# CHALLENGES OF QUANTUM INFORMATICS

Jozef Gruska

Faculty of Informatics, Brno, Czech Republik

September 20, 2006

## STARTING OBSERVATIONS

**The initial development of quantum information processing has been much stimulated by outcomes in theoretical informatics (the proofs of existence universal reversible and quantum Turing machines).**

**Apt killers in quantum information processing have been again physically counterintuitive results of people with informatics thinking (Shor's algorithms, quantum error correcting codes and fault-tolerant computations).**

**It has turned out that informatics offers for quantum physics paradigms, concepts, and results that can allows physics to see faster what is impossible, to formulate and to sharp better results and to see deeper into the physical world.**

**Currently, in connection with quantum information processing and quantum physics, theoretical informatics has enormous chance and duty to contribute to solving some of the key current problems of physics in particular and science in general.**

# CONTENTS

- **Introductory observations.**
- **Main challenges of quantum informatics:**

1. **To help to understand better the physical world and its relation to the information processing world.**
2. **To help to understand better quantum world and its relation to classical world.**
3. **To help to understand quantum entanglement and (non-signaling) non-locality.**
4. **To help to see whether we can build quantum computers and how they can be useful.**
5. **To discover variety of universal sets of quantum information processing primitives and main quantum computation modes.**

6. **To develop quantum algorithms design methodologies and to understand potentials of quantum algorithms and communication protocols.**
7. **To develop quantum computation and communication complexity theories.**
8. **To develop quantum information theory**
9. **To develop quantum programming, semantics, logic and reasoning theories**
10. **To understand limits and potentials of quantum cryptography.**

- **Closing observations.**

# BASIC STANDPOINTS and OBSERVATIONS

## COMMON SENSE REASONING

**Quantum information processing and communication can be seen as a merge of perhaps the two most important areas of science of twentieth century:**

**quantum mechanics**

**and**

**(theoretical) informatics.**

**It would therefore be astonishing if such a merge would not shed new light on both of them and would not bring new great discoveries.**

## TWO BASIC WORLDS

**BASIC OBSERVATION: All information processing and transmissions are done in the physical world.**

**Our basic standpoint is that:**

**The goal of physics is to study elements, phenomena, laws and limitations of the physical world.**

**The goal of informatics is to study elements, phenomena, laws and limitations of the information world.**

## TWO WORLDS - BASIC QUESTIONS

- **Which of the two worlds, physical and information, is more basic?**
- **What are the main relations between the basic concepts, principles, laws and limitations of these two worlds?**

Quantum physics is an elementary theory of information. *Č. Brückner, A. Zeilinger*

# DEVELOPMENT of BASIC VIEWS

on the role of information in physics:

- **Information is information, nor matter, nor energy.**

  **Norbert Wiener**

- **Information is physical**

  **Ralf Landauer**

- **Physics is informational**

  **John Wheeler**

# JOHN WHEELER's VIEW

**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**

## WHEELER's "IT from BIT"

**IT FROM BIT symbolizes the idea that every item of the physical world has at the bottom - at the very bottom, in most instances - an immaterial source and explanation.**

**Namely, that which we call reality arises from posing of yes-no questions, and registering of equipment-invoked responses.**

**In short, that things physical are information theoretic in origin.**

# DEVELOPMENT of VIEWS on QUANTUM PHYSICS

# A POPULAR VISION of QUANTUM THEORY

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)

## AN EXPERT’s VISION of QUANTUM THEORY

**I am going to tell you what Nature behaves like......**

**However do not keep saying to yourself, if you can possibly avoid it,**

**BUT HOW CAN IT BE LIKE THAT?**

**because you will get “down the drain” into a blind alley from which nobody has yet escaped.**

**NOBODY KNOWS HOW IT CAN BE LIKE THAT.**

Richard Feynman (1965): The character of physical law.

## BOHR's VIEW

- **Everybody who is not shocked by quantum theory has not understood it.**
- **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.**

# WHAT ACTUALLY QUANTUM PHYSICS TELL US?

Quantum physics

tells us

**WHAT happens**

but does not tell us

**WHY it happens**

and does not tell us either

**HOW** it happens

nor

**HOW MUCH** it costs

## FIRST PARADOX

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

## ANOTHER PARADOX

- **Quantum phenomena exhibit a variety of weird, puzzling, counter-intuitive, mysterious and even entertaining effects.**
- **Quantum information processing tries to make an effective use of these mysterious phenomena as of a new resource that allows to design new quantum information processing and communication technology and also to get a better understanding of (quantum) nature.**

# HISTORY of INFORMATICS CONTRIBUTION to QIPC

- **Bennett - the existence of universal reversible TM**
- **Vazirani and Bernstein - the existence of efficient universal quantum TM**
- **Shor's algorithms**
- **Teleportation - Bennett et al.**
- **Quantum key generation protocol - Bennett and Brassard**
- **Proof that QKG is unconditionally secure (Mayer-Yao)**
- **Proof that there is no unconditionally secure quantum bit commitment (Mayer, Lo-Chau)**
- **The existence of quantum error-correcting codes (Shor)**
- **The existence of fault-tolerant computations (Shor)**

WHY von NEUMANN

DID (COULD) NOT DISCOVER QUANTUM COMPUTING?

