Natural Computing (2007) 6:75–112
DOI 10.1007/s11047-006-9016-6

A broader view on the limitations of information processing and communication by nature*

JOZEF GRUSKA
Faculty of Informatics, Masaryk University, Botanická 68a, 60200, Brno, Czech Republic
E-mail: gruska@informatics.muni.cz

Abstract. Several new and broader views on *computation in Nature and by Nature*, and on its limitations and barriers are presented and analysed briefly. Quantum information precessing, global network information processing and cosmology-based information processing theories are seen as three extreme, but well-founded approaches to computation by Nature. It is also emphasized that a search for barriers and limitations in information processing as well as attempts to overcome their barriers or to shift limitations, can have deep impacts on science, especially if they are accompanied by a search for limitations and barriers also in communication and security. It is demonstrated that a search for barriers in communications brings a lot of interesting and deep outcomes.

Computational and communication complexity is shown to play an important role in evaluating various approaches to get through barriers that current physical theories impose. It is also argued that a search for barriers and limitations concerning feasibility in information processing and physical worlds are of equal or maybe even of larger importance than those to overcome the Church-Turing barrier and some communication barriers. It is also emphasized that relations between information processing in the real and virtual worlds, or between physical and information worlds, are likely very deep and more complex than realized. All that has even broader sense than usually realized because we are witnessing a radical shift in the main characterization of the current science in general. A shift from so called *Galilean science* dominated by mathematics, to the Informatics (based) science - an informatics methodology based science and technology.

Key words: Frontiers and barriers of information processing, Information processing by nature, Quantum information processing, Feasibility, Security, Church-Turing barrier

* This is an extended version of a paper (Thies et al. 2006) that appeared in the 12th International Meeting on DNA Computing, June, 2006.

1 Introduction

> Nothing exists except atoms and empty space: everything else is opinion.
>
> Democritus (ca. 400 BC)

The attempts to discover “ultimate” laws and limitations of information processing by Nature, as well as the attempts to overcome the already established limitations/barriers, are important for knowing the limitations of both Nature and the processes by which we utilize Nature for both information processing and the advancement of our knowledge of information processing in particular and of the Nature in general. This paper tries to discuss known and well-established barriers and merits of various attempts to beat them, as well as to point out importance of new, and perhaps even more important barriers. The subject we deal with is rich in exact results, and equally in speculations and expectations based on philosophical standpoints, experiences and extrapolations. The richness of the underlying subject and the vagueness of the limits we are attempting to reach, as well as the limitations of our knowledge, cause our reasoning and deductions to sometimes be not sufficiently exhaustive and/or quite provocative. Another our goal is to demonstrate that the whole subject of such barriers is very complex, deep, fascinating and still wide open for bright minds to tackle.

2 Overcoming the Turing barrier

It is natural that once some important limitations/barriers of our physical or other worlds are discovered, or established, some scientists immediately launch a crusade to address them, or at least to find reasonable modifications of the limitations/barriers that can be overcome, again to a reasonable extend. A belief of many, based also on the historical experience, is that so-called final, or unbeatable, limitations often get beaten, sooner or later, at least in some sense. This is also the case with the famous Turing barrier, or the Church-Turing barrier, which specifies what is computable. We can say that there have been no convincing attempts to break the Church-Turing barrier yet, but also we can say that the search for them has not been without interesting outcomes, and new, interesting and important, views on this barrier have been developed.

The Church-Turing thesis in mathematics/computing is usually understood as saying that any current and future algorithm can be implemented on a Turing machine. In other words, what is computable on Turing machines is and will be exactly that which is computable.[1]

Naturally, the attempts to beat the unbeatable mostly fail and therefore the scientific community at large rarely pays much attention to them, no matter how cleverly their faults are hidden, until the evidence that they were beaten is no longer to ignore (or the generation of scientists that grew up on these believes dies out). Common sense and historical experience also say that such attempts have no chance, unless some radically new discovery has been made that has shown that the world we deal with has different laws and limitations than has hitherto been thought. The discovery of the laws of quantum mechanics, or various other discoveries or hitherto not verified/refuted hypotheses concerning the laws and limitations of the physical world, or concerning our universe, are just such examples.

Similar situation has been regarding the attempts to overcome the Church-Turing barrier. The attempts to beat this barrier and to show the existence of *super-Turing computations* or *hypercomputations*[2] are as old as the barrier itself. In fact, these attempts have been largely ignored so far.[3]

However, recently, several new developments in computing, such as those that fall under the term *computation by Nature*, new developments in physics and cosmology, and new views concerning the relations between the physical and information worlds, as well as an understanding that a new era of science is emerging, created a new view on and a new understanding of the information processing and may well need a new understanding of the Church-Turing barrier. Moreover, the recent developments indicate that searches for limitations and barriers in the area of information processing that had been thought of as being captured by the attempts to find barriers and limitations of computation, are perhaps too narrow and that of the equal, and maybe even of greater importance for science, and deeply correlated with all of the above limitations, can be the limitations and barriers in the area of communication, feasibility and security.[4]

Searches for barriers and limitations, as well as the attempts to overcome them, are of the great interest and importance, in many ways. This is also true of the approaches to identifying the shortcomings in our current models and theories of the physical and information worlds and of the ways how to improve our understanding of these two (?) worlds. Quantum mechanics, as a theory of quantum physical world, is an excellent example of a superb theory. At this theory the study of information processing and communication potentials, as well as of the possibilities to design unconditionally secure cryptographic systems could be also a way to distinguish different (mathematical) interpretations of the theory.

The usefulness of the attempts to overcome the existing barriers, both justifies and encourages the searches for new barriers in general. This is nicely expressed in the following well-known and deep observation attributed to Leo Burnett: *When you try to reach for the stars you may not always get one, but you won*'t come up with a handful of mud either, see wikipedia—Leo Burnett—wikiquote.

3 hysical and information worlds—the emergence of a new driving force of science

The existence of the physical world is hardly to be questioned and neither is the existence of the classical world or the classical physics. Less without problems is the existence of the quantum world—as a part (?) of the physical world. Quantum mechanics, our arguably most perfect, and best tested, theory of Nature, from the point of view of an agreement between theory and experiments, is full of mysteries and counterintuitive phenomena.[5] In the case of quantum mechanics, the relation between (Hilbert space) theory and objective reality—whatever that may mean—seems to be not simple, actually very complex, even mysterious. This is also demonstrated by a number of interpretations of quantum mechanics. The question of the borders between classical and quantum worlds has bothered scientists already for almost hundred years. Recently, especially in connection with the attempts to design quantum cryptography theory and systems, as well as quantum information processing and communication systems and theory, the question of borders between the classical and quantum worlds became an important research agenda with a variety of surprising results.[6]

Complexity of the relations between classical and quantum worlds is nicely illustrated by the following citations of leading experts (see Arndt et al. 2005 for all of them but one from Bohr): *The border between classical and quantum phenomena is just a question of money* (A. Zeilinger); *The classical–quantum boundary is simply a matter of information control* (M. Aspelmeyer); *There is no border between classical and quantum phenomena—you just have to look closer* (R. Bertlman); *There is no quantum world. There is only an abstract quantum physical description. It is wrong to think that the task of physics is to find out *how Nature is. Physics concerns what we can say about Nature* (N. Bohr[7]) and especially by the following analogy:

> I believe there is no classical world. There is only quantum world. Classical physics is a collection of unrelated insights: Newtons laws. Hamiltons 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 (D. Greenberger—see Arndt et al. 2005).

Almost everybody seems to agree that the main scientific goal of physics is to study concepts, phenomena, laws and limitations of the physical world. Less familiar is a slowly emerging view that the main scientific goal of informatics is to study concepts, phenomena, laws and limitations of the information world. This leads, quite naturally, as discussed later, to the very fundamental questions, that may sound quite surprising for some: *Which of these two worlds is more basic?* and, in addition: *Which of these two worlds is more real?* And, on a more technical level, what are the relations between the fundamental concepts of these two worlds.

The above views of the physical and information processing worlds and their relations, as well as the recent observations that "computation is physical",[8] that communication is physical and, as we will see later, also that feasibility and security are important physical concepts, put the attempts to overcome the Church-Turing computation barrier (and the search for barriers concerning communication, feasibility and security), to be important challenges for both physics and informatics because they may lead to advances in their basic theories and points of views.

The question, which of the two worlds, physical or informational, is more basic and/or more proper, is, of course, likely to be one of the eternal questions. However, even the fact that such a question is being asked can help, as discussed later, to see properly the limitations and barriers of such concepts concerning information processing phenomena as computation, communication, security and therefore also to indicate where to look for a proper way to get beyond their current limitations.

The importance of the concept of information for physics seems to be at first realized by Szilard, around 1927, in connection with the famous Maxwell demon paradox. Since then, the awareness of the importance of the concept of information for physics has matured, especially in quantum mechanics. Recent developments in quantum information processing caused that importance of information for physics is even more emphasized. At the extreme is the idea that everything is information and the following "confession" is usually contributed to John Archibald Wheeler: *I think of my lifetime in physics as divided into three periods: In the first period ... I was convinced that everything is particle; I call my second period everything is field; now I have new vision, namely that everything is information* and it reflects well new trends.[9] Related to this are the recent attempts to develop an understanding of the quantum mechanics on the basis of quantum information processing and also on the basis of the axioms related to information processing, as discussed later, page 18, (see also Clifton et al. 2002).

There is also one special reason for paying great attention to the information processing world, its laws and limitations. It is related to the historical change in the main view/characterization of the science that we are currently witnessing. This is also closely related to the emergence of a new scientific methodology that seems to have the potential to dominate soon so much science that it is expected to lead to a dramatic change in the main characterization of science in general.

