UPDATINGS
to

Quantum computing

by Jozef Gruska, McGraw-Hill

February 11, 2004

This is to acknowledge corrections and updatings to to these *Updatings* by Andris Ambainis, Andrew M. Childs, Jens Eisert, Chuzo Iwamoto and Arun K. Pati.

20 main recent updatings

1. Can we have quantum computers? – A new approach to this question by complexity theory. – See page **??**
2. Coding theorem for quantum capacity of quantum channels – see page **??**.
3. Equivalence of several additivity conjectures — see 112.
4. Single photon interference over 100 km – see 67.
5. Long distance quantum teleportation experiment – see 77.
6. Hardy's axioms for quantum mechanics and their simplification – see 156.
7. Information procesing based axioms of quantum mechanics – see 157.
8. Using classical communication complexity lower bound techniques to get insides into quantum non-locality — see page 50.
9. Quantum walks as a new method to get an exponential speed-up for (oracular) computational problems – see page 56.
10. Entangled graphs: arbitrary distribution of bipartite entanglement in multipartite systems – see 150.
11. Generalized approach to entanglement – see page 153.

12. Can we (physically) compute (mathematically) uncomputable? - see page 61.
13. Information as a resource in distributed quantum systems – see page 154
14. Progresses in demonstrating quantum effects for macroscopic objects – see page 18.
15. Progresses in experimental quantum cryptography – see page 66.
16. Ambainis quantum adversary lower bound method – see page 30.
17. Not all multipartite pure states violate some Bell inequality – see page 160.
18. Distinguishibility of quantum states by LOCC – see page 9 page 112; entanglement-assisted capacity formula – see page 104; quantum reverse Shannon theorem conjecture – see page 103; how to use additivity of capacities of quantum channels to show additivity of entanglement of formation (for some states) – see page 103 .
19. Polynomial time solution of Pell's equation — see page 24.
20. Quantum lower bounds for the collision problem and their implications – see page 27
21. Basics of fermionic and bosonic quantum computations — see 90

Chapter 1 — Fundamentals

page 3, after line +27, as a new paragraph (Determination of the ultimate limitations for computation is a challenging task — both for computing and physics. As analyzed by Lloyd (1999a), the speed with which a physical device can process information is limited by its energy (needed to switch from one state to another, distinguishable, state), and therefore on the basis of quantum mechanics one can determine that for an ultimate computer with 1kg of mass and 1l of volume, the maximal ultimate speed is 2.7×10^{50} operations per second. It is harder to determine the number of bits such a "ultimate laptop" can store in general (entropy limits the amount of information a computer can store), but it can be determined for a computer that has been compressed to form a black hole (3.8×10^{16} bits). Estimations are based on using such constants as the speed of light, the Planck constant and the gravitation constant.

(The question how black holes deal with information is an interesting problem of the current physics — whether they destroy information or not.) It seems that new physics is needed to understand these problems. The need to deal with errors can be an important factor why the above limits can be hard to achieve.)

Lloyd analysis is much based on so-called Margolus-Levitin (1998) bounds. The basic bound says that for time t to switch between two orthogonal (distinguishable) quantum states it holds $t \geq h/4E$, where E is the average energy. In other words a quantum system with average energy E can be made to oscillate between two orthogonal states with a frequency of $4E/h$. However, in the case the evolution passes through an exact cycle of N mutually orthogonal states at a constant rate, then for time t it holds $t \geq \frac{N-1}{N}\frac{h}{2E}$. (A well done article on this topics can be find (as pointed out to me by Marc van Woerkom) also on http://slashdot.org/article.pl?sid=01/06/22/007233.)

Recently Lloyd (2001) extended his analysis of the computational capacity of physical systems and he quantifies the amount of information that the universe could have registered and the number of elementary operations that it can have performed over its history. He showed that the universe copuld have performed, during its overall history, no more than 10^{120} operations on 10^{90} bits.

page 6, after line -5, as new points. Reif (1998) pointed out an important problem of quantum computing that seems so far to receive insufficient attention and that has to be explored to see more clearly perspectives of quantum computing. Namely, he pointed out that there appears to be so far neither a mathematical proof nor an experimental demonstration that quantum measurements can be done by measuring devices of small (molecular) volume and with small amount of energy. Or, at least, that the amount of these resources needed does not grow exponentially with the number of qubits involved. (In contrary, Reif provides arguments, but not a proof, indicating that exponentially growing resources may be needed to perform even approximate quantum measurements). He has pointed out that the Copenhagen interpretation of the quantum measurement, that assumes that quantum measurements are done at macroscopic devices (of no clear volume, in no clear time, and with no clear amount of energy) does not seem to apply to the case of quantum computing on molecular level, where one should assume that measurements are done on microscopic level. In this case the von Neumann interpretation of quantum measurement seems to be more appropriate, at which both the measured state and the measuring device are parts of a quantum system (and measurements are done on the microscopic level first and then outcomes are measured by macroscopic level to produce classical results) may be more appropriate. It has been pointed out that in such a case the measuring device and the (first) measurement process itself can be subjected to quantum effects and, as a consequence, can lead to predictions different from those the Copenhagen interpretation would provide.

page 7, after line +14 Several prominent researchers have recently expressed their skepticim that we can have powerfull enough quantum computers (to factor large integeres, say 1000 bit long) – Gerard't Hoft (1999), Leonid Levin (2003). Their arguments can be roughly (but not fully) summarized as follows:

- Successful factorization requires that laws of quantum mechanics are valid to unlimited precission what is very unlikely.
- Neutrinos, graviation waves and other 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.

In general there the following reaqsons for skepticism concerning attempts to build quantum computers.

1. There are fundamental reasons why large quantum computers can never be build.
2. Even if (1) is not true large quantum computers will never be built.
3. Even if (2) is not true large the speed of large quantum computers will be such that they wi ll not be of theoretical interest.
4. Even if previous objections are not valid the speed of large quantum computers will be such that they will not be of practical inetrest.

See Aaronson (2003) for a reply to arguments of Levin, t'Hoft and Wolfram. He also tries to show that complexity theory can be a tool to shift usually ideological discussion whether we can build powerful quantum computers to a more rigorous grounds. Aaronson (2003) also 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.

page 7, before Section 1.2

10. **Are the results of quantum information processing of importance outside of computing and quantum physics?** Yes, in many ways. For example, Preskill (1999) and Childs et al. (1999) express, demonstrate and analyze well the growing feeling that the insights, paradigms, concepts, methods and results emerging from quantum information processing research are expected to have strong impacts on experimental physics and will help to understand various fundamental problems of physics and physical phenomena. Understanding and utilization of quantum entanglement is the key issue by that. On the experimental side, they analyze ways quantum information processing can help to improve information gathering capabilities of experimental physics and that the understanding of multi-particle entanglement can help to deal with one of the most difficult problems of dynamical systems — many body systems with strong quantum fluctuations. Preskill (1999) also discusses such fundamental problems at the interface between physics and informatics as re-normalization groups and holographic principle.

page 9, end of second paragraph and page 396, end of third paragraph Actually, Yao (1993) only claimed that QTM and quantum circuits are polynomially equivalent and only sketched the proof idea. It has turned out that to provide a full proof is not so easy and additional concepts are needed to state the result and to prove it fully. In details the proof has been given by Nishimura and Ozawa.

(1999). In order to do that they introduced two notions of uniformity for quantum circuits families. They explore separately Monte Carlo and Las Vegas computations. For the case of Monte Carlo computations they show the equivalence of the corresponding complexity classes. For the case of Las Vegas computations situation seems to be more complex and they explore relations between various complexity classes for QTM and uniform families of quantum circuits.

page 11, at the end of the last but one paragraph A new interesting step in this search for elementary quantum computational primitives, that could allow to extend the list of potentially useful technologies for quantum computing, seems to be the recent result, due to Gottesman and Chuang (1999), that the GHZ state (page 72), Bell basis (page 66) measurements and one qubit unitary operations are sufficient to perform any quantum computation.

page 11, before Section 1.3 A radically new idea in quantum computing, that has been getting a strong momentum recently, is that of **quantum computations with continuous variables** (Lloyd and Braunstein, 1999).

The field of quantum computation and communication develops rapidly. It develops both in depth and breadth. In additions, it becomes increasingly expected that it will have profound impact on numerous areas of science and technology. Corresponding to that broadness its name. In Europe the term *Quantum Information Processing and Communication (QIPC)* starts to be used and in USA the term *Quantum information science (QIS)* is getting momentum.

Chapter 2 — Elements

page 65, line -6 Add "The terms **qudit** and **qunit** start to be used for quantum state of an arbitrary d-dimensional Hilbert space."

page 66, before line -4

Remark There area various ways how to generalize Bell states.

- Instead of the states $|0\rangle$ and $|1\rangle$ one can take any pair of orthogonal states.
- For any two non-orthogonal states $|\psi_1\rangle$ and $|\psi_2\rangle$, w with $\langle\psi_1|\psi_2\rangle = \kappa$, Hirota and Sasaki (2001) defined and investigated the so called quasi Bell states of the form

$$|\Psi_1\rangle = h_1(|\psi_1\rangle|\psi_2\rangle + |\psi_2\rangle|\psi_1\rangle) \quad |\Psi_2\rangle = h_2(|\psi_1\rangle|\psi_2\rangle - |\psi_2\rangle|\psi_1\rangle),$$

$$|\Psi_3\rangle = h_3(|\psi_1\rangle|\psi_1\rangle + |\psi_2\rangle|\psi_2\rangle) \quad |\Psi_4\rangle = h_4(|\psi_1\rangle|\psi_1\rangle - |\psi_2\rangle|\psi_2\rangle),$$

where $h_1 = h_3 = 1 - \sqrt{2(1+\kappa^2)}$, $h_2 = h_4 = 1 - \sqrt{2(1-\kappa^2)}$

page 69, before 2.1.4

2.1.3.1 Cloning circuits

No-cloning theorem does not exclude a possibility to have quantum transformations (circuits) that can make non-perfect copies of unknown quantum states. The pioneering paper that explored this idea was due to Bužek and Hillery (1996). Since then the problem has been extensively explored both theoretically and experimentally and optimal imperfect cloners found a variety of applications. The main results have been recently very nicely motivated and summarized by Bužek and Hillery (2001).

The basic question was whether there is a quantum circuit that can make optimally imperfect copy of an arbitrary unknown qubit and whose quality of coping measured by fidelity, does not depend on the state to be copied.

Bužek and Hillery (1996) have shown that there is a very simple universal quantum cloner that can for any given qubit pure state $|\phi\rangle$ produce two new states $|\phi'\rangle$ such that the fidelity of $|\phi\rangle$ and $|\phi'\rangle$, defined by their fidelity – the inner product $|\langle\phi|\phi'\rangle|$ is 5/6. Later, Gisin and Masar (1997) have shown that 5/6 is the best fidelity that can be universally achieved. (They even showed that the existence of a better cloner would make superluminal communications possible.) Experimentally was cloning with optimal fidelity 5/6 achieved by DeMartine et al. (2000) and Huang et al. (2001).

A generalized problem to make $m > n$ copies from n copies of a qubit explored Gisin and Masar (1997). They have shown how to achieve optimal fidelity $\frac{nm+n+m}{m(n+2)}$. For $n = 1$ and $m \rightarrow \infty$ this has limit 2/3, what is the fidelity of cloning obtained by performing measurement of a given state and then copies of it.

Generalization of the above cloning problems to the case of quantum pure states of arbitrary finite dimension was done by Werner (1998). He has also shown that fidelity decreases with the dimensionality of the system.

It has been well known that one can make perfect copies of any state from a fixed set of states provided all states in that set are orthogonal. Duan and Guo (20??) dealt with the question how cloning of states can be done provided a given set of states contains non-orthogonal states. They suggested a cloner that produces perfect copies, but not always. The key question at this type of cloner is what is the probability that the output are perfect clones. For example, such a probability is $1/(1 + r)$

in the case that the set contains just two states $|\phi\rangle$ and $|\phi_1\rangle$ such that $|\langle|\phi|\phi'\rangle| = r$.

Several applications of quantum cloners have already been developed.

As shown by D'ariano et al. (2001), quantum cloners can be used to measure incompatible observable, (but not to beet the uncertainty principle).

Galvao and Hardy (200?) have shown that in quantum computing it can be more efficient to clone a given qubit and then to compute in parallel on both of them, then to perform sequentially operations on the initial qubit.

Surprisingly, the optimal cloning circuit is also the best possible universal *NOT* circuit — the one that produces optimally an almost orthogonal qubit to the given input qubit (Bužek et al. (200?)).

2.1.3.2 No-going theorems for other operations

A variety of results have been obtained showing that various other operations are impossible.

Pati and Braunstein (2000, 2000a) have shown "no-deletion principle". There is no quantum unitary operation to delete one qubit from a tensor product of identical unknown qubits. Namely to map $|\psi\rangle \otimes |\psi\rangle \rightarrow |\psi\rangle|0\rangle$ for any qubit $|\psi\rangle$. This has been then generalized for the case that also some ancilla is involved, that instead of qubits we have qudits and also to the case of $m \rightarrow n$ mappings of identical qubits or qudits. Namely $|\psi\rangle^{\otimes m} \rightarrow |\psi\rangle^{\otimes n}|0\rangle^{\otimes(m-n)}$. However, it is still an open problem how to do deletion approximately in the best way.

Pati (2001) has shown impossibility of other quantum operations: (a) to complement unknown qubit (to map $\alpha|0\rangle + \beta|1\rangle$ into $\alpha^*|1\rangle - \beta^*|0\rangle$; (b) to map $|\phi\rangle|0\rangle$ to $|\phi\rangle|f(\phi)\rangle$; (c) to map an unknown qubit $|\phi\rangle$ to a superposition of $|\psi\rangle$ and its complement – a sort of Hadamard transformation.

page 72, line +18 Add:

Remark An implementation of a pseudo-pure[1] GHZ state has already been reported (by ....) as well as an implementation of pseudo-pure 7-qubit cat state (by ....).

[1] See page 88

page 72, after Example 2.1.38 Design of an arbitrary superposition of 2^n basis states is a different and much more complex problem. Using classical methods $\Omega(2^n)$ steps are needed in the worst case. Quantumly, this can be done, as shown by Grover (1999), in $\mathcal{O}(\sqrt{2^n})$ steps.

page 75, after Exercise 2.2.4

Remark Experimentally perhaps more advanced is creation of entangled states $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and $\frac{1}{\sqrt{2}}(|0000\rangle + |1111\rangle)$ reported by Kielpinski et al. (2001). They have been able to produce such entangled states deterministically, in each shot of the experiment.

page 81, after Section 2.2.3 2.4 Distinguishibility of quantum states using LOCC

Of interest and importance is to determine which quantum states or sets of states of bipartite or multipartite states are distinguishible with LOCC.

Intuitively, it seems that once parties cannot communicate quantum information their capability to distinguish entangled states diminishes, but that they should not have problems to distinguish product states.

Recently several methods have been developed how to check distinguishibility of quantum states using LOCC (Terhal et al. (2000), Ghosh et al (2001). Their basic idea is to use the fact that LOCC cannot increase entanglement and to show that would a certain set of states be distinguishable we would have increase of entanglement using LOCC – what is not possible. The most powerful one seems to be the one developed by Horodecki et al. (2002). We present bellow the very basic idea of that method.

There have been various surprising results concerning the problem of distinguishibility oq quantum states by LOCC. Bennett et al. (1998?) have shown that there is a set of pureproduct states that cannot be distinguished with certainty by LOCC. Walgate et al. (2000) have shown that any two orthogonal states can be distinuished by LOCC.

One of the problems behind is that LOCC are not enough to perform all von Neumann measuremnt. Indeed, by performing Bell state measuremnt of any product state results in a Bell states. One of the ideas behind methods that have been developed is to apply measuremnt to some larger systems. ' Method of Horodecki et al. (2002) consists of two steps:

- Given states $\{\psi_i^{AB}\}_{i=1}^k$ to be distinguished, choose k "detector" states ϕ_i^{CD} and probabilities p_i with $\sum_{i=1}^k p_i = 1$.
- Apply the Jonathan-Plenio criterion[2] to check whether the state

$$\psi_{ABCD} = \sum_i \sqrt{p_i} |\psi_i^{AB} |\phi_i^{CD}\rangle$$

to $\{p_i, \phi_i^{CD}$ is possible by LOCC (in AC:BD-cut).

Using this method Horodecki et al. showed that

Let $\{\psi_i^{AB}\}$ be a full orthogonal basis of an $m \oplus n$ quantum system. Then (1) If at least one of the states is entangled, then the set cannot be perfectly distinguishable by LOCC; (2) The set cannot be probabilistically distinguised iff all states are separable.

page 95, after line +5 It can be shown that if XOR gate and all one-qubit gates are available, then any n-qubit unitary operation can be simulated by a circuit with $\mathcal{O}(4^n n)$ such gates (Barenco et al., 1995).

Another interesting sets of universal quantum computational primitives: (a) Hadamard gate, XOR gate and controlled-$\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$ gate; (b) (Boykin et al. 1999), Hadamard gate, XOR gate and the gate $T = \begin{pmatrix} 1 & 0 \\ 0 & e^{\pi i/4} \end{pmatrix}$; (c) (Gottesman and Chuang, 1999) the GHZ state, Bell basis measurement and one-qubit unitary gates; (d) Hadamard gate, XOR gate, phase gate and Toffoli gate; (d) square root of the SWAP operation and all one qubit operations.

Bowden et al. (2000) have shown that Hadamard gate and conditional shift gates form also a universal set of gates.

Another important question is how many gates are necessary to approximate quantum circuits using gates from a finite set of universal gates.

A well known is the result that each unitary operation on n qubits can be realized by a circuit with $\mathcal{O}(n^2 4^n)$ Xor and single qubits gates.

[2] This criterion provides a necessary and sufficient condition to transform a pure state $|\phi\rangle$ to an ensamble $\{p_i, \phi_i\}$.

As discussed above any single qubit gate can be approximated with arbitrary precision using gates from the set: XOR, Hadamard and T gate. The question is know how many such gates are needed to perform approximation with precision ε. The first result along these lines was due to Lloyd and said that in order to approximate an m gate quantum circuit (consisting from above gates) $\Omega(m2^{m\varepsilon})$ gates are required. This has been improved by Solovay and Kitaev to say that $\mathcal{O}(m\lg^c(m\varepsilon))$ gates are needed, where c is a constant between 3 and 4.

It can be easily shown that lower bound is $\Omega(\lg(m\varepsilon)$. Recently, cbound) Harrow et al. (2001) have shown that this lower bound is reachable and that this is actually true for any set of universal gates. (The proof is quite involved. The starting point is development of a matrix of how circuits with gates from a finite set of gates approximate any unitary matrix of dimension n (in $SU(n)$). For that purpose the Hilbert space $L_2(SU(n))$ is considered with norm defined by inner product $\langle\Psi|\phi\rangle = \int \psi^*(g)\phi(g)dg$, where integration is with respect to the Haar measure.) This way an important problem in the area of compilation of quantum circuits has been principally solved.

It is also of large importance to look for a set of basic physical operations that are sufficient to implement all quantum computations.

For example, Knill et al. (2000) have shown that quantum computation can be done using only single photon sources, passive linear optics elements, photon-detectors and feedbacks from detectors to the optical elements. This results shows that linear optics is a feasible alternative for performing a variety of quantum computation (and communication) tasks.

2 rebit gate that is universal for quantum computation

Rudolph and Grover (2002) have shown that each gate of the form

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \cos\phi & -\sin\phi \\ 0 & 0 & \sin\phi & \cos\phi \end{pmatrix}$$

where ϕ is some irrational multiple of π is universal for quantum computation (even if it is, clearly not sufficient to perform arbitrary unitary computation). (This result makes use of the well known fact from quantum complexity theory, see Theorem 4.2.17 in the book, that each quantum computation can be performed using only unitary matrices with real components.

Universality of entangling gates

A necessary and sufficent condition for a gate to be 1-universal, that is to form with one-qubit gates a universal set of gates, was show, by Brylinski and Brylinski (2001). An elementary proof for two qubit gates has been given by Bremner et al. (2002). The main result says that a two-qubit gate is 1-universal if and only if it is imprimitive or, equivalently, if it is entangling.

A gate is called primitive if it is a product of one-qubit gates or it is equivalent to the SWAP gate. (Two two-qubit gates U and V are called equivalent if there are unitary one-qubit gates A_1, A_2, B_1, B_2 such that $U = (A_1 \otimes B_1)V(A_2 \otimes B_2)$.) A two qubit gate is **entangling** if it can create entangled state when applied to a separable state.

Having any entangled gate U a natural question to explore is how many such gates are needed (together with one-qubit gates) to implement XOR gate.

A lower bound was shown by Hammerer et al. (2002). If U is expressed in the form

$$U = (A_1 \otimes B_1)e^{i(\theta_x\sigma_x\otimes\sigma_x+\theta_y\sigma_y\otimes\sigma_y+\theta_z\sigma_z\otimes\sigma_z)}(A_2 \otimes B_2)$$

then U needs to be use at least $\frac{\pi}{4\theta_{max}}$, where $\theta_{max} = \max\{|\theta_x|, |\theta_y|, |\theta_z|\}$.

Computational power of projective measurements – Nielsen-Leung approach

Nielsen (2001) has shown that universal quantum computation can be performed using preparation of the state $|0\rangle$, quantum memory, and projective (nondemolition) measurements (of at most 4 qubits). Fenner and Zhuang (2001) improved the result by showing that 3-qubit measurements are sufficient. The final result has been due to Leung(2001). She showed that actually 2-qubit measurements are sufficient. (However, these techniques allow to get result only with certain well understood probability.)

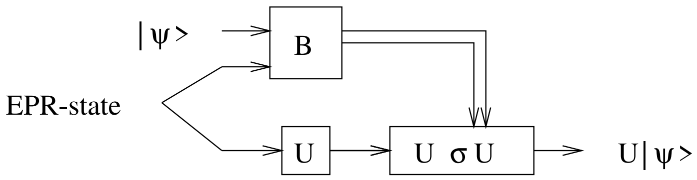

Figure 1: Generalized quantum teleportation – Alice performs not only Bell measurement B on unknown qubit and on one particle of the EPR state, but also Bob applies a unitary operation U the second particle of the EPR state. Depending on the result of the measurement some correction operation $U\sigma_j U^*$ may be needed

First basic idea in behind is that quantum teleportation is also a technique for gate construction. Indeed, a generalization of quantum teleportation shown in Figure 1 shows a way to apply a one-qubit unitary transformation to an arbitrary qubit.