# WHY von NEUMANN

# DID (COULD) NOT DISCOVER QUANTUM COMPUTING?

- **No computational complexity theory was known (and needed).**
- **Information theory was not yet well developed.**
- **Progress in physics and technology seemed to be far from what would be needed to make even rudimentary implementations.**
- **The concept of randomized algorithms was not known.**

# WHY DO WE NEED QUANTUM INFORMATION PRECESSING SCIENCE?

There are at least five main reasons why QIPC is increasingly considered as of (very) large importance:

- **QIPC is believed to lead to a new Quantum Information Processing Technology that will have deep and broad impacts.**
- **Several sciences and technologies are approaching the point at which they badly need expertise with isolation, manipulating and transmission of particles.**
- **It is increasingly believed that new, quantum information processing based, understanding of quantum phenomena can be developed.**
- **Quantum cryptography seems to offer new level of security and be soon feasible.**
- **QIPC has been shown to be more efficient in interesting/important cases.**

# QICC SCIENCE and TECHNOLOGY - STATE of the ART

- **Factorization of number 15 has been so far main experimental success in the area of quantum computation - progress in designing powerful quantum processors**
- **Proposal for 300 qubit quantum processors are on the “drawing boards”, but it is still open, and very important, problem whether we can build really powerful processors.**
- **A proof of principle for quantum key distribution has been done for 122 km; theoretical results show that 2-3 hundred km cold be possible and speed as well quality of key generation has been dramatically improved.**
- **Theory has made enormous progress though there is still a lot of controversy concerning very basic concepts and very basic experiments.**
- **More moneys go to this area more important is the question what will come out and how valid is current theory.**

# GREAT CHALLENGES of QUANTUM INFORMATICS

# CHALLENGE I

## TO HELP TO UNDERSTAND THE PHYSICAL WORLD

# BIRTH of QUANTUM PHYSICS

**Two basic events:**

- **In 1901 Planck has discovered the existence of quanta;**
- **In 1905 Einstein has discovered the existence of light quanta (and relativity theory).**

**Two basic points:**

- **Discovery of quantum mechanics and relativity started a revolution in our view of physical world;**
- **Some think that quantum revolution is unfinished yet because quantum mechanics has problems to get unified with time and space into one coherent theory and there are still problems with accepting non-locality quantum entanglement implies and randomness of quantum measurement.**

# CURRENT SITUATION

**Todays we are beginning to realize how much of all physical science is really only *information, organized in a particular way*.**

**But we are far from unraveling the knotty question: *To what extent does this information reside in us, and to what extent is it a property of nature?***

**Our present quantum mechanics formalism is a peculiar mixture describing in part laws of Nature, in part incomplete human information about Nature – all scrambled up together by Bohr into an omelet that nobody has seen how to unscramble,**

**Yet we think the unscrambling is a prerequisite for any further advances in basic physical theory.**

Edwin T. Jaynes, 1990

## SOME of FUNDAMENTAL QUESTIONS

- **Is our universe a polynomial or an exponential place?**
- **How real and useful is (quantum) randomness quantum measurement produces?**
- **How real and useful is quantum entanglement and what are the laws and limitations of quantum entanglement?**
- **What kind of non-locality we can have that does not contradict the relativity theory?**
- **How to distinguish between various interpretations of quantum mechanics?**

# BASIC STANDPOINTS and BELIEFS

- **Through the study of the laws and limitations of quantum information processes we can get a new and deeper understanding of quantum phenomena.**
- **Informatics brought for the study of quantum world in general and quantum information processing in particular, new paradigms, concepts, models, methods, tools and supplied it with a variety of useful results.**
- **Using informatics reasoning and results one show (for example) that:**
  - **Certain quantum resources can be very useful (and how much).**
  - **Certain quantum processes, algorithms and protocols can be very useful (and better than classical).**
  - **Certain assumptions concerning physical world are unrealistic.**
  - **Certain physical processes and phenomena are impossible.**

# CASE STUDY – CLASSIFICATION of IMPOSSIBLE

Some ways to show that some quantum event or phenomenon $E$ is impossible:

- **To show that $E$ would imply superluminal communication.**
- **To show that $E$ would violate NO-cloning theorem.**
- **To show that $E$ would imply that problems from some class (likely) larger than P would be solvable in polynomial time. (This way one can also classify impossible tasks).**

## EXAMPLES - COMPLEXITY THEORY WAYS to SHOW IMPOSSIBILITY

- **Abrams and Llyod (1998) showed that under the assumption that quantum mechanics is non-linear, more exactly that Weinberg's model of quantum mechanics is valid, one can solve in polynomial time NP-complete problems.**
- **Aaronson (2004) has shown that if arbitrary one-qubit nonlinear gates can be implemented without an error, then PSPACE-complete problems can be solved in polynomial time.**
- **He has also shown that if so-called *post-selection* is allowed, then PP-complete problems can be solved in polynomial time.**

# CHALLENGES

- **To formulate new , information rocessing based, principles for (quantum) physics. For example a principle that NP-complete problems are intractable in the physical world.**
- **To develop new tests for quantum mechanics.**

# CASE STUDY – RANDOMNESS in THE PHYSICAL WORLD

## FAMOUS POLEMICS between EINSTEIN and BOHR

**Randomness of the quantum collapse after a measurement has always puzzled scientists.**

**God does not roll dice.**

**is a famous comment of Einstein, a strong opponent of randomness at quantum measurement.**

**The true God does not allow anybody to prescribe what he has to do,**

**Famous reply by Niels Bohr**

# DOES GOD PLAY DICE? - NEW VIEWS

**God does play even non-local dice.**

**An observation, due to N. Gisin, on the basis that measurement of entangled states produces shared randomness.**

**God is not malicious and made Nature to produce, so useful, (shared) randomness.**

**What the outcomes of theoretical informatics imply.**

# VIEWS on QUANTUM MEASUREMENT

- **Had I known that we are not going to get rid of this dammed quantum jumping, I never would have involved myself in this business.**
  **Erwin Schrödinger**

