Quantumization of Theoretical Informatics

(Position Statement)

Jozef Gruska^{*}

Faculty of Informatics, Masaryk University,
Botanická 68a, 602 00 Brno, Czech Republic
`gruska@fi.muni.cz`

Maturing of informatics Recent developments in the area of quantum information processing and communications (QIPC) made clear that foundations of computing have to be based not on the laws and limitations of the classical physics as so far, but on the laws and limitations of quantum physics.

This discovery has several profound impacts on theoretical informatics, on its goals and methods and brings also a new series of the very basic challenges for theoretical informatics. This discovery has also significantly increased *liberalization of theoretical informatics* from being mainly a servant of computing and communication technology and applications and put it into the position of the fundamental science, that has also strong impact on creation and development of new computing and communication technologies. This liberalization is expected to have far reaching consequences on how we should and will see foundations, aims, paradigms and methods of theoretical informatics.

Another implication of the quantumization of (theoretical) informatics is that it helped to see more clearly *basic scientific goals of theoretical informatics*: to discover and study the laws and limitations of the information processing world (whatever it means). This can also be viewed as a parallel to the main goal of physics – to discover and to study the laws and limitations of the physical world (whatever it means).

Going quantum Theoretical informatics has already started to get involved in the study of problems of QIPC. Moreover, its contributions, especially concerning the power of quantum algorithms and communication protocols, security of cryptographic protocols, quantum error correction codes and fault tolerant computations, as well as the existence of efficient universal quantum Turing machines, have been crucial for the development of the field. However, one has also to see that theoretical informatics has concentrated so far mainly on problems that can be seen as natural quantum variations of the classical problems. For example, to study such models of quantum automata that can be seen as direct quantumizations of the classical models. In other words, theoretical informatics is going quantum, but only very slowly and cautiously is getting out of its old views of the information processing world and its principles, laws and limitations.

^{*} Support of the GAČR grant 201/98/0369 and of the grant CEZ:J07/98:143300001 is to be acknowledged.

The aim of this position statement is to point out that theoretically equally interesting, and perhaps even deeper and more important, are problems of quantum information processing of a different type, those that are inherently quantum, and to try to turn attention of (theoretical) informatics community to such problems for two reasons: (a) they are of large (key) importance for the development of the field; (b) the research paradigms and methods of (theoretical) informatics seem to be well suited to deal with these problems; (c) they are intellectually exciting and rewarding as well as fundamentally deep.

A related underlying thesis is that paradigms, concepts, methods and results of theoretical informatics are so fundamental that they should be expected to have a very broad range of applications, similarly as those of quantum mechanics.

Main new features theoretical informatics has to deal with when *going quantum* can be summarized as follows.

- New information processing and communication resources (quantum superposition, parallelism, channels, entanglement and measurement).
- New information processing primitives (qubits, unitary operators, projection measurements, density matrices, superoperators and POV measurements for computation and bits, qubits and ebits for communication).
- New concepts of feasibility and new computational complexity classes.
- New types of (quantum) gates, circuits, automata, algorithms and protocols.
- New concepts of (quantum) information and new (quantum) information theory.
- New concepts of security (based on the laws of physics).
- New goals: (a) Those oriented to quantum physics (for example, a deeper understanding of such quantum phenomena as measurement, non-locality, decoherence). (b) Those oriented to theoretical informatics (for example, development of complexity theory on the basis of the quantum information processing laws and limitations). (c) Those oriented to quantum information processing (for example, an understanding of the computational and communication power of entanglement, a development of quantum information theory and of new computation and communication paradigms).

Interesting and important enough, it has been to a large extend due to the insights and results on the computational power of quantum information processing that an understanding has emerged that enormous experimental and developmental effort clearly needed to build powerful quantum information processing systems could pay off. This was followed by an observation that the research in quantum information processing can contribute also to a new and deeper understanding of quantum physics and by that also of Nature. A contribution to the development of such an understandings can be seen as one of the major impacts of concepts, methods and results of theoretical informatics in general, and of (computational) complexity theory in particular, on other sciences.

Quantum information processing is an area where very fundamental questions concerning Nature are being (re)asked and need to be answered. An area

where one finds various mysterious and paradoxical phenomena. An area where it is very nontrivial to find mathematical equivalents to the basic concepts and phenomena of Nature and proper interpretations, in terms of Nature elements and phenomena, of the mathematical concepts being used.

Quantum resources Power of quantum information processing and communication is based on an appropriate use of several new quantum resources.

- *Quantum superposition.* An n qubit quantum register can be simultaneously in a superposition of all 2^n (standard) basis states $\{|x\rangle \mid x \in \{0, 1\}^n\}$ of $\mathcal{H}_{2^n}$. In addition, an equally weighted superposition of all the basis states,

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

an important initial state of many computations, can be created in a single step using only n simple quantum gates.

- *Quantum parallelism.* In one step of a quantum evolution exponentially many classical computations can be “performed”. For example, for any function $f : \{0, 1, \dots, 2^n - 1\} \rightarrow \{0, 1, \dots, 2^n - 1\}$, there is a unitary mapping $U_f : |x, 0\rangle \rightarrow |x, f(x)\rangle$ and if U_f is applied to the exponentially large superposition $|\phi\rangle |0^{(n)}\rangle$ (see 1) of two n -qubit registers, then in one step the state

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

is created and therefore exponentially many values of f can be “computed” in one step.