To perform a 1-qubit gate U, it is therefore to prepare state $(I \otimes U)|\Phi^+\rangle$, to perform Bell measurement and, sometimes, to apply a correction $U\sigma_j U^*$.

In a similar way two-qubit gates can be performed by teleportation-like circuits.

Actually, Nielsen has shown that universality can be achieved using only 2-qubit measurements and the ancilla

$$|a\rangle = \frac{1}{2}(|0000\rangle + |0101\rangle + |1011\rangle + |1110\rangle).$$

Actually, contributions of Fenner and Zhang (2001) is mainly due to the fact that the state $|a\rangle$ can be prepared using only 3-qubit measurements. Finally, Leung (2001) has shown that to prepare $|a\rangle$ can be prepared using only 2 qubit measurements.

Universality of quantum measurement – one-way quantum computers

The concept of one-way quantum computation, QC_c, has been introduced by Raussendorf and Briegel (2001). They showed that any quantum circuit can be simulated by performing a sequence of one-qubit projective measurements on a universal quantum entangled state called *substrate*.

In this way, through one-qubit measurements, information is written into the cluster, processed and read out.

It has been shown by Raussendorf and Briegel (2001), that cluster states can be created efficiently in any system with Ising-type interactions (at very low temperature) between two states in a lattice configuration. ("To create a cluster state, its qubits are first prepared in the state $|0'\rangle$ and then brought into a cluster state by switching on the Ising-type interaction for an appropriately chosen finite time span.")

No non-local operations are needed in the process of quantum computation. The term "one-way" is used to capture the fact that each substrate can be used only once, because the entanglement used in the substrate is destroyed in the process of computation.

It is quite surprising that using QC_c information processing is possible even though results of all measurements in any direction of Bloch sphere are completely random. This is due to the fact that reduced density matrices of all qubits is matrix of the random qubit.

Quite surprisingly, as shown by Raussendorf et al. (2001), computation on one-way quantum computer QC_c, cannot be always simulated by the usual quantum circuits. For example, they showed that unitary gates from the so-called Clifford group of transformations (generated by XOR-gate, Hadamard-gate and $\pi/2$ phase shift) can be performed on QC_c in a single step, seems not to be possible in case of usual quantum circuits (all known usual circuits have logical depth in the number of qubits). Secondly, bit-reversal gate can be implemented using QC_c, but not by usual quantum circuit.

page 99, at the end There are various ways how to justify that superoperators, or completely positive maps, are the proper way quantum dynamics on mixed states (density matrices) is described.

One such justification is due to Simon at al. (2001). They derive such a conclusion from the following assumptions:

- Physical states are represented by rays in a Hilbert space;
- Probabilities for measurement outcomes at any given time are calculated according to the usual trace rule (see the Appendix);
- No-signaling condition holds - namely quantum entanglement cannot be used to create faster-than-life communication between two space separated parties.

Their reasoning also constrains possible non-linear modifications of quantum physics.

page 100

2.3.6 Self-testing of quantum (superoperator) gates

Programs and gates checking and testing is one of the key practical problem (also) in (classical) computing. The novel idea of interactive program checking, self-testing and self-correcting, introduced by Blum, Luby and Rubinfeld (1993) has turned out theoretically inspiring and practically interesting. The basic ideas and methods of interactive self-testing of quantum superoperator gates have been introduced by van Dam et al. (1999).

In the following term the *gate* will be used for *superoperator gates.*

A *self-tester* is understood to be a semi-classical procedure $\mathcal{T}_{\mathcal{F}}$ that can answer the question "$\mathcal{G} \in \mathcal{F}$" for a fixed family of unitary gates $\mathcal{F}$ and an arbitrary gate $\mathcal{G}$. More exactly, $\mathcal{T}_{\mathcal{F}}$ is a randomized algorithm that can use the gate $\mathcal{G}$, but only as a black box iterated a given number of times on the standard basis states $|x\rangle, x \in \{0,1\}^n$ (and therefore actually only on "classical (input) states"),and, finally, gets the standard basis measurements results of such iterations. For $0 \leq \delta_1 \leq \delta_2$, such a procedure is said to be a (δ_1, δ_2)-tester for $\mathcal{F}$ if for every gate $\mathcal{G}$ of the distance at most δ_1 (in some norm) from $\mathcal{F}$, it accepts with high probability, and whenever the same distance is greater than δ_2, it rejects with high probability. It is said that a family $\mathcal{F}$ of quantum gates is *testable* if for every $\delta_2 > 0$ there exists $0 < \delta_1 \leq \delta_2$ such that there exists a (δ_1, δ_2)-tester for $\mathcal{F}$.

van Dam et al. (1999) developed basics of a theory of self-testing of quantum gates and also showed that self-testable is the universal set of gates consisting of XOR and Hadamard gate and the phase rotation gate $R_{\frac{\pi}{4}}$ (of angle $\frac{\pi}{4}$).

In the classical case self-testing programs are being developed for particular programs or gates. In the quantum case self-testers are possible only for families of gates that can be characterized by robust properties. (A property is robust if whenever a function satisfies the property approximately, then it is close to a function that satisfies it exactly.) The main reason being that in some cases different quantum gates are not physically distinguishable.

The key concept of self-testers are so-called *experimental equations.* They correspond to the properties of gates that a self-tester can approximately test.

Technically, the results are obtained using special representation of states (density matrices) in Bloch Ball and of gates as affine transformation in the three-dimensional real space.

2.3.7 Quantum networks compiler

The basic design task concerning quantum networks is the following one: Given an unitary matrix U and a set $\mathcal{G}$ (not necessarily finite) of quantum gates, design an (optimal) quantum circuit with gates from $\mathcal{G}$ to realize U.

One method to realize such (not necessarily optimal) design for the case that the set of computational primitives consists of the XOR gate and one-qubit rotations developed Tucci (1999).

The basic idea is simple, though far from trivial: To design a quantum network using divide et conquer method based on the so-called CSD (cosine-sine decomposition) Theorem. This theorem says that any unitary matrix U of an even degree n can be effectively decomposed as follows

$$U = \begin{pmatrix} L_0 & \mathbf{O} \\ \mathbf{0} & L_1 \end{pmatrix} D \begin{pmatrix} R_0 & \mathbf{0} \\ \mathbf{0} & R_1 \end{pmatrix},$$

where L_0, L_1, R_0, R_1 are unitary matrices of degree $\frac{n}{2}$ and

$$D = \begin{pmatrix} D_{00} & D_{01} \\ D_{10} & D_{11} \end{pmatrix},$$

where $D_{00} = D_{11} = diag(\cos\theta_1, \ldots, \cos\theta_{\frac{n}{2}})$, $-D_{10} = D_{01} = diag(\sin\theta_1, \ldots, \sin\theta_{\frac{n}{2}})$, and $0 \leq \theta_1 \leq \theta_2 \leq \ldots \leq \theta_{\frac{n}{2}} \leq 90$.

Let us call *d-matrix* the matrix D and matrices D_{ij} and let us call by *central matrix* either: (a) a single d-matrix; (b) a direct sum of d-matrices; (c) a unitary matrix.

A recursive application of the CD-decomposition can be seen as creating a binary tree at the nodes of which are central matrices and that of the root is labeled by the matrix D. The unitary matrix U is in this way decomposed into a product of central matrices. Tucci (1999) then shows a way how to realize central matrices with the XOR matrix and rotation matrices.

As reported by Tucci (1999) a publicly available software exists to perform the above decomposition.

2.3.8 Universal quantum circuits to perform optimally various nonuniform operations on quantum states

Very extensive research has recently been performed to explore "best ways" to perform "universally" quantumly various basic non-quantum manipulations on quantum states. For example the following operations on qubit states $|\psi_1\rangle, \ldots, |\psi_n\rangle$:

- $O(|\psi\rangle) = |\psi\rangle|\psi\rangle$ - copying
- creating $n > m$ copies of a given unknown qubit state $|\psi\rangle$ out of m copies of $|\psi\rangle$
- $O(|\psi\rangle) = |\psi^\perp\rangle$ - creating an orthogonal state
- $O(|\psi\rangle, |\phi\rangle) = |\psi\rangle|\phi\rangle + |\phi\rangle|\psi\rangle$

The goal is to discover for each such an operation a circuit that performs a given operation with the same (and optimal) fidelity for all input states. Surprisingly, such universal and optimal circuits do exists for a various operations.

For example (see Werner (1999)) for each $n < m$ and dimension d, there is a circuit to design m copies of an unknown d-dimensional quantum state $|\psi\rangle$ from n copies of $|\psi\rangle$ with fidelity $\frac{m-n+n(m+d)}{m(n+d)}$.

Realization of operations $O_{k,l}$, $0 \leq k \leq \pi$, $0 \leq l \leq 2\pi$, defined by $O_{k,l}(\cos(\theta/2)|0\rangle + e^{-i\phi}\sin(\theta/2)|1\rangle) = \cos((\theta - k))/2|0\rangle + e^{i(\theta-l)}\sin((\theta - k)/2|1\rangle$, representing large class of qubit operations, has been explored by Hardy and Song (2000). They showed that for $0 \leq k \leq \pi/2$ the optimal universal circuit works with fidelity $1/2$ and for $\pi/2 \leq k \leq \pi$ the fidelity varies monotonically from $1/2$ to $2/3$ — the fidelity of measurement.

2.3.9 Generalized XOR gate

There have been several attempts to generalize XOR gate for tensor product of more-, say d-dimensional quantum systems.

The most appealing seems to be generalization suggested by Albert et al. (2001). Namely,

$$GXOR((|i\rangle, |j\rangle) = |i\rangle|i \ominus j\rangle,$$

where $\ominus$ denotes the difference $i - j \bmod d$.

GXOR operation defined this way is unitary and Hermitian and it holds that $i \ominus j = 0$ iff $i = kj$ as for XOR operation.

Additional properties of GXOR still need to be explored.

Albert et al. (2001) suggest a possible implementation using nonlinear optical elements.

2.3.10 Special circuits

A variety of quantum circuits (called often quantum machines) have been recently designed for various tasks. Let us discuss some of them.

0.0.1 Quantum homogenization

Ziman et al. (2001) designed a (universal) quantum circuit with $n+1$ inputs such that if the first qubit is in an unknown state ρ and all other qubits are in an arbitrary state ϕ, then at the end all qubits are in an arbitrarily small neighborhood of the state ϕ. Actually, the circuit realizes a transformation that has ϕ as a fix point. In this way the circuit realizes a homogenization of the state ρ. The circuit is simple, it realizes the so-called partial swap operation of the qubit ρ with other qubits. It is the operation

$$\cos\theta\mathbf{I} + i\sin\theta SWAP.$$

During the homogenization process the original information in ρ is "stored" in the entanglement between the other qubits.

2.3.11 Demonstrating quantum effects at the level of macroscopic effects

Demonstration of quantum superposition and entanglement at the level of microscopic level has been an important outcome of science. They have also gave rise to an important question why we do not see quantum effects on the macroscopic objects if the whole world should be quantum mechanical.

Realization that Quantum Information Technology is to and has to emerge and the accompanying needs to make robust implementation of quantum memory, quantum operations and quantum transmissions, raised again the question whether quantum effects cannot be demonstrated also on macroscopic objects. To show when and to what extend is the case is currently one of the main challenges for experimentalist and also for theorists. There have been recently important successes along these lines.

In Zeilinger's group, see Brezger et al. (2002) interference, that is quantum superposition, has been demonstrated for large molecules (for C_{70} fullerene molecules). An important question is with how large molecules interference can be demonstrated. So far, it seems that there is no bound on that.

In Polick's group, see Julsgaard (2000), entanglement of two macroscopic objects consisting of about 10^{12} atoms. Entangled states of macroscopic objects are, of course, much more difficult to realize, but they of key importance for storage and transmission of quantum information.

Chapter 3 — Algorithms

page 109, end of Section 3.1.2 A solution of the Deutsch-Jozsa problem for $n = 4$ on a 5-qubit NMR computer (using a molecule with 5 spin-active nuclei) has been reported by Marx et al. (1999). They also report a possibility to use their technology to solve the Deutsch-Jozsa problem for $n = 5$ on a 5-qubit NMR computer.

Exercise(Arvind and Mukunda, 2000) Let $f : \{0,1\}^2 \rightarrow \{0,1\}$. f is called **even** (**odd**) if the number of 1's in the multiset $\{f(x,y) \,|\, x,y \in \{0,1\}\}$ is even (odd). Clearly, if f is given as a black-box, then each classical algorithm to determine whether f is even or odd requires 4 calls of f. (a) Construct a quantum algorithm that can determine whether f is even or odd using only two calls to a quantum box for f; (b) Show that such a quantum algorithm works with entangled states. (Observe that Deutsch-Jozsa and Grover algorithms for $n = 2$ do not use entangled states.)

page 118, add to line -11 (Another approximation for Quantum Fourier transform has been derived by Halles and Hallgren (2000). Namely, they have shown that there is a quantum algorithm which ε-approximates the Quantum Fourier Transform over $\mathbf{Z}_p$ for an arbitrary n-bit p and any $\varepsilon > 0$ and which runs in time $\mathcal{O}(n \lg \frac{n}{\varepsilon} + \lg^2 \frac{1}{n})$.

page 118, before Exercise 3.2.17 The above estimation $\mathcal{O}(n^2)$ for time needed to perform QFT is a key observation behind the conclusion that Shor's algorithm presented in section 3.2.3 is polynomial. However, the possibility of implementing the circuit from Figure 3.3 in polynomial time has been questioned by Saito et al. (2000), at least for BSR and SRT technologies (see page 88 of these updatings). Their key argument is that at these technologies time needed to perform phase shifts by $e^{\frac{2\pi i}{2^j}}$ using gates $X_j, j = 0, \ldots, n-1$, depends on how large shifts are. In the case shifts with $j = 0$ are considered as taking a time unit, the overall implementation time $\mathcal{O}(n^2)$ considered in the text is correct. However, they claim, if shifts with $j = n-1$ are taken as requiring one time unit, then the overall time is $\mathcal{O}(n2^n)$.

A new better upper bound $\mathcal{O}(n(\lg n)^2 \lg\lg n)$ for depth (time) of quantum circuits to compute QFT_{2^n} has been shown by Cleve and Watrous (2000).

page 119, add to line +2 New upper bound $\mathcal{O}(\lg n + \lg\lg(\frac{1}{\varepsilon}))$ on circuit depth (time) complexity to compute approximately QFT_{2^n} with error bound ε (and therefore even for exponentially small error there is a circuit of depth $\mathcal{O}(\lg n)$) — the best previous upper bound was $\mathcal{O}(n)$. In addition, they have shown a new lower bound $\Omega(\lg n)$ on the depth complexity of approximation of QFT_{2^n}.

page 123, after line +5 A significant improvement in depth complexity of QFT circuits obtained by Cleve and Watrous (2000) allows to decrease significantly quantum computation time for Shor's algorithm to $\mathcal{O}(m)$.

Remark Beaudrap et al. (2000) define quantum Fourier transforms also for finite fields and for finite rings. They also show that such a QFT can be implemented efficiently over finite fields and on rings of matrices over finite fields. The first of these results allowed to obtain so far the strongest separation between quantum and classical query complexity — see page 0.0.2.

page 124, at the end of Section 3.2.3

Shor's algorithm that had such an enormous influence on the development and recognition of quantum information theory assumes that the initial state is a pure state. Since the design of an initial pure state is a hard to overcome problem for some key current quantum processing technologies, for example for NMR technology, it is of a fundamental importance to explore how crucial is this requirement to have pure initial states for the existence of quantum factorization method that is essentially more efficient than classical factorization methods. This problem has been explored by Parker and Plenio (2000) for a special model of quantum computing (that is to be motivated by NMR computing, but there is some controversy about this model). They showed that there is an efficient quantum factorization method that assumes to have as the initial state only one qubit in a pure state and, to factorize a number n, $\lg n$ qubits in an arbitrary mixed state.

0.0.2 Lower bounds for query complexity of generalized order-finding problem

No nontrivial lower bound is known for classical algorithms for the order-finding problem that is the heart of Shor's approach to quantum factorization. However, Cleve (1999a) has shown an exponential lower bound for query complexity of probabilistic algorithms to solve generalized black-box version of the problem defined as follows.

Let π be a permutation on $\{0, 1, \ldots, 2^n - 1\}$. The *order* of any $y \in \{0, 1, \ldots, 2^{n-1}\}$ with respect to π, notation $ord_\pi(y)$, is defined as the smallest r such that $\pi^r(y) = y$.

For a given $m > n$ let us define

$$f : \{0, 1, \ldots, 2^m-1\}\times\{0, 1, \ldots, 2^n-1\} \rightarrow \{0, 1, \ldots, 2^m-1\}\times\{0, 1, \ldots, 2^n-1\}$$

as

$$f(x, y) = (x, \pi^x(y)).$$

(Observe that such an f can be seen as a permutation on $\{0, 1\}^{m+n}$.)

The **order finding problem** is now defined as follows: Given f as a black-box function and $y_0 \in \{0, 1, \ldots, 2^n - 1\}$ determine $ord_\pi(y_0)$. Number of queries is the measure of complexity of order-finding algorithms.

Cleve (1999) has shown that any classical deterministic (randomized) algorithm to solve the order-finding problem requires $\Omega(\sqrt{\frac{2^n}{m}})$ $(\Omega(\frac{2^{n/3}}{\sqrt{m}}))$ queries.

Although this result cannot be applied to the order-finding problem that is the key subproblem of Shor's factorization algorithm, it provides quite a significant indication that Shor's order finding problem is indeed computationally very hard.

Shor's algorithm is based on efficient quantum solution of the following **modular order-finding problem**. In that problem an n-bit integer N is given as well as $0 < a < N$ such that $gcd(a, N) = 1$. The goal is to find the smallest $r > 0$ such that $a^r \bmod N$. This is equivalent to the order finding problem with $y_0 = 1$ and

$$\pi(y) = \begin{cases} (ay) \bmod N & \text{if } 0 \leq y < N \\ y & \text{if } N \leq y < 2^n \end{cases}$$

page 127, before Section 3.3

3.2.6 Beyond Hidden subgroup problems?

Polynomial-time quantum (Monte Carlo) algorithms for group (also nonabelian) problems that are not known to be special cases of Hidden subgroup problem and for which no polynomial time classical algorithms exist have been presented by Watrous (2000). This way a new types of problems seems to be discovered for which quantum algorithms seem to be exponentially more powerful than classical ones.

Watrous (2000) considers solvable groups[3] and the following problems: (a) computing the order of a solvable group; (b) testing membership in a solvable group; (c) testing isomorphism of solvable groups.

The polynomial time algorithm to determine the order of a group produces a quantum state that approximates equally weighted superposition of all basis states $|G\rangle = \frac{1}{\sqrt{|G|}} \sum_{g\in G} |g\rangle$. This allows to apply the existing quantum algorithms for Abelian groups also to factor groups of solvable groups.

The results were shown for **black-box groups**. Their elements are supposed to be represented by strings of length n and group operations

[3]Solvable groups are defined as follows: For a group G and its elements g, h the commutator $[g, h]$ of g, h is defined by $[g, h] = g^{-1}h^{-1}gh$ and for two subgroups H, K of G we write $[H, K]$ to denote the subgroup of G generated by all commutators for any $h \in H$, $k \in K$. The derived subgroup of G is $G' = [G, G]$, and, in general, we write $G^{(0)} = G$, $G^{(1)} = G', \ldots, G^{(j)} = (G^{(j-1)})'$. A group is solvable if $G^{(m)} = \{1\}$, for some integer m.

are performed by a black-box at unit cost. (To each such group G unitary operations U_G and U_G^{-1} on $2n$ qubits are assumed such that $U_G|h\rangle|h\rangle = |g\rangle|gh\rangle$ and $U_G^{-1}|g\rangle|h\rangle = |g\rangle|g^{-1}h\rangle$.)

The paper by van Dam and Hallgren (2000) represents another attempt to get beyond the Hidden subgroup problem. It shows polynomial time algorithms for several versions of the so called *Shifted quadratic character problems* that do not seem to be special cases of the Hidden subgroup problem and for which no classical complexity is known.

In order to present the list of such problems some notation is needed. For a prime p the Legendre symbol is denoted $(x|p)$ and for an integer n the Jacobi (Legendre-Jacobi) symbol is denoted by $(x|n)$. For a finite field $\mathbf{F}_q$ and $x \in \mathbf{F}_q$ the *quadratic character* $\chi(x)$ is 1 if x is quadratic residue, -1 if x is not a quadratic residue, and 0 if $x = 0$.

- **Shifted Legendre Symbol Problem.** Given a prime $p > 2$ and a function$f_s : \mathbf{F}_p \rightarrow \{-1, 0, 1\}$ such that $f_s(x) = (x + s|p)$ for some $s \in \mathbf{F}_p$. Find s.
- **Shifted Jacobi Symbol Problem.** Given a square-free odd integer n and a function $f_s : \mathbf{Z}_n \rightarrow \{-1, 0, 1\}$ such that $f_s(x) = (x+s|p)$ for some $s \in \mathbf{F}_p$. Find $s \in \mathbf{Z}_n$.
- **Shifted Jacobi Symbol Problem – unknown n.** Given an integer m and a function $f_s : \mathbf{Z}_m \rightarrow \{-1, 0, 1\}$ such that $f_s(x) = (x + s|n)$ for some odd square-free n with $n^2 < m$. Find s and n.
- **Shifted Quadratic Character Problem**. Given $q = p^r$, where $p > 2$ is a prime and a function $f : \mathbf{F}_q \rightarrow \{-1, 0, 1\}$ such that $f(x) = \chi(x + s)$ for some $s \in \mathbf{F}_q$. Find s. Here χ is the quadratic character of $\mathbf{F}_q$.

There are two new features of these algorithms. While at the Hidden subgroup problem the Quantum Fourier transform provides sufficient distribution to solve the problem, this is not the case for problems presented above. In addition, in order to solve Hidden subgroup problems, Quantum Fourier transform defined in terms of groups is used, but to solve the above mentioned problems algorithms use transforms that depend on the fact that there is an underlying field (which support addition and multiplication).