- **There are still wise old (and prominent) physicists (Penrose, ‘t Hoft) and bright young physicists that believe that the current theory is (deeply) wrong in many aspects, especially concerning measurement and non-locality.**

# CHALLENGE II

TO UNDERSTAND BETTER RELATION BETWEEN the CLASSICAL

and

QUANTUM WORLDS

# CLASSICAL versus QUANTUM WORLDS

- **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 classical world - there is only quantum world (D. Greenberger).**
- **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)**

## CLASSICAL versus QUANTUM PHYSICS

**I believe there is no classical world. There is only quantum world.**

**Classical physics is a collection of unrelated insights: Newton’s laws. Hamilton’s principle, etc. Only quantum theory brings out their connection.**

**An analogy is the Hawaiian Islands, which look like a bunch of island in the ocean. But if you could lower the water, you would see, that they are the peaks of a chain of mountains.**

**That is what quantum physics does to classical physics.**

D. Greenberger

## WHERE is a border between CLASSICAl and QUANTUM WORLD

- An important research agenda is to find out for which macroscopic objects superposition holds.
- It has been show that superposition holds for large molecules and for systems consisting of $2^{14}$ atoms;
- There is still range of several orders of magnitude to explore where the border between the classical and quantum world is.

# CHALLENGE III

## TO UNDERSTAND QUANTUM ENTANGLEMENT AND NON-LOCALITY

# CASE STUDY - QUANTUM ENTANGLEMENT

# QUANTUM NON-LOCALITY

- Physics was non-local since Newton's time, with exception of the period 1915-1925.
- Newton has fully realized counterintuitive consequences of the non-locality his theory implied.
- Einstein has realized the non-locality quantum mechanics imply, but it does not seem that he realized that entanglement based non-locality does not violate no-signaling assumption.
- Recently, attempts started to study stronger non-signaling non-locality than the one quantum mechanics allows.

## NON-LOCALITY in NEWTON’s THEORY

**Newton realized that his theory concerning gravity allows non-local effect. Namely, that**

> **if a stone is moved on the moon, then weight of all of us, here on the earth, is immediately modified.**

## NEWTON’s words

The *consequences of current theory that implies that* gravity should be innate, inherent and essential to Matter, so that any Body may act upon another at a Distance throw a Vacuum, without the mediation of any thing else, by and through which their Action and Force may be conveyed from one to another, is to me so great an Absurdity, that I believe no Man who has in philosophical Matters a competent Faculty of thinking, can ever fall unto it.

Gravity must be caused by an Agent acting constantly according certain Laws, but whether this Agent be material or immaterial, I have left to the Consideration of my Readers.

## BEGINNINGS of MODERN STORY of NONLOCALITY

- In 1935 Einstein, Podolsky a Rosen (EPR) used entanglement to attack the validity of quantum physics as a complete theory of Nature.
- They defined an entangled state of two particles such that if a position (momentum) measurement was made on one of the particles, then position (momentum) of second particle was known.
- EPR concluded that position and momentum have to be *elements of reality*, i.e. they have to have predetermined values before measurements.
- If translated into mathematical formalism this means that Local Hidden Variable (LHV) model of Nature has to hold.
- In 1964 Bell showed that if LHV model holds, then not all predictions of QM can be correct and he also showed a way how to test which model - LHV or QM -holds.

# QUANTUM ENTANGLEMENT - BASIC DEFINITIONS

The concept of entanglement is primarily concerned with the states of multipartite systems.

For a bipartite quantum system $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$, a pure state $|\Phi\rangle$ is called entangled if it cannot be decomposed into a tensor product of a state from $\mathcal{H}_A$ and a state from $\mathcal{H}_B$.

A mixed state (density matrix) $\rho$ of $\mathcal{H}$ is called entangled if $\rho$ cannot be written in the form

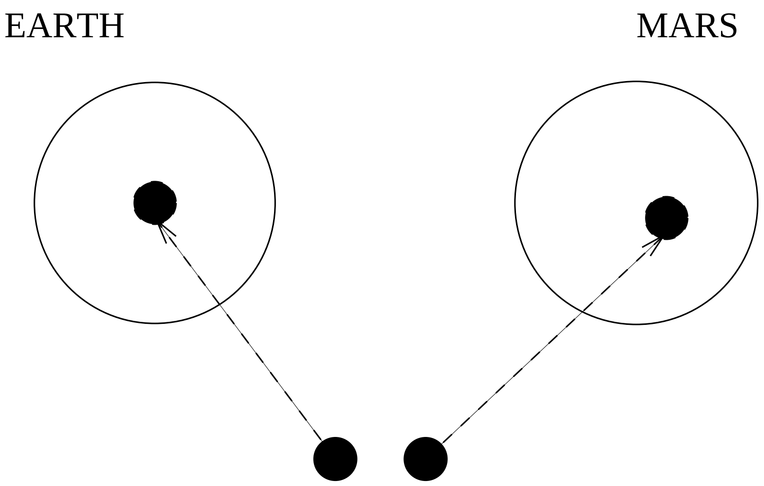
$$\rho = \sum_{i=1}^{k} p_i \rho_{A,i} \otimes \rho_{B,i}$$

where $\rho_{A,i}$ ($\rho_{B,i}$) are density matrices in $\mathcal{H}_A$ (in $\mathcal{H}_B$) and $\sum_{i=1}^{k} p_i = 1$, $p_i > 0$.