Science had so far two main methodologies; an experimental one, with observations and experiments as the main tools; and a theoretical one, with mathematics and deduction/reasoning as its main tools. The development of informatics and information processing technologies have contributed to the emergence of a new, informatics-based, methodology where simulations, visualisation, algorithmisation, complexity considerations, processes (their specifications, verifications, analysis) and so on dominate. We believe that the impact of this new methodology on science is to be soon so great that the overarching view of science, Galilean typically, with elegant mathematical formulas, equations and so on as the main goal, will be soon replaced by a new view of science where information processing paradigms, value systems, concepts, models, systems and tools will dominate and will represent the main outcomes of science as well as the way science meets its two main goals: to explain and understand basic scientific phenomena and to predict the behaviour of the systems of Nature and society.[10]

The importance of the information world can also be seen from the following vision of the main eras of the overall development of society:

Neolithic era Progress was made on the basis of man having learned how to make use of the potentials provided by the biological world so as to have *food* available in a sufficient amount and whenever needed.

Industrial era Progress has been made on the basis that man has learned how to make use of the laws and limitations of the physical world so as to have *energy* available in a sufficient amount and whenever needed.

Information era Progress is and will be made on the basis that man learns how to make use of the laws and limitations of the information world to have *information* (processing energy) available in a sufficient amount and whenever needed.

Once such a very concise division of the history of mankind has been made, it is natural to ask whether we can envision a new, fourth, era. The answer seems to be positive, at least for us, and leads to the following expectations:

Security era Progress will be made on the basis that man learns how to make use of the laws and limitations of the physical, biological and information worlds so as to have *security*[11] available to a sufficient degree and whenever needed.

As discussed below, security is far from being only of the large practical importance. The development and study of theoretical concepts related to broadly understood cryptography is of the deep importance for understanding both the information processing and the physical worlds.

4 Computation by quantum Nature

A number of phenomena and discoveries in science have recently led to an increased interest in and study of the various models of computation that are performed in Nature or/and inspired by various phenomena of Nature. For example, various models of evolutionarycomputing[12] and bio-computing,[13] as well as models of computing based on the advanced/speculative physical theories as, for example, the relativistic computing (see Etesi and Németi (2002), Aaronson (2005b), and others).

4.1 *Quantum information processing*

There has recently been great progress in the area of quantum information processing and communication that is expected to lead to a qualitatively new quantum information processing technology as well as to a new understanding of the quantum world [see Gruska (1999–2004), Nielsen and Chuang (2000)].

The basic mathematical model of quantum mechanics is based on the concept of Hilbert space that should correspond to the physical concept of quantum system.[14] An n dimensional Hilbert space $\mathcal{H}_n$ is an n-dimensional complex vector space, with vectors (of norm one) corresponding to pure states of the underlying physical system, on which a scalar product of two vectors $|\phi\rangle = (a_1, \ldots, a_n)$ and $|\psi\rangle = (b_1, \ldots b_n)$ is defined as $\langle\phi|\psi\rangle = \sum_{i=1}^{n} a_i^* b_i$,[15] where a_i^* denotes complex conjugate of a_i, and on such a basis one can define the norm of a quantum state $|\phi\rangle$ as $||\phi|| = \sqrt{|\langle\phi|\phi\rangle|}$, and then also metrics and topology. For states (vectors) ϕ of a Hilbert space, so-called Dirac notation $|\phi\rangle$—ket vector—is usually used. Notation $\langle\phi|$—called *bra vector*—is used for a functional defined by $\langle\phi|(|\psi\rangle) = \langle\phi|\psi\rangle$. The superposition principle says that if $|\phi\rangle$ and $|\psi\rangle$ are states and $0 < \lambda < 1$, then $\sqrt{\lambda}|\phi\rangle + \sqrt{1-\lambda}|\psi\rangle$ is also a state. Quantum states of $\mathcal{H}_2$ are called *qubits—qbits* in an analogy to *cbits*—classical bits. States $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ then form the so-called *computational basis* of $\mathcal{H}_2$. Physically allowed operations on pure states are those represented by unitary matrices and a (discrete) computation step is then a (unitary) matrix-vector multiplication. Two simple, so-called Pauli, operators are: $\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, representing a *bit flip* and a *sign flip*—they are also used in the Quantum One-Time pad cryptosystem that is discussed later.

Perhaps the most puzzling feature of quantum mechanics is so-called projective measurement of quantum states that can be seen as being specified by an orthonormal basis $\{|\beta_i\rangle\}_{i=1}^{n}$. The quantum result of a measurement of a state $|\phi\rangle$ with respect to such a basis $\{|\beta_i\rangle\}_{i=1}^{n}$ is one of the basis states $|\beta_i\rangle$ (we say that $|\phi\rangle$ collapses, or jumps, to $|\beta_i\rangle$), and to the classical world an information is obtained to which of the states $|\beta_i\rangle$ the state $|\phi\rangle$ collapses. The probability that the state $|\phi\rangle$ collapses to a state $|\beta_i\rangle$ is $|\langle\beta_i|\phi\rangle|^2$.[16] Very special in the quantum world is also the design of composed quantum systems. If a Hilbert space $\mathcal{H}_n$ corresponds to a quantum system $\mathcal{S}_1$ and the Hilbert space $\mathcal{H}_m$ corresponds to a quantum system $\mathcal{S}_2$, then the Hilbert space $\mathcal{H}_{nm}$, the tensor product $\mathcal{H}_n \otimes \mathcal{H}_m = \mathcal{H}_{nm}$, corresponds to the quantum system composed of $\mathcal{S}_1$ and $\mathcal{S}_2$. If $\{\alpha_i\}_{i=1}{}^{n}$ is an orthonormal basis in $\mathcal{H}_n$ and $\{\beta_j\}_{j=1}{}^{m}$ is an orthonormal basis in $\mathcal{H}_m$, then the set of all tensor products $\alpha_i \otimes \beta_j$ forms an orthonormal basis in $\mathcal{H}_{nm}$. An n-qubit quantum register is then the tensor product of n one-qubit quantum systems, that is $\bigotimes_{i=1}^{n}\mathcal{H}_2$.

A very important fact is also that in any bipartite quantum system there are states that cannot be expressed as tensor products of the states of subsystems. An example of such a state in $\mathcal{H}_2 \otimes \mathcal{H}_2$ is so-called the EPR-state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Such states are called *entangled.* According to the theory, and experiments already up to 144 km confirm that, it may happen that two particles are in such an entangled state even if they are much space separated. The most important, and extremely mysterious, is then the fact that if two particles are in an entangled state, then any measurement of one of the particles immediately determines the subsequent result of the measurement of the other particle. In other words, measurements of particles in entangled states exhibit nonlocal correlations, which greatly contradicts common sense.[17] Until 1993, entanglement was seen as a mysterious feature of the quantum world, to bother mainly the philosophers of science, but of no deeper (immediate) interest for real physicists. Nowadays, entanglement is considered an important quantum resource that is behind unexpected computational and communicational power of quantum phenomena—for details see Gruska (1999–2004, 2003). For example, quantum entanglement allows quantum teleportation, a communication feature not exhibited in the classical world, and it in turn allows unconditionally secure information transmission, see below.

Pure quantum states mentioned above are states of closed quantum systems—that is of quantum systems isolated from their environment. For open quantum systems, correlated with their environment, the ones one can meet in practice, the key concept is that of a mixed state—a probability distribution $[\phi\rangle = \{(p_i, |\phi_i\rangle\}_{i=1}^{k}$ on pure states

$\{|\phi_i\rangle\}_{i=1}^k$. So-called *density operator/matrix* $\rho_{[\phi\rangle} = \sum_{i=1}^k p_i|\phi\rangle\langle\phi|$ corresponds to each of such mixed states. Of the key importance is then the fact that two mixed states with the same density matrices are physically indistinguishable.

The existence of quantum superposition, parallelism[18] and entanglement can be seen as the existence of resources not available in the classical world. It is due to them, that quantum computations and communications can exhibit speed-ups not achievable in the classical world. On the other hand, quantum information processing has two important limitations: *Demolition of quantum measurement*: measurement of a quantum state results, in general, in its disturbance; and *No-cloning theorem:* There is no way of copying unknown quantum states faithfully. Of importance for quantum information processing is also famous Heisenberg's *uncertainty principle/relation* that has been understood as setting limitations on measurements. See Ozawa (2005) for recent, more precise, formulation of the uncertainty principle.[19] The uncertainty relation can also be seen as one of those barriers that kept developing and almost all scientists had some problem with, even its founder, who said *I myself* ... only came to believe in the uncertainty relation after many pangs of conscience ..., with the same reference as for the citation of Schrödinger above.

4.2 *From the GRID computing to the global (internet) computer*

There have also been recently important developments in the area of classical computing itself. The emergence of the global, geographically distributed, permanently evolving, *internet network*, or *web network*, with its non-uniform and distributed inputs, has caused the old paradigms, under which computing has hitherto been developed and studied, such as uniformity of inputs and finiteness of processes, to be no longer representing the information processing reality sufficiently. In spite of their enormous size and impacts, all currently existing global networks should be seen as very primitive initial steps in a trend that is expected to converge in the design of a global (so-called *grid*) computing network or a *global computer* that can be seen as the ultimate goal, and at the same time the ultimate tool of science and technology into which our scientific knowledge should merge and with which all major information processing and communication technologies should be compatible. [As a reference for grids see Berman et al. (2003).]