Polynomial time solution of Pell equation

New interesting breakthrough in finding fast quantum algorithm has been due to Hallgren (2001). He has derived polynomial time algorithm to solve so called *Pell equation* $x^2 - dy^2 = 1$, where d is an non-square integer. No classical polynomial time algorithm to find, given d, x and y such that $x^2 - dy^2 = 1$ has been known. (Already Lagrange (1768) has shown that for each d there are infinitely many solutions.) Buchman-Williams cryptosystem is based on working with numbers of the type $a + \sqrt{c}b$ and Hallgren polynomial quantum algorithm allows to break this cryptosystem. Hallgre has dveloped a clever way to sole the problem even one cannot say that some principially new technique has been used.

page 130, add at the very end Recently, as presented at Torino Workshop on quantum computing, June 20. 2001, Grover (co-authored by M. Sengupta) has shown a classical analogue of his quantum search bringing again a square root speed up. The problem is to identify one short pendulum among n pendulums in $\sqrt{n}$ time. In addition they have show how to estimate an ε-fraction of short pendulums in $\frac{1}{\sqrt{\varepsilon}}$ cycles. The results obtained bring new insights into the phenomena allowing square root speed-ups. (Actually, as pointed out by A. Ambainis, another classical analogue of Grover's algorithm has been found by S. Lloyd (1999).)

page 134, line +13 Add: "The last result is true only for the case that number of solutions is not known. Otherwise, as shown by Brassard et al. (2000), zero error probability can be obtained with $\theta(\sqrt{n})$ queries.

page 134, line -14 Add: "If such an algorithm is used as subroutine for Insertion sort, then one can show that quantum sorting can be done using $0.53n \lg n + \mathcal{O}(n)$ comparisons. A lower bound of $\frac{n}{2\pi}(\ln n1) \approx 0.11n \lg n - 0.067n + \mathcal{O}(1)$ comparisons for quantum sorting has been shown by Shi (2000), see also Hoyer et al. (2001). Another upper bound, $0.631 \lg n$ for quantum searching, but using a different methods, was shown by Hoyer and Neerbek (2000), see also Hoyer et. al. (2001). The algorithm is based on a novel quantum method of searching, that is faster than the classical ones, a binary tree at which several independent searches, initiated at the root, are performed. These searches traverse the tree faster than classically due a certain cooperation and they basically reach the leaf they search for in about $\lg_3 n$ steps if n is number of leaves. This highly nontrivial technique seems to be of a broader use.

A new lower bound for searching in order list is, due to Hoyer et. al. (2001) $\frac{1}{\pi}(\ln n - 1) \approx 0.220 \lg n$"

page 134, before Section 3.3.4 There have been already several experimental realization of Grover's algorithm: using NMR technology, Chuang et al. (1998a); photon interference (Kwiat et al. (1999); interferometry, Cerf et al. (1998), Ahn et al. (2000).

page 137, after Theorem 3.3.18 A way of making a repetitive use of the above counting algorithm demonstrated Carlini and Hosoya (1999). They have developed a technique how to transform classical probabilistic algorithms, á la Rabin, into unitary transformations that can be used as gates of other networks. (The problem with a naive transformation of probabilistic algorithms is that it requires repetitions in order to achieve high probability of success for the correct answer and that needs reversible measurements.) This way they showed quantum polynomial algorithms for such problems of number theory as primality testing, prime number theorem testing and testing of Hardy and Littlewood's conjecture about asymptotic number of representations of an even integer as a sum of two primes.

Grover (1999) has generalized the above search method to the case of multiple solutions — using again rotations in a 2-dimensional Hilbert space. As an application, this technique allows to create an arbitrary superposition in an n-dimensional Hilbert space in $\mathcal{O}(\sqrt{n})$ steps. As a consequence, this allows to create an arbitrary probability distribution in $\mathcal{O}(\sqrt{n})$ steps. (This is of importance for using sampling as an algorithm design technique to find approximate solutions in the case it is infeasible to find an exact solution.)

page 137, at the end The above result has been generalized and improved in several ways by Buhrman et al. (2000). In addition to several variants of the **collision finding problem** for a function $f : X \to Y$, they consider also the **claw finding problem** – given two functions $f : X \to Z$ and $g : Y \to Z$, find a pair $(x, y) \in X \times Y$ such that $f(x) = g(y)$ and **element distinctness problem** – given a function $f : X \to Y$ decide whether f maps different x to different values. For all these problems they provide quantum algorithms that are more efficient than classical ones and also non-trivial lower bounds.

As the complexity measure they consider the number of comparisons between elements. (They formalize a comparison between $f(x)$ and $f(y)$

as an application of the unitary transformation

$$|x, y, b\rangle \rightarrow |x, y, b \oplus [f(x) \leq f(y)]\rangle.)$$

For proving new and better upper bounds they make extensive use of the following version of the amplitude amplification technique due to Brassard et al. (2000).

Theorem There exists a quantum algorithm **QSearch** with the following property. Let A be any quantum algorithm that uses no measurements, and let $\chi : \mathbf{Z} \rightarrow \{0, 1\}$ be any Boolean function. Let a denote the initial success probability of $\mathcal{A}$ for finding a solution. Algorithm **QSearch** finds a solution using an expected number of $\mathcal{O}(1/\sqrt{a})$ applications of $\mathcal{A}$ and $\mathcal{A}^{-1}$ if $a > 0$, and otherwise runs forever.

Let us summarize results for the worst-case number of comparisons required to solve the problem. Q_e will denote complexity of exact quantum algorithms and Q_2 complexity for the case of bounded error algorithms. In addition, let $|X| = N$, $|Y| = M$.

- The comparison-complexity of the claw-finding problem is in general case
  - $\Omega(\sqrt{M}) \leq Q_2(\mathbf{Claw})) \leq \begin{cases} \mathcal{O}(N^{1/2}M^{1/4} \lg N) & \text{if } N \leq M \leq N^2 \\ \mathcal{O}(M^{1/2} \lg N) & \text{if } M > N^2 \end{cases};$
  - $\Omega(M) \leq Q_e(\mathbf{Claw}) \leq \mathcal{O}(M \lg N)$.
- The comparison-complexity of the claw-finding problem is in the case f is ordered
  - $\Omega(M^{1/2}) \leq Q_2(\mathbf{Claw}) \leq \mathcal{O}(M^{1/2} \lg N)$
  - $\Omega(M) \leq Q_e(\mathbf{Claw}) \leq \mathcal{O}(M \lg N)$
- The comparison-complexity of the claw-finding problem for the case that both f and g are ordered and $N = M$ has lower bound $\Omega(N^{1/2})$ and there is an algorithm to determine a claw with probability at least $\frac{2}{3}$ with only $\mathcal{O}(N^{1/2}c^{\lg^* N})$ for some constant c.
- The comparison complexity of the element distinctness problem is in general
  - $\Omega(N^{1/2} \lg N) \leq Q_2(\mathbf{ED}) \leq \mathcal{O}(N^{3/4} \lg N)$;
  - $\Omega(N) \leq Q_e(\mathbf{ED}) \leq \mathcal{O}(N \lg N)$.

  Comment The lower bound $\Omega\sqrt{N} \lg N$ is due to Hoyer et al. (2001).

Observe that in the classical case the claw-finding problem requires $\Theta(N \lg N)$ comparisons if $N = M$ and also the element distinctness problem requires $\Theta(N \lg N)$ comparisons.

In addition, they have shown that for triangle finding problem in a graph with n nodes and m edges the following results hold

- $\Omega(n) \leq Q_2(\text{Triangle}) \leq \mathcal{O}(n + \sqrt{nm})$
- $Q_e(\text{Triangle}) = \theta(n^2)$.

Finally, they showed several problems related to the element distinctness problem for which quantum algorithms cannot be more efficient than classical ones. They are **parity-collision problem** (to determine parity of the cardinality of the set $C_f = \{(x, y) \in X \times X : x < y, f(x) = f(y)\}$); **no-collision problem** (to find an element that is not involved in a collision); **no-range problem** (given $f : X \to Z$ to find $z \in Z$ such that $z \notin f(X)$).

Lower bounds for collision problem

Since 1998 one of the major problems concerning quantum lower bounds was to derive a non-trivial lower bound for the (2 to 1) collision problem (with upper bound $\mathcal{O}(n^{1/3})$).

At first Aaronson (2001) reported the lower bound $\Omega(n^{1/5})$ for bounded-error quantum query complexity and he also mentioned a better lower bound $\Omega(n^{1/4})$, not yet published, due to Yaoyun Shi. Actually, Shi (2001) has found even a better lower bound $n^{1/3}$.

Aaronson has obtained his lower bound using an adaptation and refinement of the polynomial method making use of results of classical approximation theory.

Aaronson (2001) mentions also several interesting implications of the existence of non-trivial lower bounds. The most immediate implication is that breaking cryptographic hash functions is not in **BQP** relative to an oracle. Another implication is that nonstandard quantum oracle model due to Kashefi et al. (2001), with oracle $|x\langle \rightarrow |f(x)\rangle$ (and effectively erasing x) is exponentially more powerful than the usual oracle model. Aaronson also announces implications for so called *dynamical quantum theory* to be presented in a future paper.

Importance of the collision problem is related to the fact that for building secure digital signature schemes, it is useful to have a family of hash functions $\{h_i\}$, such that finding a pair (x, y), with $x = y$ such that $h_i(x) = h_i(y)$ is computationally hard. A quantum algorithm for finding collisions in $\mathcal{O}(\lg^k n)$ queries would imply that all hash functions are insecure against quantum attack. The existence of a non-trivial lower bound for the collision problem implies that collision-free hashing may be possible also in quantum setting.

page 149, at the end

The above results have been extended by Buhrman et al. (1999) to show that $D(f) = \mathcal{O}(Q_0(f)^4)$, where $Q_0(f)$ is defined as the number of black-box calls in the best quantum network computing f with zero-error. ($Q(f)$ stands for bounded-error computation.)

In addition to the relation between $D(f)$ and $Q(f)$ for total Boolean functions, of interest is also to discover relations between $Q(f)$ and $deg(f)$. So far the following inequalities are known to be true

$$\frac{deg(f)}{2} \leq Q(f) \leq \mathcal{O}(deg(f)^4).$$

The first inequality is from Theorem 3.5.11. The second one has been contributed to Nisan and Smolensky by Buhrman and de Wolf (1999). However, no function f is known where $Q(f)$ is asymptotically larger than $deg(f)$.

Open problem (1) Is it true that $deg(f)$ and $Q(f)$ are polynomially related?; (2) What is the smallest k such that $Q(f) = \mathcal{O}(deg(f)^k)$ for all total Boolean functions f?

A linear dependence between non-deterministic quantum black-box complexity and the degree of approximation of polynomials for total Boolean functions has been shown by de Wolf (2000) in the form

$$\frac{ndeg(f)}{2} \leq NQ(f) \leq ndeg(f).$$

Here $ndeg(f)$ is the smallest degree of a polynomial p that nondeterministically approximate f in the sense that $p(x) = 0$ if and only if $f(x) = 0$ and $NQ(f)$ ($N(f)$) is nondeterministic quantum (classical) complexity of f. Moreover, by nondeterministic quantum (classical) algorithm for f a quantum (classical) algorithm $\mathcal{A}$ is understood such that $\mathcal{A}$ accepts an input x with some non-zero probability if and only if $f(x) = 1$.

As shown by de Wolf (2000), the difference between $N(f)$ and $QN(f)$ can be huge. Namely, that for any integer n there is a function $f : \{0,1\}^n \rightarrow$

$\{0,1\}$ such that $N(f) = n$ and $NQ(f) = 1$, what is the largest possible gap for that model.

Remark The investigation of the number of "oracle calls" or "black-box calls" of quantum algorithms for functions given by "black-boxes", or as oracles, is an research area of an increasing interest at which a variety of interesting results have been recently obtained that bring deep insights into the power of quantum computing. In connection with that the term **quantum query complexity** starts to be used and one now speaks more often about the number of queries than of oracle or black-box calls.

The strongest separation between quantum and classical query complexity has been shown by Beaudrap et al. (2000). They showed a problem that requires $\Omega(2^{n/2})$ queries for classical bounded error case, but can be solved exactly with a single query in the quantum case.

Average-case query complexity

As mentioned on page 149, $D(f) = \mathcal{O}(Q(f)^6)$, and therefore it is clear that in the case of black-box computations quantum algorithms cannot bring more than a polynomial speed-up with respect to deterministic algorithms. This result seemed therefore to be a strong indication of a limited power of quantum algorithms for oracle computations.

Quite surprisingly, as shown by Ambainis and de Wolf (1999), the above limitations of quantum black-box algorithms for computation of total Boolean functions holds only in the case of the worst-case complexity. The situation is very different if the average-case query complexity is considered.

Let us denote $D^\mu(f)$, $R^\mu(f)$, and $Q^\mu(f)$, the average-case query complexity (defined in an analogous way as for $D(f)$, $R(f)$, and $Q(f)$, respectively). Main results of Ambainis and de Wolf (1999) can be summarized as follows.

1. If μ is a uniform distribution, then both $Q^\mu(f)$ and $R^\mu(f)$ can be exponentially smaller than $D^\mu(f)$ and $Q^\mu(f)$ can be exponentially smaller than $R^\mu(f)$ for some functions f.
2. There is a function f (namely, the OR function) and a non-uniform distribution μ such that the difference between $Q^\mu(f)$ and $R^\mu(f)$ is larger than exponential (namely $Q^\mu(OR) = \mathcal{O}(1)$ and $R^\mu(OR)$ is about $\sqrt{n}$).

In the case of the parity function PARITY, see Section 3.5.1, which is one of the hardest to compute Boolean functions, even in the case of the average-case complexity with respect to the uniform distribution μ, no essential speed-up is possible — $Q^\mu(\text{PARITY}) = \Omega(n)$. Situation is not much better neither in the case of non-uniform distributions. By Ambainis and de Wolf (1999), the gap between $Q^\mu(\text{PARITY})$ and $R^\mu(\text{PARITY})$ can be quadratic, but not more.

3.5.4 Ambainis' quantum adversary lower bound method

This method, see Ambainis (2000), is a modification of *classical adversary method*. This method starts with running the algorithm on one input. Then the input is modified so that the behavior of algorithm does not change much but the correct answer changes. Consequently, the problem cannot be solved with a small number of queries.

On the other hand, **quantum adversary (Ambainis) method** starts with running the algorithm with a superposition of some inputs. Its initial (final) state has to have no (maximal) entanglement. An upper bound on the increase of entanglement by one query is shown; that bounds the total number of queries.

Ambainis (2000) used this method to show $\Omega(\sqrt{N})$ lower bound for computing AND and OR functions and for inverting permutations.

Let us now present the basics of the quantum adversary method. To do that we use the same model for black-box or query computations as in Section 3.5.2.

Let us start first with a definition.

Definition A quantum algorithm computes f **with bound error** if, for every $(x_0, \ldots, x_{N-1}$, the probability that rightmost bit of $U_T O_x U_{T-1} \ldots O_x U_0 |0\rangle$ equals $f(x_0, \ldots, x_{N-1})$ is at least $1 - \varepsilon$ for some fixed $\varepsilon < \frac{1}{2}$.

Computation will be assumed as done in bipartite Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_I$ with $\mathcal{H}_A$ standing for algorithm A Hilbert space and $\mathcal{H}_I$ is Hilbert space of inputs.

To each unitary U_i on $\mathcal{H}_A$ corresponds $U_i' = U_i \oplus I$ on $\mathcal{H}_A \otimes \mathcal{H}_I$, and O' corresponds to O_x on the subspace $\mathcal{H}_A \otimes |x\rangle$.

Let S be a set of inputs. Transformations $U'_T O' U'_{T-1} \dots U'_0$ transforms

$$|\psi_{\text{start}}\rangle = |0\rangle \otimes \sum_{x\in S} \alpha_x |x\rangle \quad \text{to} \quad |\psi_{\text{end}}\rangle = \sum_{x\in S} \alpha_x |\psi_x\rangle \otimes |x\rangle.$$

Let ρ_{start} be the density matrix corresponding to the state $\sum_{x\in S} \alpha_x |x\rangle$; with entries $(\rho_{\text{start}})_{xy} = \alpha_x^* \alpha_y$. It holds

The starting state $|\psi_{\text{start}}\rangle$ is unentangled and the final state $\Psi_{\text{end}}\rangle$ is maximally entangled.

Therefore, one can show a lower bound on the number of queries by showing that we cannot obtained maximally entangled end state $|\psi_{\text{end}}\rangle$ with less than a certain number of queries.

Technically, the basic idea of the method uses the following result.

Lemma Let A be an algorithm computing f with probability at least $1-\varepsilon$. Let x, y be such that $f(x) \neq f(y)$. Then

$$|(\rho_{\text{end}})_{xy}| \leq 2\sqrt{\varepsilon(1-\varepsilon)} |\alpha_x|\, |\alpha_y|.$$

To prove the lower bound on the number of queries, it is sufficient to bound the change in ρ_{xy} caused by one query.

3.5.5 Power of different types of oracles

Given a Boolean function $f : \{0,1\}^n \rightarrow \{0,1\}^n$, in addition to

- the **standard oracle** $S_f : |x\rangle|b\rangle \rightarrow |x\rangle|b \oplus f(x)\rangle$,

defined above, we can consider

- the **phase oracle** $P_f : |x\rangle|b\rangle \rightarrow e^{2\pi i f(x)b/2^n} |x\rangle|b\rangle$,

and, in the case f is one-to-one

- the **minimal oracle**

It is easy to show that oracles S_f and P_f are equivalent in power. On the other hand, it is not yet clear what is in general relation between the power of the standard and minimal oracle.

In the special case that not only the oracle for S_f, but also for $(S_f)^{-1}$ is available on one side and oracles for M_f and $(M_f)^{-1}$ are available on the other side, relative power of the standard and maximal oracle has been recently explored by Kashefi et al. (2001).

They have shown that to construct S_f one needs one invocation of M_f and one of $(M_f)^{-1} = M_{f^{-1}}$. On the other hand $\Theta(\sqrt{n})$ invocations of S_f and $(S_f)^{-1}$ are needed to construct M_f and, in general this is the best possible result.

The key underlying result is that $S_{f^{-1}}$ can be simulated by a quantum circuit that uses $\Theta(\sqrt{n})$ invocations of S_f and $(S_f)^{-1}$.

Grover's algorithm is to show the upper bound and Ambainis (2000) result that $\Omega(\sqrt{n})$ invocations of S_f is needed to invert in general a permutation f.

Given S_f and $S_{f^{-1}}$ we can simulate M_f as follows

$$M_f \otimes I = S_{f^{-1}} \otimes \mathrm{SWAP} \otimes S_f.$$

3.6 Quantum games

Other area where quantum tools seem to have a chance to bring a dramatical change in outcomes are (mathematical) games.

Actually, modern game theory was originally developed to the large extent also by von Neumann.

Let us now introduce some very basic concepts concerning (classical) games.

Let X and Y be nonempty sets. Mappings $p_X : X \times Y \rightarrow \mathbf{R}$ and $p_Y : X \times Y \rightarrow \mathbf{R}$ are called **payoff functions** and the quadruple (X, Y, p_X, p_Y) is called **game**. Sets X and Y are called **pure strategies** of two players. A **mixed strategy** is a probability distribution on pure strategies.

A pair of strategies $(x, y) \in X \times Y$ is said to form the **(Nash) equilibrium** of the game (X, Y, p_X, p_Y) iff $p_X(x', y) \leq p_X(x, y)$ for $\forall x' \in X$, and $p_Y(x, y') \leq p_Y(x, y)$ for $\forall y' \in Y$.

An example of the game that has two Nash equilibriums is the following so-called **Battle of sex games**.

Alice and Bob have to decide where to spent evening. Alice prefers to go to opera (O), Bob wants to watch TV (T). However, both prefer to be together than to be apart. Pay-off function is given by the matrix

$$\begin{array}{ccc} & O & T \\ O & (\alpha,\beta) & (\gamma,\gamma) \\ T & (\gamma,\gamma) & (\beta,\alpha) \end{array}$$

where $\alpha > \beta > \gamma$.

The two equilibria are (O, O) and (T, T). Players are faced with a tactics dilemma. They have to choose their tactics without knowing the tactics that will be chosen by the other player. Moreover, even the two equilibria bring them different payoffs.

Battle of sex is an example of *static games of complete information* (about potential strategies of players).

A game (X, Y, p_X, p_Y) is called a **zero-sum game** if $p_X(x, y) = -p_Y(x, y)$ for $\forall x \in X, y \in Y$.

One of the basic result of the classical game theory is that not every two-parties zero-sum game has an equilibrium in the set of pure strategies, but there is always an equilibrium if players follow mixed strategies.

A pair of strategies is said to be **Parento optimal** if deviating from these strategies it is not possible to increase the pay-off of one player without decreasing the pay-off of the other one.

Informally, in the case of quantum games players play in some compound Hilbert space, each on his component, start with some initial quantum state, and apply as their strategies some local quantum operations.

It has been shown for some zero-sum games, that if one of the players can use fully quantum tools and thereby *quantum strategies*, then he can increase his/her chance to win the game. This way from a fair game, in which both players have the same chance to win if only classical computation and communication tools are used, an unfair game can arise and from an unfair game a fair one.

In addition, it has been shown that in some cases of quantum games the dilemma that exists in the classical game does not exist in the quantum case and also that the payoffs are larger if the initial state (of the game) is more entangled — see Du et al. (2001).

In addition, a game-theory view of quantum query algorithms has been developed, see Meyer (2000), in which one player is classical and one is quantum.

Quantum games have been discussed by Meyer (1998, 2000), Goldenberg et al. (1999), Eisert et al. (1999), Eisert and Wilkens (2000), Benjamin (2000), Benjamin and Hayden (2000, 2000a), Marinato and Weber (2000) and Du et al. (2000, 2000a).

Interesting enough, in some cases, but not in all ones, entanglement is needed to make quantum strategies more powerful than classical ones.

The very basic insights into the power of quantum players (those using quantum tools and processes), have been developed by Meyer (1998) for the case of two player zero-sum games.

In Meyer's approach, moves (strategies) are quantum operations. It has been shown by Meyer (1998) that in general quantum strategies are always at least as good as classical strategies. Moreover, in case both players use quantum strategies there need not be any equilibrium, but if both players can use mixed quantum strategies, then there has to be an equilibrium.

The basic Meyer's definition of the quantum game where one player can use a quantum strategy and the other one uses the classical strategy reads as follows.

Definition A quantum two player game (with players P and Q) consists of

- Hilbert space H_n of dimension n and of the possible states of the game.
- Subsets Q_i, $i = 1, 2, \ldots$ of unitary transformations — the elements of Q_i represent possible moves of the player Q on turn i.
- Subsets P_i, $i = 1, 2, \ldots$ of the permutation group on n elements — the elements of P_i are the moves player P chooses on turn i.
- A projection operator Π on H_n — the subspace fixed by Π consists of the winning strategies of the player Q.