**Let two particles originally in the EPR-state**

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

**move far from each other**



**then measurement of any one of these particles makes the EPR-state to collapse, randomly, either to one of the states $|00\rangle$ or $|11\rangle$. As the classical outcomes both parties get at their measurements, no matter when they make them, the same outcomes.**

**Einstein called this phenomenon “spooky action at a distance” because measurement in one place seems to have an instantaneous (non-local) effect at the other (very distant) place.**

# VIEWS of QUANTUM ENTANGLEMENT - II

- Quantum entanglement is an observable phenomenon. It has been observed between various quantum objects (photons, atom and photon, ...) and for distance more than 10 km.
- Quantum entanglement used to be seen as theoretical curiosity of no significant practical importance. Nowadays, quantum entanglement is seen as so important computation and communication resource, that it can be seen as a gold mine of current science.
- Quantum entanglement does not exist. Its theoretical existence is only due to incomplete theory. Claims on an observation of entanglement by experience are based on wrong reasoning.

# POWER of ENTANGLEMENT

Quantum entanglement as a resource allows:

- to perform processes that are classically impossible;
- to speed-up (quantum) algorithms;
- to make communications more efficient;
- to generate classical cryptogr. keys in absolutely secure way;
- to make transmission of quantum informatio in an absolutely secure way;
- to enlarge capacities of (quantum) channels;
- to act as catalyst.

# FUNDAMENTAL PROPERTIES of ENTANGLEMENT

- Entanglement is an observable phenomenon that does not depend on a physical representation.
- Entanglement enables and is consumed by a variety of tasks.
- Entanglement obeys a set of as yet not fully understood principles of behaviour.
- Entanglement is shared according to strict laws and limitations.
- Entanglement cannot be increased by local actions and classical communications

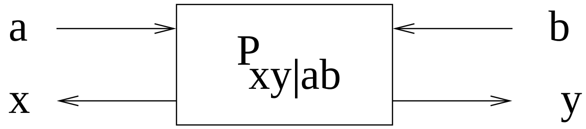
# IMPORTANCE of MULTIPARTITE ENTANGLEMENT

- ME provides a unique means to check Einstein’s locality without invoking statistical arguments;
- ME is the key ingredient to have polynomial time quantum algorithms for problems that do not have polynomial time classical algorithms;
- ME is central for quantum error correcting codes and fault-tolerant computations;
- ME helps better to characterize the critical behaviour of different many-body systems giving rise to a unified treatment of the quantum phase transitions;
- ME is crucial for understanding various condense matter phenomena and might solve some unresolved problems such as high-T superconductivity;
- ME is considered as irreplaceable for performing various multipartite tasks as quantum secr et sharing, Byzantine agreement, remote entangling and so on

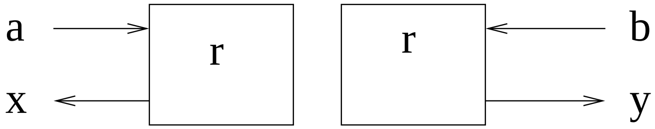
# CASE STUDY - QUANTUM NON-LOCALITY

# NON-LOCAl and LOCAL SYSTEMS

**The behaviour of a bipartite quantum state under measurement can be described by a conditional probability distribution $P_{xy|ab}$ - so called two-party information-theoretic primitive - where $a$ and $b$ denote the chosen bases and $x$ with $y$ are corresponding outputs.**



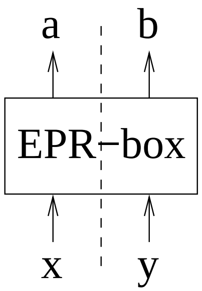
**John Bell was the first to recognize that there are measurement bases such that resulting behaviour is not local, i.e. cannot be explained by shared classical information $r$. He showed existence of *Bell inequalities* that cannot be violated**



**by any local system, but are violated when the EPR-state is measured.**

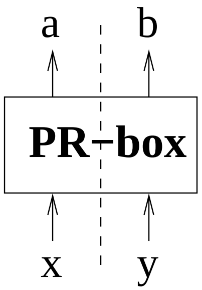
# EPR-box versus RP-box

Non-locality exhibited by the measurement of the EPR state can be seen as the implementation of the following *EPR-box*



**x = y implies a = b**

Also non-locality exhibited by the following *PR-box* does not allow superluminal c ommunication and therefore does not contradict special relativity.



**x . y = (a + b) mod 2**

# MOTIVATION for PR-BOXES

**The idea of PR-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.**

# POWER OF PR-BOXES

- **Using one PR-box one can simulate measurement of the EPR-state.**
- **Using PR-boxes one can make bit commitment and 1/2-oblivious transfer unconditionally secure.**
- **Having PR-boxes one can simulate any secret multiparty computation and solve any multipartite communication problem by communicating a single bit - what is not possible**

**On the other hand (quant/ph-0601122) claims that there is an aposteriori realization of PR-boxes.**

# CHALLENGE IV

TO HELP TO SEE WHETHER WE CAN BUILD POWERFUL

QUANTUM COMPUTERS

## WHY WE SHOULD TRY to have QUANTUM COMPUTERS?

If you try to reach for stars you may not quite get one, but you won’t come with a handful of mud either.