The main properties of grid networks can be briefly enumerated as follows:

- Grids will be very high performance, geographically distributed, heterogeneous, and dynamically changing/evolving communication networks of very powerful information processing nodes;
- Grids will be enhanced by capabilities to dynamically share information acquiring, storing, processing and transmitting resources (including various sensors, special equipments, ...);
- Grids will allow software, knowledge and physical resources to be shared on the scale hitherto unimagined;
- Grids will be enhanced by capabilities of using sophisticated tools for mining data and knowledge, and for locating and allocating resources needed to process/solve given tasks;
- Grids will create an illusion of a single, very powerful and self-managing, virtual computer of heterogeneous and distributed resources;
- Grids will allow to solve complex problems that could not be tackled otherwise; to perform number-crunching computations not yet possible, to perform monitoring processes and simulations unthinkable nowadays and to perform data collection and processing currently unimaginable;
- Grids will allow creation and management of virtual and dynamic collaboratories, collaborations and organizations from and among geographically distributed parties;
- Grids will provide new stimuli for major industries and business and will lead to a new quality of life in general.

It seems to be quite safe to expect that the existence of grid networks will bring new quality to all major aspects of society, especially to economy, finances, industries, science, technology, health and environmental care, and also to education, exploration and utilization of our cultural heritage and to art, culture and entertainment. Such expectations are based, on one side, on extrapolations of the recent developments and experiences with impacts of the current, still primitive, networks, and also on a variety of technical results demonstrating the power of non-uniformity, interactions and so on.

To a large extent, only such GRID networks are expected to lead to a full and qualitatively new, use of new informatics based, scientific methodology.

The idea of global computer networks is not new. However, only recently the progress in the underlying computation and communication technologies raised such an idea from the science fiction and dreams to a developmental stage and potential reality.

Currently, perhaps the most important grid network is in Europe. It is the LCG Grid developed by CERN and other physics institutes (in connection with the design of Large Hadron Collider, that has to be in use by 2007, the largest and most powerful particle generator ever built with its four detectors placed around the 27 km LHC tunnel producing 16 Petabytes (2^{54} bytes) of data per year). LCG has already over 5,000 CPUs, more than 7,000 TB of storage at more than 70 sites around the world and is expected to connect about 100,000 CPUs.[20]

Quantum information processing (including classical computing as a special case) can be seen as our current lower bound on the models of computing by Nature in the sense that all other well-established models are built on it, in one sense or another. Conversely, GRID computing, through which all other models and ways of computing by Nature can be viewed as being its components, can be seen as our upper bound for models of computation by Nature.

5 The quest for overcoming the Church-Turing barrier

As already mentioned, the quests to overcome the Church-Turing barrier are as old as the barrier itself. They can be roughly divided into purely mathematics/informatics based attempts and those inherently based on special physical phenomena.

Some ‘‘classical’’ approaches to overcome the Turing barrier are the following:

- To assume the existence of infinite resources, for example,
  - Turing machines that run for an infinite period of time (Hamkins and Lewis 2000);
  - Idealized analogue computers that can work with all reals (even with uncomputable reals) and can harness them (Siegelman 2003);
- To assume the existence of exponentially growing resources (for example Turing machines which increase their speed exponentially over time)—see Svozil (1997) for an analysis.
- To use highly chaotic dynamical systems for computation (Wolfram 2002).

The main reasons for trying to overcome the Turing barrier can be summarized as follows:

- It is interesting and intellectually usually very rewarding to try to overcome limitations that seem to be unquestionable;
- It is an attempt to demonstrate that the limits of mathematics ought to be determined not solely by mathematics itself but also by physical principles;
- It is connected with attempts to see limitations of artificial intelligence and to find the border lines between thinking and computing;
- Attempts to show that there is a way to overcome Turing barriers are an important way to improve our understanding of the physical world, and Nature in general, and to find in Nature new important resources and new theories for Nature.

In this connection, it is worth noting the following citation from Lewis Carol's *Through the Looking-glass, 1872*:

> I can't believe that! said Alice. Can't you? the Queen said in a pitying tone. Try again: draw a long breadth, and shut your eyes. Alice laughed. There's no use in trying, she said: one can't believe impossible things. I daresay you haven't had much practice said the Queen. When I was your age, I always did it for half-an-hour a day. Why, sometimes I've believed as many as six impossible things before breakfast.

5.1 *The quest for overcoming the Church-Turing barrier in informatics*

In 2001, Wiedermann and van Leeuwen formulated an extended version of the Church-Turing thesis, namely, that any non-uniform and interactive network computation can be described in terms of *interactive Turing machines with advices* that are equivalent to so-called *site machines* and also equivalent to so-called *internet machines (GRID-networks)*—that is a model inspired by computer networks and distributed computing. They have also shown that all of these models accept all recursively enumerable sets and their complements.

As they pointed out, the Extended Church-Turing Thesis, or the *WV-thesis of Wiedermann and van Leeuwen*, does not aim to attack the Church-Turing thesis. The WV-thesis merely tries to identify a new proper extension of the Church-Turing thesis to cover computations that share the following features: non-uniformity of programs, interaction of machines and infinity of operation.[21] WV-thesis tries to see the concept of computation in a broader sense, based on different assumptions and as the one suited to answer different questions, that theory and applications pose nowadays.

5.2 *The quest for overcoming the Church-Turing barrier in physics*

Since all attempts to perform computations require physical resources, it is natural that there is also a physical version of the Church-Turing thesis (PhCT), or conjecture. It says that any physical computing devise, and any computational physical Gedanken experiment, can and will always be simulated by a Turing machine. The physical version of Church-Turing thesis should therefore be considered as a conjecture concerning physics, mathematics, computing and, as discussed later, also of cosmology.[22]

The Church-Turing thesis used to be generally considered valid within the framework of mathematics, computing and Newtonian physics, representing our view of the physical world at the time the thesis was formulated. However, the general view of the physical world and our understanding of the universe has radically changed since then and it is therefore natural to try to explore the consequences of new discoveries for the validity of PhCT thesis.

Recently, several attempts have appeared that claim to present approaches to solve (in some sense) some specific unsolvable problems using certain mathematical representations of some quantum phenomena, in a way that does not seem to contradict neither the laws nor the limitations of quantum theory.[23]

Such attempts have been based on the following phenomena:

- One uses tools and/or assumes phenomena that (quantum) physics might allow—tools that seem to be physically possible, or at least they have not been shown to be physically unrealizable, and they do not seem to contradict any known physical law. For example
  - Németi and Dávid (2003) investigated the question whether attempts to break the Turing barrier can be consistent with the general relativity theory. They conclude that beating the Turing-Church barrier may be consistent with the spacetime theory and cite also other researchers that have tried to make use of the latest findings in spacetime theory to break the Turing barrier. For an analysis, see Aaronson (2005a).

– Etesi and Németi (2002), see also Hogarth (1994), explored the physical theory that exhibits the capability to get finite information from infinite data in a finite time to overcome the Turing-Church barrier.

A variety of other approaches have been developed which try to make use of (a) a special infinite-dimension Hamiltonian and the possibility to obtain its ground state via measurement; (b) some special measurements; (c) some special continuity; (d) some exponentially growing feature; (e) infinite superposition of states; (g) infinite number of the Fock states.

Example Calude and Pavlov (2002) have shown a "mathematical quantum device" to solve the Halting problem in such a way that if the device says that a given Turing machine *M* halts then this is true, but if it says that it does not halt, then it is very unlikely that an error is possible. The catch behind this promising result is that designing such a real devise does not seem to be feasible (and the authors also make no indication that they indeed expect so).

Of the recent interest is also the idea to make use of so-called *quantum advices*[24] to get an extra computational power. Interesting theoretical results, to be discussed next, indicate that advices can indeed have enormous computational power. As a physical motivation behind the use of advices in computation one can see observations (Nielsen and Chuang 2000) that many systems in Nature prefer to sit in highly entangled multipartite states. It is therefore natural to ask whether it is possible to make use of such entanglement to get an extra computational power. One of the basic open question is then whether quantum advices are more powerful than classical (that is whether **BQP**/qpoly = **BQP**/poly?).[25] An interesting recent result in quantum complexity theory (Raz 2005) shows an enormous power of quantum advices. Indeed, he has shown that a quantum interactive proof system, at which the verifier gets quantum advices, can solve any problem whatsoever.

It is also natural to assume that any quest for ways to overcome the Turing barrier is outside quantum theory, although within modern cosmology and its spacetime theories. One of the starting points is that since the idea of computability is inherently related to the nature of time, one should look into modern spacetime theories for ideas to overcome the Church-Turing barrier. And indeed, some of the recent results indicate that the possibility to have systems computing non-Turing computable functions may be consistent with spacetime theory.

For example, Etesi and Németi (2002) have shown as consistent with general relativity that, by certain relativistic experiments, one might solve Turing-uncomputable problems. In these experiments, they assume the existence of huge slowly rotating black holes "the existence of which has been made more and more likely by recent astronomical observations."[26]

To be more specific, Etesi and Németi showed that certain relativistic space-time theories license the idea of observing the infinity of certain discrete processes in finite time. This has led to the observation that certain relativistic computers can carry certain undecidable queries in finite time. On this basis Wiedermann and van Leeuwen (2002) designed a *relativistic Turing machine* that models the above computations and recognizes exactly Δ_2 sets of the Arithmetic Hierarchy.

6 Pushing the limitations and barriers of feasibility

Recursive functions theory can be seen as the area of logic that explores the concept of computability as well as the properties and relations between problems that are beyond the border of computability as established by the Turing-Church thesis.

An introduction, around 1960, of the computational complexity class **P** and of the computational complexity theory, were beginnings of the attempt to search for another important limitations and barriers in computing, namely those concerning feasibility. The complexity theory has been very successful in doing this and one can perhaps say that the attempts to develop a proper concept of feasibility has turned out not only at least as inspiring for science as attempts to study the limits of computability, but likely even more important for science in general.

To come up with a proper concept of feasibility, that would be both simple enough and excellent for theoretical study, while being adequate for practical purposes, was far from simple, and maybe even more difficult than to come up with a proper concept of computability. The problem was that such a concept should be independent of the progress in technology and, at the same time, it should capture well what is physically possible. The class of problems that are feasible should be infinite and, at the same time, small in some reasonable sense.