A **pure quantum strategy** for Q is a sequence $u_1, u_2, \ldots$ with $u_i \in Q_i$. A pure (classical) strategy for P is a sequence $s_1, s_2, \ldots$ with $s_i \in P_i$.

In order to illustrate possibilities quantum strategies bring, let us discuss some other games.

The next game, the so-called **PQ Penny Flip** game, see Meyers (1998). There are two players, P and Q. P is to place a penny head up in a box, and after that they make in the following order (Q, P, Q) the following moves: they either flip the penny or not. Q wins if the penny is head up when they open the box.

It is easy to check that using pure strategies the chances to win are $\frac{1}{2}$ for each player and there is no equilibrium in the case of pure classical strategies. However, there is equilibrium if Q chooses its strategy with probability $\frac{1}{2}$ and Q chooses each of the four possible strategies with probability $\frac{1}{4}$.

In addition, in the case Q uses a quantum strategy, it can win with probability 1. The strategy is simple. Q starts with choosing the state $|0\rangle$. P has always only two choices: either "to flip the coin" (to use mapping σ_x) or "not to flip" (to use mapping I). Q always applies Hadamard transform. It is now clear that no matter what strategies P chooses the final state will be $|0\rangle$.

There has been an attempt to show (Marinato and Weber (2000)) that for the Battle of sexes game quantum strategies lead to one Nash equilibrium, and therefore the dilemma that exists in the classical case does not exist any longer, but Benjamin (2000) has questioned their reasoning. In their approach "strategies" are states and (quantum) operations are "tactics".

In Marinato and Weber's approach the worst case payoffs occur when tactics are "mismatched". Nawaz and Toor (2001) demonstrated that this has been due to a special initial state $\frac{1}{\sqrt{2}}(|OO\rangle + |TT\rangle)$ and that if a more general initial state is chosen then the worst-case payoffs do not occur even for the case of mismatched tactics.

Another approach to the quantization of the Battle of Sexes game developed Du et al. (2001). In their approach strategies are quantum operations and any unitary operations are allowed. They showed that if both players used mixed quantum strategy, then there are still several Nash equilibria, but the possible tactics mismatch has no influence on the payoffs.

Another famous game is the so-called **Prisoners Dilemma**[4]:

Two prisoners, Alice and Bob, can use, independently, any of the following two strategies: **cooperate** or **defect (not to cooperate)**.

The problem is that the payoff function is a very special one:

[4] This game was introduced by A. W. Tucker and has since been an important example of a classical non-zero game in economics, evolutionary biology and in other areas

	C	D
C	$(3,3)$	$(0,5)$
D	$(5,0)$	$(1,1)$

What is the best way for Alice and Bob to proceed to maximize their payoffs? A rational analysis leads both players to "defect" against one-another – what is quite destructive.

A strategy s_A is called **dominant** for Alice if for any other strategy s'_A of Alice and s_B of Bob, it holds

$$P_A(s_A, s_B) \geq P_A(s'_A, s_B).$$

Clearly defection is the dominant strategy of Alice in the case of Prisoners' Dilemma game.

Prisoners Dilemma game has therefore **dominant-strategy equilibrium**, and has also unique Nash equilibrium.

Eisert and Wilkens (2000) showed that in the quantum case, if maximally entanglement states are used, there is a unique Nash equilibrium and that mutually destructive rational approach from the classical case is replaced by an effectively cooperative one that gives reward to both players. Benjamin and Hayden (2000) have questioned their approach and conclusions. Namely, due to a special restriction Eisert and Wilkins make on the strategies to be used. However, objections of Benjamin and Hayden do not seem to be valid once all comments of the published version of the paper. Moreover, they show that if all available quantum strategies are used, then there is no Nash equilibrium. Eisert and Wilkens's approach(2000) in which they use an entangled state with a parameter has been further analyzed by Du et al. (2001a), and they have shown that properties of the quantum game can much change with the variation of the entanglement parameter - a measure of game's entanglement. In addition, they experimentally realized the game using their NMR quantum computer.

Meyer (together with M. Henziker) - as reported at Torino Workshop on quantum computing, June 2001, showed that it is insightful to see search algorithms as strategies for two player games.

- Player 1 (the oracle) chooses an $a \in \{0, \ldots, n-1\}$.
- Player 2 queries: "what about x?".

- Player 1 tells player 2 the value $g_a(x)$ for some function $g_a(x)$ defined on $\{0,\ldots,n-1\}$; The goal for the Player 2 is to find a (and the goal for the Player 1 is to prevent this).

On this basis they showed that for a variety of new search problems there are one-query algorithms.

Multi-player quantum games

Multi-player quantum games can posses new forms of equilibria that have no analogue in the classical games or even in quantum two-player games (see Benjamin and Hayden (2000a), Du et al. (2001)).

This is true in the case parties share entanglement that allows them a new form of cooperation.

Indeed, entanglement can act as a contract - it can prevent players to successively betray one another.

Example – Minority Game

This is a famous game that occurs often in social systems.

Each player chooses randomly 0 or 1.

In case one of the choices is made by less players than the other one, then each of the players of the "minority group" gets a point.

In case all players make the same choice or the same number of them make each choice, none of them gets a point.

Interesting enough, in the case of 3 players no pure quantum strategy is better, however, this is not the case if there are 4 players.

In the classical case 4 players cannot do better than to toss the coin and therefore their expected payoff is 1/8.

Using quantum strategies they can obtain payoff 1/4.

In the case of 4 parties, they are expected to share the cat state $\frac{1}{\sqrt{2}}(|0000\rangle + |1111\rangle)$ and each of them performs the quantum operation

$$\frac{1}{\sqrt{2}}\cos(\frac{\pi}{16})(I + i\sigma_x) + \frac{1}{\sqrt{2}}(\sin(\frac{\pi}{16}(i\sigma_y - i\sigma_z)$$

Example - Three players Prisoners Dilemma

This is an example of the quantum game at which the dilemma that exists in the classical case does not exist any longer and at which the payoff depends on the amount of entanglement in the initial state of the game.

In the classical three players Prisoners Dilemma game there are three players A, B, C, each has two choices for strategies D (defect) or C (cooperate) with payoffs $P(D,D,D) = (1,1,1)$; $P(D,D,C) = (4,4,0)$; $P(D,C,C) = (5,2,2)$ and $P(C,C,C) = (3,3,3)$ and symmetrically for other choices of strategies. The unique Nash equilibrium is (D,D,D) with payoff $(1,1,1)$ what is Parento inferior outcome because for strategies (C,C,C) all three players have payoff 3.

Let the underlying Hilbert space is the three qubit Hilbert space and that the initial state is $J|000\rangle$, where $J = e^{i\frac{\gamma}{2}\sigma_x\otimes\sigma_x\otimes\sigma_x}$, where $0 \leq \gamma \leq \pi/2$ (γ can be seen here as a measure of entanglement). The set of strategies is the set of unitary qubit operations.

In case $\gamma = 0$ both the initial state and also states at each instance of the game are separable.

In case $\gamma \neq 0$ the triple of strategies $(i\sigma_y$,
$sihgma_y, i\sigma_y$ is a new Nash equilibrium that is Parento optimal and the payoff grows with γ, that is with respect to the amount of the game's entanglement. The payoff is $1 + 2\sin^2\gamma$. That also means that in this case dilemma that exists in the classical case is removed.

QUANTUM GAMES without ENTANGLEMENT

It is natural to ask for which type of games can quantum strategies outperform classical ones and still don't use entanglement.

A quantum algorithm for an oracle problem can be seen as a quantum strategy for a player in a two-player zero-sum game in which one player is constrained to play classically.

An example of such a problem is Bernstein and Vazirani problem: Task is to identify an $a \in \{0,\ldots,2^n-1\}$ given an oracle which responds to query x with $f_a(x) = x \cdot a \bmod 2$.

Classically, n queries are necessary to determine a. However, there is a quantum algorithm that does not use entanglement and can do that using a single (quantum) query.

Meyer (2001) has recently exhibited a variety of search problem for which more e efficient quantum algorithms exist than classical ones and they do not use entanglement.

Making unfair games fair

As demonstrated by Du et al. (2000b) a quantum strategy can, even without entanglement, make from an unfair game a fair one.

Here is a simple example of such a game.

There are three coins: one fair, with both sides different, and two unfair, one with two heads and one with two tails.

The game proceeds as follows.

- Alice puts coins in a black box and shakes it.
- Bob picks up one coin.
- Alice wins if coin is unfair, otherwise Bob wins

Clearly, in the classical case, the probability that Alice wins is $\frac{2}{3}$.

A simple quantum strategy of Bob can make out of it a fair game.

Evolutionary quantum games

Kay et al. (2001) demonstrated importance of entanglement in an evolutionary version of a static classical game.

In an evolutionary version each player has a memory to remember his/her outcomes in the last m steps, for some m, and accordingly change his/her strategy.

For the game of three players, at which each of players get initially bit 0 and has an option to flip it, with the payoffs given in the following table, where first three columns specify actions of the players and the last three payoffs

0	0	0	0	0	0
1	0	0	1	−9	−9
0	1	0	−9	1	−9
0	0	1	−9	−9	1
0	1	1	1	9	9
1	0	1	9	1	9
1	1	0	9	9	1
1	1	1	2	2	2

they have shown that for small m classical players outperform quantum, but for large m the opposite is true.

Chapter 4 — Automata

page 156, after Exercise 4.1.4

Remark It has been shown by Valdats (2000) that the class of languages accepted by 1QFA is not closed under union and, actually under any binary Boolean operation. Namely, he has showed that the languages $L_1 = (aa)^*bb^*a(b^*ab^*a)^*b^* \cup (aa)^*$ and $L_2 = aL_1$ can be accepted by 1QFA with probability $\frac{2}{3}$, but their union is not acceptable by a 1QFA. In addition, it has been shown that the above example represents a border case in the following sense. If two languages L_1 and L_2 can be accepted by 1QFA with probabilities p_1 and p_2 such that $\frac{1}{p_1} + \frac{1}{p_2} < 3$, then their union is accepted by a 1QFA with probability $\frac{2p_1p_2}{p_1+p_2+p_1p_2}$.

page 160, after line -10 **Remark** The language L_0 has been shown, by Yamasaki et al. (2000), in a similar way as above, not to be acceptable by bounded-error quantum one-way counter automata, see page 41.

page 160, before line -2 As shown by Ambainis and Kikusts (2001) Theorem 4.1.13 has not been correct enough. New results along the same line has the form

Theorem If a language L can be accepted by a 1QFA which gives the correct answer with probability greater than $\frac{52+4\sqrt{7}}{81}$, then L is accepted by 1RFA; there is a language accepted by a 1QFA with the probability $\frac{52+4\sqrt{7}}{81}$, but cannot be accepted by any 1RFA.

page 160, line -0 Ambainis et al. (1999) established a hierarchy of regular languages L_n, $n = 1, 2, \ldots$, $L_n = a_1^*a_2^* \ldots a_n^*$, $a_i \neq a_j$ if $i \neq j$, such that L_n, $n > 1$, can be recognized by a 1QFA with a probability smaller than that with which L_{n-1} is accepted, and probabilities that languages L_n are accepted converge to $\frac{1}{2}$ for $n \rightarrow 0$. Namely, they have shown:

- There is a constant ε such that L_n can be recognized by a 1QFA with the probability of correct answer at least $\frac{1}{2} + \frac{\varepsilon}{n}$.
- L_n cannot be recognized with probability greater than $\frac{1}{2} + \frac{3}{\sqrt{n-1}}$.

Open problem. Can one show a similar hierarchy results also for languages over only two letter alphabet? (In the case of classical automata, one can usually easily show that a hierarchy result that holds for a sequence of languages over increasing alphabets, holds also for the two-letter alphabet. In a more general setting the question is whether this proof methodology holds also in quantum case.) This open problem was solved by Kikusts and Rasščevskis (2000). They considered the languages L_n defined as follows $L_1 = a^*$, $L_i = L_{i-1}b^*$ if i is even and $L_i = L_{i-1}a^*$ if i is odd. Such a language L_n can be recognized with probability p such that $p^{\frac{n+1}{n-1}} + p = 1$ by the automaton of Ambainis and Freivalds, page 155. For these sequences of languages it holds that the language L_n can be recognized with probability $\frac{1}{2} + \frac{1}{4n}$, but not with probability greater than $\frac{1}{2} + \frac{3}{\sqrt{n-1}}$.

page 161, lines 9-11 As estimated by Berzina et al. (2000), already on a 7-qubit computers one could implement a 1QFA recognizing the language L_{1223} with probability 0.6517.

page 161, lines 12-14 The lower bound result that any 1QFA accepting the language $L_n = \{w0 \mid w \in \{0,1\}^*, |w| \leq n\}$ has to have size $2^{\Omega(n/\lg n)}$ has been improved by Nayak (1999) to be $2^{\Omega(n)}$ (even for a more general type of one-way quantum finite automata).

page 161, after line +26

Remark An overview of succinctness methods and results in quantum finite automata and a variety of related (open) problems are discussed by Gruska (1999a) and Gruska (2000).

page 161, at the end of Section 4.1.5

Remark Another generalization of 1QFA, the so-called *quantum one-counter automata* (Q1CA), that have one counter the content of which can be increased at each reading of an input symbol by a $d \in \{-1, 0, 1\}$, have been introduced and studied by Kravtsev (1999). He considers several recognition modes, for example on the empty stack, and shows the bounded-error acceptance of several non-context-free languages, as $\{0^i10^j10^k \mid (i = j \wedge j = k) \vee (i \neq k)\}$ by Q1CA. However, Yamasaki et al. (2000) have shown that all these languages can be accepted by probabilistic reversible classical one-counter automata and with probabilities that are not smaller, and in some cases strictly larger, than shown by Kravtsev (1999). In addition, they have shown an example of the language that seems to be recognizable with bounded-error by a Q1CA with larger probability than by any probabilistic reversible classical one-counter automata. However, it remained as an open problem to show that Q1CA can recognize languages that are not recognizable by probabilistic (reversible) one-counter automata. This problem was solved by Bonner et al. (2000a).

For quantum one-counter automata the emptiness problem is undecidable, as shown by Bonner et al. (2000). (Let us recall that the emptiness problem is decidable for pushdown automata.)

In a way Q1CA are a generalization of 1QFA, **two-way quantum one-counter automata** – 2Q1CA – introduced by Yamasaki et al. (2001) are a generalization of 2QFA. They provide definition of 2Q1CA, well formedness conditions and show that languages $\{0^n1^{n^2} \mid n \geq 1\}$ and $\{a^mb^nc^{mn} \mid m, n \geq 1\}$ are recognizable by 2Q1CA.

Remark Amano and Iwama (2001) have demonstrated a novel way how to exploit difference in probability calculations between probabilistic and quantum automata for demonstration of a difference in the number of states between probabilistic and quantum one-way automata. They have shown that for any integer constant $c > 1$ there is a language L_c which contains sentences of length up to $\mathcal{O}(n^{c+1})$ such that there is a MM-1QFA of $\mathcal{O}(n^{c+4})$ states which recognizes L_c, but if we try to simulate this automaton by a PFA using the same algorithm, then this automaton needs $\Omega(n^{2c+4})$ states.

page 168 before Section 4.2

4.1.8 Two-way finite automata with quantum and classical states

The models of QFA considered so far have all been natural quantum versions of the classical models of automata. Of a different type is the model introduced by Ambainis and Watrous (1999), and called *two-way finite automata with quantum and classical states* (2QCFA). This model is also more powerful than classical (probabilistic) 2FA and at the same time it seems to be more realistic, and really more "finite" than 2QFA because 2QFA need quantum memory of size $\mathcal{O}(\lg n)$ to process an input of the size n. 2QCFA can be seen as an intermediate model between 1QFA and 2QFA.

A 2QCFA $\mathcal{A}$ is defined similarly as a classical 2FA, but, in addition, $\mathcal{A}$ has a fixed size quantum register (which can be in a mixed state) upon which the automaton can perform either a unitary operation or a measurement. A 2QCFA has a classical initial state q_0 and an initial quantum state $|\phi_0\rangle$.

The evolution of a quantum state of the register is specified by a mapping Θ that assigns to each classical state q and a tape symbol σ an action $\Theta(q, \sigma)$.

One possibility is that $\Theta(q, \sigma) = (q', d, U)$, where q' is a new state, d is the next movement of the head (to left, no movement, or to right), and U is a unitary operator to be performed on the current quantum register state.

The second possibility is that

$$\Theta(q, \sigma) = (M, m_1, q_1, d_1, m_2, q_2, d_2, \ldots, m_k, q_k, d_k)$$

where M is a measurement, $m_1, \ldots, m_k$ are its possible classical outcomes and for each measurement-outcome a new state and a new movement of the head is determined. In such a case the state transmission and the head movement are probabilistic.

Ambainis and Watrous (1999) have shown that 2QCFA with 1 qubit of quantum memory are already very powerful. Such 2QCFA can accept the language of palindromes over the alphabet $\{0, 1\}$, which cannot be accepted by probabilistic 2FA at all, and also the language $\{0^i 1^i \mid i \geq 0\}$, in polynomial time — this language can be accepted by probabilistic 2FA, but only in exponential time.

In the above model only projection measurements have been considered. It is not clear whether something, especially concerning the number of the classical states, could be obtained by considering also POVM measurements.

An interesting open problem seems to be also to investigate the impact of the number of qubits in the quantum memory of 2QCFA on their recognitional and descriptional power.

4.1.9 Quantum finite state transducers

The concept of 2-tape quantum finite automata introduced by Bonner et al. (2000) has been recasted and studied by Freivalds and Winter (2000) as a model of quantum finite state transducers (QFST) that can be used to study the acceptance of the class of binary relations on strings. Quantum finite state transducers are defined in such a way that if the output tape is thrown away one gets quantum finite (one-way) automata. Namely, it holds

Theorem A language L is accepted by a 1-way quantum finite automaton with probability bounded away from 1/2 if and only if the relation $L \times \{0\} \cup \bar{L} \times \{1\}$ is computed with an isolated cut-point.

The first key problem studied by Freivalds and Winter (2000) is that of the decidability of the emptiness problem. The result depends much on the probability the transducer computes a relation with. It holds

Theorem (1) The emptiness problem is undecidable for QFST computing a relation with probability 2/3.

However, it is conjectured that situation can be different for QFST computing relations with larger probabilities.

Conjectures: (1) The emptiness problem is decidable for QFST computing a relation with probability 0.99. (2) The emptiness problem is decidable for QFST computing a relation with one-letter alphabet with probability $1/2 + \varepsilon$.

The second key problem studied by Freivalds and Winter (2000) is that of the power of QFST with respect to the probabilistic finite state transducers (PFST). It turns out that power of QFST is incomparable to that of PFST.

Theorem (1) The relation

$$R_3 = \{(0^m 1^n 2^k, 3^m) \,|\, n \neq k \wedge (m = k \vee m = n)\}$$

can be computed by a QFST with probability $4/7 - \varepsilon$, for any $\varepsilon > 0$, but the relation R_3 cannot be computed by a PFST with an isolated cut-point.

(2) The relation

$$R_5 = \{(wx, x) \,|\, w \in \{0,1\}^*, x \in \{0,1\}\}$$

cannot be computed by a QFST with an isolated cut-point, but it can be computed by PFST with probability 1.

4.1.10 Quantum pushdown automata

The first attempt to introduce a model of quantum pushdown automata (QPDA) has been made by Moore and Crutchfield (1997). A more proper seems to be definition introduced by Golovkins (2000), based on the concept of 1QFA introduced by Kondacs and Watrous (1997). Golovkins

(2000) also provides for his model well-formedness conditions that are necessary and sufficient for the evolution to be unitary.

QPDA accept all regular languages. Reversible PDA, as a special case of QPDA all amplitudes of which are from the set $\{0, 1\}$, can accept non-regular languages. Golovkins (2000) provides an example of a language $L = \{w \in \{a, b, c\}^* \mid |w|_a = |w|_b \text{ xor } |w|_a = |w|_c\}$ which can be accepted by QPDA, but not by deterministic PDA.

Open problems (1) Are QPDA more powerful than classical PDA? (2) Are QPDA more powerful than probabilistic PDA (PPDA)?

page 192, at the end

4.3.5 Quantum lattice gas automata

A concept similar to that of cellular automata is that of lattice gas automata.

In the case of classical one-dimensional lattice gas automata configurations are labeled by pairs (x, α), where x is an integer denoting the position and $\alpha \in \{\pm 1\}$ represent velocity. A classical gas automata evolution rule consists of an **advention stage** $(x, \alpha) \rightarrow (x + \alpha, \alpha)$ followed by a **scattering stage**.

The concept of quantum lattice gas automata (QLGA) was introduced by Meyer (1996). QLGA model was generalized to higher dimensions, to include more particles, potential and various boundary conditions – see Meyer (2001) for references.

The evolution rule for one dimensional QTGA resembles a random walk. On this basis Meyer (2001) has shown that QLGA provide a quadratic improvement in the number of steps required comparing to a classical random walk. In addition, he has shown that QTGA with a lattice of size n can be simulated classical in $o(n)$ steps. On this basis he has shown that using quantum systems we can speed up simulation of classical lattice gas automata – to illustrate that using quantum systems we can speed up simulation of classical systems.

Chapter 5 — Complexity

page 201, end of Section 5.1 A detailed proof of the existence of a universal QTM simulating efficiently any multitape QTM has been given by Nishimura and Ozawa (1999).

page 204, at the very end A variety of other results concerning the power of amplitudes have been shown. Three sets of amplitudes have played by that an important role: $A = \{0, \pm 3/5, \pm 4/5, \pm 1\}$, $B = \{0, \pm 1/\sqrt{2}, \pm 1\}$, $C - \Theta_\theta = \{0, \pm\cos\theta, \pm\sin\theta, \pm 1\}$, for various θ.

It has been shown already by Adleman et al. (1998) that $\mathbf{BQP} = \mathbf{BQP}_A$. In addition, it follows from basic results on the sets of universal circuits that $\mathbf{BQP} = \mathbf{BQP}_B$. These results, together with results reported already in the book show that the classes **BQP** and **NQP** are not sensitive to the class of amplitudes allowed.

Situation is different with respect to the classes **EQP** and **ZPP**

– that is with respect to the classes of exact and zero-error (Las Vegas) quantum polynomial time computations. As already mentioned in the book, Adleman et al. (1998) have shown that $\mathbf{EQP}_{\Theta_\theta} = \mathbf{P}$ for the case that $\sin\theta$ and $\cos\theta$ are transcendental. Nishimura (2001) has shown that the same is true if $\cos\theta$ and $\sin\theta$ are rational. This implies that the set of amplitudes A is useless for exact quantum polynomial time computation.

