From Informatics to Quantum Informatics

Jozef Gruska*

Faculty of Informatics, Masaryk University, Brno, Czech Republic
gruska@fi.muni.cz

Abstract. Quantum phenomena exhibit a variety of weird, counter-intuitive, puzzling, mysterious and even entertaining effects. Quantum information processing tries to make an effective use of these phenomena to design new quantum information processing and communication technology and also to get a better understanding of quantum and information processing worlds.
During the recent years, exploration of the quantum information processing and communication science and technology got a significant momentum, and it has turned out quite clearly that paradigms, concepts, models, tools, methods and outcomes of informatics play by that a very important role. They not only help to solve problems quantum information processing and communication encounter, but they bring into these investigations a new quality, and to such an extend, that one can now acknowledge an emergence of a quantum informatics as of an important new area of fundamental science with contributions not only to quantum physics, but also to (classical) informatics itself.
The main goal of this paper is to demonstrate the emergence of quantum informatics, as of a very fundamental, deep and broad science, its outcomes and especially its main new fascinating challenges, from informatics and physics point of view. Especially challenges in the search for new primitives, computation modes, new quality concerning efficiency and feasibility of computation and communication, new quality concerning quantum cryptographic protocols in a broad sense, and also in a very new and promising area of quantum formal systems for programming, semantics, reasoning and verification.
The paper is targeted towards informaticians that are pedestrians in the mysterious quantum world, but would like to see what are new driving forces in informatics, where they drive us, why and how. In the paper, oriented towards broad audience, main mysteries, puzzles and specific features of quantum world are dealt with as well as basic models, laws, limitations, results and the state-of-the-art of quantum information processing and communication.

1 Introduction

In quantum computing we witness a merge of two arguably the most important areas of science of 20th century: quantum physics and informatics. It would

* Support of the grants GAČR 201/04/1153 and MSM0021622419 is acknowledged.

therefore be astonishing if such a merge would not shed new light on both of them and would not bring new great discoveries. This merge is surely bringing new aims, challenges and potentials for informatics and also new approaches to explore quantum world. In spite of the fact that it is hard to predict particular impacts of quantum computing on computing in general, it is quite safe to expect that the merge will lead to important outcomes.

Since the very beginning of quantum mechanics, various its mysterious and counterintuitive phenomena have been discovered, but science community did not pay too large attention to them because they looked as innocent features that largely exist due to our, still not perfect, mathematical model/understanding of the quantum world, or as phenomena investigation of which can be postponed. Randomness of quantum measurement and resulting collapse of the quantum state being measured, quantum entanglement and non-locality in correlations exhibited due to it[2], are perhaps the most puzzling ones. Quantum counterfactual effects with its peculiar consequences[3] are even more weird phenomena.

In between, situation has radically changed. Quantum entanglement has been shown to be useful to perform actions, as quantum teleportation (Bennett et al, 1993), that is not possible in the classical world, to achieve in computation the efficiency that seems to be impossible in the classical world, as Shor's polynomial time algorithms for factorization and discrete logarithms (Shor, 1994)), to achieve level of security not possible in the classical world (for example for classical keys generation (Ekert, 1991)), to increase exponentially efficiency of communicating protocols (Raz, 1999), to introduce new important capacities and to increase old capacities of quantum channels (see Gruska (1999-2005) and Nielsen and Chuang (2000) for an overview, and so on. All that is still only a small list of the success story of quantum entanglement that has been experimentally demonstrated for distance of up to 50km using fiber (Marcikic et al., 2004) and up to 13km over noisy ground atmosphere (see Peng at al., 2004). It is, for example, believed, and expected by some, that quantum entan-

[2] As formally defined later, entanglement of quantum states is defined using Hilbert space formalism for quantum phenomena. However, the existence of non-local correlations is an experimentally observed phenomenon and therefore independent of the choice of formalism. At the moment, the only observed non-local correlations are those exhibited by entangled states. This, however, does not exclude that some other non-local correlations will be discovered.

[3] The term counterfactual is usually used for things that might have happened, although they did not really happened. An important point is that while classical counterfactuals do not have physical consequences, quantum counterfactuals can have surprisingly big consequences because the mere possibility that some quantum event might have happened can change the probabilities of obtaining various experimental outcomes. For example, it can be shown that a quantum computer can provide the result of a computation without performing the computation provided it would provide the same result of computation by really performing the computation (Mitchinson and Jozsa, 1999).

glement will have also large practical impacts. For example, to increase quality of measurements (see Childs et al. 1999).

To summarize, quantum entanglement is now considered as a new very important resource for quantum information processing and communication, a resource that has, in addition, the following potentials (see also Gruska 1999-2005, 2003):

– To provide a new gold mine for science and technology;
– To give an edge to quantum versus classical information processing and communication.
– To help to understand better various important physical phenomena.

Surely, the most puzzling and powerful consequence of the existence of entangled quantum states is non-locality their measurements exhibit. Namely, if a set of particles is in an entangled state and one of the particles is measured, then this measurement immediately influences/determines results of subsequent measurements of other particles. There are therefore non-local correlations between results of the measurements of particles in an entangled state.

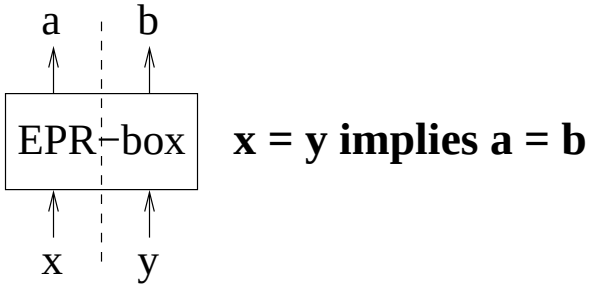


Fig. 1. EPR-box

Quantum nonlocality, exhibited by the measurement of so-called EPR-state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, can be modelled by so-called EPR-box shown in Figure 1. There are two parties involved, A and B, much separated by space, that do not communicate with each other, and an imaginary box with two input-output ports, each for one of the parties. If the party A puts in its input port a, it gets out, immediately, an output x, and if the party B puts in an input b it gets out, as the output, immediately, a y. The key property of the EPR-box is that if $a = b$, then $x = y$, no matter in which order the parties put their inputs in and how much time is between their entries. No-scommunication (no-signaling) condition meanes that output of Alice (Bob) does not depend on the input of Bob (Alice). Nonlocality exhibited in the EPR-box can be manifested by the measurement of entangled states, namely of the EPR-state. However, non-locality exhibited in so called PR-box, shown in Figure 2, where inputs and outputs are always in the relation $x \cdot y = (a \oplus b)$, seems to be beyond

the possibilities of the physical world. Indeed, would there be a physical system that would allow to implement the PR-box, then any multiparty communication could be done by transmitting only a single bit (van Dam, 2005) what can be indeed seen as impossible. Interesting enough, none of these non-localities allows instantaneous communication and therefore they actually do not contradict the no-signaling condition of special relativity[4].[5]

The task to understand nonlocality is one of the most important in current science. In this connection, the recent experiment (Scarani et al., 2000) is of importance, from which it follows that there are reasons to believe that either space-time is an illusion or free will is an illusion or, as their experiment confirms, there is a special "quantum information" that travel faster then light (but cannot be used directly to communicate classical information).

[4] No-signaling condition actually says that local choice of measurements may not lead to observable differences on the other ends. PR-box may seem as an artificial construction, but it is not so and it comes out very naturally when non-classical correlations and their limits are considered.

Indeed, the basic scheme is that two parties separated in space, say A and B, that cannot communicate have an access to a physical state and can use it to generate correlations. This can be seen as that both parties to perform one of two randomly chosen measurements and then the outcomes of these measurements are given by random variables and one asks the question how much can these outcomes be correlated. Both classical physics and quantum mechanics put certain limits on strength of such correlations. The limits that any classical theory (i.e. local hidden variable theory) provides are known as *Bell inequalities* (Bell, 1964). There are many of them and among them special position has so-called CHSH inequality

$$\sum_{a,b\in\{0,1\}} \mathrm{Prob}(x_a \oplus y_b = a \cdot b) \leq 3,$$

where a and b denote choices of the measurements of A and B, and x_a, y_b are outcomes of measurements. Quantum mechanics allows violation of this inequality, but only up to so-called *Cire'lson's bound* $2+\sqrt{2}$. The PR-box captures maximal possible, mathematically, violation of this bound.

[5] In spite of the fact that van Dam's result strongly indicates/proves physical impossibility of PR-boxes, they keep been intensively studied. For example, it has also been shown (Short et al., 2005), that availability of PR-boxes would allow unconditional secure oblivious transfer protocol, an important cryptographical primitive. Cerf et al. (2005) have also shown that a single PR-box could be used to simulate the EPR box, and therefore a maximally entangled state (its measurements), though not any two-qubit entangled state and that the PR-box would be a strictly weaker resource than a bit of communication. The PR-box can also be used to show that no-cloning theorem holds. PR-boxes have a variety of other surprising and also counterintuitive properties. They are surveyed nicely and referenced well by Scarani (2006). For example, two parties may need 2^n PR-boxes for some tasks that can be performed using n EPR states. In addition, for all natural measures of non-locality non-maximally entangled states exhibit more non-locality than maximally entangled states.