The first important idea, broadly explored, was to see the class **P** as the one containing exactly those problems for whom obtaining solutions is feasible. Behind such an approach was also a belief, based on the experiences from the physical world, that natural problems that can be briefly specified will have solutions bounded by small degree polynomials if they have a polynomial time bounded solution at all. One can see how nontrivial the class **P** is also from the fact that we still do not know whether $\mathbf{P} = \mathbf{NP}$. The introduction of the class **P** was also closely related to the view that dominated at that time, namely that algorithms and computations are deterministic processes. This paradigm of determinism dominated in computing from the very beginning. The class **P** has been seen as the one providing limitations for feasibility in a similar way as the classes of recursive sets provided limitations for computability.

A discovery of the large computational power of randomness brought a new paradigm to computation and led naturally to the introduction of various randomized complexity classes. From them the class **BPP**, as the class of problems solvable in polynomial time with bounded error using randomized classical polynomial time algorithms, has emerged as a new candidate or a new frontier/barrier for the class of feasible decision problems. A study of the class **BPP**, and of its relation to other complexity classes, has brought a lot of insights into computing. Though we still do not know whether $\mathbf{P} \subsetneq \mathbf{BPP}$, we know quite a few specific properties of this class and they provide us with strong reasons to assume that the class **BPP** is likely larger than the class **P**. [However, one should also notice that Impagliazo and Widgerson (1997) gave quite convincing evidence that these two classes are the same.]

Some of the important and/or interesting properties of the class **BPP** are (see Balcázar et al. (1990)):

- All languages in **BPP** have polynomial size circuits.
- No inclusion relation between **NP** and **BPP** is known.
- No complete sets for **BPP** are known.
- If $\mathbf{NP} \subseteq \mathbf{BPP}$, then $\mathbf{NP} = \mathbf{RP}$[27]
- **BPP** is closed under polynomial-time reducibility, that is $\mathbf{BPP}^{\mathbf{BPP}} = \mathbf{BPP}$.

The idea of pushing frontiers and barriers of feasibility even further came when another new paradigm in computing started to be explored, namely that of quantum computing or quantum information processing. This led naturally to the introduction of the class **BQP** of problems solvable using quantum algorithms with bounded error in polynomial time (number of (quantum) steps). Although we still do not know whether $\mathbf{BPP} \subsetneq \mathbf{BQP}$[28] we know quite a few specific properties of the class **BQP** and they provide us with the reasons to assume that **BQP** is likely larger than **BPP**.

Some of the important properties of the class **BQP** are [see Gruska (1999–2004) and the web extension of the book for exposition and references]:

- Factoring and discrete logarithm are in **BQP**;
- **BQP** is very robust—$\mathbf{BQP}^{\mathbf{BQP}} = \mathbf{BQP}$;
- $\mathbf{NP} \subsetneq \mathbf{BQP}$ relative to a random oracle;
- $\mathbf{BQP} \subseteq \mathbf{PP}$;
- If $\mathbf{UP} \cap \mathbf{coUP} \subseteq \mathbf{BQP}$, then public key cryptosystems cannot be secure against quantum computer attacks;[29]
- $\mathbf{NP} \subsetneqq \mathbf{BQP}$, unless $\mathbf{PP}^{\mathbf{PH}} = \mathbf{PP}$.

Some of the interesting open problems are: (a) Is graph isomorphism in **BQP**?; (b) Is $\mathbf{UP} \cap \mathbf{coUP} \subseteq \mathbf{BQP}$?

One should, however, observe that though the introduction of the class **BPP**, as that of a new barrier of feasibility, has been without problems, and practically fully accepted by the complexity theory community, the same has not been true with the class **BQP**.

Similarly, as it is the case with quantum computing in general, where there are still sceptics with doubts whether we can have really powerful quantum computers at all, and there are also sceptics who find it difficult to accept that the usual model of quantum computation complexity (measures) is an appropriate one, especially when we want to use it to extend the concept of feasibility. These doubts of pessimists have been clearly pointed out recently by Goldreich (2005):[30]

- "Laws of quantum mechanics are only a refutable model about the real world, they are not the reality itself nor can they ever be proved to provide a full description of reality."
- "Quantum mechanics says that certain things are not impossible, but it does not say that every thing that is not impossible is indeed possible".
- "Quantum computing model consists of exponentially-long (with respect to the input) vectors and some "simple" operations on such vectors. The key point is that the associated complexity measure postulates that each such operation can be effective at

> unit cost (time). My main concern is with this postulate ... Is this an adequate model of reality?"

Recently, counter arguments of optimists have been nicely formulated by Aaronson (2005b):

- Without believing that quantum states are exponentially long vectors we would have troubles explaining even current experiments.
- For most complexity-theoretic purposes, the exponentiality of quantum states is not that much "worse" than the exponentiality of classical probability distributions, which nobody complains about.
- Quantum states seem to be more "like" probability distributions over *n*-bit strings than like exponentially long strings to which one has random access.

The existence of a certain scepticism among computer scientists towards quantum computing and its complexity measures is quite natural. Quantum mechanics creates a very strange view of the physical world and even physicists have had problems to accept fully its laws and limitations. This is still the case after practically 100 years since their discoveries. One can therefore assume that it will also take some time for the informatics community, especially for quantum complexity community, to accept them fully.

There are, however, also important points on which likely all optimists and pessimists agree in this area: Namely that the following research challenges are of great importance for current science: (a) To discover the ultimate *Secret of Secrets*: is our universe a polynomial or an exponential place?[31] (b) To provide a proper quantitative complexity theory of quantum information processing that would account for the real cost of obtaining, manipulating and measuring quantum states. In other words, the question whether **BQP** is a proper concept of feasibility and the question whether we can design a really powerful quantum computer are much related. Both of them are very non-trivial and important.

It is now natural to ask whether we have good reasons to assume the existence of a new physical theory that would still move farther limitations of feasibility. Some arguments supporting such an option run as follows: The birth of quantum mechanics can be seen in two discoveries: In 1901 Planck discovered the existence of quanta; in 1905 Einstein discovered the existence of light quanta (and relativity theory). The discovery of quantum mechanics and relativity started a revolution in our view of the physical world. Some believe that the quantum revolution remains unfinished because quantum mechanics has problems to get unified with spacetime into one coherent theory capturing also gravitation. The basic question in this context is whether quantum theory is correct or needs to be modified before it can be unified with our understanding of space-time? Concerning feasibility, the related question is then whether a new theory and a new view of the physical world will result also in a new concept of feasibility (and computability). In other words, will there be a next step in the sequence **P**, **BPP**, **BQP** ...?

For example, as already mentioned, relativistic Malament-Hogarth space-time theory, [see Németi and Dávid (2003), Etési and Németi (2002)], leads to the concept of relativistic computer that can carry certain classically undecidable queries in finite time and therefore would lead to a substantially broader concept of feasibility.

One should also observe that proofs that under certain physical assumptions it is possible to solve in polynomial time problems from the classes that are expected to be larger then **P**, are now seen as proofs that such physical assumptions are not to meet. For example, it has been shown that under the assumption that quantum mechanics is non-linear, more exactly that Weinberg's model of quantum mechanics is valid, see Abrams and Lloyd (1998), one can solve in polynomial time **NP**-complete problems. Aaronson (2004) has shown that if arbitrary one-qubit non-linear gates can be implemented without an error, then **PSPACE**-complete problems can be solved in polynomial time. Moreover, if so-called *post-selection* is allowed, then **PP**-complete problems can be solved in polynomial time.

Complexity theory results can therefore much influence search for ways to overcome computational barriers by restricting search space within various suggestions for new physical theory. Complexity theory results could also bring new barriers in case some sharp relations between complexity classes could be shown.

6.1 *Feasibility in physics*

An important research challenge for (quantum) physics is the development of a proper and sufficiently abstract concept of feasibility: which quantum states are indeed feasible, which quantum processes (operations, measurements) are feasible, and so on.

Such a concept of feasibility could perhaps be used, for example, to determine whether we can factorize really big integers using quantum computers. This would allow us to decide whether quantum mechanics would break down before factorizing very large integers.

An interesting idea along these lines have been pursued by Aaronson (2003) who has pointed out that in case quantum mechanics breaks down before factoring large integers, there should be a natural "Sure/Shor separator", which is a set of quantum states that account for all experiments performed so far, but not for all states in Shor's algorithm for factorizing large integers.

Aaronson (2003) suggests as a candidate for such a separator the set of so-called *quantum tree-states*, expressible by a polynomial number of superpositions and tensor products. For example,

$$\alpha|0\rangle^{\oplus n} + \beta|1\rangle^{\oplus n}, \quad (\alpha|0\rangle + \beta|1\rangle)^{\oplus n}.$$

He has also shown that certain states that are used in quantum error correction area, some codeword states of the stabilizer codes, require $n^{\Omega(\lg)}\ n$ superpositions and tensor products, even to approximate.

7 The quest for overcoming the NP-barrier

Closely related to the feasibility barrier or to the **BQP**-barrier is the **NP**-barrier.

Since **NP**-complete problems are so important, both practically and theoretically, and so abundant in practice, it is natural that there are many attempts to show that there are ways to solve these problems in polynomial time.

The **NP**-barrier says that **NP**-complete problems cannot be solved in polynomial time using resources of the physical world.

There have been many attempts to beat the **NP**-barrier and they are to a large extent well-summarized and analyzed by Aaronson (2005a). He discuss such ideas as quantum adiabatic computing, variations on quantum mechanics (non-linearity, hidden variable theories), analogue computing,[32] but also more esoteric ones such as relativity computing, time travel computing, quantum field, string and gravity theories, and even *anthropic computing*[33] The main conclusions are: (a) searches for overcoming **NP** barriers are important, since they can bring a better understanding of the physical worlds; (b) none of the well-specified attempts has been successful, yet. They usually forget to count all of the resources needed and/or all of the known physics.