Concerning the class **ZPP**, Nishimura (2001) has shown that $\mathbf{ZQP}_A \subseteq \mathbf{ZQP}_B$ and that factorization is in $\mathbf{ZQP}_A$.

page 205, Theorem 5.2.7 Theorem has been extended, by Watrous (1999a), to the case of machines with algebraic transition amplitudes and unrestricted measurement during their computation.

In addition, Theorem 5.2.7 has been extended by Watrous (1999a) as follows: Any space $\mathcal{O}(s(n))$ uniform family of quantum circuits, where $s(n) = \Omega(\lg n)$ is space-constructible, acting on $s(n)$ qubits consisting of unitary gates and (unrestricted) measurements defined in a usual way by matrices of algebraic numbers can be simulated by an unbounded error space $\mathcal{O}(s(n))$ classical probabilistic Turing machine. (Observe that quantum circuits are not required to operate with bounded error and they may have depth exponential in $s(n)$.)

All above extensions, due to Watrous (1999a), are actually corollaries of a general result saying that a very general class of decision problems, concerning a class of quantum stochastic processes, can be efficiently solved classically in the space bounded case. Proofs use a special technique that may be of a more general interest to simulate quantum and probabilistic processes with transitions specified by algebraic numbers. In addition, the results obtained imply the following result for classical probabilistic computations.

Any unbounded error PTM running in space $s(n)$ with algebraic transition probabilities and an algebraic cut-point can be simulated by a space $\mathcal{O}(s(n))$ bounded PTM with the cut-point $\frac{1}{2}$.

page 205, footnote 6. Add to line +4 This is a version of quantum **NP** for which the notation **BQNP** starts to be used. Interesting enough, it has been shown that the "ground state energy problem" (to decide whether a "local" Hamiltonian has eigenvalue smaller than a specified energy E), is complete for this class Another notation used for **BQNP** is **QMA**.

page 206, continuation of Remark 5.2.9. Quantum analogues of parallel complexity classes **AC** and **ACC** have been investigated by Moore (1999). Let $\mathbf{QAC}^0$ be the quantum analogue (using circuits with one-qubit gates and XOR-gates) of the classical complexity class $\mathbf{AC}^0$ of the constant depth circuits with AND and OR gates and arbitrary fan-in. Similarly, let $\mathbf{QACC}^0$[q] be a quantum analogue of the class $\mathbf{ACC}^0$[q] defined by circuits of the constant depth that can use also n-ary mod q gates $(x_1, \ldots, x_n) \rightarrow (x_1, \ldots, x_{n-1}, z)$, where $z = \bar{x_n}$ if $(x_1 + \ldots x_{n-1}) \bmod q \neq 0$ and $z = x_n$ otherwise. In addition, let $\mathbf{QACC}^0 = \bigcup q > 1\mathrm{QACC}^0[q]$. Moore (1999) has shown that modulo-2 gates or special "fanout gates" (i.e. those producing $\alpha|0^{(n)}\rangle + \beta|0^{(n)}\rangle$ out of $\alpha|0\rangle + \beta|1\rangle$) allow to construct MOD_q gates by quantum circuits of constant depth for any q and therefore $\mathbf{QACC}^0[2]$ $=\mathbf{QACC}^0$. Since $\mathbf{ACC}^0[\mathrm{p}] \neq \mathbf{ACC}^0[\mathrm{q}]$ if $gcd(p,q) = 1$, the class $\mathbf{QACC}^0[2]$ and $\mathbf{QAC}^0$ are strictly more powerful than its classical counterparts. Moore (1999) left open the question whether $\mathbf{QACC}^0[q]$ $=\mathbf{QACC}^0$ for all q. This problem was answered positively by Green et al. (2000).

page 207, add to line +18 This approach has been recently developed by Nishimura and Ozawa (2000). They solved positively the following basic problem "If a unitary transformation U is efficiently computable by a quantum Turing machine, is there a quantum Turing machine carrying out an oracle quantum Turing machine with U efficiently?" also for the case of Las Vegas computations.

page 209, after line +12 A complexity class **C** is called **robust** if $\mathbf{C}^{\mathbf{C}} = \mathbf{C}$. Nishimura and Ozawa (2000) have shown robustness also for classes **EQP** and **ZQP**, what is the quantum analogue of the classical class $\mathbf{ZPP} = \mathbf{RP} \cap \mathbf{co} - \mathbf{RP}$.

page 209, before Section 5.3 This is to list some other results concerning relativized quantum complexity

- (Fortnow and Rogers, 1999) There exists relativized world where $\mathbf{P} = \mathbf{BQP}$.
- (Fortnow and Rogers, 1999) There exist a relativized world where **BQP** has no complete sets.

page 213, at the end Raz (1999) presents another example of a communication problem, to compute a partial function, for which there is a quantum communication protocol with exponentially less communication complexity than any probabilistic communication protocol needs.

Another interesting and important communication problem is the **scheduling problem**. Informal formulation of the problem is that Alice and Bob have their appointment books for n slots of time and they want to find a free slot for a meeting.

On a more technical level each of two parties A and B have n-bit strings X_A and X_B and they want to find an i such that $x_A(i) = x_B(i) = 1$.

Classically one may need to communicate n bits to solve the problem. Buhrman et al. (1998) found a quantum algorithm that needs only $\mathcal{O}(\sqrt{n}\lg n)$ qubit exchanges. The basic idea is to use quantum search of n possible bits to find the one with 1s. This has been improved recently slightly by Grover (2002). He showed, by a modification of the algorithm of Buhrman et al (1998), that if we denote εn the number of ones in string with less ones, then there is quantum algorithm that needs to exchange only $\mathcal{O}(\sqrt{\varepsilon n}\lg n)$ qubits.

Remark 5.3.9 In addition to the concept of quantum communication complexity $QC(f)$ of a total Boolean function f also the concept of quantum nondeterministic communication complexity $QNC(f)$ of f has been introduced by de Wolf (2000) using the concept of a non-deterministic protocol for $f : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}$ to be such a protocol that has positive acceptance probability if and only if $f(x,y) = 1$. As shown by de Wolf (2000), $NQC(f)$ can be well estimated using the concept of nrank(f) — to be the minimal rank of a matrix whose (x,y) entry is non-zero if and only if $f(x,y) = 1$. Namely, he has shown that

$$\frac{\lg \mathrm{nrank}(f)}{2} \leq NQC(f) \leq \lg \mathrm{nrank}(f).$$

(This is actually a generalization of the well-known lower bound for $CC(f)$ — $\frac{\lg \operatorname{rank}(f)}{2} \leq CC(f)$, where rank$(f)$ is the rank of the the following "communication matrix" $M_f(x,y) = f(x,y)$. It is an open problem of classical communication complexity whether there is a k such that $CC(f) \leq (\lg \operatorname{rank}(f)^k)$.)

Remark In the classical communication complexity of importance is also to study communication complexity of problems for the case that the number of communication rounds is fixed (by a parameter k). The round communication complexity for the following *pointer jumping function* is one of the most studied issue in this connection.

Definition Let A and B be disjoint sets with n elements each and let $F_A = \{f_A \,|\, f_A : A \rightarrow B\}$, and $F_B = \{f_B \,|\, f_B : B \rightarrow A\}$. Let $f(v) = f_A(v)$ (resp. $f_B(v)$) if $v \in A$ (resp. $v \in B$). Define $f^{(0)}(v) = v$ and $f^{(i)}(v) = f(f^{(i-1)}(v))$ for $i > 0$. Moreover, let $g_i : F_A \times F_B \rightarrow (A \cup B)$ is defined by $g_i(f_A, f_B) = (f^{(i+1)}(v_1))$, where v_1 is fixed. Finally, let $f_i : F_A \times F_B \rightarrow \{0,1\}$ is the XOR of all bits in the binary code of the output of g_i

Klauck (2000) reports lower bound $\Omega(n/k^3)$ communication complexity for computation of f_k in k rounds. As referenced by Klauck (2000) the classical lower bounds known are $\Omega(n/k^2 - k \lg n)$ and $\Omega(n/k + k)$.

5.3.3 Spooky quantum communication complexity

Another interesting question concerning the power of entanglement for communication concerns the idea whether entanglement can be used instead of communication. In other words, whether quantum pseudo telepathy is possible and what we can say about it quantitatively.

One way to approach the problem (Brassard, 2001), could seem to be to ask whether we can have a function $f : X \times Y \rightarrow Z$ such that it is not possible to determine $f(x,y)$ from the knowledge of either x or y, but two entangled parties can compute $f(x,y)$, if one is given an x and other a y. However, this cannot be the case, because this would allow faster than light communication. However, there is a way to find a positive answer to the above problem when computation of relations and not of functions is considered. *Spooky communication complexity*, Brassard et al. (1999), has been introduced as follows.

Let X, Y, A and B be sets and $R \subset X \times Y \times A \times B$. In the initiation phase, two later physically separated and entangled parties, Alice and

Bob, are allowed to establish a strategy. After they are separated one of them is given an $x \in X$ and second a $y \in Y$ and their goal is to produce $a \in A$ and $b \in B$, each of them one, such that $(x, y, a, b) \in R$. It is said that *spooky communication* or *pseudo-telepathy* takes place, if the above task cannot be done for sure classically, but it can be done once these two parties share entanglement. **Spooky communication complexity** of the task is then defined as the amount of entanglement required to perform the task.

Brassard et al. (1999) has shown, for the relation R defined bellow, that the number of bits to compute the relation classically is exponentially larger than the number of entangled pairs shared by the parties at spooky communication (and therefore that spooky communication can be exponentially more effective).

Let k be an integer, $n = 2^k$, $X = Y = \{0,1\}^n$, $A = B = \{0,1\}^k$ and

$$(x, y, a, b) \in R \leftrightarrow \begin{cases} x = y \text{ and } a = b; \\ \Delta(x, y) = \frac{n}{2} \text{ and } a \neq b; \\ \Delta(x, y) \notin \{0, n/2\}. \end{cases}$$

where again $\Delta(x, y)$ denotes the Hamming distance. (In other words, if Alice and Bob are promised that their inputs are either the same or differ in half of bits and they have to produce the same outputs only if their inputs are the same.)

It has been shown that there is a constant c such that the above relation cannot be established classically with fewer than $c2^k$ bits provided k is sufficiently large, but k entangled pairs are sufficient for a spooky communication solution.

Using communication lower bounds to study non-locality

It would seem that to study non-locality is the task of physics with little theoretical computer science (methods) can do in that area. However, it has been recently shown, by Buhrman et al. (2002), that this is not the case and that, for example, combinatorial techniques used to study lower bounds for classical communication complexity can be used to quantify the amount of non-locality exhibited by quantum correlations. For example, these methods have been used to get some insight, for some Bell experiments, into the minimum detector efficiency, as a non-locality measure, for which the resulting correletions can still be reproduced, by a local hidden-variable theory. In particular, it has been shown that at least $\mathcal{O}(n \lg n)$ classical communications are needed in case of n-partite systems and that the maximum detector efficiency required to close detection loop decreases with n by $O(1/n)$.[5]

page 215, at the end of the chapter

5.5 Quantum interaction complexity

Another important/interesting type of complexity of the classical computation is the number of rounds of interactive protocols called *interactive proof systems.*

Informally, a language $L \subset \Sigma^*$ is said to have an interactive proof system if here exists a communication protocol P, and a party, called **verifier**, V of limited (polynomial) computational power, such that

- there exists another party, called **prover**, P, working in probabilistic polynomial time, that can, given an $x \in \Sigma^*$, always convince V, following the protocol P, by the overwhelming statistical evidence, that $x \in L$ if this is so, and
- no prover P' following the protocol P can convince V to accept with non-negligible probability an $x \in \Sigma^*$ if $x \notin L$.

The above concepts can be formalized, see, for example, Gruska (1997), Section 9.2, for a presentation, using the concept of an *interactive Turing machine* with a special communication tape and private tape with random bits, and the concept of interactive proof system as consisting of a pair of interactive Turing machines with a common communication tape which is used by both interactive Turing machines, in rounds, to read message written by other one and to write its own message.

The class of languages having interactive proof system with polynomially large amount of communication rounds, with respect to the length of input, is denoted **IP** and one of the important results of modern complexity theory is, due to Shamir, that

$$\mathbf{IP} = \mathbf{PSPACE}.$$

[5]In order to study how much classical communications are needed to reproduce quantum correlation a model is used in which parties are classical and they are not allowed to communicate after receiving inputs, but can share random bits. Such a model is known in physics as a LHV-model (local hidden variables).

For a function f let us denote IP($f(n)$) the class of languages for which there are interactive proof systems with $f(n)$ rounds communication when processing an input of length n.

All known methods to design for a given language $L \in$ **PSPACE** an interactive system are such that they require for some languages interactive proof systems with non-constant number of rounds provided the polynomial time hierarchy does not collapse.

An important generalization is to consider multi-provers proof systems. In this connection two results are of basic importance:

- **MIP** = **NEXP**
  MIP – class of languages having interactive proof with several provers and polynomially many interactions between verifier and provers.
- Any language in **NEXP** has a two-prover interactive proof system with just one round.

The idea of an interactive proof system can be naturally generalized, see Watrous (1999), to consider the case that communicating parties (interactive Turing machines) have the power to process and communicate quantum information (are quantum Turing machines). In such a case, as shown by Watrous (1999), quantum interactions are much more powerful as classical ones and if we denote QIP($f(n)$) the class of languages having quantum interactive proof system with $f(n)$ rounds when processing an input of length n, then informally

$$\mathbf{PSPACE} \subset \mathrm{QIP}(2)$$

and more precisely it holds

Theorem Every language in **PSPACE** has a 2-round quantum interactive proof system with exponentially small probability of error.

The above theorem has been proved by providing a two-rounds quantum interactive proof system for the so-called *quantified Boolean formula problem*, a **PSPACE**-complete problem.

The above result implies that quantum interactive proof systems are strictly more powerful than classical ones in the case of constant number of rounds unless polynomial time hierarchy collapses. This provides another strong evidence that additional power is gained by interactive proof systems in quantum setting.

The above result give rise to a variety of natural open problems:

Open problems(Watrous (1999)) (1) Does equality **PSPACE** = QIP(2) holds true?
(2) What can be said about classes QIP(k) for $k > 2$?
(3) Do languages in **NEXP** have constant round quantum interactive proof systems?

The above results have been improved by Kitaev and Watrous (2000). They showed that any polynomial-round quantum interactive proof system can be "parallelized" to a quantum interactive proof system with exponentially small one-sided error in which the prover and the verifier exchange only three messages. In addition, they showed that any language having a quantum polynomial-round interactive proof system can be decided in deterministic exponential time, implying that single-prover quantum interactive proof systems are strictly less powerful than multi-prover classical interactive proof systems, unless **EXP** = **NEXP**.

Kobayashi and Matsumoto (2001) have consider the case of quantum multi-prover proof systems. Two cases of special importance: provers share entanglement or they do not share entanglement. The main new results are the following ones

- Class of languages having one-prover quantum interactive proof system at which prover has no private bits equals **NEXP**.
- (Kobayashi and Matsumoto) If provers do not share entanglement, or only polynomial amount of entanglement, then the class of languages having quantum multi-prover interactive proof system is equal to **NEXP** – **QMIP** = **NEXP** – that is no advantage with respect to the classical case.

5.6 Quantum zero-knowledge proofs

For quite a while quite several people tried to find a quantum equivalent of the classical concept of zero-knowledge proof. While the problem is not yet resolved fully, the approach of Watrous (2002) is of interest.

Classical zero-knowledge proofs are special cases of interactive proof systems; they are of large importance for modern cryptography. Informally a proof is of a claim is zero-knowledge if the knowledge of the proof is no way more useful than the belief that the claim is true. Several concepts of zero-knowledge proofs have been introduced; the most usual one are statistical zero-knowledge proofs in which the prover convinces the verifier by compelling statistical evidence. The class of languages having zero-knowledge proofs is denoted SZK; it is closed under complement and it contains such problems as Graph Isomorphism (which is not known to be in **BPP**.

Watrous's definition is of interest from computational point of view. It brings essential restriction of the concept of quantum interactive proof system. His definition gives rise to a new complexity class **QSZK** – quantum statistical zero-knowledge – that has analogous properties as the classical class **SZK**. For example, the class is closed under complement and has natural complete promise problems, the so-called Quantum State Distinguishibility problem: given instructions for preparing two mixed quantum states, are the states close together or far apart in the trace norm metric (the promise is that two states are either close or far apart). **QSZK** $\subseteq$ **SPACE** – in spite of he fact that inclusion in]**PSPACE** is not known for even one round quantum interactive proof systems. Any honest verifier quantum statistical zero-knowledge proof system can be parallelized to a two-message honest verifier quantum statistical zero-knowledge proof system (in the quantum interactive proof system three messages may be needed).

(α, β)-Quantum State distinguishability.

Input: Quantum circuits Q_0 and Q_1, each acting on m qubits and having k specified output qubits.

Promise: Let ρ_i denote the mixed state obtained by applying Q_i on state $|0^{(m)}\rangle$ and tracing out the non-output qubits, for $i = 0, 1$, we have

$$\text{either} \;\; ||\rho_0 - \rho_1||_{tr} \leq \alpha \;\; \text{or} \;\; ||\rho_0 - \rho_1||_{tr} \geq \beta.$$

Output: Accept if $||\rho_0 - \rho_1||_{tr} \geq \beta$; reject if $||\rho_0 - \rho_1||_{tr} \leq \alpha$.

It is not clear how strong is the restriction to honest verifiers. In the classical case it has been shown that any honest verifier statistical zero-knowledge proof system can be transformed into a statistical zero-knowledge against any verifier.

Difficulties with developing a concept of quantum zero-knowledge proof suitable for quantum cryptography is due to the fact that it is not clear how to define security well enough from cryptography point of view.

Watrous's definition of quantum zero-knowledge protocol should be satisfied for honest verifier case, by any reasonable definition of quantum zero-knowledge proofs. Consequently, derived complexity results can be seen as upper bounds for other concepts of quantum zero-knowledge proofs.

5.7 Complexity and Feasibility of Quantum Phenomena

There are several reasons why complexity and feasibility problems have to be explored in a broader range and more in depth in quantum physics in general and in QIPC in particular.

Till very recently quantum physics (theory) has been developed under a silent and idealized assumption that each quantum state can be constructed (that a preparation procedure for it exists) and that for each observable there is a corresponding measurement procedure. In order to develop quantum computation and communication complexity theories it is needed to explore questions how much it really cost, in terms of various resources, to do that or that or to have that or that. This silent assumption that all constructs of the Hilbert space model of the quantum world are (efficiently) constructible is clearly not acceptable any longer from the point of view of needs to get deeper insights into the power, limitations and laws of QIPC.

Also the recent attempts to build quantum processors brought a need to get some bounds on what is really possible concerning preparation of the states, performance of the unitary operators and concerning measurements. One such class of problem that has already came up very clearly is connected with the preparation of pure states using different technologies.

The question of how much resources are needed to prepare a pure state, or to realize an observable, has been investigated, for example, by Janzing and Beth (2000). They have shown, in addition to other results, a lower bound on the depth of quantum circuits for preparation of certain highly entangled multi-particle mixed states. They gave also a bound on the depth of circuits to perform certain observable.

A related question concerning the *cooling limitations* has been explored by Janzing et al. (2000). Their starting observation is that a preparation of a physical system in a pure state always mean preparation of a state without entropy — it means of a system without heat. In order to achieve that some cooling mechanism needs to be used. For the currently used technologies the size of the required cooling mechanism is very large comparing with the tiny size of the quantum systems to be cooled. It is natural that for quantum computing to be successful miniaturization concerning cooling devices has to make big progress. This brings up a question about the fundamental limitations on the size of cooling systems and on the amount of energy needed for cooling. Good lower bounds on scaling down the cooling apparatus and resources are much needed.

Janzing et al. (2000) study the quantum cooling problem as related to the problem of a reliable bit erasure and they tightened the bound obtained using thermodynamics and Landauer's principle. According to that paper, the reliability of such an erasure procedure is bounded by the statistical properties of the energy source. They develop also a general framework to describe the *thermodynamic worth* of the resources with respect to the reliable bit erasure.

5.8 Quantum random walks

Classical random walks on finite graphs are an important tool with many applications in mathematics, computing, natural sciences and so on. Randomized computations is one of them. They provide a general paradigm for sampling and exploring large set of combinatorial structures by using simple, local transitions.

Technically, a step of a random walk on an undirected graph $G = (V, E)$ is described by a stochastic matrix P, such that $P(u, v) = \frac{1}{d_u}$, if (u, v) is an edge and d_u is the degree of u. In case G is connected and non-bipartite, then the probability distribution D_t on nodes of G after t steps is determined by $D_t = P^t D_0$, where D_0 is the initial probability distribution. One of the main results of the classical random walks is that D_t converges to a stationary distribution π which is independent of the initial distribution D_0 and actually $\pi_u = \frac{2m}{d_u}$.

The following quantities are of importance for random walks:

- **Hitting time** h_{uv} is the average number of steps needed to come from the node u to the node v.
- **Cover time** is the average number of steps needed, in the worst case to walk over all nodes of the graph.

- **Mixing time** $M_\varepsilon = \min\{T \,|\, \forall t \geq T, D_0 : ||D_t - \pi|| \leq \varepsilon\}$ - it is time needed for the distribution D_t to get ε-close to the stationary distribution
- **Filling time** $\tau_\varepsilon = \min\{T \,|\, \forall t \geq T, D_0, X \subset V : D_t(X) \geq (1 - \varepsilon)\pi(X)\}$.
- **Dispersion time** $\chi_\varepsilon = \min\{T \,|\, \forall t \geq T, D0, X \subset V : D_t(X) \leq (1 + \varepsilon)\pi(X)\}$.

The idea to develop quantum versions of random walks has been around already for a while. It is a non-trivial problem to do that because the idea of a random step, of a coin-tossing, seems to be outside the paradigm of the reversible unitary computation and comes in quantum computing only in connection with irreversible measurements. Moreover, due to the unitarity of evolution, it is clear that one cannot expect that also in the quantum case we can have convergence of the distributions to a stationary distribution. It is also not so obvious how could such a concept be really useful for quantum information processing.

There have been two reasons behind a hope that a quantum version of random walks could provide a new technique to create quantum algorithms that would be asymptotically faster than classical ones for some algorithmic problems.

The first one, and perhaps the original one, was a natural extrapolation from the classical computing where using random walks on graphs an asymptotic speed-up has been obtained for several algorithmic problems.