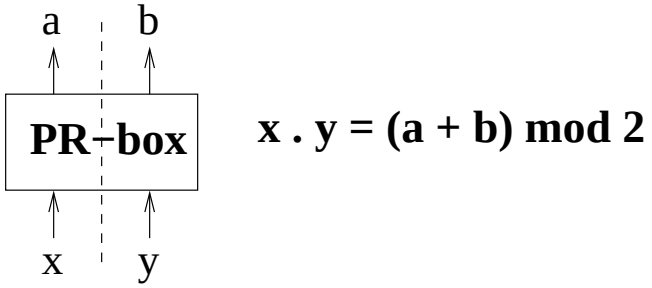


Fig. 2. PR-box

Quantum superposition, that stands for the fact that any quantum state is a weighted superposition (with complex numbers as weights - probability amplitudes specifying probabilities of the transfer from a given state to particular state of the basis) of the states of a basis, is another very special quantum phenomenon. One of the implications of that is *quantum parallelism* that allows, for example, on a single state of n quantum bits to perform, in a single step, an action that corresponds, in some sense, to 2^n computation steps in the classical world. For example, one can get, in one step, into amplitudes of a quantum n-qubit state, all values of a function $f : \{0, \ldots, 2^n - 1\} \rightarrow \{0, \ldots, 2^n - 1\}$.[6] There is a certain catch in this result/fact, because there is no way to get faithfully out all these values from the resulting quantum state. However, in some important cases, as it is in Shor's algorithm for factorization of integers n, this does not really matter, because what one needs to compute is only a single value, a period of a properly chosen function $f(x) = a^x \bmod n$, and in such a case such a massive quantum parallelism is indeed useful.

A mysterious fact is why we do not observe superposition and entanglement between objects of the classical world if our world is actually fully quantum.[7]

[6] With more technical details, it works as follows: If $f : \{0, 1, \ldots, 2^n - 1\} \leftrightarrow \{0, 1, \ldots, 2^n - 1\}$, then the mapping $f' : (x, 0) \Longrightarrow (x, f(x))$ is one-to-one and therefore there is a unitary transformation U_f such that for any $x \in \{0, 1, \ldots, 2^n - 1\}$.

$$U_f(|x\rangle|0\rangle) \Longrightarrow |x\rangle|f(x)\rangle$$

The state $|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i\rangle|0\rangle$ can be obtained in a single step, using Hadamard transform, from the basis state $|0^{(n)}\rangle$ and with a *single application* of the mapping U_f, on the state $|\psi\rangle$ we get

$$U_f|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i\rangle|f(i)\rangle$$

Hence, in a single computation step, 2^n values of f are computed! We have therefore a really massive parallelism.

[7] Of interest in this context are two well known citations: *There is no quantum world. There is only an abstract quantum physical description. It is wrong to think that the*

This strange situation was already long time ago well demonstrated by famous Schrödinger's cat Gedanken experiment with a cat that is in a superposition of states $|alive\rangle$ and $|dead\rangle$ - though none has ever seen a cat that would be both alive and dead. An important agenda of the current experimental research is therefore to find some border lines, if they exist at all, between the world in which superposition exists and the one where no superposition can be detected.[8] There have been surprising results in such investigations recently. For example, entanglement has been demonstrated at a group of 10^{12} atoms (see Julsgaard et al., 2000) and quantum interference for large molecules (see Brezger et al. 2002). However, there is still a range of several orders of magnitudes to explore where border between classical and quantum world is.

Concerning quantum measurement, there are also several mysterious and counterintuitive things. The first one is the fact that results of quantum measurement are random. Einstein's position was expressed by his famous words *God does not roll dice*, but equally famous is Bohr's reply *The true God does not allow anybody to prescribe what he has to do.*[9] and the puzzling fact about quantum measurement is that theory does not say anything about how much a particular measurement really costs in terms of some physical resources. Because of that it is usually considered, in efficiency calculations, that a measurement step requires a unit time. However, this does not seem to be realistic because sometimes we can see at a quantum measurement as that Nature performs, in a "unit time", quite complicated computation, what is again against our common sense. Quantum measurement can therefore be seen as a special resource that, if properly used, can do miracles, from quantum information processing point of view.

---

task of physics is to find out how Nature is. Physics concerns what we can say about Nature. by N. Bohr and *There is no classical world - there is only quantum world* by D. Greenberger (see Arndt et al., 2005), who actually said: *I believe there is no classical world. There is only quantum world. Classical physics is a collection of unrelated insights: Newton's laws. Hamilton's principle, etc. Only quantum theory brings out their connection. An analogy is the Hawaiian Islands, which look like a bunch of island in the ocean. But if you could lower the water, you would see, that they are the peaks of a chain of mountains. That is what quantum physics does to classical physics.*

[8] In this context another views are of interest from Arndt et al. (2005): *The border between classical and quantum phenomena is just a question of money*, by A. Zeilinger, *The classical-quantum boundary is simply a matter of information control*, by M. Aspelmeyer, and *There is no border between classical and quantum phenomena – you just have to look closer*, by R. Bertlman.

[9] Experiments performed recently actually imply not only that *God does play dice*, but actually that *God plays with non-local dice*, beause measuement of an entangled state can produce shared randomness, see Gisin (2005).

2 Basics of quantum information processing and communication

Quantum physics deals with fundamentals entities of physics — particles, like (a) protons, electrons and neutrons (from which matter is built); (b) photons (which carry electromagnetic radiation); (c) various "elementary particles" which mediate other interactions of physics. We call all of them *particles* in spite of the fact that some of their properties are totally unlike the properties of what we call particles in our ordinary world. (Actually, it is not clear in which sense these "particles" can be said to have properties at all.)

It is also clear that quantum physics is an elegant and conceptually simple theory that describes with surprising precision a large spectrum of the phenomena of Nature. Predictions made on the base of quantum physics have been experimentally verified to 14 orders of precision. No conflict between predictions of the theory and experiments is known. Without quantum physics we cannot explain properties of superfluids, functioning of laser, color of stars, ...

Quantum physics is of special interest for informatics for several reasons. One of them is similarity, in a sense, and close relation between these two areas of science. Indeed, the goal of physics can be seen as to study elements, processes, laws and limitations of the physical world. Goal of informatics can then be seen as to study elements, processes, laws and limitations of the information world. Of large importance is therefore to explore which of these two worlds, physical and information, is more basic, if any, and what are the main relations between the basic concepts, principles, laws and limitations of these two worlds.

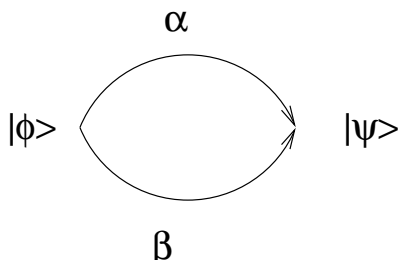
Quantum physics can be also seen as an excellent theory to predict probabilities of quantum events. Such predictions are to a large extend based on three simple principles:

P1 To each transfer, from a quantum state ϕ to a state ψ, a complex number $\langle\psi|\phi\rangle$ is associated, which is called the *probability amplitude* of the transfer, and $|\langle\psi|\phi\rangle|^2$ is then the *probability* of such a transfer.

P2 If a transfer from a quantum state ϕ to a quantum state ψ can be decomposed into two subsequent transfers $\psi \leftarrow \phi' \leftarrow \phi$, then the resulting amplitude of the transfer form ϕ to ψ is the *product* of the amplitudes of subsequent subtransfers: $\langle\psi|\phi\rangle = \langle\psi|\phi'\rangle\langle\phi'|\phi\rangle$

P3 If the transfer from a state ϕ to a state ψ has two independent alternatives, then the resulting amplitude is the sum of the amplitudes of two subtransfers, which can be zero if $\alpha = -\beta$. (This has surprising consequences. It may happen that there are two ways, each with positive probability $k = |\alpha|^2$, how to get from a state $|\phi\rangle$ to a state $|\psi\rangle$, but if both options are possible, then such a transfer has zero probability.)

To the physical concept of *quantum system*, the mathematical concept of the *Hilbert space* is usually associated, and to the physical concept of a (pure) state of a closed (that is not interacting with environment) quantum system, the mathematical concept of a vector/state of a Hilbert space corresponds.



Hilbert space H_n is an n-dimensional complex vector space on which the *scalar product*

$$\langle\psi|\phi\rangle = \sum_{i=1}^{n} \phi_i \psi_i^* \quad \text{of any two vectors } |\phi\rangle = \begin{vmatrix} \phi_1 \\ \phi_2 \\ \vdots \\ \phi_n \end{vmatrix}, |\psi\rangle = \begin{vmatrix} \psi_1 \\ \psi_2 \\ \vdots \\ \psi_n \end{vmatrix},$$

is defined as well as the *norm of a vector* $||\phi|| = \sqrt{|\langle\phi|\phi\rangle|}$ and the *metric* $\text{dist}(\phi, \psi) = ||\phi - \psi||$. This allows to introduce on H a topology and such concepts as continuity.

Two quantum states are called *orthogonal* if their scalar product is zero. This is a very important concept because physically are perfectly distinguishable only orthogonal states.

Dirac introduced the following handy notation, so called bra-ket notation, to deal with amplitudes, quantum states and linear functionals $f : H \to \mathbf{C}$.