- *Quantum entanglement.* Some quantum states of a bipartite quantum systems cannot be expressed as tensor products of the states of its subsystems, for example the state $\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$. Such pure states are called *entangled* and they are a puzzling phenomenon because they exhibit non-locality features. Indeed, it may be the case that two particles in an entangled state are far from each other. In spite of that any measurement of one of the particles “automatically” determines the state of the second particle.

Quantum limitations Quantum physics imposes also several severe limitations on quantum information processing.

- *Heisenberg’s uncertainty principle* says that measuring the value of one observable more accurately makes the value of another, noncommutative, observable less certain. In addition, there is a certain intrinsic uncertainty with which values of two observables can be measured, and once a way of measurement is fixed, this uncertainty, in general, increases.

- *No cloning theorem.* Very important for quantum information processing is the result that an unknown quantum state cannot be cloned. (Namely, there is no unitary transformation U , such that for any one-qubit state $|\psi\rangle$, $U(|\psi, 0\rangle) = |\psi, \psi\rangle$.) No cloning theorem seems to be a bad news. For example, it was to a large extent due to this theorem that quantum error-correcting codes seemed to be impossible. However, no cloning theorem is also a good news. Due to the impossibility to copy quantum information safely we have quantum key generation systems that are provably unconditionally secure.
- *Holevo theorem.* It seems that a state of a quantum register can contain unlimited amount of information because amplitudes can be numbers with infinite decimal expansion. However, because of the peculiarities of quantum measurement the amount of information we can get out of a quantum state to the classical world is very limited. Holevo theorem says that into an n -qubit register state we can encode and later decode safely only n bits.
- *Decoherence.* This is a term for the processes of coupling of quantum systems (processor) with their environment, if they are not perfectly isolated. As a consequence, quantum states of the system are modified due to the interactions of the system with the environment. Such interactions mean that quantum dynamics of the environment is also relevant to the operations of the quantum computer and its states become entangled with the states of the environment. Decoherence tends to destroy irreversibly information in a superposition of states in a quantum computer in a way we cannot control and therefore long computations, as well as long-term memories, seem to be impossible.

Successes of quantum information processing Perhaps the main apt killer for quantum information processing so far are Shor's quantum polynomial algorithms to factorize integers and to compute discrete logarithm and Grover's result that one can search in an unordered database of n elements using only $\mathcal{O}(\sqrt{n})$ queries. and not $\mathcal{O}(n)$ queries as in the classical case. The main open problem is whether there are quantum polynomial algorithms to compute the so-called Hidden subgroup problem for non-Abelian groups.

Quantum teleportation, due to Bennett and Brassard, experimentally verified, has been shown to be the most novel and useful tool for quantum communication.

Quantum cryptography, initiated by Wiesner, showed that provably, on the basis of the laws and limitations of quantum physics, unconditionally secure quantum key generation is possible. This brings new dimension to the problem of secure communication.

Due to the ideas coming from theory several ways have been found to fight quantum decoherence – the main enemy of the potential quantum computers – for example, Shor's quantum error-correcting codes and quantum fault-tolerant computations.

Main quantum challenges can now be seen as follows.

- To understand quantum measurement and to get insights how much resources it needs.
- To study quantum entanglement, and its different types, as a new and powerful computation and communication resource – to study ways entanglement is detected, measured, created, stored, transmitted (even teleported), manipulated, transformed (from one form to another), quantified and consumed (to do some useful work).
- To study multipartite entanglement, its use for distributed quantum information processing and for physics in general and to discover the laws and limitations how entanglement can be shared.
- To study quantum (pure) states as a precious resources. (Of the large importance is to find out how much of quantumness we really need and how pure it has to be in order to have systems that are still more powerful than classical ones).
- To develop quantum information theory. The importance of quantum information theory follows from the observation that if we want to be able to understand and to utilize fully the information processing potential available in Nature, then the concepts of classical information theory need to be expanded to accumulate quantum information carriers.
- To discover new techniques (in addition to those of Simon/Shor and Grover) to design quantum algorithms more powerful than classical ones – if they exist.
- To deal with quantum mysteries. (The existence of various mysterious quantum phenomena, often termed as paradoxes, accompanies the development of quantum mechanics from its beginnings.) Quantum mysteries did not used to bother too much “working physicists” and therefore there has been a tendency to see these mysteries as topics mainly the philosophers of science should deal with. However, now when research in quantum information processing and communication aims to discover the laws and limitations of both physical and informational world, the existence of these mysteries cannot be ignored any longer. Moreover, theoretical informatics seems to have a potential to help to deal with these mysteries.

Conclusion Potential of QIPC starts to be widely recognized. A number of national and international programs and initiatives has been set up for QIPC. For basics and main outcomes of QIPC see Gruska (1999). For main challenges of QIPC, especially for theoretical informatics, see Gruska (1999a).

References

1. Jozef Gruska. Quantum challenges. In *Proceedings of SOFSEM'99, LNCS 1375*, pages 1–28, 1999.
2. Jozef Gruska. *Quantum computing*. McGraw-Hill, 1999. See also additions and updatings of the book on <http://www.mcgraw-hill.co.uk/gruska>.