The second, much more surprising, but perhaps also deeper, reason was a discovery, due to Childs et al. (2001), that, in some sense, as discussed in details later, any evolution of a finite-dimensional Hilbert space can be seen as a "quantum (random) walk".

These two motivations lead to two concepts of quantum (random) walks. The first one, called usually *discrete quantum walk*, considers random walks of "directed particles" on a graph. Second one is called usually *continuous-time quantum walk*. In this case, a quantum walk evolves, as a Markov process, by considering the adjacency matrix of a graph as a Hamiltonian and the evolution is then described by the Schrödinger equation with such an Hamiltonian. The origins of this approach can be found implicitly in Farhi and Gutmann (1997) – more explicitly is this approach described by Childs et al. (2001).

For several problems asymptotic separation has been shown between classical and quantum walks. One of them was the *hitting (or propagation) time* and the other one was *mixing time*.

It was first shown, by Farhi and Guttman (1997) (for the continuous quantum walk model) that for a special graph and two its special vertices there is an exponential gap between the hitting time for classical and quantum walks. This has been then shown also for a simpler graph by Childs et al. (2001).

It was also shown, for both types of quantum walks, that mixing time[6], that plays an important role in the theory of classical random walks, can be asymptotically, and even exponentially faster in some cases, for quantum walks. For example, Moore and Rusell (2001) have shown that quantum walks mixes in $\mathcal{O}(n)$ time on an n-dimensional hypercube, while classical walks mix in $\mathcal{O}(n \lg n)$ time.[7]

The most important, and very surprising, result so far seems to be that of Childs et al. (2002) showing that continuous quantum walks represent a new technique to obtain an exponentially speed-up for oraculum algorithmic problems. For that reason we first describe basic concepts and main results concening continuous random walks approach.

In the classical computing a continuous time random walk on a graph $G = (V_G, E_G)$ is a Markov process on G. A step in the classical random walk on G occurs from a node u to one of the connecting nodes v and it occurs at the given *jumping rate* γ — the probability of jumping in a time t is $t\gamma$. Such a random walk is then described by an $N \times N$ matrix M, where $N = |V_G|$ is the number of vertices of G and it holds

$$M(u,v) = \begin{cases} \gamma & \text{if } u \neq v, (u,v) \in E_G \\ 0 & \text{if } u \neq v, (u,v) \notin E_G \\ -d_u\gamma & \text{if } u = v. \end{cases}$$

If $p_u(t)$ denotes the probability of being in vertex u at time t, then

$$\frac{dp_u(t)}{dt} = \sum_v M(u,v)p_b(t). \tag{1}$$

[6]First time when the distribution induced by a random walk is sufficiently close to the stationary distribution

[7]As pointed out by Moore and Russell (2001) there are actually at least two reasonable concepts of mixing time for quantum walks and the exact relation between them is not known yet.

Since columns and rows of M sum-up to zero, it holds $\sum_u p_u(t) = 1$ for all t.

Consider now quantum evolution in an N-dimensional Hilbert space. In the basis $|1\rangle, \ldots, |N\rangle$, the Schrödinger equation for the state $|\psi(t)\rangle$ has the form

$$i\frac{d}{dt}\langle u \mid \psi(t)\rangle = \sum_v \langle u|H|b\rangle\langle v|\psi(t)\rangle. \qquad (2)$$

There is a clear similarity between (1) and (2), if we take $M(u,v) = \langle u|H|v\rangle$. Concerning probabilities, in the quantum case we have

$$\sum_u |\langle u|\psi(t)\rangle|^2 = 1.$$

It is quite easy to describe an algorithmic problem for which it has been shown, By Childs et al. (2002), that using quantum continuous walk we get exponential speed up.

Let us consider two complete binary trees of depth n. In case we identify corresponding leaves of both trees we get a graph G_n of $2^{n+1} + 2^n - 2$ nodes. For this graph and classical random walk, the probability that one can reach the root of one of the trees from the root of other one in time that is polynomial in n must be exponentially small, as a function of n. Informally, this means that starting in one of the roots, it takes a time exponential in n to reach the other root. For quantum walk situation is quite different, one root can be reached from the other one in polynomial time. (However, for the above graph, the algorithmic problem of reaching one root from the other root can be solved classically in $\mathcal{O}(n^2)$ time.)

Childs et al. (2002) have shown how to implement their continuous time quantum walk in the "conventional" quantum computing framework for the case that the structure of the graph is provided in the form of an oracle (that is how to simulate efficiently the appropriate Hamiltonian evolution on a quantum computer). Let us now modify the above graph G_n in the following way. Again we take two complete binary trees T_1 and T_2 of depth n, but their leaves are now connected as follows. At first a leave of T_1 is randomly chosen and then connected to a randomly chosen leave of T_2. That node is again connected randomly to a not-yet-chosen leave of T_1 and this process continue till every leaf of T_1 (T_2) is (randomly) connected to two leaves of T_2 (T_1). For this graph G'_n we consider the following reachability problem: how to get as fast as possible from the root of one of the subtrees to the root of of another subtree.

For this problem Childs et al. (2002) have show that there is a quantum algorithm, based on continuous random walk, that is exponentially faster than any classical algorithm. (Interesting enough, as already mentioned and what is quite easy to see, the same reachability problem can be solved in $\mathcal{O}(n^2)$ time for graph G_n.)

The basic difficulty at the development of the discrete quantum walk approach is how to make a quantum version of a random quantum step, a quantum random move. The basic idea has been then to consider, in addition to a Hilbert space spanned by the nodes of the graph also an ancilla Hilbert space in which a unitary transformation is used to simulate coin-tossing. The quantum walk is then a unitary transformation on the composed Hilbert space having the property that probability amplitudes are non-zero only on edges of the graph.

More technically, let H_V be Hilbert space spanned by states $|v\rangle$, where $v \in V$. Let us also assume first that the underlying graph is d-regular for some d. In addition, let H_A be the ancilla Hilbert space, a "coin-tossing space", spanned by states $|1\rangle$ through $|d\rangle$. Let now C be be a unitary operation on H_A - a coin-tossing operator. Let edges from each nodes are labeled by labels $1, \ldots, d$ in such a way that for each $a \in \{1, \ldots, d\}$ directed edges labeled by a define a permutation. Due to that, the shift operator S on $H_A \otimes H_V$ is defined by $S|a, v\rangle = |a, u\rangle$, where u is the a-neighbor of v, is unitary. One step of the quantum walk is then defined by $U = S \circ (C \otimes I)$.

Example – quantum walk on the cycle. Hilbert space of the walk on n node cycle would be $H_2 \oplus H_n$ As the coin tossing operator we can take the Hadamard transform

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

and the shift operation is defined by

$$S|0, i\rangle = |0, (i+1) \bmod n\rangle$$

$$S|1, i\rangle = |1, (i-1) \bmod n\rangle$$

where 0 (1) stands for a move to right (left).

The above approach can be generalized by relaxing the restriction on the exact form of U. It is sufficient that U "respects the structure of the graph".

As already mentioned, quantum walks do not converge to a stationary state. Indeed, for an initial state $|\alpha_0\rangle$ $\lim_{t\rightarrow\infty} U^t|\alpha_0\rangle$ does not exist.

Probability distribution $P_t(v \mid \alpha_0) = \sum_{a\in A} |\langle a, v|\alpha_t\rangle$ also does not converge.

However, a useful concept of convergence has turned out possible if the limiting distribution is defined as the limit of the average of the probability distributions over time. This can be defined as

$$\bar{P}_T(v|\alpha_0) = \frac{1}{T}\sum_{t=0}^{T-1} P_t(v|\alpha_0).$$

In general, this limiting distribution is dependent on the initial state of the quantum walk, but for special/important cases of graphs (for example for Calley graphs), limiting distribution does not depend on the initial state.

Various measures have been defined, such as quantum versions of *mixing time*, *sampling time*, *filling time* and *dispersion time*.

It has been shown, using the above model of random walk, surprisingly, that on the unbounded line and on cycle, quantum walks spread out quadratically faster than the classical walks, with respect to the above mentioned measures. Moreover, polynomial lower bound on the speed-up for any graph has been shown – quantum walks can be at most polynomially faster than their classical random walks. Moreover, for bounded degree graphs speed-up can be at most quadratic.

A variety of other (often quite surprising) results on random walks have been shown by various authors. For example, for walks on semi-infinite lines and on finite line it has been shown that probabilities of the walk ending at boundaries have unusual properties, very different from the classical case.

5.9 Can we (physically) compute (mathematically) uncountable

In the recent years a bunch of papers has appeared discussing possibilities to overcome so called Turing's barrier – that is to compute what is uncomputable according to the classical computability theory.

Some of these attempts are based on developing models that would generalize brain or neural computations. Other approaches try to see qualitatively new features that global networks and massively distributed computations offer. Other approaches are based on a belief that new power is obtained by considering *interactions* and not only *computations*.

It is therefore only natural that there are also attempts to explore whether some quantum phenomena cannot be used to compute what cannot be computed on classical computers.

In a bunch of papers, see Kieu (2001, 2001a, 2002, 2002a), it is argued, in an interesting and stimulating way, that on the basis of quantum physics we can extend the concept of computability (which has been set actually solely by mathematical reasoning until now). The approach developed leads to the conclusion that, physically, we can compute such unsolvable problems as the Hilbert's tenth problem, and the Halting problem for Turing machines, but that this approach is not sufficient to challenge Gödels incompleteness theorem.

In order to show a possibility to have quantum solution of the Hilbert tenth problem, several reductions and steps are made that do not seem to contradict known physical principles and therefore we can consider them as feasible (unless new physical limitations are discovered).

First of all, to solve Hilbert's Tenth Problem the basic strategy is not to search for zeroes of the given Diophantine polynomial, which may not exist, but to search for the absolute minimum, in the domain of non-negative integers, of the square of the polynomial, which always exist and it is finite. This way absolute minimum is encoded in the energy of the ground state of a quantum Hamiltonian having infinite numbers of energy levels. It is then shown how to design such a Hamiltonian and how to identify unambiguously its ground state. Actually, this way Hilbert's Tenth problem has been reformulated in terms of a set of infinitely coupled differential equations over continuous variables.

Concerning limitations of quantum computability, it is argued that there does not seem to be possible to evaluate Chaitin's Ω number of wisdom, because that would imply that it is possible to create or simulate Hamiltonians in Quantum field theory, what has not been neither proved nor tested yet.

The above ideas arise the question of the difference between classical and quantum proof. On one side, any classical proof (result of a classical verification process) is a statical objects with intermediate records. On the other side, quantum proofs, verification processes, have to be seen as dynamical processes at which intermediate steps cannot be recorded.

A natural question is whether quantum proofs of a theorem should be accepted even if we have no way to prove it using classical means. One way to look at this problem is that situation is actually the same as with classical proofs; our trust in theorems being proved is based on our acceptance of certain laws of physics.

As an another approach, Calude and Pavlov (2001) argue that they have a *theoretical quantum model* to solve the infinite variant of the *merchant problem*[8] that is equivalent to the halting problem. The idea is to be make use of continuity of quantum programs and to be able to compute,

Given any ε and γ the number of steps $t_{\gamma,\varepsilon}$ that a simple procedure has to be iterated in order to be able to determine, with probability larger than $1 - \varepsilon$ whether one of the stacks contains coins different in weight by γ from the normal ones.

However, it is not clear whether the suggested quantum procedure is feasible.

Another approach to "non-Turing" computations has been suggested by Etesi and Németi (2001).

Chapter 6 — Cryptography

page 230, before Section 6.2.5 There are now a variety of different proofs of unconditional security of basic key distribution protocol. Of special interest and importance are proofs of Shor and Preskill (2000) and Gottesman nd Lo (2001). One common point of both proofs that they show unconditional security of entanglement-based protocols first and finally of such protocols as BB84 and of 6-state protocol through error correction techniques, especially through entanglement purification for error correction. The paper of Shor and Preskill (2000) uses entanglement purification technique with one-way classical communication and paper of Lo and Gottesman (2001) uses entanglement purification techniques with two-way communication.

Of special interest is the fact that these proofs are not only of theoretical interest. They also derive threshold error bounds for practical cryptography to be secure at various types of attacks. Some of these results are

[8] A merchant learns that at most one of his countable many stacks of coins contain false coins, all the same, of different weight, by γ grams, comparing to the normal coins. The task is to find out whether some of the stacks contains indeed false coins.

now summarized. Those for the case that quantum purification is used with two-way classical communication, the current best bounds, are due to Gottesman and Lo (2001).

BB84 protocol:

Intercept-resent attacks:

One-way communication purification: 15%.
Two-way communication purification: 23%.

Coherent attacks:

One-way communication purification: 11%.
Two-way communication purification: 17%.

Six-state protocol:

Intercept-resent attack:

One-way communication purification: 16.6%.
Two-way communication purification: 33.3%.

Coherent attacks:

One-way communication purification: 13%.
Two-way communication purification: 23%.

page 232, before Section 6.2.6

Remark Recently several experiments have been reported to perform entanglement based quantum cryptography using entangled photons (Jennewein et. al (2000), Naik et al. (2000), Tittel et al. (2000)).

page 235, at the end

Remark There are several others, principally different, proofs of unconditional security of BB84 protocol: Biham et al. (1999), Shor and Preskill (2000) and Gisin et al. (2001) for BB84 and Inamoro (2000) for entanglement based QKG. A proof of unconditional security of the BB84 protocol, pretty much similar in the overall setting and in the overall security statements, to the proofs of Mayer and You has been provided by Biham et al. (1999). Their proof is based on a different idea of a careful analysis of *information versus disturbance* relations. The proof uses a variety of new concepts and results of a broader interest and asymptotic security is shown even for instances in which the error rate in the transmission from Alice to Bob is up to 7.56%. The proof by Gisin et al. (2001) applies also to the 6-state protocol due to Bruß (199?), and to protocols using larger dimension states.

page 236, at end of Section 6.2.6

L99 protocol and its unconditional security

A new simple entanglement based QKG protocol with conceptually simple proof of unconditional security is due to Lo (1999).

The advantage of the new protocol is that its security can be guaranteed even in the case of arbitrarily large distance between key generating parties, of not perfect source, channels and devices and any eavesdropping strategy. Moreover, error rate can be computed. This is of importance from the practical point of view. On the other side, the protocol requires that both parties have quantum computers and it is therefore of a different category than BB84 and B92 protocols.

The protocol makes an essential use of the fact that with quantum fault-tolerant techniques and quantum repeaters, discussed in Chapter 7, one can securely send quantum information to an arbitrarily large distance. In addition, it makes an essential use of the nice properties of teleportation channels established by Lo (1999).

The protocol uses an $[r, n, t]$ error correcting code to produce a random r bit key.

L99 protocol to generate an r-bit random key.

1. Alice creates $N = n + m$ pairs of particles in the singleton state and sends from each pair of particles one to Bob. (m is a security parameter.)
2. Bob publically announces the receipt of N particles.
3. Alice randomly chooses m singletons for testing and makes her choice public. For each of the chosen singletons Alice and Bob randomly choose one of the operators σ_x, σ_y and σ_z and perform the measurement on the corresponding particles.
4. Alice and Bob make public the results of their measurements and they use the classical sampling theory to estimate error rate on

the untested singletons. If they are happy with the outcome, they continue with the protocol — otherwise they stop to use it.

5. Alice prepares r singletons and encodes r halves of the pairs into n qubits, using the chosen error correcting code, and teleport n states to Bob.
6. Alice and Bob measure the states of their particles and perform necessary decoding (using their quantum computers) to get a random r-bit key. The error rate established in Step 4 can be used to produce a bound on the amount of eavesdropper information in r bits. At the same time, unless there are more than t errors, the eavesdropper knows absolutely nothing about the encoded state and, consequently, about the r bit key produced.

Security — sketch of the proof. The error rate in Step 1 can be made arbitrarily small for arbitrarily long distance using the techniques for quantum fault-tolerant computation and quantum repeaters, as well as the entanglement purification techniques.

The key step is that from the error rate obtained in Step 3 on m (that is on the number of chosen singletons), it is possible, using the classical sampling theory, to estimate error rate on arbitrary sequence of singletons. (Lo (1999) has shown that in the case of teleportation channels the error rate is independent of the states teleported — this is actually quite an important property of quantum teleportation channels and a simple consequence of the fact that both the error operators and the recovery operators of Bob at the teleportation are Pauli operators and from the basic properties of these operators, page 17.)

page 236, line +25 Add to the end of the sentence: “and 1.6km in full day light time (see Buttler et al. 2000). This transmission distance was limited only by the length of the range available for experiment and therefore the experiment seems to represent a significant step forward earth-to-satellite and other long distance QKG. (As pointed out by Butter et al. (2000), the success of QKG over atmospheric optical paths depends on the transmission and detection of single-photons against high background through a turbulent medium.)”

Significant progresses has been reported recently at Euro conference on quantum information in Spain on transmission of photons. N. Gisin reported transmition of photons for distance 67km, from Geneva to Lousane, through optical fibres and H. Weinfurter reported transmission for distance 23.4km in open air and night time from Zugspitze (2950m), in German Alps, to Karwendelspitze, using small, low cost and robust devices (QBER 5%).

Next goal seems to be to provide already practically usable devices (for two km).

Of importance is also demonstration of a single photon interference over 100km (Kosaka et al. 2003) using a balanced gated-mode photon detector. The visibility with 0.1 photon pulse was more than 80%. This correpsonds to the fidelity of a quantum cryptography system of more than 90% and OBER of less than 10% what satisfies security criteria.

page 238, before Section 6.3

6.2.8 Other QKG protocols

A variety of other QKG protocols has been suggested and explored to some degree. They are of two main types.

1. Modifications of the "classical" BB84, E91 and B92 protocols.

   Huttner-Imoto-Gisin-Mor (1995) 4+2 protocol.
   It combines features of BB84 and B92 (in its original form) protocols.

   QKD protocols that use quantum systems of larger dimension than 2 has been suggested and and explored by Bechmann-Pasquinucci and Tittel (2000), Bechmann-Pasquinucci and Peres (2000). However, it is not yet clear how is the idea practically important, although availability of many-path interferometers opens up such a possibility.

2. Protocols based on other physical phenomena.

   Goldenberg-Vaidman (1995) protocol. Two orthogonal states $\frac{1}{\sqrt{2}}(|a\rangle \pm |b\rangle)$ are used to represent bits, where $|a\rangle$ and $|b\rangle$ are localized normalized wave-packets sent from Alice to Bob along two different "length" channels. The packet $|b\rangle$ is delayed until $|a\rangle$ has reached Bob. (For example, by using an interferometer with arms of different length.) Bob has to wait with the readout of the superposition till both signals arrive. To make eavesdropping impossible the times when the states $|a\rangle$ are sent are random.

Koashi-Imoto (1997) protocol. They found a way to avoid necessity of random timing at the previous protocol by using asymmetric beam splitters.

Hillery (1999) protocol. This protocol is based on the use of squeezed vacuum states.

6.2.9 From earth (plane) to satellite QKD

Distance is surely a big limitation of fiber-based QKD. In principle, quantum repeaters could help to overcome the problem, but this does not seem to be possible soon.

Another option that started to be investigated is open-air QKD. Butter et al. (2000) report transmission of photons to the distance 1.7 km and Gormen et al. (2000) to the distance 1.2 km.

All that led to various estimations and expectations that an earth-to-satellite QKD should be feasible and it could have applications (for example, to change keys in communication or TV satellites).

Earth-to-satellite QKD could also lead to transcontinental QKD. The idea is to establish first a key between Alice and a satellite, then between satellite and Bob. Afterwords, the satellite would xor both key and make the result public. This would allow Bob to determine Alice's key. The fact that the key would be known to satellite could actually be a positive feature for the development of QKD — due to the current trends that authorities should have some control over secret communications.

At the implementation of the above earth-to-satellite QKD photons would actually be always send from a satellite to earth and not vice versa. The reason being that it is actually one kilometer above earth surface where there are main sources of perturbation. This is also the reason that as the first step concentration is on developing plane-to-satellite transmission as in the project ??????.

6.2.10 Quantum cryptography as a (potential) technology

An interesting and insightful analysis of the potential of quantum cryptography to become a real technology is due to Lo (1999a). He observes that academia and real world have often different perspectives and the customer acceptance is crucial for the real and full success of a technology. Several roadblocks to the potential deployment of quantum cryptography are identified and analyzed: limited distance (it needs to be increased by two orders of magnitude); limited data rate (it needs to be increased by a ten orders of magnitude); too big equipments needed (it needs to be reduced to such small components as smart cards or CD); no integration with existing infrastructure in information technology is available; various loopholes concerning security are either known (and actually none of the current implementations is fully secure) or may be hidden; hostile positions can be expected from classical cryptographers (because it may put them out of jobs) and from the vendors of classical cryptography (because it may put them out of business). One has also to realize that concerning security, as it is in the case of classical cryptography, the real problems are not on fundamental, but on implementation side. A big need for new quantum cryptography applications is also emphasized and analyzes. We need quantum public-key cryptography, quantum signature schemes and also quantum authentication schemes.

In this connection an interesting open theoretical problem is mentioned: are there quantum one way (trapdoor) functions? That is functions that are easy to compute classically, but computation of their inverse is infeasible even with quantum computers? The existence of such functions would allow to design classical cryptography unbreakable by quantum computers and that could be a nightmare for quantum cryptography.

For an interesting approach to the design of quantum one-way functions see Gottesman and Lo (2001).

6.2.11 Quantum one-time pad cryptosystem

Classical one-time pad cryptosystem is perfectly secure provided for each encoding a new random key is used.

Perfect security of one-pad cryptosystem is also a consequence of Shannon theorem that says that n bits are sufficient and necessary to hide (perfectly) n bits.

Quite surprisingly, there is a quantum version of the classical one-time pad cryptosystem, due to Boykin and Roychowdhury (2000) and a quantum version of the above Shannon theorem

Quantum Shannon theorem (due to Mosca et al. 2000) says that $2n$ bits are sufficient and necessary to hide (to encrypt perfectly) n qubits.

This is very surprising. In spite of the fact that actually infinitely large amount of classical information can be needed to specify n qubits only $2n$ bits are needed to encrypt these qubits perfectly.

The very basic idea is actually very simple and we illustrate it on the way two parties can use two secretly shard bits b_1b_2 to encrypt perfectly one qubit.

Encryption of a qubit ρ is done using the unitary transformation $\sigma_x^{b_1}\sigma_z^{b_2}$ and decryption using the unitary transformation $\sigma_z^{b_2}\sigma_x^{b_1}$. An eavesdropper Eve cannot learn anything by getting the transmitted qubit because what she gets is actually the density matrix $\sum_{b_1,b_2}\sigma_x^{b_1}\sigma_z^{b_2}\rho\sigma_z^{b_2}\sigma_x^{b_1} = \frac{1}{2}I$ corresponding to a random bit.

