S. Bandyopadhyay and V. Roychowdhury. Supercatalysis. Technical report, quant-ph/0107103, 2001.

[2] Ch. H. Bennett, P. W. Shor, J. A. Smolin, and A. V. Thapliyal. Entanglement-assisted classical capacity of noisy quantum channels. Technical report, quant-ph/9904023, 1999a.

[3] Ch. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Physical Review Letters*, 70:1895–1899, 1993.

[17] In E. Polzik group in Aarhus (see Julsgaard et al.(2001)), they entangled two samples of caesium atoms, each contains about 1012 atoms for half a millisecond – quite a long time by quantum standards. See also Brezger et al. (2002) for experiment with superposition of large molecules.

[4] D. Bouwmeester, J-W. Pan, K. Mattle, M.Eibl, H. Weinfurter, and A. Zeilinger. Experimental quantum teleportation. *Nature*, 390:575–579, 1997.

[5] B. Brezger, L. Hackermüler, S. Uttenhalter, J. Petachinka, M. Arndt, and A. Zeilinger. Matter-wave interferometer for large molecules. Technical report, quant-ph/0202158, 2002.

[6] H. Buhrman, R. Cleve, and A. Widgerson. Quantum vs. classical communication and computation. In *Proceedings of 30st ACM STOC*, pages 63–68, 1999.

[7] S. C.Benjamin and P. M. Hayden. Multi-player quantum games. Technical report, quant-ph/0007038, 2000.

[8] I. I. Chuang and M. A. Nielsen. *Quantum computation and quantum information*. Cambridge University Press, 2000.

[9] D. Deutsch. Quantum theory, Church-Turing principle and the universal quantum computers. *Proceedings of the Royal Society, London A*, 400:97–117, 1985.

[10] D. Deutsch and R. Jozsa. Rapid solution of problems by quantum computation. *Proceedings of Royal Society of London A*, 439(553-558), 1992.

[11] O. Goldreich. *Modern cryptography, probabilistic proofs and pseudo-random generators*. Springer-Verlag, 1999.

[12] D. Gottesman and I. L. Chuang. Quantum teleportation is a universal computational primitive. Technical report, quant-ph/9908010, 1999.

[13] L. K. Grover Quantum mechanics helps in searching for a needle in a haystack. *Physical Review Letters*, 78:325–328, 1997a.

[14] J. Gruska. *Quantum computing*. McGraw-Hill, 1999. See also additions and updatings of the book on http://www.mcgraw-hill.co.uk/gruska.

[15] J. Gruska. Quantum challenges. In *Proceedings of SOFSEM'99*, pages 2–29, 1999a.

[16] J. Gruska. *Mathematics unlimited, 2001 and beyond*, chapter Quantum computing challenges, pages 529–564. Springer, 2000.

[17] J. Gruska, H. Imai, and K. Matsumoto. Power of quantum entanglement. In *Proceedings of TCS conference of IFIP Congress, 2002*, pages ???–???, 2002.

[18] M. Horodecki, P. Horodecki, and R. Horodecki. Mixed-state entanglement and distillation: is there a "bound" entanglement in nature? Technical report, quant-ph/9801069, 1998a.

[19] I. D. Jonathan and M. B. Plenio. Entanglement-assisted local manipulation of pure quantum states. Technical report, quant-ph/9905071, 1999.

[20] R. Jozsa and N. Linden. On the role of entanglement in quantum computational speed-up. Technical report, quant-ph/0201143, 2002.

[21] B. Julsgaard, A. Kozhekin, and E. S. Polzik. Exprimental long-lived entanglement of two macroscopic objects. Technical report, quant-ph/0106057, 2001.

[22] A. Kent. Unconditional secure bit commitment. *Physical Review Letters*, 83:1447–1450, 1999.

[23] E. H. Knill, R. Laflamme, and K. Milburn. Efficient linear optics quantum computation. 409:46–52.

[24] C. F. Lee and N. Johnson. Theory of quantum games. Technical report, quant-ph/0207012, 2002.

[25] D. W. Leung. Quantum Vernam cipher. Technical report, quant-ph/0012077, 2000.

[26] N. D. Mermin. From cbits to qbits: teaching computer scientists quantum mechanics. Technical report, quant-ph/0207118, 2002.

[27] M. Mosca, A. Tapp, and R. de Wolf. Private quantum channels and the cost of randomizing quantum information. Technical report, quant-ph/0003101, 2000.

[28] R. Rausschendorf and H. Briegel. Quantum computing via measurements only. Technical report, quant-ph/0010033, 2000.

[29] R. Raz. Exponential separation of quantum and classical communication complexity. In *Proceedings of* 31*st ACM STOC*, pages 358–367, 1999.

[30] P. W. Shor. Algorithms for quantum computation: discrete log and factoring. In *Proceedings of 36th IEEE FOCS*, pages 124–134, 1994.

[31] P. W. Shor. Fault-tolerant quantum computation. In *Proceedings of 37th IEEE FOCS*, pages 56–65, 1996.

[32] P. W. Shor Scheme for reducing decoherence in quantum computer memory. *Physical Review A*, 52:2493–2496, 1995.

[33] D. R. Simon. On the power of quantum computation. In *Proceedings of* 35*th IEEE FOCS*, pages 116–123, 1994.

[34] J. A. Smolin. A four-party unlockable bound-entangled state. Technical report, quant-ph/0001001, 2000.

[35] R. Werner. *Quantum information*, chapter Quantum information theory: an introduction, pages 14–55. Springer, 2001.