In connection with the **NP**-barrier of interest and importance is the question, see Aaronson (2005a), 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, the Second Law of Thermodynamic is). This principle actually starts to be used. Perhaps the main problem with it is that why **NP**, why not **BQP** or some other complexity class as #**P** or **PSPACE**. It seems that in order to come to some consensus more technical results are needed. A new generation of physicists with a better education in complexity theory could also be needed.

8 The quest for overcoming the communication barriers

An interest in finding barriers of communication, for physical objects and information, seems to be as old as philosophy, and science in general. The discovery of the importance of communication for parallel and distributed computation has been behind the needs to explore the amounts of communication needed for solving different communication tasks which also raises the question of feasibility in communication.

There are several factors of communication that are of concern: causality, correlations between distant parties' actions, non-locality, speed, communication channel capacities and security.

The main carriers of information are bits and qubits. The question how many bits can qubits carry is also an interesting and basic question. Surprisingly, shared randomness and shared entanglement are resources that cannot be used for transmission of information, but can decrease the amount of communication needed. This fact is also an indication how complex the problem of finding communication barriers is.

The speed-of-light was the first very important communication barrier that had been established. Since that time the quest for overcoming this barrier has been a great challenge.

The non-locality principle, established by Einstein, can be seen as another important barrier to communication and transferability.[34] The discovery, at which Einstein was also much involved, that quantum mechanics seems to overcome this barrier and exhibits correlations with non-local effects caused an uproar in physics. The experimental confirmation of the existence of non-local correlations can be seen as one of the most important outcomes in physics of the 20th century.[35]

Surprisingly, quantum non-locality does not contradict relativistic causality. This led naturally to the following idea. Since special relativity can be deduced from two axioms, the equivalence of inertia reference frames, and the constancy of the speed of light, is it not possible to deduce also quantum mechanics from some simple axioms that have a clear physical meaning?[36] To get closer to an answer to such a challenging question, it is natural to ask whether quantum mechanics puts, with its correlations, the only possible barrier on non-locality that does not contradict relativistic causality. A surprising answer, that has emerged from the paper by Popescu and Rohrlich (1997), is NO, and this result has recently had a lot of surprising impacts on our understanding of the barriers for communication. They introduced, and others explored, a model of a toy-theory where the key elements are so-called non-local boxes (*NL-boxes*, also called Popescu-Rohrlich boxes, *PR-boxes*).

An NL-box is used by two parties, say Alice and Bob, and has two input- and two output-ports. If Alice inputs a bit x on her input port, she gets immediately on her output-port a bit b, and if Bob inputs a bit y, he gets as an output a bit b. Moreover, both possibilities for a and b should have probability $\frac{1}{2}$. However, and this is the key point here, the outputs should be correlated as follows

$$a \oplus b = x \cdot y$$

and therefore they exhibit non-local correlations. It can be easily shown that these nonlocal correlations do not allow super-luminal communications and therefore NL-boxes are non-signaling boxes.[37]

Entangled states (more precisely measurements on entangled states) also exhibit non-local correlations that are non-signaling. The existence of non-local correlations exhibited by entangled states is behind the very important no-bit-commitment result: an unconditionally secure quantum bit commitment is not possible (see Mayer 1998; Lo and Chau 1997a)[38] It is therefore very surprising, as shown by Buhrman et al. (2005), that super-strong non-local correlations exhibited by NL-boxes, that are stronger than correlations exhibited by entangled states, allow unconditionally secure bit commitment. Buhrman et al. (2005) have actually shown an even stronger claim. Namely, that so-called 1-out-of-2 oblivious transfer, and even that any two-party computation, can be performed in a secure way if enough NL-boxes are available, see also Short et al. (2005).

NL-boxes look like quite special, even strange, boxes with non-local correlations. However, this is not quite true. It has been shown by Barrett et al. (2004) that all bipartite no-signaling boxes with binary inputs and outputs can be constructed from NL-boxes and a mixture of local operations. An NL-box can therefore be seen as a unit of non-locality as an *nl-bit*, in an analogy to an *e-bit* as a unit of entanglement exhibited by maximally entangled two qubit states (by the EPR state). There are also other interesting similarities and relations between correlations exhibited by entangled states and by NL-boxes. For example, NL-boxes exhibit a monogamy similar to that exhibited by entangled states. Moreover, NL-boxes have already inspired development of a framework, by Barrett (2005), in which a variety of theories can be introduced that share two features with quantum mechanics: non-signaling property for states and the fact that a global state of a multi-particle system can be completely specified by correlations between local measurements of the individual subsystems. One of them is so-called *Generalized non-signaling mechanics*. This is just another example of how investigations of various barriers concerning communications inspire the development of science in general.

Results concerning the NL-boxes also show how close searches for unconditional security are to searches for limitations and barriers concerning security, as well as to our attempts to understand the essence of such fundamental physical theories as quantum mechanics is. Results concerning the NL-boxes also indicate that non-locality and causality could coexist also in other potential ‘‘physical’’ theories than quantum mechanics. The above results concerning the NL-boxes are also a demonstration of the impact a study of (unconditional) security has on our understanding of the fundamental theories—in spite of the fact that no non-local correlations except quantum correlations have so far been observed in Nature.

An important insight into the power of super-strong correlations has been obtained by van Dam (2005). He has shown that super-strong correlations imply that any distributed computation can be performed, if enough NL-boxes are available, using a single classical bit of communication. Since our experience shows that there are communication tasks that require communications with different amounts of classical bits for their realization than others do, the above result implies that super-strong quantum correlations (that allow the maximal bound 4 in the Bell-CHSH inequality) are implausible. An interesting task is now to find out whether there is a limit on the strength of correlations that would not lead to such implausible communication complexity outcomes. Moreover, since there is a tight connection between the communication complexity of distributed functions and the depth of circuits for such functions (see Kushilevitz and Nisan 1997), it is also possible, and of interest, to consider implications of super-strong correlations on computational complexity, see van Dam (2005). In spite of the fact that van Dam's result provides a strong evidence of the physical impossibility of NL-boxes, they keep being intensively studied. NL-boxes have a variety of other surprising and also counterintuitive properties. These results are surveyed nicely and referenced well by Scarani (2006). For example, two parties may need 2^n of the NL-boxes for some tasks that can be performed using n EPR states only.

Interesting insights into quantum mechanics and its correlations have been obtained through the study of communication complexity problems related to the simulation of some of the key quantum operations. For example, Cerf et al. (2005) have shown that a single NL-box is enough to simulate exactly all possible projective measurements that can be performed on the singlet state of two qubits, with no communication needed. Other deep results along these lines are thanks to Shi and Zhu (2005). They investigate the minimum amount of classical communications to simulate non-local quantum measurements and from that they derive a general upper bound that in turn translates to the systematic classical simulations of quantum communication protocols.

An interesting idea to overcome the speed of light barrier came from the science fiction: teleportation.

So-called *classical no-teleportation theorem* says that *classical teleportation is impossible*. By that it is understood that there is no way to use classical channels to transmit faithfully quantum information (states).

On the other hand, as shown by Bennett et al. (1993), quantum teleportation is possible, and though it does not lead to overcoming the speed-of-the-light barrier, it has led to various surprising discoveries concerning communication and also allows absolutely secure transmission of quantum states, if shared entanglement is available as a resource. The basic idea of quantum teleportation is actually very simple.

In order to teleport an unknown quantum qubit state $|\phi_u\rangle$, of a particle P_u, from a Sender to a Receiver, let us assume that the Sender and the Receiver share two particles P_s and P_r in the EPR-state

$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. If the Sender performs the Bell measurement[39] on particles P_u and P_s and sends the classical outcomes of this measurement—two bits—to the Receiver through a classical public channel, then the Receiver knows which of the Pauli operations he has to apply to his particle P_r in order to make it to get into the state $|\phi_u\rangle$, which was the state of the Sender's particle before teleportation.

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 the teleportation itself—neither the state to be teleported nor the location of the intended receiver. One can also see the quantum teleportation as a protocol that allows one to teleport all characteristics of an object embedded in some matter and energy and localized at one place to another piece of energy and matter located at a distant place.

Before the Receiver gets two bits from the Sender, but after the measurement by the Sender, his particle is in the maximally mixed state $\{(\frac{1}{4}, |\phi_u\rangle), (\frac{1}{4}, \sigma_x|\phi_u\rangle), (\frac{1}{4}, \sigma_z|\phi_u\rangle), (\frac{1}{4}, \sigma_x\sigma_z|\phi_u\rangle)\}$, whose density matrix is the same as for the mixed state $\{(\frac{1}{2}, |0\rangle), (\frac{1}{2}, |1\rangle)\}$, and therefore the Receiver knows nothing about the state $|\phi_u\rangle$ being teleported.

Quantum teleportation can be used to transmit quantum states absolutely securely as follows.

1. Quantum information is encoded using a sequence of some n qubits.
2. The resulting qubits are teleported, one after another.

Any transmission through teleportation is absolutely secure because no particles are being transmitted. However, the catch is that the communicating parties have to share at least n EPR-states.

Non-local correlations between classical events that entanglement manifests are one of the most puzzling phenomena not only of quantum mechanics, but of all current science. That has also been illustrated by the recent experiment in Geneva, see Scarani et al. (2000) and Gisin (2005b). From these experiments and from the experiments confirming Bell inequalities, it follows that there are reasons to believe that either space-time is an illusion, or free will is an illusion, or (as the above mentioned experiments confirm), there is a special "quantum information" speed of which is either infinite or travel faster (if at all) than light (faster than 10^7 c, in the "natural reference frame").