Other encryption methods to achieve perfect secrecy are presented by Mosca et al. (2000).

Sharing of two bits to encrypt one qubit can be replaced by sharing two Bell states as shown by Leung (2000). This encryption scheme has the advantage that in the case of noisy channel carrying encrypted bit one can detect and correct errors.

It is also interesting to observe that n bits are necessary and sufficient to encode securely n qubits that do have only real amplitudes.

page 251, before Section 6.3.5

Quantum bit commitment in a very general setting

The proof that unconditionally secure quantum bit commitment is impossible naturally arises the question about the exact setting to which this result applies and also the question whether some other modifications and generalizations of the problem cannot lead to different results.

For example, it seems, as pointed out by Kent (1999b), that the above negative result known proofs apply actually only to the case when non-relativistic physics is assumed. A new question therefore arises how it is in the case when we assume validity of special relativity theory, or general relativity theory.

In addition, in the quantum bit commitment problem as formulated above, Alice commits itself to a classical bit, 0 or 1. What happens if we start to explore quite a natural generalization that Alice can commit herself to an arbitrary state of a qubit. Finally, in addition to the setting investigated above, where Alice is fully aware of which bit she commits herself, it is also natural to explore the case that she does not know that (for example, she uses a random bit generator to produce a bit she does not know, but to which she commits herself).

The above modifications of quantum bit commitment problem have been investigated by Kent (1999, 1999a, 1999b). They are of theoretical interest and in this way the bit commitment problem has turned out to be an excellent example to demonstrate that more general physical theories may bring new insights and new results about the very basic quantum information processing and communication problems.

The main results and insights due to Kent (1999, 1999a, 1999b) can be summarized as follows.

For the so-called **classically certified bit commitment problem** (CCBC), at which it is guaranteed that Alice commits herself to the state which has a classical value (even she does not know which one), no unconditionally secure protocol exists in case we assume that special relativity theory holds.

Several relativistic classical bit commitment protocols have been proposed (Kent, 1999, 1999a). They are secure against classical attacks and are conjectured to be secure against quantum attacks.

The cases that general relativity theory or the field theory is assumed to hold have not been investigated yet. Neither protocols and attacks making use of inherently general relativity features are known yet.

A step from considering non-relativistic setting to relativistic setting is quite nontrivial. For example, it requires new definitions of security and actually only in this setting one can talk about a complete definition of security.

Founding of mistrustful quantum cryptography

Kilian (1988) has shown that mistrustful classical cryptography[9] (that deals with the problems when mistrusted parties need to cooperate in order to solve some information generation, processing or communication

[9]Mistrustful cryptographic problems require security against all parties.

tasks) can be based on the oblivious transfer protocol as a primitive from which other basic and secure cryptographic primitives can be built.

In the case of quantum protocols situation is quite different. First of all, there are several concepts of security: unconditional security in relativistic quantum physics setting, unconditional security in non-relativistic quantum physics setting and computational security with respect to quantum computers.

Two surprising results showed that in quantum setting it is interesting/useful to consider a larger variety of fundamental protocols: ideal coin-tossing (ICT), coin-tossing[10] (CT), bit commitment (BC), classically certified bit commitment[11] (CCBC), bit string commitment (BSC)[12] and oblivious transfer (OT)[13]

The first of this results was that unconditionally secure quantum bit commitment is impossible and second result, due to Kent (1999), see page 70, that unconditional secure quantum bit commitment is possible in relativistic quantum setting.

The following table summarizes our current knowledge concerning the above basic protocols in non-relativistic and relativistic quantum setting.

	ICT	CT	BC	CCBC	BSC	OT
non-relative. setting	no	?	no	no	yes	no
relative. setting	yes	yes	yes	no	yes	no

Importance of the CCBC follows from the fact that secure CCBC protocol can be used to develop secure OT and other important protocols.

Since no unconditionally secure protocols exist for many important tasks, the next natural task is explore in which cases one can develop computationally secure quantum protocols.

[10]Two mistrustful parties, Alice and Bob, are to generate a random bit in such a way that each has confidence that the resulting bit is genuinely random if (s)he behaves honestly (independent of the honesty of the other party). More exactly, the protocol is to guarantee that $\Pr(b = 0) = 0.5$ if both parties are honest and if only one party is honest, then $\Pr(b = 0) < \frac{1}{2} + \varepsilon$ and $\Pr(b = 1) < \frac{1}{2} + \varepsilon$. A secure coin-tossing

[11]In the case of classically certified bit commitment it is excluded the possibility that bit commitment is described, until unveiling, by a superposition of quantum states.

[12]Informally, a (m, n) bit string commitment protocol securely commits n classical bits in such a way that the recipient can extract at most m bits of information about the committed string.

[13]Several other variants of very basic cryptographic protocols have been considered by Hardy and Kent (1999) and Aharonov et al. (2000).

Another idea to explore is to use temporarily secure protocols. For example, temporarily secure BC can be used to implement computationally secure coin tossing. As discussed by Kent (2001), BC protocols that are computationally secure for long time can be build from secure CT protocols, which themselves can be build using BC protocols that are computationally secure only for a relatively short time.

It is also important to realize that reductions and relations between cryptographical tasks can change when different concepts of security are considered. For example, in the classical setting BC and BSC are essentially equivalent tasks. As shown by Kent (2001a), situation is different in the case of non-relativistic setting, where unconditionally secure BC (BSC) is impossible (possible).

Situation concerning quantum computational security, with respect to quantum computers, in the area of mistrustful quantum cryptography has been recently analyzed by Kent (2001) and he suggested that this cryptography can be based on (computationally) secure quantum coin-tossing. More exactly, Kent (2001) has presented a method how to build CCBC, and therefore computationally secure protocols for other mistrustful cryptographic tasks using some computationally hard problems as that of subgraph isomorphism or subset sum problems. He also provides strong arguments, but no proofs, in favor of security of suggested protocols.

The above results are very interesting. However, the task to characterize the range of cryptographic tasks for which secure secure protocols exist, with respect to different concepts of security, is still to be to deal with.

page 251, before Section 6.4

6.3.6 Quantum gambling and quantum coin tossing

It has been shown, from the fact that there are no unconditionally secure bit commitment protocols, that there is neither unconditionally secure quantum 1-out-of-2 oblivious transfer protocols nor unconditionally secure quantum ideal coin tossing protocol. It is therefore naturally to ask whether there are some other interesting/important communication problems for which unconditionally secure protocols exist. A positive answer was obtained by Goldenberg et al. (1999), for the task called "quantum gambling", a purely quantum task — closely related to the coin tossing. An open problem is whether there is an unconditionally secure protocol for (non-ideal) quantum coin tossing problem.

We present here at first the quantum gambling task and an unconditionally secure protocol for it and then the recent "candidate protocol for coin tossing" unconditional security of which has still to be proved or disproved.

Quantum gambling — the rules of gambling

Alice and Bob are gamblers. Alice has a particle and two boxes, A and B, to store the particle. Let $|a\rangle$ ($|b\rangle$) denote the quantum state for the particle to be in the box A (B).

Step 1 Alice prepares the particle in some state $|\psi\rangle$ and sends the box B to Bob.

Step 2 Bob has two choices:

1. To open the box B. If he finds there the particle, Alice should pay him a coin; otherwise Bob pays Alice a coin.
2. To ask Alice to send him also the box A. Bob then checks whether

$$|\psi\rangle = |\psi_0\rangle = \frac{1}{\sqrt{2}}(|a\rangle + |b\rangle).$$

   If yes, Bob pays Alice a coin; otherwise Alice pays him R coins. (R is here a "security parameter". For the case $R = 1$ we have a coin tossing protocol.)

Quantum gambling — a protocol

Alice's strategy: To prepare $|\psi\rangle$ as $|\psi_0\rangle$ — as defined above. *Bob's strategy*: After receiving the box B, he performs the unitary mapping

$$|b\rangle \rightarrow \sqrt{1-\theta(R)}|b\rangle + \sqrt{\theta(R)}|b'\rangle = |\psi'\rangle,$$

where $\langle b\,|\,b'\rangle = 0$ and $\theta(R)$ is a "splitting parameter", to be specified later. Afterwords, Bob performs the projection measurement on $|\psi'\rangle$, with respect to the basis $\{|b\rangle, |b'\rangle\}$. If he finds, by doing that, that the particle is in the box B, he then asks Alice to pay him a coin; otherwise he asks her for the box A and verifies whether she prepared the state $|\phi_0\rangle$. If yes, he pays a coin; otherwise Alice pays him R coins.

Quantum gambling — security

Since this is a zero-sum game, and an expectation value of Alice's gain is clearly nonnegative (independently of Bob's strategy), the expectation value of Bob's gain, G_B, has to be non-positive (independently of Alice's strategy). It has been shown by Goldenberg et al. (1999) that at a proper choice of $\theta(R)$ (roughly $\frac{1}{\sqrt{2R}}$), $G_B \geq \delta(R)$, (with $\delta(R)$ approximately $-\sqrt{\frac{2}{R}}$), where $\lim_{R\rightarrow\infty}\delta(R) = 0$.

Non-ideal quantum coin tossing

In a coin tossing protocol two distant parties, say Alice (A) and Bob (B), generate a random bit over a communication channel and each party has a way to test whether the other party did not try to create a bias on the resulting bit. In the case the protocol uses a (security) parameter R such that for each of the parties, A or B, for the probability A_b (B_b) that A (B) generates the bit b, it holds $|A_b - \frac{1}{2}| \leq \theta(R)$ and $|B_b - \frac{1}{2}| \leq \theta(R)$, where $\lim_{R\rightarrow\infty}\theta(R) = 0$. If a party cheats, the other party should be able to detect it.

Exercise 0.1 *Show that the existence of an unconditionally secure bit commitment protocol would imply the existence of unconditionally secure coin tossing protocol.*

Coin tossing protocol by Mayers et al. (1999) — notation

An interesting protocol for coin-tossing has been due to Mayers et al. (1999). It is shown here even if recently Leslau (quant-ph/0104075) and independently several other people have shown its insecurity.

Let

$$|\psi_0\rangle = \alpha|0\rangle + \beta|1\rangle, \quad |\psi_1\rangle = \alpha|0\rangle - \beta|1\rangle,$$

where α and β be reals. (Their choice is still to be optimized — a suggestion is to choose them in such a way that the angle between $|\psi_0\rangle$ and $|\psi_1\rangle$ is $\frac{\pi}{9}$.) Let $|\Psi_0\rangle = |\psi_0\rangle^{\oplus n}$, $|\Psi_1\rangle = |\psi_1\rangle^{\oplus n}$.

Let $\{E_0, E_0^\perp\}$ and $\{E_1, E_1^\perp\}$ be observable on H_{2^n}, where E_0 (E_1) is the subspace spanned by $|\psi_0\rangle$ ($|\psi_1\rangle$) and $E_i^\perp$ is the orthogonal complement of E_i, $i = 1, 2$.

Coin tossing protocol by Mayers et al. (1999) — protocol

Step 1. Alice (Bob) randomly choose a_j (b_j), for $j = 1, \ldots, m$.

Step 2. For $1 \leq i \leq n$ and $1 \leq j \leq m$, Alice (Bob) randomly chooses the bit c_{ij} (d_{ij}) and sends to Bob (to Alice) a pair of particles in the state $|A_{ij}\rangle = |\Psi_{c_{ij}}\rangle \otimes |\Psi_{\bar{c}_{ij}}\rangle$ ($|B_{ij}\rangle = |\Psi_{d_{ij}}\rangle \otimes |\Psi_{\bar{d}_{ij}}\rangle$.)

Step 3. for $i \leftarrow 1$ **to** n **do for** $j \leftarrow 1$ **to** m **do**: Alice (Bob) sends Bob (Alice) $e_{ij} = a_j \oplus c_{ij}$ ($f_{ij} = b_j \oplus d_{ij}$) and Bob (Alice) sends back the second particle from the $|B_{ij}\rangle$ ($|A_{ij}\rangle$). (At the end of this step all m particles sent by Alice (Bob) in Step 2, for any i, j, and not returned, are in the state $|\Psi_{a_j}\rangle$ ($|\Psi_{b_j}\rangle$).

Step 4. For $1 \leq j \leq m$ Alice (Bob) announces a_j (b_j) and Bob (Alice) performs measurement with respect to the observable $\{E_{\bar{a}_j}, E_{\bar{a}_j}^\perp\}$ ($\{E_{\bar{b}_j}, E_{\bar{b}_j}^\perp\}$). If at least one outcome is $\perp$, the protocol aborts.

Alice's (Bob's) final bit is $A \oplus \bar{B}$ ($\bar{A} \oplus B$), where $A = \bigoplus_{j=1}^m a_j$, $B = \bigoplus_{j=1}^m b_j$, $\bar{A} = \bigoplus_{j=1}^m \bar{a}_j$, and $\bar{B} = \bigoplus_{j=1}^m \bar{b}_j$.

page 256, before Remark 6.4.3 Even if quantum teleportation is mathematically simple, it is a puzzling phenomenon, if one believes that anything physically significant cannot move faster than light. How is it possible that an unknown quantum state, no matter how complex it is, no matter how many bits are needed to write down its amplitudes, is transmitted instantaneously — up to only two classical bits. An interesting explanation, within the many world interpretation, page 362, provides Vaidman (1998) and it basically goes as follows. The unknown state $|\psi\rangle$ is actually not moved from Alice's position to Bob's position during the teleportation. The state *was* at Bob's position from the very beginning. The local measurement provided by Alice only split the world in such a way that in each of the new worlds the state of Bob's particle is different from $|\psi\rangle$ just by a known transformation and the number of these transformations just happened to be very small, only 4.

A detailed analysis of the reported quantum teleportation experiments, till November 1998, is provided by Vaidman (1998). The main conclusion is that even though a perfect teleportation of an unknown state has not been yet achieved, with the Innsbruck experiment ranking highest, the experiments performed show that it can be done. In addition, the so-called continuous variables teleportation, suggested by Braunstein and Kimble (1998), was fully successfully implemented by Furusawa et al. (1998).

The term "teleportation" is now used in quantum computing papers in several ways and one has to be careful to get correctly the results reported. An interesting contribution was made by Pati (1999) who has shown that quantum teleportation of **known** qubit can be done using only one classical bit provided parties share an EPR-pair, and using only 1.19 bits in average, provided parties share local hidden variables. Actually, this is the first paper that describes Remote State Preparation protocol of special class of qubits. This protocol has been tested using NMR technology (see quant-ph/0202004).

It seems intuitively clear that quantum teleportation is due to non-locality that measurement of entangled states exhibits. However, quite surprisingly, Hardy (1999) has shown that concepts of teleportation and non-locality are conceptually independent. Namely, he constructed a toy model which is local, for which no-cloning theorem holds, but in which teleportation still holds.

Long distance quantum teleporation

Gisin's group, see Marcikic et al. (2003), has achieved a significant progressin quantum teleportation that can be seen at the same time as progress towards deisgns of quantum repeaters.

Elementary 2-dimensional quantum states (qubits) encoded in 1300 nm wavelength photons are teleported onto 1550 nm photons. The use of telecommunication wavelengths enables to take advantage of standard optical fibre and permits to teleport from one lab to a distant one, 55 m away, connected by 2 km of fibre. A teleportation fidelity of 81.2 This is large enough to demonstrate the principles of quantum teleportation, in particular that entanglement is exploited. This experiment constitutes a first step towards a quantum repeater.

page 256, at the end of Section 6.4.2

Remark (Gottesman and Chuang, 1999) Teleportation illustrates well the known fact that quantum measurements can be seen as an important quantum computational primitives and that in some cases quantum measurement does not have to destroy quantum information irreversibly. Just the opposite, it can help to transfer quantum information from one place to another. In addition, as shown by (Gottesman and Chuang, 1999), generalized quantum teleportation can be seen as a universal quantum computational primitive.

Remark A related problem is how **to teleport quantum unitary operations** — in other words how to implement an arbitrary unitary operation upon a distant quantum system. In other words how to perform the so called **quantum remote control** using LOCCSE. Huelga et al. (2000) have shown that if the remote control is to be implemented as a classical black box, then the required resources are, necessarily, those needed for the implementation of the bidirectional state teleportation.

Remark A natural generalization of the "classical" quantum teleportation would be that Alice teleports an unknown qubits to one of n other parties in such a way that any one of them, but only one of them, of course, can get the teleported qubit. Is this possible?

Brunn (2001) has shown that yes, if Alice and n parties share the cat state $\frac{1}{\sqrt{2}}(|0^{(n+1)}\rangle + |1^{(n+1)}\rangle$ and all n parties can agree, by classical communication, who of them, should get the teleport ed qubit.

Actually, protocol is very simple. Those $n-1$ parties that agreed not to get teleported qubit just perform measurement of their particles in the dual basis.

Alice can perform her Bell measurement on the particle with an unknown state and her particle in the shared cat state, even before parties decide who gets the bit. Alice then just broadcast the classical information obtained by measurement (2 b its) to all n parties.

Generalized teleportation schemes There are, as one would expect, several generalization of the basic teleportation scheme to explore. One of them is to consider two party teleportation, but of more dimensional states than qubits. The other natural possibility is to consider multipartite teleportation.

A general approach to two-party quantum teleportation has been worked out by Accardi and Ohya (1999) and especially by Albeverio and Fei (2000). The problem that has been solved is the following one: Given a state $|\phi_1\rangle$ of a Hilbert space H_1, and an entangled state $|\psi_{2,3}\rangle$ of the tensor product of Hilbert spaces $H_2 \otimes H_3$, with all three Hilbert spaces having finite dimension and with dimension of H_1 being not smaller than that of H_3, conditions are established for a unitary transformation U on $H_1 \otimes H_2$ such that if on the state $U \otimes I(|\phi_1\rangle|\psi_{2,3}\rangle)$ a proper measurement is performed than the resulting state $|\psi_3\rangle$ of H_3 is such that the result of the above measurement uniquely determines a unitary transformation, not dependent on $|\phi_1\rangle$, which, when applied on $|\psi_3\rangle$, yields the state $|\phi_1\rangle$.

Concerning multipartite teleportation, Gorbachev and Trubilko (1999) at first showed a simultaneous teleportation of an unknown state $\alpha|00\rangle + \beta|11\rangle$ through a GHZ-channel to two parties. However, Marinatto and Weber (2000) showed that it is not possible to perform teleportation of any two-qubit state. Gorbachev et al. (2000) then showed how to teleport any entangled two qubit state using GHZ channel and three bits of classical information.

Remote state preparation (RSP) Let us now consider the case that the party in need of teleporting a state has a full classical knowledge of the state. Is it reasonable to expect that in such a case either less ebits or less bits are needed for teleportation? At least in some cases?

The answer is, quite surprisingly, positive. As shown by Lo (1999) and Bennett et al. (2001), in such a case there is a non-trivial tradeoff between the ebits and bits. Bennett et al. (2001) showed, for example, that asymptotically classical communication cost of RSP, in the presence of a large amount of preshared entanglement, can be reduced to one bit for qubit provided four ebits are used (and becomes even less when transmitting part of a known entangled state). During RSP most of the preshared entanglement is not consumed and it can be recovered, using a backward communication, from Bob to Alice. On the other hand, if a large number of bits is used, say n, the number of ebits needed grows like $n2^{-n}$. Protocols developed by Bennett et al. (2001) work even for finite number of (identical) states Alice wants to prepare for Bob. A certain catch is that no protocol is known that creates states always faithfully and uses in all cases less classical communication, per qubit, than quantum teleportation.

Another variations of the RSP problem is to consider the cases when Alice and Bob (or only Alice) have some partial information about state to be teleported.

For example, Henderson et al. (1999) have shown, surprisingly, that even "two-state teleportation" requires one ebit. In other words, even if Alice knows that state to be teleported is one of two possible states, but she does not know which one, one ebit is needed. (However, in the asymptotic case situation is different.)

For an illustration of the case that also Bob has some information about state to be teleported let us consider the example due to Lo (1999). Let Alice and Bob are given values a and b such that $|a|^2+|b|^2=1$. Let they also share nS ebits of entanglement where $S=-|a|^2\lg|a|^2-|b|^2\lg|b|^2$ for large n. Then nS bits of classical communication are sufficient for Alice to help Bob to prepare n states of the form $a|0\rangle+be^{i\theta_j}|1\rangle$, where θ_j's are known only to Alice.

page 257, after Exercise 6.4.5 Implementation: An implementation of the above secret sharing protocol using pseudo–GHZ states[14] based on energy-time entanglement has been described by Tittel et al. (1999). This also represents the first implementation of a quantum protocol using more than two qubits. A detailed error analysis (quantum bit error rate 4%) indicates that quantum secret sharing over tens of kilometers seems to be possible.

Teleclonning

A related problem to quantum teleportation is that of **quantum teleclonning** (see Murao et al., 1999) – an optimal teledistribution, using a shared entangled channel between all parties involved and LOCC, of an unknown quantum state from one party, say Alice, to several parties. If the number of parties is n we speak about 1-to-n teleclonning. The term "teleclonning" has its justification due to the result that quality of distributed "copies" can be achieved to be the same as at the universal cloning and that it does not depend on the state being telecloned.

For the case of 1-to-2 teleclonning, the teleclonning protocol is similar to that of teleportation. The initially shared entangled state is

$$\frac{1}{\sqrt{3}}[|00\rangle|00\rangle+|11\rangle|11\rangle+\frac{1}{2}(|01\rangle+|01\rangle)(|01\rangle+|01\rangle)].$$

The first particle is that of the telecloner (Alice), the second one of the ancilla and the last two of the two parties to receive clones (Bob and Charles). Teleclonning is performed at first by performing (by Alice) a

[14]By Tittel et al. (1999): "In opposition to "true" GHZ states, the three photons being in the pseudo-GHZ state do not consist of three down-converted photons, but only of two down-converted ones plus a pump photon." Moreover, in opposition to "true" GHZ states they do not enable tests of non-locality, but otherwise they have the same correlations as "true" GHZ states.

Bell measurement on unknown state and Aliceṕarticle. Classical outcomes of the measurement are then distributed to Bob and Charles and they are used by them to perform on their particles corresponding one qubit operations.

page 257, before Section 6.4.4 Another general approach to quantum secret sharing is due to Gottesman (1999).

Secret sharing in a strong sense

In the secret sharing schemes discussed in the book and mentioned above there is no guarantee that shared secret remains hidden if two involved parties start to communicate classically. Moreover, as shown by Walgate et al (2000), there is no way to hide a bit between two parties if classical communication is possible and shares consist of parts of two orthogonal pure states.