Leo Burnett

# KEY STEPS in the DEVELOPMENT of QIPC

Key steps in the development of QIPC were separations of four problems:

**P1 Can we build powerful quantum computers?**

**P2 What could be achieved with powerful quantum computers?**

**P3 What are the laws and limitations of quantum information processing and communication?**

**P4 Can we develop a better understanding of the quantum world on the basis of the laws and limitations of QIPC?**

This separation allowed complexity theory to make substantial contributions to the attempts to solve problems P2 and P3, especially P2, and to set as its new goal a contribution to the solution of the problem P4.

New recent goal and challenge of complexity theory is to help to deal with the problem P1.

## CAN QM BREAK DOWN BEFORE FACTORING LARGE INTEGERS?

Some prominent researchers claim that it can (Gerard't Hoft, 1999; Leonid Levin 2003).

It is believed that complexity theory can make debate whether quantum computing is possible less ideological and more scientific and can lay groundwork for a rigorous discussion of such problems?

For example, Aaronson (0311039) tries to develop complexity classification of quantum states and to refine vague ideas about breaking quantum mechanics into a specific hypothesis that might be experimentally testable soon.

# WHY COULD QM FAIL TO FACTORIZE

- **Successful factorization requires that laws of quantum mechanics are valid to unlimited precision what is very unlikely.**
- **Neutrinos, gravitation waves and other peculiar sources of decoherence may not satisfy rules on which quantum error correcting methods are based.**
- **Universe is too small to test states needed to factor 1000 bit integers.**

# TREE-STATES

- **In case QM breaks down before factoring large integers, there should be a natural “Sure/Shor separator”, that is a set of quantum states that accounts for all experiments performed so far, but not for all states in Shor’s algorithm at 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 additions and tensor products. For example,**

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

- **Aaronson also showed that certain states arising in quantum error correction, some codeword states of stabilizer codes, require $n^{\Omega(\lg n)}$ additions and tensor products, even to approximate.**

# CHALLENGE V

TO FIND UNIVERSAL SETS of QUANTUM COMPUTATION PRIMITIVES

# BASIC OBSERVATIONS

**Nature offers many ways – let us call them technologies – various quantum information processing primitives can be exhibited, realized and utilized.**

**Since it appears to be very difficult to exploit the potential of nature for QIP, it is of large importance to explore which quantum primitives form universal sets of primitives, and are (quite) easy to implement.**

**Also from the point of view of understanding of the laws and limitations of QIP and also of quantum mechanics itself, the problems of finding rudimentary and universal QIP primitives are of large experimental and fundamental importance.**

**The search for quantum computation universal primitives, and their optimal use, is actually one of the major tasks of the current QIP research (both theoretical and experimental) that starts to attack the task of building quantum processors seriously.**

## MOTTO II.

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

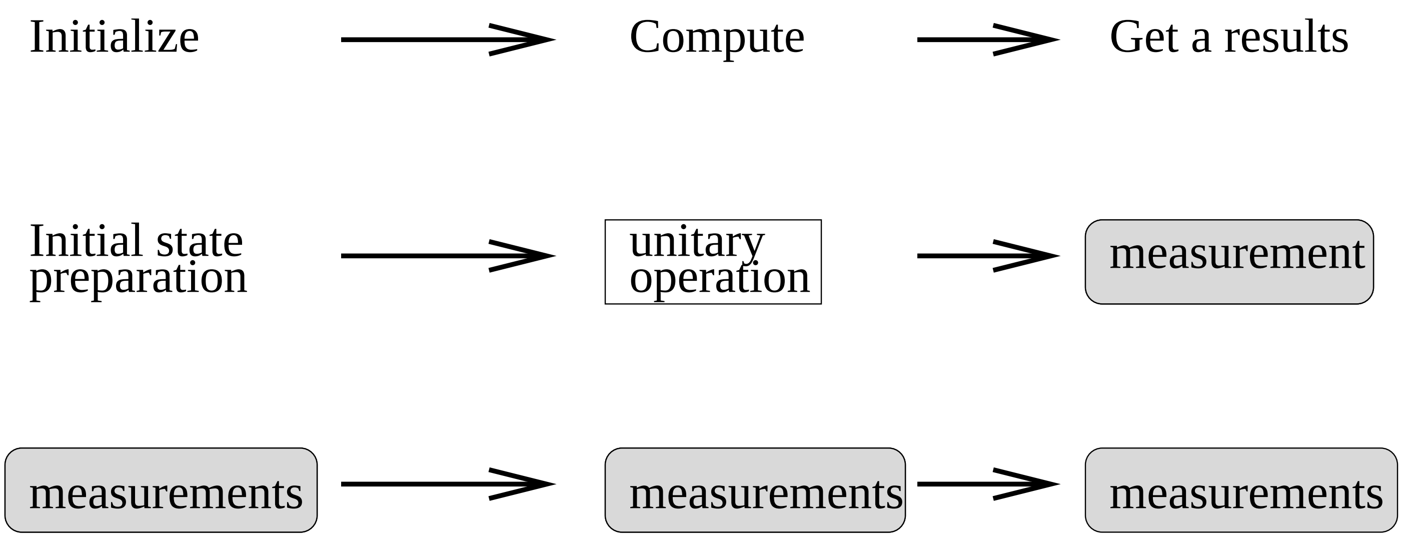
# ONE STORY TO REMEMBER

- **The proposal to build Collosus, the first electronic computer for cryptanalysis purposes, was during the 2WW rejected by a committee of prominent specialists as impossible to make, in spite of the fact that British cryptanalysts needed it badly to crack communication between Hitler and his generals.**
- **Collosus was then built by an ingenious optimist, Tommy Flowers, within 10 months in a Post office laboratory, and worked from the beginning successfully to break Lorenz cipher, starting January 1944.**
- **The key point was that Flowers realized that velvets were reliable provided they were never switched on and off. (Of course, nobody believed him.)**