However, such a *quantum information* cannot be used to transfer classical information.[40]

The results of communication complexity have also been used to show that some communication phenomena are very likely to be impossible in the physical world. For example, they were used, see van Dam (2005), Brassard et al. (2005a), to explore the question of how well can processes of quantum mechanics approximate PR-boxes, see page 18, that would exhibit the strongest correlations preserving the non-signaling condition. They have shown, on one side, that the availability of an prior shared entanglement allows the PR-boxes to be approximated with a success probability $\cos^2\frac{\pi}{8} \approx 0.854$ and that would it be possible to do that with a probability greater than 0.908, then any Boolean function could be computed using only one bit of communication, which is considered impossible. An interesting challenge is to close the gap between 0.854 and 0.908.

Concerning communications, another important question is how much of the classical information can carry quantum states. So-called Holevo theorem, that says that n quantum qubits can faithfully store only n bits, puts on another "insurmountable barrier". A first interesting way of getting around the Holevo barrier was shown by Ambainis et al. (1998). They have shown that if it is required that only one bit (but arbitrary one) can be retrieved with a sufficiently large probability, then one can encode slightly more than n bits into an n-qubit state. A dramatically more powerful, but very special indeed, way of getting around the Holevo barrier has been shown recently by Raz (2005): namely that one can encode 2^n bits $a_1, \ldots, a_{2^n}$ by a single quantum state of the size $\mathcal{O}(n)$ qubits, such that: for any integer k and any $i_1, \ldots, i_k \in \{1, \ldots, 2^n\}$, the values of all bits $a_{i\_1}, \ldots, a_{i\_k}$ can be retrieved from $|\psi\rangle$ by a one-round Arthur-Merlin interactive protocol of the polynomial size in n.

Classical channels capacity problems are dealt with in the classical information theory. The key results and barriers have been established by Shannon (1948). In the case of quantum channels, there is a variety of different channel capacities and their study is the main, and perhaps also the most inspiring, subject of quantum information theory (see Gruska (1999–2004), Nielsen and Chuang (2000)). Perhaps the main new point is that shared entanglement can increase quantum channels capacities.

8.1 *Feasibility in communication*

Similarly, since we consider a computation problem as feasible if it can be solved in a polynomial time (deterministic, randomized or quantum), we consider a communication problem as feasible if the number of bits needed to solve the problem, having some additional resources available or not, grows polynomially with respect to the size of the problem instance.

The availability of some shared entanglement has radically changed our understanding of what is feasible in solving communication problems. It has been shown that for both one-way communication and two-way communication [Buhrman et al. (1998), Kerenidis (2005)], there are problems that require an exponential number of communication bits in order to solve them classically, but only a polynomial number of bits is sufficient when they are solved quantumly in the presence of shared entanglement.

In case that enough of the shared entanglement is available, sending qubits is, surprisingly, of no significant advantage, comparing with sending bits, in spite of the fact that a qubit can "contain" unlimited number of bits. This is due to the fact that the Teleportation protocol allows us to send one qubit by sending 2 bits if communicating parties share one EPR state (that is, however, consumed during the protocol).

9 Barriers and limitations concerning security

Cryptography, that develops and explores tools to provide and break security and privacy is some thousands of years old—see Kahn (1967).[41] During the last 15 years, it has turned out, surprisingly, that new basic concepts of modern and broadly understood classical cryptography are actually not only the fundamental concepts of the whole area of the classical information processing, but they also actually seem to be at least of such fundamental importance as the basic concepts related to the efficiency and complexity of computation as well as quests to overcome the Church-Turing and other barriers in computing, communication and feasibility.

During the last 10 years, it has turned out that the basic concepts and tools of the broadly understood quantum cryptography and quantum cryptographical protocols are of the fundamental importance for the understanding of the laws and limitations not only of the quantum information processing, but also of the whole quantum physics.

9.1 *Security problems and the foundations of information processing*

The recent study of the laws and limitations of security and privacy brought a variety of new concepts of fundamental importance for the theory of computing: interactive and zero-knowledge proofs; one-way functions; trapdoor one-way function; computationally perfect security; randomized encryptions; cryptographically secure hash functions; hard core predicates and cryptographically secure pseudo-random generators.

A study of the security questions brings not only a deep understanding of the nature of computation, but can also help to characterize the better nature of the quantum world.

9.2 *Hiding bits and qubits*

Sending bits in an absolutely secure way is one of the key communication problems. It is well-known that using the One-Time Pad cryptosystem we can perfectly hide n bits. Actually, so-called *Shannon bit hiding theorem* says that n bits are necessary and sufficient to hide perfectly n bits. It is natural to ask whether we can beat this Shannon barrier concerning hiding, in some way, in the quantum case.

It is well-known that one can put even an infinite number of bits into one qubit, into its complex amplitudes. It would therefore seem that to hide qubits, and by that also infinitely many bits, one needs enormous resources. Surprisingly, this is not the case. So called *Quantum Shannon qubits hiding theorem* says that $2n$ bits are necessary and sufficient to hide perfectly n qubits (see Mosca et al., 2000).[42]

To hide n qubits perfectly, so-called Quantum One-Time Pad cryptosystem can be used. To use this cryptosystem, two parties, Alice and Bob, have to share either two n bit strings or $2n$ pairs of the EPR states.

The basic idea of the Quantum One-Time Pad is very simple. Let b_1,b_2 be two shared secret bits and $|\phi\rangle$ be a qubit to be hidden.

- *Encoding*

$$E_{b_1b_2}|\phi\rangle = \sigma_x^{b_1}\sigma_z^{b_2}|\phi\rangle = |\psi\rangle$$

- *Decoding*

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

After the encoding, one actually creates the mixed state

$$\left\{\left(\frac{1}{4}|\phi\rangle\right), \left(\frac{1}{4}\sigma_x|\phi\rangle\right), \left(\frac{1}{4}\sigma_z|\phi\rangle\right), \left(\frac{1}{4}\sigma_x\sigma_z|\phi\rangle\right),\right\}$$

and since the corresponding density matrix is the same as the one for a random bit, corresponding to the mixed state $\{(\frac{1}{2}, |0\rangle), (\frac{1}{2}, |1\rangle)\}$, the transmission of the encoded state is absolutely secure.

9.3 *Zero-knowledge proofs*

A very peculiar on one hand, and unusually important for the theory and practice of secure communication and cooperation on the other, was the establishment of a reachable zero-knowledge communication barrier for interactive proof systems.[43] The proof that such a barrier is widely achievable for important communication tasks (interactive proofs of important theorems) has been of enormous importance for classical computing, communication and security. Once quantum information processing and communication tools have appeared, this barrier started to be challenged. By 2005, all attempts to come up with a sufficiently natural and powerful concept of quantum zero-knowledge proof systems failed and therefore a feeling started developing that the concept of zero-knowledge proofs does not transfer naturally into the quantum setting. However, as an important result, Watrous (2005) has shown that several important classical zero-knowledge proofs are secure also against quantum attacks and that all languages in **NP** have such zero-knowledge proofs.

10 Conclusions, challenges and acknowledgment

Due to the fact that informatics based methodology can be seen as soon coming to dominate science and technology, it is of large importance to explore barriers concerning computation, communication, security and feasibility. The existence of global computers, and the potential new physical theories provide, are significant new features that can change our views of old barriers.

Thoughts and results presented in this paper gave rise to the following intriguing question that could stimulate further research.

- In which respect are computational barriers really different from those of communication and security? (This seems to be a difficult questions. Some relations are known. For example, no-cloning theorem that provides a limitation for communication of unknown quantum state without destroying it, is of large importance for security and plays an important role in the proofs of unconditional security of key distribution.)

Notes

[1] As Hodges (2006) recently pointed out and analysed, there is no unanimity regarding what the Church-Turing thesis actually claims. The issues are: what kind of computers can be considered as having the same power as Turing machines—humans, classical computers, quantum computers, "Internet" computers ...? It seems natural that our view of the Church-Turing thesis should evolve and one should take it by its spirit more than by those wordings Church and Turing used.

[2] Terms *Challenging Turing barrier*, *Super-Turing computation* or *Hypercomputation* are used for attempts to show that there is a way to solve decision problems and/or to compute functions that are not decidable or not computable in the Church-Turing sense. Interesting enough, the term *hypercomputation* was introduced by Turing in 1939, in his paper *Systems of logic based on ordinals* which investigated mathematical systems in which an oracle was available to compute a single arbitrary function.

[3] The reason being that it is actually easy to get beyond Turing, if one assumes, in some way, that one can manipulate some infinite objects in a unit of time. For example, one can perform an arithmetic operation with any real number in one time unit.

[4] A deeper understanding of the similarities and differences of all such barriers is another interesting subject that we only lightly touch on here.

[5] Observe that the name *quantum mechanics* is actually misleading and reflects confusions its discovery and development have accompanied for many years.

[6] For example, entanglement has been demonstrated at a group of 10^{12} atoms (see Julsgaard et al. 2001) and quantum interference for large molecules (see Brezger et al. 2002). However, there is still a range of several orders of magnitude to explore where the border between classical and quantum world is and to what extent we can find out that macroscopic objects exhibit such inherently quantum world phenomena as interference and entanglement.

[7] See http://www.musr.physics.ubc.ca/˜jess/p200/quotes.html, also for citations of Heisenberg and Schrödinger.

[8] This claim is usually attributed to Landauer (1991) as the one saying *Information is physical, but slippery*. This is mostly understood that physical carriers are needed in order to store, process and transmit information and that the laws and limitations of the underlying physical world also determine the laws and limitations of information processing and communication.

[9] Views emphasizing a close relation between the physical and information worlds are, of course, not shared by everyone and they even make some scientists furious. See, for example, the reaction in Daumer et al. (2006), on views of Wheeler and especially of Zeilinger (2005) that quantum mechanics is fundamentally about information and that *the distinction between reality and our knowledge of reality, between reality and information, cannot be made*.