If $\psi, \phi \in H$, then $\langle\psi|\phi\rangle$ is the *scalar product* of ψ and ϕ (and an amplitude of going from ϕ to ψ); $|\phi\rangle$ is called a *ket-vector* - a column vector, an equivalent to ϕ; $\langle\psi|$ is a *bra-vector* - a row vector, a linear functional on H such that $\langle\psi|(|\phi\rangle) = \langle\psi|\phi\rangle$.

Evolution in a quantum system is described by the *Schrödinger linear equation*

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

where $\hbar$ is the Plank constant, $\psi(t)$ is the state of the system in time t and $H(t)$ is a quantum analogue of a Hamiltonian of the classical system. In case H is constant, the Schrödinger equation has as solution $\psi(t) = e^{-\frac{i}{\hbar}Ht}\psi(0)$ and from that it follows that a discretized evolution (computation) of any quantum system is performed by a *unitary operator* and a step of such an evolution we can see as a multiplication of a *unitary matrix*[10] A with a vector $|\psi\rangle$, i.e. as $A|\psi\rangle$.

[10] A matrix A is *unitary* if $A \cdot A^\dagger = A^\dagger \cdot A = I$, where $A^\dagger$ is the matrix obtained from A by transposition and then by replacement of each element by its complex conjugate.

A *quantum bit*, called usually *qubit*, is then a quantum state in H_2, $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$, where $\alpha, \beta \in \mathbf{C}$ are such that $|\alpha|^2 + |\beta|^2 = 1$ ($\{|0\rangle, |1\rangle\}$ is the *standard basis* of H_2).

Important operations on one qubit are Hadamard transform, represented by the matrix

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}^{11} \text{ and Pauli matrices } \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ and } \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Now we can say that the essence of the difference between the *classical computers* and *quantum computers* is in the way information is stored and processed. In *classical computers*, information is represented on *macroscopic level*, by *bits*, which can take on one of two values, 0 or 1. In *quantum computers*, information is represented on *microscopic level*, using *qubits*, which can take on any from uncountable many values $\alpha|0\rangle + \beta|1\rangle$, where α, β are arbitrary complex numbers such that $|\alpha|^2 + |\beta|^2 = 1$.

Very important is also difference between the ways compound classical and compound quantum systems are created. In the classical case, any state of a composed system is composed of the states of subsystems. This is not so in the quantum case.

If a Hilbert space $\mathcal{H}$ ($\mathcal{H}'$) corresponds to a quantum system $\mathcal{S}$ ($\mathcal{S}'$), and $\{\alpha_i\}_i$ ($\{\beta_j\}_j$) is a basis of $\mathcal{H}$ ($\mathcal{H}'$), then the tensor product of $\mathcal{H}$ and $\mathcal{H}'$, notation $\mathcal{H} \otimes \mathcal{H}'$, corresponds to the quantum system composed of $\mathcal{S}$ and $\mathcal{S}'$ and this Hilbert space has a (standard) basis consisting of all tensor products of states $|\alpha_i\rangle$ and $|\beta_j\rangle$.

For example, Hilbert space $\mathcal{H}_4$ can be seen as the tensor product of two one-qubit Hilbert spaces, $\mathcal{H}_2 \otimes \mathcal{H}_2$, and therefore one of its (standard) basis consists of the states $|0\rangle \otimes |0\rangle$, $|0\rangle \otimes |1\rangle$, $|1\rangle \otimes |0\rangle$, $|1\rangle \otimes |1\rangle$ These states are usually denoted shortly as:

$$|00\rangle, \quad |01\rangle, \quad |10\rangle, \quad |11\rangle.$$

Another important orthogonal basis in $\mathcal{H}_4$ consists of the following four so-called Bell states:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle, \quad |\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle),$$

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

Similarly, the (standard) basis states of an n-qubit Hilbert space $\mathcal{H}_{2^n}$ are the states

$$|i_1 i_2 \dots i_n\rangle = |i_1\rangle \otimes \dots \otimes |i_n\rangle,$$

where $i_k \in \{0, 1\}$ for all k.

[11] Hadamard operation transforms the standard basis $\{|0\rangle, |1\rangle\}$ into the dual basis, consisting of the vectors $\{|0'\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |1'\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$

A general state, $|\phi\rangle$, of an n-qubit register has therefore the form:

$$|\phi\rangle = \sum_{x\in\{0,1\}^n} \alpha_x|x\rangle, \quad \text{where} \quad \sum_{x\in\{0,1\}^n} |\alpha_x|^2 = 1.$$

Operators on n-qubits registers are unitary matrices of degree 2^n. If a state $|\phi\rangle$ of an n-qubit register is measured with respect to the standard basis $\{|x\rangle\}_{x\in\{0,1\}^n}$, then in the quantum world the state $|\phi\rangle$ collapses, with probability $|\alpha_x|^2$, into the state $|x\rangle$, and into the classical world information about that, as x, emerges.

The key concept of so called *open quantum systems*, that is quantum systems interacting with environmnet, is the concept of a *mixed state*, what is a probability distribution $\{(p_i, |\phi_i\rangle)\}_{i=1}^k$ on pure states $\{|\phi_i\rangle\}_i$. To each such a mixed state the *density operator* $\rho = \sum_{i=1}^k p_k|\phi_i\rangle\langle\phi_i|$ is associated, and its matrix representation is called *density matrix*. A very important fact is that it may happen that the same density matrix corresponds to two mixed states and that two mixed states are physically undistinguishable if their density operators (matrices) are the same. In modern quantum information processing literature, the concept of the state is often associated with that of the density operator.

Now we are in the position to define formally a so important concept of entangled states. A pure state $|\phi\rangle$ of a tensor product of Hilbert spaces $H_1 \otimes \ldots \otimes H_n$ is called *entangled* if it cannot be decomposed in the form $|\phi\rangle = |\phi_1\rangle \otimes \ldots \otimes |\phi_n\rangle$, where $|\phi_i\rangle$ is a pure state of H_i. A mixed state ρ of n qubits is called (fully) *separable* if it can be decomposed as

$$\rho = \sum_i p_i \rho_i^{(1)} \otimes \ldots \otimes \rho_i^{(m)},$$

where $\sum_i p_i = 1$ and $\rho_i^{(j)}$ is a density matrix of j-th qubit, for any j. Otherwise, ρ is called *inseparable* or *entangled*.

We can now formulate one important limitation of quantum information processing and to summarize differences between the classical and quantum information.

The limitation is that there is no universal way how to copy/clone unknown quantum states - what so called *no-cloning theorem* says. On the level of qubits, no-cloning theorem says that there is no unitary transformation U such that for any one-qubit state $|\phi\rangle$ it holds $U(|\phi\rangle|0\rangle) = |\phi\rangle|\phi\rangle$.[12]

[12] Proof. Let us assume that a unitary U with such a property exists and that for two different states, $|\alpha\rangle$ and $|\beta\rangle$, $U(|\alpha\rangle|0\rangle) = |\alpha\rangle|\alpha\rangle$ $U(|\beta\rangle|0\rangle) = |\beta\rangle|\beta\rangle$. Let

$$|\gamma\rangle = \frac{1}{\sqrt{2}}(|\alpha\rangle + |\beta\rangle),$$

then

$$U(|\gamma\rangle|0\rangle) = \frac{1}{\sqrt{2}}(|\alpha\rangle|\alpha\rangle + |\beta\rangle|\beta\rangle) \neq |\gamma\rangle|\gamma\rangle = \frac{1}{2}(|\alpha\rangle|\alpha\rangle + |\beta\rangle|\beta\rangle + |\alpha\rangle|\beta\rangle + |\beta\rangle|\alpha\rangle).$$

We can now also say that important properties of the classical information are: (a) transmission of information in time and space is very easy (b) making unlimited number of copies of information is very easy. On the other side, important properties of the quantum information are: (a) transmission of the quantum information in time and space is very difficult; (b) there is no way to make faithful copies of unknown quantum information. (c) attempts to measure the quantum information destroy it, in general.

3 Outcomes and challenges of quantum computation

Quantum polynomial time algorithms of Shor, in 1994, that could be used to break important classical cryptosystems, were so far main apt killers for quantum information processing. A natural quantum version of the Fourier transform has been the main tool[13] and the quantum Fourier transform has been also used later to design various other quantum algorithms that are more efficient than the most efficient classical algorithms for the same algorithmic problems. Main generalized result is that there are quantum polynomial time algorithms for so called Hidden Subgroup Problem for Abelian groups.[14] Perhaps the most important open problem in the design of quantum algorithms is to determine whether the Hidden Subgroup Problem is always solvable in polynomial time also for non-Abelian groups. Would this be true, it would imply, for example, that there is a quantum polynomial time algorithm also for the graph isomorphism problem.

Even of large impact on the design of efficient quantum algorithms have had the discovery of Grover (1996). who has shown that one can find in an unordered database of N elements a unique element satisfying a given condition P in $\sqrt{N}$ quantum steps. His idea was generalized and applied in numerous ways and resulted also into so-called probability amplification technique. Recently, quantum random walks got a momentum as a way to design quantum algorithms (see Aharonov et al., 2001). Of interest are also non-traditional modes of quantum computation as adiabatic (see Farhi et al., 2000). Several ingenious techniques have also been developed to prove lower bounds: for example, the polynomial method (Beals et al., 1998), the quantum adversary method (Ambainis, 2000) and its various variants. They have been used to show a variety of impressive lower bound results (see Gruska, 1999-2005, for an overview).

[13] Also other quantum generalizations of transforms known from signal processing and applied mathematics have turned out to be useful for the design of quantum algorithms.