# MODELS of UNIVERSAL COMPUTERS

- **Classical models: circuits, Turing machines, cellular automata, RAM a PRAM**
- **Quantum models**
  - **(Unitary operations based ) Quantum Turing Machines**
  - **(Unitary operations based) Quantum Circuits**
  - **Quantum cellular automata ????**
  - **Measurements based quantum circuits**
  - **Measurements based quantum Turing machines**
- **Emerging idea: Classically controlled quantum computation (automata).**

# TWO COMPUTATION MODES



Initialize → Compute → Get a results

Initial state preparation → unitary operation → measurement

measurements → measurements → measurements

Measurement = projective measurement.

# A UNIVERSAL SET of QUANTUM GATES

**The main task at quantum computation is to express solution of a given problem $P$ as a unitary matrix $U$ and then to construct a circuit $C_U$ with elementary quantum gates from a universal se ts of quantum gates to realize $U$.**

**A simple universal set of quantum gates consists of gates**

$$\textbf{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \sigma_z^{1/4} = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{\pi}{4}i} \end{pmatrix}$$

## A THIN BORDER between UNIVERSALITY and NON-UNIVERSALITY

**It is well known, as Gottesman-Knill theorem, that quantum circuits with operators in so called**

$$\textbf{\textit{Clifford set}} = \left\{CNOT, H, \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{\pi}{2}i} \end{pmatrix}\right\}$$

**can be simulated on classical computers in polynomial time. However, if the set of the above operators is “slightly enlarged”, by one of the states**

1. $|H\rangle = \cos\frac{\pi}{8}|0\rangle + \sin\frac{\pi}{8}|1\rangle$**;**
2. $|G\rangle = \cos\beta|0\rangle + e^{i\frac{\pi}{4}}\sin\beta|1\rangle$**, where** $\cos(2\beta) = \frac{1}{\sqrt{3}}$**;**

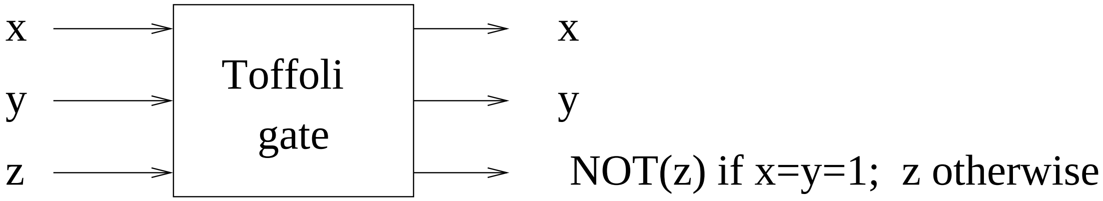
**we get already a universal set of quantum primitives (Bravyi and Kitaev, 2004).**

# COMPUTATIONALLY UNIVERSAL SET of GATES

**From the computation point of view universal is the following simple set of gates**

**TOFFOLI GATE and HADAMARD GATE**

## Toffoli gate



**is universal for classical reversible computing.**

## MINIMAL RESOURCES for UNIVERSAL MEASUREMENTS

**Perdrix (2004) has shown that**

**one auxiliary qubit and**

**one two-qubit Pauli measurement specified by the observable $(X \otimes Z)$ and three one-qubit Pauli measurements $(X, Z, \frac{1}{\sqrt{2}}(X+Y))$**

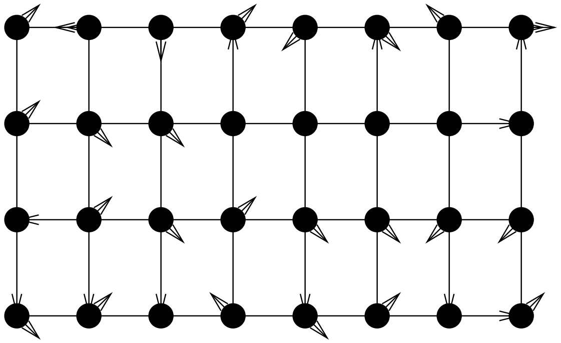
**are sufficient to approximate, up to a Pauli operator, any unitary operation.**

$(X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \ Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ **are so called Pauli matrices**$)$

## BASIC COMPUTATION MODES

- **Unitary operations + measurements based model of computations.**
- **Measurements-only model of computations**
- **One-way quantum computations.**
- **Adiabatic computations**

# ONE-WAY QUANTUM COMPUTER



- **A rectangular grid of qubits.**
- **Initialization in a cluster state - a global entangled state.**
- **Execution = a sequence of one-qubit measurements (to perform disentanglement).**
- **(Some measurements can be performed in parallel.)**
- **The key resource is the cluster state that is “consumed” step by step through measurements.**

Raussendorf, Browne, Briegel - quant/ph/03001052

# CHALLENGE VI

TO DETERMINE WHETHER WE CAN HAVE ENOUGH

POWERFUL QUANTUM ALGORITHMS

# EFFICIENT QUANTUM ALGORITHM DESIGN TECHNIQUES

**MAIN PROBLEM: Number of “impressive” quantum algorithms is still small (Shor’s factorization, Grover’s search algorithm and few others).**

## MAIN ALGORITHM DESIGN METHODOLOGIES:

- **Fourier transform and other transforms**
- **Amplitude amplification**
- **Random walks**

Recently, useful ways have been found to combine these techniques.

