QUANTUM INFORMATICS
or
QUANTUM INFORMATION PROCESSING

1 INTRODUCTION

(Classical) Informatics concerns a variety of aspects of theory, technology and practice of information processing for the case that the underlying phenomena follow the laws and limitations of classical physics valid for the classical world. Quantum informatics is driven by the laws and limitations of the very different, and more basic , quantum world.

Quantum informatics has two goals: (a) to use informatics paradigms, concepts, models, theories, results and methods in order to explore how to harvest inherently quantum phenomena and resources (especially such counterintuitive ones as superposition, entanglement and non-locality) to bring new quality tools (with respect to efficiency and/or security) for information processing and communication and also how to realize processes that are impossible using phenomena of the classical world only; (b) to use informatics paradigms, concepts, models, theories, results and methods in order to bring new insights into the laws, limitations, phenomena and processes of the quantum (physical) world and to testing quantum mechanics.

In the classical information processing, classical objects are carriers of information and the most basic element is a *bit* that can take on one of the two values 0 or 1. In quantum information processing quantum objects, say particles, for example photons, are carriers of information and the most basic element is a *qubit* that can be seen as taking on always one of the infinitely many values $\alpha|0\rangle + \beta|1\rangle$, where $|0\rangle$ and $|1\rangle$ in the above superposition can be seen as representing classical 0 and 1 and α, β are such complex numbers that $|\alpha|^2 + |\beta|^2 = 1$. Similar *superpositions* of "classical" states are one of the key features of quantum states.

Historically, three outcomes of Quantum Information Processing and Communication (QIPC), during the years 1984-94, can be seen as killers upps for the whole field: a proof that one can have unconditionally secure quantum cryptography (generating random shared classical keys); the demonstration of the quantum teleportation and the design of quantum polynomial time algorithm for factorization (what could jeopardise most of the currently used encryption and signature systems).

Currently, the main research areas of quantum informatics are:

- To design quantum algorithms and protocols that would be (asymptotically) more efficient than their classical counterparts and to understand what quantum phenomena are behind their superiority.
- To design efficient quantum simulations of complex quantum processes.
- To explore power of various models of quantum computation such as quantum finite automata, quantum Turing machines and quantum cellular automata.

- To develop quantum computational and communication complexity; to explore main quantum complexity classes, their mutual relations and relations to the classical complexity classes.
- To explore various non-traditional models of quantum computation such as: one-way quantum computation, measurement based quantum computation, adiabatic computation and topological quantum computation.
- To explore whether and how we can build powerful quantum processors.
- To discover various sets of quantum primitives that could be used to build a quantum computer.
- To discover new methods to design quantum algorithms and new methods to analyse them and to show lower bounds for various algorithmic problems.
- To explore which quantum processes can be efficiently simulated on classical computers.
- To develop and explore tools, such as quantum error correcting codes, that could be used to efficiently fight *decoherence* - a destructive impact of the environment - the main, often exponentially fast growing, obstacle of the powerful quantum information processing and transmission.
- To develop the quantum information theory including the theory of quantum channels and their capacities.
- To develop a theoretical basis for formal specification of quantum programming and reasoning languages and for design, verification and analysis of quantum programs.

Some of the main outcomes in QIPC

- An understanding has developed that it could pay off, in a dramatic fashion, to have powerful quantum processors to simulate quantum phenomena and to solve important classical computational and communication problems.
- A proof that the so-called Hidden Subgroup Problems for Abelian groups could be solved in polynomial time on quantum computers. As a consequence there are fast quantum algorithms to factorize integers and to break many currently used encryption and digital signature systems.
- A proof that for some important cryptographic tasks there are unconditionally secure quantum protocols (security of which is based on the laws of nature) and for some other cryptographic primitives (bit commitment) no unconditionally secure quantum protocols can exist.

- Discovery of the enormous computational and communication power of quantum entanglement and non-locality - perhaps of the two most mysterious quantum phenomena.
- Non-locality issues have been explored in breadth and depth.
- Experimental demonstration of quantum teleportation has been done.
- Distribution of photons even in the open air has been carried out over the distance of 148 km (on Canary islands).
- Design of basic quantum cryptography tools reached a semi-commercial level.

Some of the main current challenges of QIPC

- To help to develop the information processing model of the evolution of cosmos that would help to deal with major fundamental problems of theoretical physics and cosmology;
- To help to unify quantum mechanics and the theory of relativity,
- To help to answer such foundational questions as: (a) What is the nature of computing; (b) What is the nature of quantum mechanics?; (c) Is our world polynomial or exponential? (d) What are the relations between our physical world and our (also virtual) information processing worlds?
- To design powerful quantum processors.
- To explore how much and how good quantumness is indeed needed to get more power than classical information processing and communication resources may provide.
- To explore how much quantum tools can contribute to finding better solutions for tasks of broadly understood cryptography.
- To make quantum cryptography commercially fully attractive.
- To develop earth-to-satellite quantum communication that could be also used to make new tests of quantum phenomena. For example a test of quantum non-locality for a distance about 1000km
- To find out whether for any hidden subgroup problem there exists efficient quantum algorithms or to decide whether this is true at least for the graph isomorphism problem.
- To formulate new, quantum information processing based, principles for quantum physics.

2 QUANTUM THOUGHTS

- You have nothing to do but mention the quantum theory, and people will take your voice for the voice of science, and believe anything *Bernard Shaw (1938)*
- Quantum physics is, from the point of view of explaining quantum phenomena, a very unsatisfactory theory. Quantum physics is a theory with either some hard to accept principles or a theory leading to mysteries and paradoxes. Quantum theory seems to lead to philosophical standpoints that many find deeply unsatisfying. At best, and taking its descriptions at their most literal, it provides us with a very strange view of the world indeed. At worst, and taking literally the proclamations of some of its most famous protagonists, it provides us with no view of the world at all. *Rogert Penrose*
- Quantum physics, that mysterious, confusing discipline, which none of us really understands, but which we all know how to use. *Murray Gell-Mann*
- 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 fields; Now I have new vision, namely that everything is information. *John Archibald Wheeler*
- There is no quantum world. There is only an abstract quantum physical description. It is wrong to thin k that the task of physics is to find out how Nature is. Physics concerns what we can say about Nature . *Niels Bohr*
- 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 it 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 quantum physics. *Daniel Greenberger*
- The world is a dangerous place, particularly, if you are a qubit. *Folklore*
- It is well known that it is very hard to understand quantum physics. However, it is less known that understanding of quantum physics is child's play comparing with understanding of child's play.
- One who is serious all day will never have good time, while one who is frivolous all day, will never establish a household. *Ptahhotep, 24 century B.C.*