[14] The Hidden Subgroup Problem is the following one: Given is an (efficiently computable) function $f : G \to R$, where G is a finite group and R a finite set and a *promise* that there exists a subgroup $G_0 \leq G$ such that f is constant on any left cosset and distinct on different cossets of G_0. The task is to find a generating set for G_0 (in polynomial time (in $\lg |G|$) in the number of calls to the oracle for f and in the overall polynomial time).

There are several, and some quite surprising, models of quantum universal computation. The most basic one is that of quantum unitary-operations based circuits, that is defined in a similar way as in the classical case, only gates have to be quantum, representing quantum unitary operations. Given an algorithmic problem P, in order to solve it using a quantum circuit one has to find at first a unitary operations U_P that solves P and then to create a quantum circuits C_{U_P}, with quantum gates from some universal set of quantum gates, that implements U_P.

A variety of special problems concerning quantum computation comes from the fact that quantum unitary operations have to be reversible, that is such that one can uniquely determine inputs from their outputs. This seems to be a very special and strong restriction because from the most basic logical operations only NOT is reversible and none of the basic arithmetical operations. An important contribution to the understanding of the computational power of quantum phenomena was a surprising result of Bennett (1973) that says that *if a function f is computable by a one-tape Turing machine in time $t(n)$, then there is a 3-tape reversible Turing machine computing, with constant time overhead, the mapping $a \rightarrow (a, g(a), f(a))$, where $g(a)$ is so called* garbage *that can be removed using a special technique.* For classical reversible computations of Boolean functions universal is so called Toffoli operation, or control-control-not operation, $\mathrm{CCNOT}(x, y, z) = (x, y, (x \cap y) \oplus z)$.

Nature offers many ways – let us call them technologies – various quantum information processing primitives can be exhibited, realized and utilized. Since it appears to be very difficult to exploit potential of the Nature for QIP, it is of large importance to explore which quantum primitives form universal sets of primitives. Also from the point of view of the understanding of the laws and limitations of QIP, and also of quantum mechanics itself, the problems of finding rudimentary and universal QIP primitives are of large importance.

Concerning universal sets of computation primitives, the very basic result says that a single two-qubit operation control-not, $CNOT(|x\rangle.|y\rangle) = |x\rangle|x \oplus y\rangle$, and all one-qubit gates form a universal set of gates that can be used to design, for any unitary operation and any given precision $\varepsilon > 0$, a quantum circuit to approximate this operation with precession ε. (The catch is that it is very difficult to create the CNOT-gate because such a gate has to be able to transform two separable states into an entangled state.[15] Universal is also the set of the

[15] There are many ways how to create entangled states. For example, using various special physical processes. Of importance for understanding problems with the design of quantum processes is the fact that if CNOT is applied to two simple and separated one-qubit states, then CNOT may produce an entangled state: Indeed, $\mathrm{CNOT}(|0\rangle, \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Another surprising way how to create an entangled state of two separated particles is so-called entanglement swapping: If particles P_1 and P_2 are in the EPR-state and so are particles P_3 and P_4, then Bell measurement of particles P_2 and P_3, makes particles P_1 and P_4, that have never interacted before, to get into the maximally entangled EPR-state: In other words,

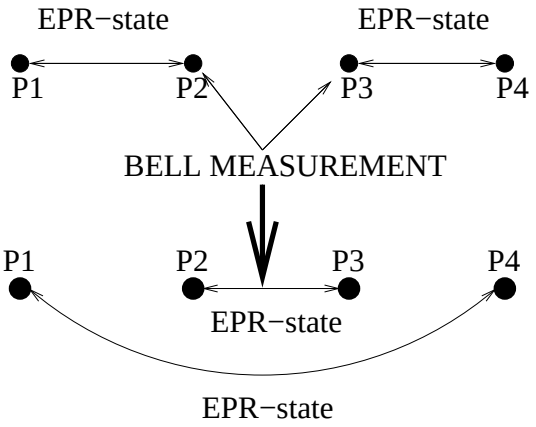


Fig. 3. Entanglement swapping

following three operations: CNOT, Hadamard and $\sigma_z^{1/4} = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{\pi}{4}i} \end{pmatrix}$. For computational purposes with classical input and output, universal is also the set of only two simple gates: the Toffoli gate and the Hadamard gate (Shi, 2002). This actually means that in order to get universality for quantum computation one has to add the Hadamard gate to the Toffoli gate that is universal for classical reversible computation. (Hadamard gate can actually create a perfectly random bit.) It is also known that any n-qubit unitary operation can be implemented by a circuit consisting of $\mathcal{O}(4^n)$ gates CNOT and one-qubit gates (see Vartianen et al., 2003). One of the recent surprising results in QIPC is that universal, from the computational point of view, are also circuits with gates performing only measurements and that what is needed for that are measurement-gates from only a very small set of gates. Measurement gates can be specified by Hermitian operators and measurements then correspond to the orthogonal basis created by the orthogonal set of eigenvectors of these Hermitian matrices. Actually, universal is a set of only four different Hermitian operators (measurements, see Perdrix, 2004). Measurement-based computations are probabilistic, up to a Pauli matrix, but this is only a small handicap. Another surprising model of universal computation are so-called one-way computers at which computation starts with a special entangled, so-called cluster state, but then only one qubit measurements are performed (Raussendorf and Briegel, 2000). All these results indicate that search for primitives in quantum computation is likely still to be full of surprises and options, what is actually not so strange because Nature offers so many way quantum information processing processes can be exhibited.

CNOT gate has to be able to make entangled two particles that have never before interacted, see Figure 3.

Two types of circuits are of special importance. Universal circuits, for certain number k of qubits, that can perform any unitary operation on k qubits if some classical parameters are fixed appropriately. Such universal circuits, with 3 CNOT gates and 15 elementary rotation gates for the case of two qubits and with 40 CNOT gates and 98 elementary rotation gates in the case of three qubits were derived by Vatan and Williams (2003, 2004), see also Gruska (2005).

Programmable circuits (sometimes called programmable processors) are another type of circuits that are universal in some restricted sense and that are of theoretical and also of large application interest. The basic idea is similar to that in case of classical universal circuits: certain inputs form so-called *operation register* and are used to specify, through a quantum state, an operation U that is to be performed on the state $|\phi\rangle$ given on the remaining inputs - on *data register*. There are several reasons why are such circuits are of importance. They may be universal for a set of operations and the operation to be performed can be result of some previous computation. The idea of programmable circuits has a limited use in case it is required that the outcome $U(\phi)$ is determined uniquely and perfectly, because in such a case in order for a programmable circuit to be able to perform n unitary operations the dimensionality of the program space has to be n, in order for the circuit to be able uniquely distinguish the program given. More interesting and practical seem to be the cases that the outcomes should be correct only with some (sufficiently large) probability, or should only approximate the correct result, again with a given precision. Approximate programmable circuits also better reflect reality because circuits with perfect outcomes are an idealization only. For an overview of the subject and latest results on approximate programmable circuits that can approximate a set of unitary operations see Hillery et al. (2005). There are many interesting/important problems associated with such programmable circuits. For example, how to determine input that makes the circuit/processor to make best approximation of a given unitary.

Of interest and importance are also investigations what kind of circuits can be simulated in polynomial time on classical computers. Almost "classical" result of Gottesman and Knill (see Nielsen and Chuang, 2000), says that circuits composed of the CNOT-gate, Hadamard-gate and the standard basis measurement, so called Clifford circuits, can be simulated on classical computers in polynomial time. Recently, Markov and Shi (2005) have shown that a quantum circuit with n gates, whose underlying graph has tree-width d can be simulated classically in $n^{\mathcal{O}(1)}e^{\mathcal{O}(d)}$ time, which is polynomial in n if $d = \mathcal{O}(\lg n)$. This result has a variety of implications: for example in classical polynomial time one can simulate any log-depth circuit whose gates apply to nearby qubits only. Another approach to the problem of simulation on classical computers was taken by Somma et al. (2006). They consider a special Lie-algebraic models of computation and showed that these models can be efficiently simulated on classical computers in time polynomial in the dimension of algebra. Their results generalize those on fermionic linear optics computations.

Another very basic model of quantum computation are quantum finite automata. Actually, there are several versions of them. Three very basic problems for models of quantum automata to explore are: (a) What is the class of languages accepted by a given model? (b) Which accepting probabilities can be achieved with a given model of automata? (c) How does the size of automata of the model (the number of states) compares to the size of equivalent minimal deterministic finite automata?

Comparing with classical finite automata, quantum finite automata have special strength, due to the power of quantum superposition (parallelism), but also a special weakness, due to the requirement that they have to be reversible. (It is important to notice that negative impacts of reversibility can be, to a large extent, compensated by a suitable distribution of suitable measurements.) For some models, quantum finite automata accept a smaller class of languages as regular languages and for some other models they accept exactly the class of regular languages. Of large importance is what kind of measurements are performed and which measurement policy is used. For example, a measurement is performed after each computation step or only at the end of computation - two extreme options. It has also be shown that in some cases quantum finite automata can be exponentially more succinct than classical deterministic finite automata. However, in some cases the opposite situation occurs. The very basic models of quantum finite automata, so called one-way (or real time) quantum automata, are defined similarly as probabilistic automata, only instead of probabilities, probability amplitudes are used and there is one additional requirement, namely that the overall evolution has to be unitary. More peculiar are quantum two-way automata. In the most basic model, they are a natural generalization of the classical two-way probabilistic finite automata. Quantum two-way automata can accept, with high probability, even some non-regular or non-context-free languages. In another model, quantum two way automata work almost as classical ones, they only have an additional quantum memory and at each step they either perform a usual classical move and a unitary operation on the state of their quantum memory, or a measurement on quantum memory is performed that then specifies, in a random way, the next move. Such automata have been shown to be much more powerful than classical probabilistic two-way finite automata (Ambainis and Watrous, 1999), even in the case quantum memory is restricted to one qubit (for an overview of concepts and results concerning quantum finite automata, see Gruska (2000).