[10] An obvious challenge, not easy to deal with, is to specify in a simple way the difference between mathematics-based and informatics-based methodologies. One way to see this, in a very simplified way, is as having a mathematics-based methodology to concentrate on relations and formalism and as trying to understand the real world in mathematical terms. On the other hand, informatics-based methodology concentrates on processes (represented by algorithms, protocols, software systems and networks), on simulations and visualisations in the real and virtual words and in such a way to get understanding of the laws, limitations and phenomena of Nature and society. (Mathematics has also tried to understand some processes, especially those described by differential equations, but they seem to be only a (small) part of all important processes supported by (relatively) simple laws. For other arguments concerning the new methodology see Gruska and Jürgensen (1991)).

[11] Security is here understood in a very broad sense to include problems related also to privacy, authentication of data and senders, anonymity and cryptographic protocols.

[12] We have in mind especially models within artificial life investigations capturing various aspects of the evolution, as self-reproducibility and the transfer of genetic information over generations—see, for example, Wiedermann (2005).

[13] Various models including DNA-computing, membrane-computing and so on.

[14] One should also note that while the Hilbert space platform for studying the quantum world dominates, it is not the only one possible and, actually, more and more one can encounter thoughts that the Hilbert space view of the quantum world is too limiting [see, for example, the attempts of Abramsky and Coecke (2004) to recast the axiomatic presentation of quantum mechanics, due to von Neumann, at a more abstract level of compact closed categories with biproducts., and many other approaches].

[15] Two vectors are called *orthogonal* if their scalar product equals zero. This concept of orthogonality is of great importance because physically are fully distinguishable only orthogonal states.

[16] Outcomes of quantum measurements are therefore random and this randomness is one of the most puzzling, and for some still hard to accept, features of our current theory of the quantum world. (Even E. Schrödinger, one of the fathers of quantum mechanics, said: *Had I know that we were not going to get rid of this dammed quantum jumping, I never would have involved myself in this business.*, see *quantum quotations* http://www.musr.physics.ubc.ca/˜jess/p200/quotes.html) Since the birth of quantum mechanics, there have been attempts to develop a deterministic theory of the quantum world. In behind is a belief that quantum randomness is actually not inherent in Nature and that it is only a consequence of our ignorance or the lack of understanding of the physical reality. Even nowadays, some prominent physicists as Penrose and 't Hooft (2006) seem to believe in a deterministic foundation of quantum physics. Current experimental quantum information processing not only see Einstein's *God does not play dice!* as wrong, but would like to replace it by *God does play even non-local dice*, see Gisin (2005b), that produces shared randomness. From informatics point of view, problems with accepting that randomness is inherent in Nature sounds strange because the power of randomness for information processing and security has already been convincingly demonstrated, as well as the existence of processes producing almost perfect randomness and therefore one would expect that *God is not malicious and made Nature to produce, so useful, randomness.*

[17] Actually, as clearly pointed out and analysed by Gisin (2005a), physics gave us local description of Nature only during the 10 years between 1915 (when Einstein presented General relativity theory) and 1925 (when quantum mechanics was established). Non-locality was introduced to modern physics actually by Newton, who was very unhappy with such consequences of his theories and he realized that, according to the theory developed, "moving a stone on a planet should immediately decrease the wight of people on earth". However, Newton's non-locality was essentially different from the one measurement of quantum entangled states can exhibit.

[18] One of the implications of quantum superposition 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 any function $f\colon \{0,\ldots,2^n-1\} \longrightarrow \{0,\ldots,2^n-1\}$. With more technical details, this works as follows: If $f\colon \{0,1,\ldots,2^n-1\} \longrightarrow \{0,1,\ldots,2^n-1\}$, 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 the 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.

[19] Ozawa, in a series of papers, gave such a universal valid relation between the noise and disturbance in general quantum measurement that plays a role of "first principle" to be used to derive various limitations on measurements in quantum information processing.

[20] References to projects building very large grids: http://www.eu-egee.org (EU); http://www.opensciencegrid.org (USA); http://www.naregi.org (Japan).

[21] All these features are inherent in the grid networks where all nodes are autonomous and can change their hardware, software or data in a fully non-uniform way.

[22] Deutsch (1985) formulated the so-called physical version of the Church-Turing thesis as ollows: *Every finitely realizable physical system can be perfectly simulated by a universal computing machine operating by finite means.*

[23] See for example, the controversial paper(s) by Kieu (2001) and its (their) recent analysis by Hodges (2006).

[24] Computation with advices is defined similarly to the ones with oracles, but without the requirement on uniformity of external inputs (advices). Advice is an information (string or a quantum state) supplied by an external source and only its size is bounded by a fixed polynomial, with respect to the size of the input.

[25] **P** (**BPP**) [**BQP**] is the class of (decision) problems solvable by deterministic (randomized) [quantum] algorithms in polynomial time—with bounded error; **NP** is the class of problems solvable by non-deterministic algorithms in polynomial time, or the class of problems solution of which can be tested in polynomial time.

[26] These ideas are discussed in detail by Németi and David (2003), where one can also find references to the related attempts to overcome the Turing-Church barrier.

[27] A language L is in **RP** (Random Polynomial time) if there is a polynomial non-deterministic Turing machine such that: - if $x \in L$, then *at least half* of all computations of M on x terminate in the accepting state; - if $x \notin L$, then *all* computations of M terminate in the rejecting state.

[28] In case $\mathbf{BPP}\subsetneq\boldsymbol{BQP}$ the limits of feasibility for quantum computations would be different than those in the classical physics. Concerning computability, with standard interpretations of quantum theory, this does not seem to be the case.

[29] A language L is in **PP** (Probabilistic Polynomial time) if there is a polynomial time non-deterministic Turing machine M, such that for any input all its computations have the same length and at each step there are two non-deterministic choices, such that: $x \in L$ iff *more than half* of computations of M on x terminate in the accepting state (so called the *acceptance by majority*); **UP** is the class of problems solved in polynomial time on such non-deterministic Turing machines at which the way to acceptance is unambiguously determined. **PH** stands for the polynomial hierarchy.

[30] Of course, there are other reasons the pessimists from among physicists like to emphasize: destructive impacts of decoherence; likely limitations of the laws of quantum mechanics to only physical phenomena of certain range (say at the Planck scale) and so on. Well known are also the sceptical words of Ralf Landauer, one of the founders of the field, commenting on the enthusiasm the pioneers of quantum information processing shared: *It will need more than rain to stop this parade.*

[31] *Is our universe (efficiently) computable at all?* See Srikanth (2004) for an analysis.

[32] The idea behind the relativity computing can be informally described as follows: one makes a computer to deal with an intractable problem, then boards a spaceship and accelerates it to

almost the speed of light. After returning to Earth, the answer will be waiting for him (though all his friends, and even enemies, would be long dead).

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

[34] As pointed by Gisin (2005b), non-locality was actually introduced to physics by Newton, but his non-locality is essentially different to quantum non-locality that does not violate no-signaling assumption of special relativity.

[35] Not everyone is already convinced of the existence of quantum non-locality. See, for example, the recent views on the concept of truth used by opponents of Einstein's view of the completeness of quantum mechanics by Carola (2005). (He claims that opponents of Einstein's arguments aiming to prove incompleteness of quantum mechanics work with different concept of truth and that with a "proper" concept of the truth one gets an interpretation of quantum mechanics in which quantum mechanics is incomplete, non-contextual and local). See also the very innovative approach, category theory based, to quantum mechanics, by Coecke (2005) and related scientists. Actually, the truth without doubts is that practically nobody is able to fully accept the non-locality that Hilbert space quantum mechanics offer. Could it be the case that some quantum non-local correlations are "unmakeble" in a similar way as some real numbers are uncomputable and some quantum states are non-constructable?

[36] There is quite widespread view that, at least some, axioms of quantum mechanics have no clear physical meaning. One approach that has been recently advocated, is to derive quantum mechanics of no-signaling, no-broadcasting and no-bit-commitment assumptions—see Clifton et al. (2002). They have actually shown that observable and state space of a physical theory must be quantum mechanical if the following conditions hold: (a) no superluminal information transmission is possible between two systems by measurement on one of them; (b) no broadcasting of information contained in an unknown physical state is possible; (c) no unconditionally secure bit-commitment is possible. Actually, to be more precise, they showed that *the above constrains force any theory formulated in* C^* *-algebraic terms to incorporate a non-commuting algebra of observables for individual systems, kinematic independence for the algebras of space-like separated systems and the possibility of entanglement between space-like separated systems.*

[37] Non-signaling condition of the special relativity says that a local choice of measurements may not lead to the observable differences at the other end. The idea of NL-boxes arises in the following setting: let us have two parties, A and B, and let the party X performs two measurements on a quantum state with two outcomes $m_0{}^x$ and $m_1{}^x$ with 0 and 1 as potential values. Let us denote a bound on correlations between two such measurements as $B = \sum_{x,y\in\{0,1\}} Prob(m_x^A \oplus m_y^B = x \cdot y)$. So called Bell/CHCS inequality says that $B \leq 3$ in any classical hidden variable theory. So-called Cirel'son's bound (Cirel'son 1980), says that the maximum for B in quantum mechanics is $2 + \sqrt{2}$. Popescu and Rohrlich developed a model in which the maximal possible bound, 4, is achievable.

[38] Bit commitment is a protocol between two parties in which one party, say Alice, commits herself to a bit in such a way that the other party, say Bob, has no way to find out what is Alice's commitment and Alice has no chance to change her commitment once she has made it. Bit commitment is a very important primitive for cryptographic protocols.

[39] It is a projection measurement with respect to the four Bell states:

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

[40] Actually, there is no quantum information, there are only quantum states and quantum representation of the (classical) information; in this way one has also understand the term "quantum information processing".