For example, combining Grover’s search and random walks a $\mathcal{O}(n^{13/10})$ algorithm has been found to determine whether an undirected graph contains a triangle (Magniez et al. (2003)).

# MAIN OUTCOMES and CHALLENGES

- **Main result:** **There are quantum polynomial algorithms for Hidden Subgroup Problems for Abelian groups.**
  - **Main consequence: There are polynomial time algorithms for factorization and discrete logarithm computation.**
- **Main challenge:** **Are there polynomial time algorithms for** ***Hidden subgroup problems*** **for any subgroup?**
  - **Main potential consequence in case of a positive answer: A quantum polynomial time algorithm for the graph isomorphism problem.**

# HIDDEN SUBGROUP PROBLEM (HSP)

**Given: An (efficiently computable) function $f : G \rightarrow R$, where $G$ is a group and $R$ is a finite set.**

**Promise: There exists a subgroup $G_0 \leq G$ such that**

- **$f$ is constant on each left coset of $G$ (with respect to $G_0$).**
- **$f$ is distinct on different cossets of $G$ (with respect to $G_0$).**

**(and in this sense $G_0$ is hidden by $f$)**

**Task: Find a generating set for $G_0$ (in polynomial time (in $\lg |G|$) in the number of calls to the oracle for $f$ and in the overall polynomial time).[1]**

[1] A way to solve the problem is to show that in polynomial number of oracle calls (or time) the states corresponding to different candidate subgroups have exponentially small inner product and are therefore distinguishable.

# GROVER’s QUANTUM SEARCH ALGORITHM

**Another important outcomes in the area of quantum algorithms is algorithm of Grover to search in an unordered set of $n$ elements in $\sqrt{n}$ steps.**

**Any classical algorithm for such search requires in average $\frac{n}{2}$ steps in the worst case.**

Grover’s search algorithm has numerous applications.

# CHALLENGE VII

## TO UNDERSTAND POTENTIAL and LIMITS of QUANTUM CRYPTOGRAPHY

# QUANTUM ONE-TIME PAD CRYPTOSYSTEM

## CLASSICAL ONE-TIME PAD cryptosystem

plaintext: an $n$-bit string $p$
shared key: an $n$-bit string $k$
cryptotext: an $n$-bit string $c$
encoding: $c = p \oplus k$
decoding: $p = c \oplus k$

## QUANTUM ONE-TIME PAD cryptosystem:

plaintext: an $n$-qubit string $|p\rangle = |p_1\rangle \ldots |p_n\rangle$
shared key: two $n$-bit strings $k, k'$
cryptotext: an $n$-qubit string $|c\rangle = |c_1\rangle \ldots |c_n\rangle$
encoding: $|c_i\rangle = \sigma_x^{k_i}\sigma_z^{k'_i}|p_i\rangle$
decoding: $|p_i\rangle = \sigma_z^{k'_i}\sigma_x^{k_i}|c_i\rangle$ where $|p_i\rangle = \begin{pmatrix} a_i \\ b_i \end{pmatrix}$ and $|c_i\rangle = \begin{pmatrix} d_i \\ e_i \end{pmatrix}$ are qubits and

$\sigma_x = X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ with $\sigma_z = Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ are Pauli matrices.

## WHY IS QUANTUM ONE-TIME PAD ABSOLUTELY SECURE?

**At quantum one-time pad cryptosystem a qubit $\phi$ is transmitted through a mixed state**

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

**whose density matrix is**

$$\frac{1}{2}I_2$$

**that is the same as the density matrix for the mixed state**

$$\{(\frac{1}{2}, |0\rangle), (\frac{1}{2}, |1\rangle)\}$$

**that corresponds to the transmission of a random bit.**

# TWO SHANNON THEOREMS

- **Classical Shannon Theorem** says that $n$ bits are necessary and sufficient to hide perfectly $n$ bits.

  Consequently: ONE-TIME-PAD CRYPTOSYSTEM is perfectly secure if parties always share new $n$ random and secret bits.

- **Quantum Shannon Theorem** says that $2n$ bits are necessary and sufficient to hide perfectly $n$ qubits.

  Consequently: QUANTUM ONE-TIME-PAD CRYPTOSYSTEM is perfectly secure if parties always share either new $2n$ secret bits.