The very basic model of quantum Turing machines, originally due to Deutsch (1985), is again a modification of that of a probabilistic Turing machine - probabilities are only replaced by probability amplitudes. However, a non-trivial additional requirement is that the overall evolution of a quantum Turing machine has to be unitary. A state of such a quantum Turing machines can be seen as a weighted superposition of many configurations of a classical Turing machines. This model has been used to define basic quantum complexity classes and to develop quantum structural complexity. Such a model has classical inputs and outputs, only its evolution is quantum. Two new quite different models

of Turing machines are of interest and importance. Both of them have quantum inputs and outputs (as sequences of qubits). One model (Jorrand and Perdrix, 2004), works with one additional qubit as memory and only measurements as operations. Another model is that of quantum Turing machines with classical control and quantum operations (Jorrand and Petrix, 2004a). The basic philosophy behind many of such models is that measurement is the basic tool to make quantum world to perform computations we need in the classical world.

An important challenge concerning quantum computation is to develop a really good model of quantum cellular automata. There have been numerous attempts to do that, with variety of interesting results, but one can say that theory of quantum cellular automata is still not in a good shape. At the same time, quantum cellular automata are of large importance for quantum physics because interactions with neighbours is the very basic way Nature works. Those versions of quantum cellular automata that are O.K., are modifications of the partitioned or block-type of the classical cellular automata, see Schumacher and Werner (2004), for recent results.

Quantum (structural) complexity theory is also being developed and it is an important part of quantum information processing science. One of the goals of quantum complexity theory is to challenge our basic intuition how physical world behaves. One can also say that quantum complexity theory is of great interest because one of its goals is to understand two of great mysteries of 20th century: what is nature of quantum mechanics and what are the limits of computation. It would be astonishing if a merge of such important areas would not shed light on both of them and would not bring new great discoveries. Taking complexity theory perspective can lead us to ask better questions about quantum nature – nontrivial, but answerable questions, which put old quantum mysteries in a new light even if they fall short of answering them (Aaronson, 2005).

Quantum complexity theory has as the basic complexity class **QP** (as a quantum variant of the class **P**) and the class **BQP** (as a quantum variant of the class **BPP**). There are also two quantum versions of the class **NP**, namely the classes **NQP** and **QMA**. There are also many variants of the classes of relativistic quantum computing. Unfortunately, an introduction of all these classes did not help to make order in the ZOO of more than 470 classical complexity classes. Just opposite happened, the mess got larger. For an overview of recent results see Gruska (1999-2005)). From the recent surprising results in this area we mentioned that of Raz (2005) showing enormous power of quantum advices.[16]

In connection with theoretical investigations concerning quantum information processing and communication, of large importance is to find out whether we can really build powerful quantum computers and what is required for success. In this connection, one of the main goals of quantum informatics in general,

[16] Raz has shown that a quantum interactive proof system at which the verifier gets quantum advices can solve any problem whatsoever.

and quantum complexity theory in particular, is to help to resolve this puzzle. In behind is actually question whether our world is polynomial or exponential, as pointed out by Aaronson (2005). The fact that such a basic question is unresolved makes also of large importance the task to study more elementary models as are that of quantum circuits, quantum programmable circuits and quantum finite automata.

Main new challenges of quantum complexity theory can be seen as follows (see also Gruska (2005): (a) To help to determine whether we can build (and how) powerful quantum computers. (b) To help to determine whether we can effectively factorize large integers using a quantum computer. (c) To use complexity theory paradigms to classify quantum states (d) To use complexity theory (computational and communication) to study quantum entanglement and nonlocality. (e) To use complexity theory to determine power of decoherence and to find ways to fight decoherence. (f) To use complexity theory to formulate laws and limitations of physics. (g) To study feasibility in physics on a more abstract level. (h) To study various quantum theory interpretations from a new and more abstract (complexity) point of view. (e) To develop a more firm basis for quantum mechanics. (f) To develop new tests of quantum mechanics.

4 Outcomes and challenges of quantum communication

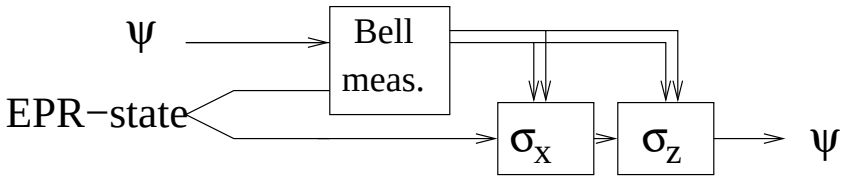


Fig. 4. Quantum teleportation

Quantum teleportation was the first and is still the most amazing new feature of quantum communication. The basic idea is very simple: if two parties, say Alice and Bob, share two particles, say A and B, in the EPR-state and Alice gets a new particle P in an unknown state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, then by performing the Bell measurement (that is the measurement using the Bell states), on her two particles, Bob's particle gets with the same probability into one of the four states $|\psi\rangle$, $\sigma_x|\psi\rangle$, $\sigma_z|\psi$ and $\sigma_x\sigma_z|\psi\rangle$, and Alice gets information (say, in the form of two bits) which of these four cases took place. If Alice sends this information to Bob, through a classical public channel, for example by email. Bob can then make his particle B to get into (still unknown for him) state $|\phi\rangle$ by performing on his particle one of the operations σ_x, σ_z or $\sigma_x\sigma_z$, because $\sigma_x^2 = \sigma_z^2 = I$. This way Alice can teleport, not knowing what, to not knowing where.

Quantum teleportation allows therefore to send one qubit by sending two classical bits (if shared entanglement is available). In some sense, an inverse process is so called *dense coding* that allows in one qubit to send two bits (if shared entanglement is again available). This is also surprising because so-called *Holevo theorem* says that in one qubit we can store faithfully only one bit.

Quantum teleportation allows perfectly secure transmission of quantum information (encoded via qubits) provided communicating parties share enough of EPR-states.

Shared entanglement can be also used to exhibit so called pseudo-telepathy, see Brassard et al., 2003. For example, in various games that look as having participants to use telepathy to make agreements, but actually correlations between their actions are achieved by proper measurements of proper shared entangled states.

It has been shown that shared entanglement can be used to improve exponentially protocols for a variety of communication tasks. For example, see Buhrman et al. (1998), Raz (1999). However, for some other communication tasks, as for computation of the *inner product*, it cannot.

Results of communication complexity have also been used to show that some phenomena are likely impossible in physical world. For example, they were used to show, see van Dam (2005), Brassard et al. (2005), why are the correlations achievable by quantum processes not maximal among those that would preserve non-signaling condition of special relativity. They were also used to explore the question how well can processes of quantum mechanics approximate PR-boxes, see page 19, that would exhibit strongest correlations preserving the non-signaling condition. They have shown that, on one side, that availability of prior shared entanglement allows to approximate PR-boxes with a success probability $\cos^2 \frac{\pi}{8} \approx 0.854$ and that would it be possible to do that with probability greater than 0.908, then any Boolean function could be computed using only one bit of communication, what is considered as impossible. An interesting challenge is to close the gap between 0.854 and 0.908, in the above context.

Large progress in understanding various aspects of quantum communication has been made during the recent years. We mention here only some results concerning quantum entanglement, and capacities of quantum channels.

4.1 Outcomes and challenges of quantum entanglement

In this area very large progress has been made in recent years. In spite of that in almost all its areas there are big challenges.

Basic problem is how to generate entangled states and how far entangled particles can be. A large variety of physical processes have been explored that result in entangled states. Importance of entangling unitary operators, those that can transform a product state to an entangled state has also been demonstrated. For example, any such two qubit entangling operation and all one qubit operations form a universal set of unitary operations. Entanglement swapping

is perhaps the most counterintuitive way to generate entangled states. To decide whether a given mixed state is entangled is another important problem and many methods to do that were developed. Problem how many pure and maximally entangled states one can get from a given set of mixed states is also pretty good understand and many methods to do that were explored. The same is true for entanglement concentration problem: to get some maximally entangled pure states from a set of less entangled pure states. Discovery of bound entangled states - those mixed entangled states from which one cannot get pure entanglement - has been a big surprise and so were discovery of various properties of such states and of various ways how bound entangled states can be useful. Study of entanglement monotones, invariants and measures[17] is another important area of research with many interesting and important results. The fact that entanglement can be used as a catalyst that can help, without being destroyed, to transform one quantum state to another using local quantum operations and classical communication (LOCC) has been another surprising discovery. laws and limitations of entanglement sharing and also quantitative and qualitative classification of multipartite states is another big challenge. On a more applied level, a big challenge is still to understand how important is entanglement for quantum computation. Another big challenge is to get a proper understanding how frequent is entanglement and how robust such a concept can be (for example that in some vicinity of some entangled states all states are entangled). For a review of results in all these areas see Gruska (2003).