[41] Development of tools and methods to create "unbreakable security systems" and also of methods and tools to break "unbreakable security systems" have a fascinating history embracing thousands of years. Security tools played an exceptionally important role not only in both world wars, but also greatly motivated the development of information processing and communication technology. For example, the computer Collosus, designed to break the cryptosystem used for communication between Hitler and his generals, was actually the first very powerful electronic computer.

[42] This barrier can be beaten in case qubits have real amplitudes and in such a case the new barrier is *n*.

[43] The interactive proof systems are two-party protocols at which all powerful Prover(s) try to convince, by communication, a Verifier (or verifiers) working in polynomial time, about the validity of a specific statement (theorem). An interactive proof system is said to be *zero-knowledge* if it has the property that if the Verifier interacts with the honest Prover(s) of the system he learns nothing from the interaction beyond the validity of statement being proved. There are actually several variations of the concept of zero-knowledge proof systems. Number and power of provers is one factor to consider. The main one is the way of specifying the notion of ''learning nothing''. In each variant, it is considered that a particular verifier learns nothing if there exists a polynomial time *simulator* whose output is indistinguishable from the output of the verifier after interacting with the prover on any possible instance of the problem. In case of *perfect* or *statistical* zero-knowledge distinguishibility is in the statistical sense; in case of *computational* zero-knowledge, distinguishibility is computational.

Acknowledgments

The author is much thankful to both referees of the first version of the paper for two unusually useful and stimulating reports and questions presented above. They also asked a variety of other deep and sometimes hard to respond questions. Support of the grants GACR 201/04/1153, 201/07/0603 MSM00211622419 and VEGA 1/0172/03 is to be acknowledged.

References

Aaronson S (2003) Multilinear formulas and skepticism of quantum computing. quant-ph/0311039

Aaronson S (2004) Quantum computing: postselection and probabilistic polynomial time. quant-ph/0412187

Aaronson S (2005a) NP-complete problems and physical reality. quant-ph/0502072

Aaronson S (2005b) Are quantum states exponentially long vectors. quant-ph/0507242

Abrams DS, Lloyd S (1998) Nonlinear quantum mechanics implies polynomial-time solution for NP-complete and #P complete problems. quant-ph/9801041

Abramsky S, Coecke B (2004) A categorical semantics of quantum protocols. quant-ph/0402130

Ambainis A, Nayak A, Ta-Shma A, Vazirani U (1998) Dense quantum coding and a lower bound for 1-way quantum finite automata. quant-ph/9804043

Arndt M et al (2005) Quantum physics for A to Z. quant-ph/0505187

Balcázar JL, Díaz J, Gabarró J (1990) Structural complexity I, II. Springer-Verlag, Berlin

Barrett J (2005) Information processing in non-signaling theories. quant-ph/0508211

Barret J, Linden N, Massar S, Pironio S, Popescu S, Roberts D (2004) Non-local correlations as an information theoretic resources. quant-ph/0404097

Bennett CH, Brassard G, Crépeau C, Jozsa R and Peres A Wootters WK1993 Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. Phys Rev Lett70: 1895–1899

Berman F, Fox G, Hey T (2003) Grid computing: making the global infrastructure reality. Wiley, Chichester

Brassard G, Buhrman H, Linden N, Methot AA, Tapp A, Unger F (2005a) A limit on nonlocality in any world in which communication complexity is not trivial. quant-ph/0508042

Brezger B, Hackermüller L, Uttenthaler S, Petschinka J, Arndt M, Zeilinger A (2002) Matter-wave interferometer for large molecules. quant-ph/0202158

Buhrman H, Cleve R, Wigderson A (1998) Quantum versus classical communication complexity. In: Proceedings of 30th STOC, pp 63–68

Buhrman H, Christandl M, Unger F, Wehner S, Winter A (2005) Implications of superstrong nonlocality for cryptography. quant-ph/0504133

Calude CS, Pavlov B (2002) Coins, quantum measurements and Turing's barrier. Quantum Information Processing

Carola C (2005) Truth and completeness in quantum mechanics: a semantic viewpoint. quant-ph/0510199

Cerf N, Gisin N, Masar S, Popescu S (2005) Quantum entanglement can be simulated without communication. Phys Rev Lett 94: 220403

Cirel'son BS (1980) Quantum generalization's of Bell's inequality. Lett Math Phys 4(2): 93–100

Clifton R, Bub J, Halvorson H (2002) Characterizing quantum theory in terms of information-theoretic constraints. quant-ph/0211089

Coecke B (2005) Kindergarten quantum mechanics. quant-ph/0510032

Daumer M, Dürr D, Goldstein S, Maudin T, Tumulka R, Zanghi N (2006) The message of the quantum? quant-ph/0604173

Deutsch D (1985) Quantum theory, the Church-Turing principle and the universal quantum computer. In: Proceedings of the Royal Society London A, 400: 97–117

Etesi G and Németi I (2002) Non-Turing computations via Malament-Hogarth spacetimes. Int J Theor Phys 41: 341–370

Gisin N (2005a) Can relativity be considered complete? from Newton nonlocality to quantum nonlocality and beyond. quant-ph/0512168

Gisin N (2005b) How come the correlations. quant-ph/0503007

Goldreich O (2005) Quantum computing. http://www.wisdom.weismann.ac.il/˜oded/on-qc.html

Gruska J (1999–2004) Quantum computing. McGraw-Hill. See also additions and updatings of the book on http://www.mcgraw-hill.co.uk/gruska

Gruska J (2003) Quantum entanglement as a new quantum information processing resource. New Generation Comput 21: 279–295

Gruska J, Jürgensen H (1991) Maturing of informatics. In: Bjrner D, Kotov V (eds) Images of programming. North-Holland, Amsterdam, pp I-55–I-69

Hamkins JD, Lewis A (2000) Infinite time Turing machines. J Symb Logic 65: 567

Hodges A (2006) Can quantum computing solve classically unsolvable problems? quant-ph/0512248

Hogarth J (1994) Non-Turing computers and non-Turing computability. In: Proceedings of biennial meeting of the philosophy of science association, pp 126–138

Impagliazo R, Wigderson A (1997) **P** = **BPP** unless **E** has subexponential circuits: derandomization. In: Proceedings of 29th STOC, pp 220–229

Julsgaard B, Kozhekin A, Polzik ES (2001) Experimental long-lived entanglement of two macroscopic objects. quant-ph/0106057

Kahn D (1967) The codebreakers: the story of secret writing. Maxmillan

Kerenidis I (2005) Quantum multiparty communication complexity and circuit lower bound. quant-ph/0504087

Kieu TD (2001) Quantum algorithm for Hilbert's tenth problem. quant-ph/0110136

Kushilevitz E, Nisan N (1997) Communication complexity. Cambridge University Press, Cambridge

Landauer R (1991) Information is physical Phys Today 44: 23–29

Lo H-K, Chau HF (1997a) Why quantum bit commitment and ideal quantum coin tossing are impossible? quant-ph/9711065

Mayers DC (1998) Unconditionally secure quantum bit commitment is impossible. Phys Rev Lett 78: 3414–3417

Mosca M, Topp A, de Wolf R (2000) Privite quantum channels and the cost of randomizing quantum information. quant-ph/0003101

Neméti I, Dávid G (2003) Relativistic computers and the Turing barrier. Rényi Institute of Mathematics, Dept. Atomic Physics, Eötvös University

Nielsen MA, Chuang II (2000) Quantum computation and quantum information. Cambridge University Press, Cambridge

Ozawa M (2005) Universal uncertainty principle in the measurement operator formalism. quant-ph/0510083

Popescu S, Rohrlich D (1997) Causality and non-locality as axioms for quantum mechanics. quant-ph/9709026

Raz R (2005) Quantum information and the PCP theorem. quant-ph/0504075

Scarani V (2006) Feats, features and failures of the PR-box. quant-ph/0603017

Scarani V, Tittel W, Zbinden H, Gisin N (2000) The speed of quantum information and the preference frame: analysis of experimental data. quant-ph/0007008

Shannon CE (1948) Mathematical theory of communication. Bell Syst Tech J 27:379–423, 623–656

Shi Y, Zhu Y (2005) Tensor norms and the classical communication complexity of non-local measurements. quant-ph/05111071

Short T, Gisin N, Popescu S (2005) The physics of no-bit commitment generalized quantum non-locality versus oblivious transfer. quant-ph/0504134

Siegelman H (2003) Neural networks and analog computation: beyond the Turing limit. Birkhäuser

Srikanth R (2004) Computable functions, the Church-Turing thesis and the quantum measurement problem. quant-ph/0402128

Svozil K (1997) The Church-Turing thesis as a guiding principle for physics. quant-ph/9710052

't Hooft G (2006) The mathematical basis for deterministic quantum mechanics. quant-ph/0604008

van Dam W (2005) Implausible consequences of superstrong nonlocality. quant-ph/0501159

van Leeuwen J, Wiedermann J (2001) The Turing machine paradigm in contemporary computing. In: Enquist B, Schmiet W (eds) Mathematics unlimited: 2001 and beyond. Springer Verlag, Berlin, pp 1139–1155

Watrous J (2005) Zero-knowledge against quantumproofs. quant-ph/0511020

Wiedermann J (2005) Global universe and autopoietic automata: a framework for artificial life. In: Proceedings of ECAL 2005, LNAI 3630. Springer-Verlag, Berlin, pp 21–30

Wiedermann J, van Leeuwen J (2002) Relativistic computers and non-uniform complexity theory. In: Proceedings of UMC'02, LNCS 2509. Springer-Verlag, Berlin, pp 287–299

Wolfram S (2002) A new kind of science. Wolfram Media.

Zeilinger A (2005) The message of the quantum. Nature 438: 743–745