# BASIC QUANTUM LIMITATIONS

- **Heisenberg uncertainty principle: There are measurements that cannot be perform ed simultaneously with arbitrary precision: For example**
  - **One cannot determine simultaneously both the position and the momentum of a particle with arbitrary precision;**
  - **One cannot measure polarization of a photon in the vertical-horizontal basis and simultaneously in the diagonal basis.**
- **No-cloning theorem : unknown quantum states cannot be copied perfectly.**
- **Measurement in general destroys the state being measured.**
- **There is no way to distinguish on 100% non-orthogonal states.**
- **Two mixed states with the same density matrix are undistinguishable**

## MAIN OUTCOMES

- **Proofs that there is unconditionally secure quantum generation of the shared classical random keys.**
- **A proof that there are no unconditionally secure quantum bit commitment and 1/2 oblivious transfer protocols.**
- **Experimentally successful transmission of photons for long distances through fibers and also in the open air and experimentally successful implementations of quantum cryptographic networks.**

## CHALLENGES

- **To develop quantum protocols for digital signature, authentication, privacy preservation and for anonymity tasks.**
- **To study in depth potentials of quantum attacks.**
- **To study composition of quantum cryptographic protocols.**

# CHALLENGE VIII

## TO DEVELOP QUANTUM COMPLEXITY THEORIES

# QUANTUM COMPUTATIONAL COMPLEXITY CLASSES

Main quantum versions of the classical complexity classes:

- **QP** - quantum version of the class **P**
- **BQP** - quantum version of the class **BPP**
- **QNP** - a quantum version of the class **NP** - defined through acceptance with positive probability.
- **QMA** - another quantum version of the class **NP** - defined through testing using a witness.

# PROPERTIES of the class **BQP**

- **Factoring and discrete logarithm are in BQP;**
- **BQP is very robust –** $\mathrm{BQP}^{\mathrm{BQP}} = \mathrm{BQP}$**;**
- $\mathrm{NP} \not\subseteq \mathrm{BQP}$ **relative to a random oracle'**
- $\mathrm{BQP} \subseteq \mathrm{PP}$**.**
- **If UP** $\cap$ **coUP**$\subseteq$ **BQP, then public key cryptosystems cannot be secure against quantum computer attack.**
- $\mathrm{NP} \not\subseteq \mathrm{BQP}$ **unless** $\mathbf{PP}^{\mathbf{PH}} = \mathbf{PP}$**.**

**OPEN PROBLEMS**

- **Is graph isomorphism in BQP?**
- **Is** $\mathrm{UP} \cap \mathrm{coUP} \subseteq \mathrm{BQP}$

# OLD CHALLENGES of QUANTUM COMPLEXITY THEORY

- **To design quantum algorithms that would be asymptotically more efficient than fastest classical algorithms for a given problem.**
- **To develop methods for design of efficient quantum algorithms**
- **To develop methods to show lower bounds for quantum algorithms**
- **To study quantum complexity classes and their relations to classical complexity classes.**
- **To develop efficient quantum communication protocols.**
- **To study cases when quantum communication protocols are asymptotically more efficient than classical communication complexity.**
- **To develop broadly understood quantum cryptography, and related theoretical concepts.**

# MAIN NEW CHALLENGES of QUANTUM COMPLEXITY THEORY

- **To help to determine whether we can build (and how) powerful quantum computers.**
- **To help to determine whether we can effectively factorize large integers using a quantum computer.**
- **To use complexity theory paradigms to classify quantum states**
- **To use complexity theory (computational and descriptional) to study quantum entanglement and non-locality.**
- **To use complexity theory to formulate laws and limitations of quantum physics.**
- **To study feasibility in physics on a more abstract level.**
- **To develop a more firm basis for quantum mechanics.**
- **To develop new tests of quantum mechanics.**

## FOUR BASIC POINTS

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

# CHALLENGE IX

## TO DEVELOP QUANTUM PROGRAMMING THEORY

## TWO GOALS

- **To develop quantum specification, programming, reasoning and verification theories as a way to get a new understanding of the quantum world.**
- **To develop quantum specification, programming, reasoning and verification theories as tools to specify and verify quantum processes.**

# NEW DEVELOPMENTS

A sample of new approaches:

- Quantum programming languages, compilers and simulators
- Dynamic quantum logic for quantum programs (Brunet, Jorrand, 2003)
- A lambda calculus for quantum computation (Tonder, 2003)
- Quantum constrain programming (Pierro, Wiklicky, 2001)
- Quantum process algebra (Jorrand, Laire, 2003).
- Formal verification of quantum protocols (Nagarajan, Gay, 2002)
- A categorical semantics of quantum protocols (Abramsky, Coecke, 2004)
- The logic of entanglement (Coecke, 2004)

## EXAMPLE

- **Abramsky and Coecke (2004) started to develp categorical smantics for quantum protocols.**
- **They started to study quantum computation from a novel point of view.**
- **They recasted standard axiomatic presentation of quantum mechanics, due to von Neumann, at a more abstract level, of compact closed categories with biproducts.**
- **They showed how essential structures found in key quantum information protocols, such as teleportation, can be captured at such an abstract level.**

- **They claim that this new abstract point of view opens new possibilities for describing and reasoning about quantum systems.**

# CHALLENGE X

## TO DEVELOP QUANTUM INFORMATION THEORY

# CLOSING OBSERVATIONS

# CHANGING WORLD

**Views on the role of physics in the understanding of the physical world keep developing.**

- **Nothing exists except atoms and empty space; everything else is opinion.** ***Democritus of Abdera (ca. 400 BC)*.**
- **In Science there is only Physics: all the rest is stamps collecting.** ***Ernest Rutherford (1912)***
- **Physics is like sex; it produces sometimes practical results, but this is not reason why we do it. Feynman (19??)**
- **Physics is not the only science to get deep understanding of physical world. Informatics can and should help. Or, even, it should take an initiative?**

## WISDOM

When a distinguished but elderly scientist states that something is possible, he is almost certainly right.

When he states that something is impossible,
he is almost certainly wrong,

Arthur C. Clarke