Concerning quantum channels perhaps the main issue is to study various types of channels and various capacities. Entanglement plays by that a very important role. An important task was to find nice formulas to express different capacities and to find relations between different capacities, see Nielsen and Chuang (2000) and Gruska (1999-2005).

5 Outcomes and challenges of quantum cryptography

So called BB84 quantum protocol, due to Bennett and Brassard (1984), for generation of classical shared and perfectly secret keys, and numerous proofs, using a variety of techniques, under more and more realistic conditions (concerning perfection of the photon sources, quality of channels and perfection of the receivers), that BB84 protocol is unconditionally secure, have been the first highlights of quantum cryptography. The first experiment, due to Bennett and Brassard (1989), demonstrated feasibility of such a protocol for the distance of 32 cm. This has been increased, step by step to 120-150 km what used to be seen as limit set up by photon loses and detectors loses. Zhang et al., (2005) claim to increase maximal distance to 260km exploiting entanglement swapping

[17] An important measure is so called entanglement of formation E_f (how many maximally entangled states are needed to create a given state) is one of such measures and the additivity problem for this measure - that is if always $E_f(\rho_1 \otimes \rho_2) = E_f(\rho_1) + E_f(\rho_2)$) - is a very important open problem.

and quantum relays. A big challenge for classical key generation is still to make quantum generation of the classical keys more robust, more reliable and with much better performance. The DARPA network, that was launched in 2003 in Boston connecting Boston and Harvard universities on one side, and BBN Technology on the other side, is one of the most complex attempts to create a network for quantum key distribution. Such networks for metropolitan areas are currently seen as feasible.

So-called unconditional security of the classical keys generating quantum protocols actually says that undetectable eavesdropping is impossible, in a very reasonable probabilistic sense. Behind this results is impossibility of quantum cloning and destructive impacts of quantum measurement.

Another highlight of quantum cryptography has been the proof that unconditionally secure bit commitment is impossible, due to the fact that the existence of quantum entanglement is impossible to detect locally, and therefore quantum entanglement can always be used for cheating. There are again many proofs of this result and many consequences for such protocols as oblivious transfer, coin tossing and multipartite computation.

There are many other task of broadly understood cryptography, where quantum protocols have been developed and/or are under development: quantum authentication, digital signatures, public key cryptography, secret sharing, data hiding, anonymity, voting and so on. An open problem, recently resolved, by Watrous (2005), was to find a proper approach to quantum zero-knowledge proofs.

One of the most particular aspects of security in quantum cryptography is that in the quantum case a variety of possible quantum attacks is much larger and they can be more complex than in the classical case. All that makes security consideration in quantum case much more complex.

Of surprising elegance, simplicity and power, is quantum version of the classical ONE-TIME PAD cryptosystem. In the classical case, to encode an n-bit plaintext p, using a shared n-bit random key k, one performs bit-wise $\oplus$-operation to get the cryptotext $c = p \oplus k$. Decryption is done then using the same procedure: $p = c \oplus k$. Another way to see the classical ONE-TIME PAD cryptosystem is that n bits (of the shared key) are sufficient (and necessary) to hide perfectly n bits (of the plaintext) so one can get them all back (by decryption).

Quantum ONE-TIME PAD uses two n-bit keys k and k', to encode a plaintext of n qubits $|p_1\rangle, \ldots, |p_n\rangle$. An encryption of the ith qubit is done by multiplication with Pauli matrices $|c_i\rangle = \sigma_z^{k_i} \sigma_x^{k_i'} |p_i\rangle$ and its decryption can be obtained analogically as $\sigma_x^{k_i'} \sigma_z^{k_i} |c_i\rangle$. This way a qubit $|p_i\rangle$ is encrypted and sent through a mixed state $\{(\frac{1}{4}, |p_i\rangle), (\frac{1}{4}, \sigma_x|p_i\rangle), (\frac{1}{4}, \sigma_z|p_i\rangle), (\frac{1}{4}, \sigma_x\sigma_z, |p_i\rangle)\}$ that is undistinguishable from a random bit and therefore this quantum ONE-TIME PAD is perfectly secure. Amazing by that is that inspite of the fact that one qubit can hide infinitely many bits, in its amplitudes, to hide such a qubit as a whole, so

one can get the qubit back perfectly, only two classical bits are sufficient (and necessary) - see Mosca et al. (2000).

6 Outcomes and challenges of quantum formal systems

In the classical informatics, the development of high level formal systems, based on the concepts and tools of logic and formal semantics, to precisely specify and reason about computation, cooperation and communication processes in general, and about algorithms, protocols and concurrent systems in particular, has turned out of large importance for design and analysis of provably correct software for computation and communication systems. At the same time, this line of research in the classical informatics has brought theoretically surprisingly deep and practically very important and useful insights and outcomes concerning the laws and limitations of very large information processing, cooperation and communication systems.

Classical complexity theory research community, with emphasis on lower bounds, clearly underestimated, for a long time, an importance of this area of research. However, step by step, this, logic and formal semantics and abstraction based, area of research started actually to dominate in broadly understood theoretical computer science and there are good reasons to believe that it can be so, and even more, also in the area of the classical/quantum computing. Moreover, there is also a good chance that also this area of research can bring new view points and tools to deal with quantum mechanics in general, and with quantum information processing and communication in particular, and to put new lights on these areas.

There are two main reasons why quantum (quantum/classical) programming theory is much needed and has a chance to be insightful and useful. At first, any formal description of algorithms, protocols and processes, that make use of quantum phenomena has to to take into account both quantum and classical computation, cooperation and communication components and assemble them in such a way that they coexist, communicate and cooperate. (For example, preparation of quantum states is an (always inevitable) example of classical/quantum interaction and quantum measurement (and control actions that depend on its random outcome) is an (always inevitable) example of a classical/quantum/classical interaction. One can also say that classical/quantum interaction and cooperation is inherent in the classical/quantum information processing and communication. Fortunately, concepts and tools developed in the classical programming theory have been so abstract and powerful that they are now quite easy to adjust to cover classical-quantum case in a homogeneous way. Secondly, concepts and tools developed in the classical programming theory are so abstract and powerful that they allow to generalize naturally current (von Neumann) quantum mechanical framework that was created to deal just with "minimal view of quantum mechanics". This more general framework, that

allows to consider current view of quantum mechanics as a possible model, has its advantages.

Some of the main challenges in this area can be seen as follows:

- To develop quantum and classical/quantum versions of formal systems, for description, analysis and verification of algorithms, protocols and computation/communication systems, that have turned out to be so important for the classical information processing (see, for example, Lalire and Jorrand (2004)[18]).
- To develop abstract (for example category theory based) approaches to quantum/classical information processing and communication and also to quantum mechanics itself (see, for example, the approach of Abramsky and Coecke (2004)[19]).
- To develop new understanding of fundamental quantum phenomena using ideas and concepts coming from logic- and semantics-based formal systems, see, for example, Coecke (2005)[20].

7 Outcomes and challenges in beating decoherence

Decoherence - a destructive impact of the environment on any information processing quantum process - used to be seen, and it is still seen by many, as the main, and even unbeatable, obstacle for our goal to have reliable and powerful quantum information processing. One of the reason for that was a conviction that, from the physics point of view, sufficiently powerful quantum error correction is impossible for a variety of reasons. Some of them were beliefs that in the quantum case the number of the potential quantum errors[21] is infinite, that any attempt to detect errors by measurement would destroy, in an irreversible way, the erroneous state, and, finally, that quantum error correcting codes would need to fight successfully, and in polynomial time, exponentially fast growing decoherence, what looked again as impossible. However, it has, fortunately, turned out that, under very reasonable assumptions, it is sufficient to consider two types of errors - a *bit error* that is actually performed by the Pauli σ_x operator $(\sigma_x(\alpha|0\rangle + \beta|1\rangle) = \alpha|1\rangle + \beta|0\rangle)$ and a *sign error*, performed by the Pauli σ_z operator $(\sigma_z(\alpha|0\rangle + \beta|1\rangle) = \alpha|0\rangle - \beta|0\rangle)$. It was then shown, especially by Shor (1995, 1996), that not only sufficiently powerful error correcting codes and processes do exist, but that also quantum information processing

[18] They developed a process algebra approach to concurrent and distributed quantum computation.

[19] They recasted standard axiomatic presentation of quantum mechanics at a more abstract level in terms of category theory and this new and more abstract approach creates new possibilities to reason about quantum mechanics

[20] He developed so called *picture calculus* for quantum mechanics (as a natural extension of Dirac's notation).

[21] Nature actually does not make errors. It can only behave differently than we wish or expect.

can be realized in a fault-tolerant way. All that has been achieved by a clever generalizations of the ideas known from the classical linear codes. Second major breakthrough came with the discovery of threshold theorems that say that if elementary gates and channels have certain reliability,'then, using so-called concatenated codes, arbitrarily long, in time and space, reliable quantum information processing and communication is possible. Each such threshold theorem establishes some bounds and any improvement of upper and lower bounds on such thresholds is currently an important task and challenge that could help to see realistically what needs to be achieved and where we are currently concerning the development of elements for QIPC. Concerning fighting the decoherence, the main current challenges are: (a) to develop error models for specific QIPC technologies and for them also quantum error correcting codes; (b) to develop error detecting and preventing codes; (c) to generalize the concept of errors (see, for example, the concept of *nice error bases*, see, for example, Klappenecker and Rotteller (2000); (d) to explore various ideas of so called error-free subspaces.

8 Outcomes and challenges in beating quantum limitations and barriers

We will discuss here only three limitations: the one established by no-cloning theorem and its variations (no-deletion theorem and so on), and so called Turing barrier and **BQP**-barrier.

Buzek and Hillery (1996) were first to show that one can determine a reachable upper bound on the best way how to do cloning on qubits in an approximate way. Their results have been generalized in various ways to cover Hilbert space of larger dimension and other mathematically well defined operation that cannot be realized perfectly physically.

Finally, let us discuss Turing barrier or better Church-Turing barrier. Turing thesis, or Church-Turing thesis, can be formulated as follows: Every function that can be computed by what we would naturally regard as an algorithm is a computable function, and vice versa. So called Turing principle, formulated by Deutsch, reads as follows: Every finitely realizable physical system can be perfectly simulated by a universal computing machine operating by finite means. It is important to realize that Church-Turing thesis can be seen as one of the guiding principles for mathematic, physics and informatics and that since its very beginning Church-Turing thesis is under permanent attack from both mathematical and physical sciences. In mathematics and computing, all these attack used to be based on uncritical use of infinity, continua and density. It is also important to realize that recognition of physical aspects of the Church-Turing thesis has had important impacts also for physics. Turing barrier puts important restriction when searching for new physical theories

It is interesting and important to ask and answer the question what is the sense of trying to beat such a barrier that seems to be unbeatable. To that one can say the following: (a) It is interesting and intellectually usually very

rewarding to overcome limitations that seem to be unquestionable; One has to realize that limits of mathematics ought to be determined not solely by mathematics itself but also by physical principles; Attempts to show that there is a way to overcome Turing barriers are an important way to improve our understanding of physical world and nature in general and to find in it new important resources and/or theories.[22]

Two other questions are of interest for us now. Is there a chance to overcome this barrier and can we use quantum phenomena to do that? An extended version of Church-Turing thesis, that captures an important new phenomenon in computing - the existence of global computing network that continuously interact with environment, keep changing/evolving, works practically without an end and have inputs that can be seen as non-uniform. van Leeuwen and Wiedermann (2001) have shown that any (non-uniform interactive) network computation can be described in terms of *interactive Turing machines with advices*[23] that are equivalent to so called *site machines* and also equivalent to *internet machines (GRID-networks)* (that is a model inspired by computer networks and distributed computing). All these models accept all recursively enumerable sets and their complements.

The Extended Church-Turing Thesis (or VW-thesis of van Leeuven and Wiedermann) does not aim to attack the Church-Turing thesis; VW-thesis merely tries to identify a new proper extension of Church-Turing thesis (to cover computations that share the following features: non-uniformity of programs, interaction of machines and infinity of operations). VW-thesis tries to see the concept of computation in a broader sense, based on different assumptions and suited to answer different questions.

Since it is possible, in a sense, to get beyond, in the classical world, it is natural to see as a challenge to do so even more in quantum world. The attempts, as those of Kieu (2001), who has tried to show a quantum way to solve Hilbert's 10th problem, can hardly be seen as successful, as analysed by Hodges (2006). On the other hand, there seem to be more successful attempts to do so using some other physical principles. For example, Etesi and Németi (2002) showed that certain relativistic space-time theories license the idea of observing the infinity of certain discrete processes in finite time. That led to the observation that certain relativistic computers could carry certain undecidable queries in finite time. On this basis Wiedermann and van Leeuwen (2005) designed a

[22] In this context one can see as especially valid the following thought *When you try to reach for stars you may not quite get one, but you won't come with a handful of mud either.* by Leo Burnett.

[23] The idea of advices has the following motivation: Many systems in Nature prefer to sit in highly entangled multipartite states. Is it possible to make use of that to get an extra computational power (see Nielsen and Chuang, 2000)? Technically, we get to the following problem: Are quantum advices more powerful than classical? In other words, is (**BQP**/qpoly = **BQP**/poly?) Concerning the power of advices, the following result of (Raz, 2005) is of interest. A quantum interactive proof system at which the verifier gets quantum advices can solve any problem whatsoever.

relativistic Turing machine that models the above relativistic computer and that recognizes exactly Δ_2 set of Arithmetical Hierarchy.

BQP-barrier says that effectively computable are problems that are in **BQP**. The question whether we can beat this barrier seems to be more intriguing and it does not have (yet) such a statue of unbeatability as other barriers. Actually, previous versions of this barrier, that included complexity classes **P** and **BPP**, seem to be beaten, though we are not sure, yet.[24]

There are still many mysteries concerning the class **BQP**. Not only we do not know whether **NP** $\subseteq$ **BQP**, but we even do not know whether **NP** $\subseteq$ **BQP** would imply **P=NP**.

Related to that is the **NP**-barrier that says that not all **NP**-complete problems can be solved in polynomial time using the resources of the physical world.

There have been many attempts to beat **NP**-barrier and they are to large extend well summarized and analyzed by Aaronson (2005a). He discuss such ideas as quantum adiabatic computing, variations on quantum mechanics (nonlinearity, hidden variable theories), analog computing, but also more esoteric ones as relativity computing[25], time travel computing, quantum field, string and gravity theories, and even *anthropic computing*[26] Main conclusions are: (a) searches for overcoming **NP** barriers are important, they can bring a better understanding of the physical worlds; (b) none of the well specified attempts is successful - they usually forget to count all resources needed and/or all physics known.

In connection with **NP**-barrier, of interest and importance is the question, see Aaronson (2005) whether we should not take "**NP**-hardness assumption" saying that **NP**-*complete problems are intractable in the physical world* as a new principle of physics (as, for example, Second Law of Thermodynamic is). This principle starts to be used. Perhaps main problem with it is that why **NP**, why not **BQP** or **#P** or **PSPACE**.

On a more philosophical level, all above considerations lead to two basic questions: Is universe computable? Is it efficiently computable? It is nowadays clear that the assumption of the founders of the Hilbert space quantum mechanics that any state and observable are in principle implementable is wrong. That would allow to compute uncomputable functions. Less clear is what to consider as feasible.

[24] In this connection it is perhaps worth to observe that, on one side, likely nobody believes that classes **P** and **BPP** are identical, and, on the other side, Impagliazo and Widgerson (1997) gave quite convincing evidence that they are.

[25] The idea behind relativity computing can be informally described as that one makes a computer to deal with an intractable problem, then boards a spaceship and accelerates it to nearly speed of light. After returning to Earth, answer will wait for him (though all his friends would be long dead).

[26] They are models of computing in which the probability of one's own existence might depend on a computer's output.

9 Impact of quantum informatics

Let us try to summarize briefly three impacts of quantum informatics: on quantum physics, quantum information processing and communication and on (classical) informatics itself.

Impacts on (quantum) physics: Quantum informatics brings to quantum physics a new way of thinking, new value systems, new ways, more general and more precise, of formulation of quantum physics laws and limitations, new ways to get around, in a reasonable way, of otherwise its strict laws and also a variety of new technical concepts, methods, tools and results. It brings new paradigms, concepts, models, measures and so on. It helps to increase quality of reasonings and findings in quantum physics. Quantum complexity theory helps to establish principles, see Aaronson (2003, 2004, 2005, 2005a), that allow to see impossibility of some physical phenomena and to restrict search space for new physical theories in general and for variations of quantum mechanics in particular.

Impacts on quantum information processing and communication technology: Quantum informatics helps to discover and analyse power of quantum information processing primitives and their optimal use (see, for example, Gruska (2005)); to see merits, potentials and limitations of the potential technologies also without doing experiments; and to discover ways to manage and fool quantum decoherence.

Impacts on informatics itself: In a similar way as the development of probability theory brought a variety of powerful method to solve problems of "classical" (that is non-probabilistic in this context) mathematics and brought powerful tools practically for all areas of science and technology in general, the development of quantum informatics can be expected to bring (and already brings) a variety of paradigms, methods and tools that can be used to deal with problems of classical informatics for and also many areas of science and technology, especially for those dealing with microworld. Some of the first examples how one can use quantum tools to solve non-quantum problems have been demonstrated by de Wolf (2005). Moreover, taking into consideration that *computation, communication, security and feasibility are also physical concepts,* in a way, quantum informatics allows also informatics to meet its main goals in a more proper way.

10 Conclusion

The development of quantum information processing science and technology has come to the point that in order to make further significant progress in this area a new view is needed and pursued concerning the overall aims, scope, methods, primitives of the underlying sciences and technologies that need to be developed. Pursuing much more paradigms, viewpoints, methods, and tools of quantum informatics is one of the ways to go.

References

1. S. Aaronson. Multilinear formulas and skepticism of quantum computing. quant-ph/0311039, 2003.
2. S. Aaronson. Is quantum mechanics an island in Theoryspace? quant-ph/0401062, 2004.
3. S. Aaronson. Are quantum states exponentially long vectors? quant-ph/0507242, 2005.
4. S. Aaronson. NP-complete problems and physical reality. quant-ph/0502072, 2005a.
5. S. Abramsky and B. Coecke. A categorical semantics of quantum protocols. quant-ph/0402130, 2004.
6. D. Aharonov, A. Ambainis, J. Kempe, and U. Vazirani. Quantum walks on graphs. Proc. of 33th STOC, 50-59, 2000.
7. A. Ambainis. Quantum lower bounds by quantum arguments. quant-ph/0002066, 2000.
8. A. Ambainis. Quantum walks and and their algorithmic applications. quant-ph/0403120, 2004.
9. A. Ambainis and J. Watrous. Two-way finite automata with quantum and classical states. quant-ph/9911009, 1999.
10. Ch. H. Bennett Logical reversibility of computation. *IBM Journal of Research and Development*, 17:525–532, 1973.
11. Ch. H. Bennett and G. Brassard. The dawn of a new era for quantum cryptography. The experimental prototype is working! *SIGACT News*, 20(4):78–82, 1989.
12. Ch. H. Bennett and G. Brassard. Quantum cryptography: public key distribution and coin tossing. In *Proceedings of IEEE Conference on Computers, Systems and Signal processing, Bangalore (India)*, pages 175–179, 1984.
13. 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.
14. G. Brassard, A. Broadlent, and A. Tapp. Quantum telepathy. quant-ph/0306042, 2003.
15. B. Brezger, L. Hackermüller, S. Uttenthaler, J. Petschinka, M. Arndt, and A. Zeilinger. Matter-wave interferometer for large molecules. quant-ph/0202158, 2002.
16. H. Buhrman, R. Cleve, and A. Wigderson. Quantum versus classical communication complexity. In *Proceedings of 30th STOC*, pages 63–68, 1998.
17. V. Bužek and M. Hillery. Quantum copying: beyond the no-cloning theorem. *Physical Review A*, 54:1844–1852, 1996.
18. N. Cerf, N. Gisin, S. Masar, and S. Popescu. Quantum entanglement can be simulated without communication. *Physical Review Letter*, 94:220403, 2005.
19. A. M. Childs, J. Preskill, and J. Renes. Quantum information and precision measurement. quant-ph/9904021, 1999.
20. B. S. Cirel'son. Quantum generalization's of Bell's inequality. *Letters in Mathematical Physics*, 4(2):93–100, 1980.
21. B. Coecke. Kindergarten quantum mechanics. quant-ph/0510032, 2005.
22. R. de Wolf. Lower bounds on metric rigidity via a quantum measurement. quant-ph/0505188, 2005.

23. D. Deutsch. Quantum theory, the Church-Turing principle and the universal quantum computer. *Proceedings of Royal Society of London A*, 400:97–117, 1985.
24. A. K. Ekert. Quantum cryptography based on Bell's theorem. *Physical Review Letters*, 67(6):661–663, 1991.
25. C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, and H. Yeh. Current status of the DARPA quantum network. quant-ph/0503058, 2003.
26. A-N. Zhang et al. Quantum-relay-assisted key distribution over high photon loss channels. quant-ph/0508062, 2005.
27. Ch-Z. Peng et al. Experimental free-space distribution of entangled photon pairs over a noisy ground atmosphere of 13 km. quant-ph/0412218, 2004.
28. M. Arndt et al. Quantum physics from A to Z. quant-ph/0505187, 2005.
29. E. Farhi, J. Goldstone, S. Gutmann, and M. Sipser. Quantum computation by adiabatic evolution. quant-ph/0001106, 2000.
30. G.Brassard, H. Buhrman, N. Linden, A. A. Methot, A. Tapp, and F. Unger. A limit on nonlocality in any world in which communication complexity is not trivial. quant-ph/0508042, 2005.
31. N. Gisin. Can relativity be considered complete? from Newton nonlocality to quantum nonlocality and beyond. quant-ph/0512168, 2005.
32. L. K. Grover Quantum mechanics helps in searching for a needle in a haystack. *Physical Review Letters*, 78:325–328, 1997a.
33. J. Gruska. *Quantum computing*. McGraw-Hill, 1999-2005. See also additions and updatings of the book on http://www.mcgraw-hill.co.uk/gruska.
34. J. Gruska. Descriptional complexity issues in quantum computing. *Automata, Languages and Combinatorics*, 5(3):198–218, 2000.
35. J. Gruska. Quantum entanglement as a new quantum information processing resource. *New Generation Computing*, 21:279–295, 2003.
36. J. Gruska. *General Theory of information transfer and combinatorics*, chapter Universal sets of quantum information processing primitives and optimal use of such primitives, pages 356–377. Springer-Verlag, 2005.
37. J. Gruska. Quantum complexity theory goals and challenges. *International Journal of Quantum Information*, 3(1):31–39, 2005.
38. M. Hillery, V. Bužek, and M. Ziman. Approximate programmable quantum processors. quant-ph/0510161, 2005.
39. A. Hodges. Can quantum computing solve classically unsolvable problems? quant-ph/0512248, 2005.
40. R. Impagliazo and A. Widgerson. **P=BPP** unless **e** has subexponential circuits: derandomization. In *Proceedings of 29th STOC*, pages 220–229, 1997.
41. B. Julsgaard, A. Kozhekin, and E. S. Polzik. Experimental long-lived entanglement of two macroscopic objects. quant-ph/0106057, 2001.
42. T. D. Kiew. Quantum algorithm for Hilbert's tenth problem. quant-ph/0110136, 2001.
43. A. Klapenecker and M. Rötteler. Beyond stabilizer codes I: nice error bases. quant-ph/0010082, 2000.
44. M. Lalire and Ph. Jorrand. A process algebraic approach to concurrent and distributed quantum computation: operational semantics. quant-ph/0407005, 2004.
45. D. A. Lidar, I. L. Chuang, and K. B. Whaley. Decoherence-free subspaces for quantum computing. *Physical Review Letters*, 81:2594–2598, 1999.
46. I. Marcikic, H. de Riedmatten, W. Tittel, H. Zbinden, M. Legre, and N. Gisin. Distribution of time-bin entangled qubits over 50 km of optical fiber. quant-ph/0404124, 2004.

47. G. Mitchison and R. Jozsa. Counterfactual computations. quant-ph/9907007, 1999.
48. M. Mosca, A. Tapp, and R. de Wolf. Private quantum channels and the cost of randomizing quantum information. quant-ph/0003101, 2000.
49. M. A. Nielsen and I. I. Chuang. *Quantum information processing*. Cambridge University Press, 2000.
50. M. A. Nielsen and I. L. Chuang. Programmable quantum gate arrays. quant-ph/9703032, 1997.
51. S. Perdrix. State transfer instead of teleportation in measurement-based quantum computation. quant-ph/0402204, 2004.
52. S. Perdrix and P. Jorrand. Classically controlled quantum computing. quant-ph/0407008, 20004a.
53. S. Perdrix and Ph. Jorrand. Measurement-based quantum Turing machines and questions of universalities. quant-ph/0402156, 2004.
54. S. Popescu and D. Rohrlich. Causality and non-locality as axioms for quantum mechanics. quant-ph/9709026, 1997.
55. R. Raussendorf and H. J. Briegel. Quantum computing by measurements only. *Phys. Rev. Lett, 86*, 2004.
56. R. Raz. Exponential separation of quantum and classical communication complexity. In *Proceedings of* 31*st ACM STOC*, pages 358–367, 1999.
57. V. Scarani. Feats, features and failures of the PR-box. quant-ph/0603017, 2006.
58. V. Scarani, W. Tittel, H. Zbinden, and N. Gisin. The speed of quantum information and the preference frame: analysis of experimental data. quant-ph/0007008, 2000.
59. B. Schumacher and R. F. Werner. Reversible quantum cellular automata. quant-ph/0405184, 2004.
60. Y. Shi. Both Toffoli and controlled-NOT need little help to do universal computation. quant-ph/0205115, 2002.
61. P. W. Shor. Algorithms for quantum computation: discrete log and factoring. In *Proceedings of 36th IEEE FOCS*, pages 124–134, 1994.
62. P. W. Shor Scheme for reducing decoherence in quantum computer memory. *Physical Review A*, 52:2493–2496, 1995.
63. P. W. Shor Fault-tolerant quantum computation. In *Proceedings of 37th IEEE FOCS*, pages 56–65, 1996.
64. T. Short, N. Gisin, and S. Popescu. The physics of no-bit commitment generalized quantum non-locality versus oblivious transfer. quant-ph/0504134, 2005.
65. R. Somma, H. Barnum, and G. Ortiz. Efficient solvability of hamiltonians and limits on the power of some quantum computational models. quant-ph/0601030, 2006.
66. W. van Dam. Implausible consequences of superstrong nonlocality. quant-ph/0501159, 2005.
67. J. van Leeuwen and J. Wiedermann. *Mathematics unlimited, 2001 and beyond*, chapter The Turing machine paradigm in contemporary computing, pages 1139–1156. Springer Verlag, 2001.
68. J. J. Vartiainen, M. Möttönen, and M. M. Salomaa. Efficient decomposition of quantum gates. quant-ph/0312218, 2003.
69. F. Vatan and C. Williams. Optimal realization of a general two-qubit quantum gate. quant-ph/0308006, 2003.
70. F. Vatan and C. Williams. Realization of a general three-qubit quantum gate. quant-ph/0401178, 2004.

71. J. Watrous. Quantum zero-knowledge proofs. quant-ph/0511020, 2005.
72. J. Wiedermann and J. van Leeuwen. Relativistic computers and non-uniform complexity theory. In *Proceedings of CMU'02, LNCS 2509*, pages 287–299, 2002.