Let us say that a secret is *shared by two parties in a strong sense* if classical communication between parties is not sufficient for them to get the secret.

Terhal and al. (2000) have shown that it is possible to share a single bit, using mixed quantum states, between two parties in such a way that using classical communication they can obtain only arbitrarily little information about the bit, but they can get the bit only by joint quantum measurement. Moreover, surprisingly, not too much entanglement is needed to share/hide one bit.

The protocol suggested by Terhal et al. (2000) is surprisingly simple and the integer n used in the protocol is the security parameter of the protocol. The hider Alice chooses uniformly randomly n Bell states with the only restriction that the number of singlets between chosen states is even (odd) if the bit to hide is 0 (1). Alice then distributes the chosen states to Bob and Charles, in such a way that the first (second) particle of each entangled pair goes to Bob (Charles).

page 258, to add

6.4.5 All teleportation and super dense coding schemes

Werner (2000) brought an important new insight on possible teleportation and dense coding protocols. He showed not only that there is one-to-one correspondence between (optimal) teleportation and dense coding schemes (realized with minimal resources (with respect to Hilbert space dimension and classical information)), but that there is also a one-to-one correspondence between such schemes and schemes for the three other tasks: (a) construction of orthonormal bases of maximally entangled states; (b) construction of orthonormal basis of unitary operators with respect to Hilbert-Schmidt scalar product; (c) de-polarizing operations whose Kraus operators can be chosen to be unitary.

On one side it is not surprising that there is a close relation between teleportation and dense coding protocols because actually they often perform basically the same operations only in the opposite order. One-to-one relations to other problems is more surprising. However, it helps to see complexity of the problem to design teleportation schemes because, for example, the problem of constructing orthonormal basis of unitary operators is shown to involve such not well understood tools as Hadamard matrices and Latin Squares.

6.4.6 Teleportation, mixedness and dense coding

A very natural question is how good are mixed states for teleportation and dense coding. One reason to ask this is that pure entangled states are harder to produce than mixed states. Second reason is that mixed states can have more entanglement than pure separated states, if von Neumann entropy is taken as a good measure of mixedness.

Horedeckis (1999?) have shown that optimal fidelity in the case of two-qubit bipartite systems is $f(\rho) = \frac{2F(\rho)+1}{2}$, where $T(\rho)$ is the singlet fraction of ρ.

Horodeckis (1999) have also shown that in the case of bipartite systems of dimension n the singlet fraction $F(\rho) < \frac{1}{n}$ implies that teleportation with ρ cannot be done with better than classical fidelity. Bose and Vedral (1999) improved that condition to $S(\rho) > \lg n + (1 - \frac{1}{n}) \lg(n+1)$. This means that for quantum systems of very large dimension, even an entropy close to maximal is not sufficient to ensure failure of teleportation.

Bose et al. (1998) started to deal with the case that parties performing superdense coding protocol share not a pure, but a mixed state. They started to explore the question in what way does the capacity to do dense coding depend on the degree of entanglement as specified by various measures of entanglement and they provided various lower and upper bounds.

Concerning dense coding, an entangled mixed state ρ fails to be useful for dense coding when $S(\rho) > \lg n$. Since the threshold $\lg n$ is smaller than that for teleportation, $\lg n + (1 - \frac{1}{n}) \lg(n+1)$, we can conclude that teleportation is "more robust" with respect to the external noise than dense coding. For a general case that two parties A and B share mixed state ρ over $n \times n$-space the problem to determine capacity $C(\rho)$ of dense coding channel of ρ is almost solved.[15] Hiroshi (2000) established the bound $E_r(\rho) \leq C(\rho) \leq \lg n + E_r(\rho)$. Bowen (2001) conjectured that $C(\rho) = S(\rho_B) - S(\rho) + \lg 3$ and showed this for $n \leq 3$.

6.5 Quantum authentication protocols

Several quantum user identification protocols have already been suggested.

Authentication using entangled states as counterparts of secret keys

The protocol is due to Zhang et al. (2000). Here is the basic idea:

Alice and Bob share $2K$ Bell states $|\Phi^+\rangle$ and let a_i and b_i be particles of Alice and Bob for i-th of the shared Bell states.

Bob prepares K random qubits $|\phi_i\rangle$ using particles p_i and in i-th round he sends particle p_i to Alice. Alice applies XOR with a_i as the control bit and p_i as the target bit and then sends the particle p_i back to Bob. Finally, Bob applies XOR with b_i as the control bit and p_i as the target bit and checks whether his particle is in the state $|\phi_i\rangle$. If yes, the authentication succeeded.

The above basic protocol has to be slightly modified in order to be secure with respect to possible attacks by an eavesdropper.

[15] In general dense coding over bipartite $n \times n$ quantum system Alice first performs one of the local unitary transformations (from a basis) U_i on her n-dimensional quantum system to transform the initially shared mixed state ρ in $\rho_i = (U_i \otimes I_n)\rho(U_i^* \otimes I_n)$, with a priori probability $p_i (i = 0, 1, \ldots, n^2 - 1)$, and then she sends her quantum system to Bob. On the compound system Bob then performs the measurement. Hiroshi (2000) determined in such a case capacity $C(\rho)$ of the quantum channel as $C(\rho) = S(\sum_{i=0}^{n^2-1} p_i \rho_i) - S(\rho)$.

Authentication using entanglement as catalyst The basic idea for one round of such a protocol is very simple.

Alice and Bob share a bipartite state $|c\rangle$ (catalyst) and Bob creates a state $|b\rangle$ such that there is no way to transform $|b\rangle$ into $|c\rangle$ using LQCC, but there is a way to transform $|b\rangle|c\rangle$ into $|c\rangle|c\rangle$ using LQCC.

Bob then sends to Alice one particle from the state $|b\rangle$ and work with her to transform $|b\rangle$ to $|c\rangle$. At the end Alice has to send the resulting particle to Bob who just checks whether his two particles, originally in the state $|b\rangle$, are indeed in the state $|c\rangle$.

6.6 Quantum public-key cryptography

An important new challenge for quantum cryptography is to develop quantum public-key cryptography, including quantum digital signature schemes.

One of the basic task is to explore the concept of **quantum one-way functions** and to show that for some specific functions there is a good evidence that they are quantum one-way functions.

Random permutation is expected to be a candidate for a quantum one-way function. The reason being is the proof that any quantum algorithm for inverting random permutation requires $\sqrt{2^n}$ steps.

The first attempt to come with a general approach to quantum public-key cryptography (QPKC) is due to Okamoto et al. (2000). They define the concepts of quantum one-way function, quantum public-key cryptosystem and quantum digital signature. Their definitions are natural generalizations of the classical ones. All variables and channels are classical and only instead of the probabilistic polynomial time Turing machines quantum polynomial time Turing machines are used to design the systems and to perform encryption, decryption, signing and signature verification.

They also suggest a particular QPCK, a modification of classical knapsack cryptosystem and the RSA cryptosystem. To design the cryptosystem QTM are used to compute discrete logarithms.

The above suggestions are interesting, but quite complex, and so it is still premature to judge its importance.

Another important new idea is that of **quantum digital signatures**, due to Gottesman nd Chuang (2001).

The basic idea is very simple. To use, as the quantum one-way functions f, the so called **fingerprints mappings**, that map strings w of length L into n-qubit states $|f(w)\rangle$, where L is much larger than n and $\langle f(w_1)|f(w_2)\rangle \leq \delta$ for all L bit strings w_1 and w_2 and small δ.

A digital signature protocol consists of two stages and it assumes that all parties involved know how to implement the mapping $w \rightarrow |f(w)\rangle$. All parties are also to know two numbers c_1 and c_2, thresholds for the acceptance and the rejection, used in the protocol.

We assume that Alice signs a message and there are t parties that could verify the signature. We show how to sign and verify the signature of one bit. Generalization to any binary message is then straightforward.

- **Key distribution stage.** The goals of this stage is that Alice creates and distributes quantum states that will act as her public key (they will be public in the sense that no special security is needed when they are distributed) and that participants check that keys are truly indistinguishable.

  The key distribution stage works as follows.
  - Alice creates M pairs of randomly and independently chosen pairs of L-bit strings $\{w_0^i, w_1^i\}$, $1 \leq i \leq M$.
  - Alice creates $2t$ copies of each pair of states $\{|f(w_0^i)\rangle, |f(w_1^i)\rangle\}$. These are her public keys and she sends them to the key distribution center.
  - Each of t participants downloads two copies of each pair $\{|f(w_0^i)\rangle, |f(w_1^i)\rangle\}$.(One copy will be used to verify the message and one copy to test for Alice cheating.)
  - For each value i all recipients verify, using a simple quantum "swap test", that they have received the same public keys.
- **Signing and verification of the signature.**
  - Alice sends the signed bit in the form $(b, w_b^1, w_b^2, \ldots, w_b^M)$, over a classical (insecure) channel. (By doing that Alice reveals half of her public keys.)
  - Each recipient of the signed message checks each of the public keys to verify whether $w_b^i \rightarrow |f(w_b^i)\rangle$. Let s_j be the number of incorrect keys of the recipient number j.
  - Recipient j accepts the message if $s_j \leq c_1 M$, and rejects the message if $s_j \geq c_2 M$. Otherwise, the action depends, for example, on the agreed strategy of all recipients.

Gottesman and Chuang (2001) have shown that the above scheme is secure against two scenarios of cheating.

- Only Alice is dishonest and her goal is to get recipients to disagree whether the signature is valid or not.
- Alice and one recipients are honest. Other recipients, or some third party, are dishonest, and they wish to convince Bob that a message $b' \neq b$ is valid.

One disadvantage of this approach is that the number of public key produced is limited by a security parameter.

Chapter 7 — Processors

page 285, after line -6

Remark Implementation of LMPZ code — of its encoding, decoding and error correcting circuits — has been recently accomplished by Knill et al. (2001) using nuclear magnetic resonance on a five spin subsystem of labeled crotonic acid. The ability to correct each error was verified by tomography of the process.

page 291, after line -5 A variety of other quantum codes have been recently developed.

Quantum BCH-codes (QBCH codes) have been introduced by Grassl et al. (1997), see also Steane (1998b). For a systematic presentation of QBCH codes and for extensive results on parameters of QBCH codes over various fields see Grassl and Beth (1999).

Grassl et al. (1999) introduced quantum version of the classical Reed-Solomon codes, see page 277. In addition, they show how to derive encoding and decoding quantum circuits based on the discrete cyclic Fourier transform over finite fields.

page 296, before Section 7.5

7.4.6 Quantum error detection

Similarly as in the case of classical codes, error detection is of importance also for quantum codes.

One of the main questions to explore is how the probability of undetected errors falls for the main types of quantum codes.

The problem how to define probability of undetected errors is not trivial in the case of quantum codes. Ashikhmin et al. (1999, 1999a) provide a definition which seems to be a good one because in the general case it is derived from natural physical assumptions and in the case of stabilizer codes it is analogous to the classical error detection definition. They show that formulas for average probability of undetected errors are in all cases (including the case that transmitted state is entangled with states of some other system), the same (up to a constant factor).

Ashikhmin et al. (1999a) also show the existence of a family of stabilizer codes for which the probability of undetected errors declines exponentially. They also established an upper bound on such a probability for all quantum codes.

0.0.3 7.4.7 Algorithmic aspects of encoding and decoding

Methods to design efficient encoding and decoding circuits for QECC are of large importance for the overall use of QECC. There has been significant progress in this area.

Cleve and Gottesman (1997) have developed a general method how to construct efficient encoding circuits for the stabilizers codes. Beth and Grassl (1998) showed a general method how to design decoding circuits for QECC and Grassl and Beth (1999) showed how to use quantum variant of one of the most efficient classical techniques for encoding and decoding, shift registers, for encoding and decoding quantum cyclic error-correcting codes.

page 303, at the end

Remark Boykin et al. (1999) have shown that the set of three gates: XOR, Hadamard gate and $R_{\frac{\pi}{4}}$ forms a universal fault-tolerant set of gates.

page 313, line +25 Add:

The most advanced experimental use of NMR technology has been recently reported by Steffen et al. (2001). On a 5-qubit quantum processors based on NMR they tested the main components of Shor's algorithm: modular exponentiation and QFT. The main global goal was to solve a generalization of Shor's algorithm, to solve the order finding problem for permutations of four elements.

As expository and pedagogical papers on liquid state NMR technology see Cory et al. (1998a) and Jones et al. (1998).

Remark 7.6.3 What has been termed above as NMR technology is sometimes considered only as a special implementation, by the use of organic molecules with the conventional NMR technology, of the so-called BSR (Bulk Spin Resonance) technology.

Remark 7.6.4 A large controversy has raised recently concerning the quantumness of the liquid state NMR technology. It has been first observed that none of the states used so far in NMR experiments is entangled. The point is that this technology for an n qubit register works with so-called pseudo-pure states of the form

$$\frac{1-\varepsilon}{2^n}I + \varepsilon|\phi\rangle\langle\phi|,$$

where $|\phi\rangle$ is a pure state (and for $|\phi\rangle = |0^{(n)}\rangle$ there is the initial state). This controversy has been recently overviewed and analyzed by Fitzgerald (2000). It is an open problem whether computers working with pseudo-pure states can be more powerful than classical computers.

page 314, line +3 Kane's proposal is sometimes also seen as a case of SRT (Spin Resonance Transistor) technology. For an other approach to SRT see Vrijen et al. (1999).

page 314, before "Moral"

7.6.6 Nonstandard models of quantum computation

An exploration of nonstandard models of quantum computation is, of course an important topic. Two such naturally to consider modes of computation are that of fermionic and bosonic computations. Recent results have shown that these two models of quantum computation have quite different computational power under reasonable conditions.

Perhaps no one expect that search for such new models of computation will lead to essentially more powerful models than the standard model of quantum computation (unless some surprises come from investigation of quantum gravity). In spite of that, these models are so much different that there deeper investigation can bring new insights also to "classical" quantum computing. For example, to get some new insights into quantum computational classes.

As shown by Knill et al. (2001), bosonic quantum computation with linear optics operators and partial detectors with feedback are sufficient to realize quantum computation.

The situation seems to be radically different concerning fermionic computations. It has been shown, in the papers discussed below, that fermionic linear optics computations are efficiently simulable by classical computers.

Quantum fermionic computation model was described in details and explored by Bravyi and Kitaev (2000). For example, they have found an exponentially faster simulation of fermionic gates and a set of universal fermionic gates.

Another interest in the fermionic quantum computation was inspired by the paper of Valiant (2001), that at first glance has absolutely nothing to do with fermionic computations. He has shown that circuits with certain special gates, the so-called *matchgates*, that look to be defined in a sophisticated way (but they do not include, for example, XOR gates), can be simulated in polynomial time on classical computers. More exactly, Valiant has shown that two-qubit operations characterized by 4×4 matrices in which the sixteen entries obey a set of five polynomial relations can be composed according certain rules to yield a class of circuits that can be simulated classically in polynomial time. (Actually, in Valiant constructions unitarity play no special role and therefore, in a sense, his circuits are more general than real quantum ones). Valiant saw his approach as the one that brings the quantum computational model within 'the realm of algebraic complexity theory in which computational gates are simulated by graph matching properties".

It was hard to imagine that this class of circuits could be of some significant importance. However, very surprisingly, Terhal and DiVincenzo (2001) have shown that circuits considered by Valiant correspond to a model of non-interacting fermions in one dimension. They have also shown that the possibility of having efficient simulation by classical computers can be extended to computation performed by noninteracting fermions with arbitrary pairwise interactions, "where gates can be conditioned on outcomes of complete von Neumann measurements in the computational basis on other fermionic modes in the circuit. Knill (2001) have shown in addition, that the set of states achievable with fermionic linear optics and particle measurements is the closure of a low dimensional Lie group. He has also shown that the two qubit matchgates and and matchcircuits introduced by Valiant generate a monoid of extended fermionic linear optics operators.

4. Josephson junctions (see Shnirman et al. (1998) and Averin (1998).
5. Due to the recent results by Gottesman and Chuang (1999), the current optical technology, which has been already used to implement almost perfectly basic computational primitives, seems to be another candidate technology that needs to be explored more for quantum information processing.

7.7 Basics of quantum fermionic and bosonic computations

If fermions are used as the carriers of quantum information, then we get a model of quantum computation that is, on one side, quite different from the Hilbert space model with the unitary operators, and, on the other side, quite similar.

Fock space

Quantum fermionic computation, more exactly quantum computation with local fermionic modes (LFM), is performed in the so called **Foch space**.

This space is at first glance quite different from Hilbert space, but actually relations are quite close.

Fock space of dimension 2, is the space with two basis states $\{|0\rangle, |1\rangle\}$, where $|1\rangle$ is interpreted as "fermion exists" and $|0\rangle$ is interpreted as "no fermion" (or vacuum). Two basis states $|1\rangle$ and $|0\rangle$ can be seen as being represented by column vectors $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$.

There are two basic operators and every action is represented using these two very simple (non-unitary) operators:

- Creation operator, $a^\dagger$, represented by the matrix $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ and
- Annihilation operator, a, represented by the matrix $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$.

The basic properties of these operators can be expressed as follows

$$a^\dagger|0\rangle = |1\rangle, \quad a^\dagger|1\rangle = 0,$$

(where the last zero is the number!)

$$a|0\rangle = 0, \quad a|1\rangle = |0\rangle.$$

We can consider the tensor products of m basic Fock spaces, or of m LFM, or sites, and consider binary vectors $m_1, m_2, \ldots, m_i$ with the interpretation that there is (there is not) a fermion in the site (or mode or position) i, if $m_i = 1$ ($m_i = 0$).

Important are also the following relations between the annihilation and creation operators, where indices refer to certain positions or the modes.

$$\{a_i, a_j\} = 0, \quad \{a_i^\dagger, a_j^\dagger\} = 0, \quad \{a_i^\dagger, a_j\} = \delta_{ij}.$$

As shown later there is a simple relation between the Fock space of m LFM and Hilbert space of m qubits.

Fock space of m sites can be seen as being spanned by basic binary vectors $|n_1, \ldots, n_{m-1}\rangle$.

Quite surprisingly, annihilation and creation operators act on these vectors, in a different way than one would expect. The key point is that order of sites really matter. Moreover, if operators $b_{i_1} b_{i_2} \ldots b_{i_k}$, where b is either the annihilation or the creation operator, are applied to some sites, then the natural order is that $i_1 \leq i_2 \leq \ldots \leq i_k$. (The order represents, in some sense, time.) Here are the basic rules for the annihilation operator a_j:

$$a_j|n_0, \ldots, n_{j-1}, 1, n_{j+1}, \ldots, n_{m-1}\rangle = (-1)^{\sum_{k=0}^{j-1} n_k}|n_0, \ldots, n_{j-1}, 0, n_{j+1}, \ldots, n_{m-1}\rangle$$

$$a_j|m_0, \ldots, n_{j-1}, 0, n_{j+1}, \ldots, n_{m-1}\rangle = 0$$

and, analogically, for the creation operator. The following example illustrate why is that so

$$a_2|1,0,1\rangle = a_2 a_0^\dagger a_2^\dagger|0,0,0\rangle = -a_0^\dagger a_2 a_2^\dagger|0,0,0\rangle = -a_0^\dagger a_2|0,0,1\rangle = -a_0^\dagger|0,0,0\rangle = -|1,0,0\rangle$$

Foch space F of m LFM splits into two subspaces $F = F_0 \oplus F_1$. One is generated by the basis vectors with even number of ones (fermions), the other one by basis vectors with odd number of ones (fermions).

Physical operators are those that preserve parity. The algebra of physical operators is spanned by products of even number of annihilation and creation operators.

More specifically, if $S \subset \{0, 1, \ldots, m-1\}$, then physical operators on sites from S are linear combinations of even products of operators $a_j, a_j^\dagger$, where $j \in S$. We could say that if an operator $a_j^\dagger$ applies to a state $|n_0, n_1, \ldots, n_{m-1}\rangle$, then all sites $0, \ldots, j$ are involved. We have therefore a special type of non-locality.

The occupation number n_j is an eigenvalue of the operator $a_j^\dagger a_j$. It can be measured locally, but it cannot be changed locally. . The concept of unitarity for operation is defined in a standard way. Bravyi and Kitaev have shown that the following set of operations is universal in acting on Fock space, if all values of β and γ are considered:

- $e^{i\beta a_j^\dagger a_j}$ (an action by an external potential).
- $e^{i\beta a_j^\dagger a_j a_k^\dagger a_k}$ (two particle interaction).
- $e^{i(\gamma a_k a_j + \gamma^* a_j^\dagger a_k^\dagger)}$ (an interaction with a superconductor).
- $e^{i(\gamma a_j^\dagger a_k + \gamma^* a_k^\dagger a_j)}$ (tunneling).

In spite of the fact that this set of operations can sound weird, it can derived, as discussed later, in quite a natural way.

Hilbert versus Fock space

Hilbert m qubits can be identified with Fock space of m fermion sites. For a state $|n_0, n_1, \ldots, n_{m-1}\rangle$ the measurement of n_j in the Fock space is the same as measurement of $\sigma_{z,j}$ in the Hilbert space.

A physical fermion operator corresponds to a qubit operator which preserves the parity, i.e. it commutes with $\prod_{j=0}^{m-1} \sigma_{z,j}$.

However, an application of a gate is different in the Foch space case than in the Hilbert case. The reason being is a peculiar rule an operator a_k or $a_k^\dagger$ applies to a state $|n_1, \ldots, n_{m-1}\rangle$, as discussed above.

Because of that if a gate applies to consecutive qubits (sites), then in both spaces it works in the same way. However, the difference, concerning sign, is in the case a gate is applied to not consecutive qubits (sites).

There is a way in qubit computations how to reduce the problem of applying a gate to non-consecutive qubits to that of the consecutive ones, by using the SWAP operator. However, in the case of Foch space the SWAP operator is expressed in a slightly different way. Fermionic SWAP, denoted here by SWAP is defined as the operator satisfying the identities:

$$\mathrm{FSWAP} \cdot a_0 \cdot \mathrm{FSWAP}^* = a_1 \qquad \mathrm{FSWAP} \cdot a_1 \cdot \mathrm{FSWAP}^* = a_0$$

and these equations have the following solution

$$\mathrm{FSWAP} == I - a_0^\dagger a_0 - a_1^\dagger a_1 + a_1^\dagger a_0 + a_0^\dagger a_1 = e^{i(\frac{\pi}{2}(a_0^\dagger - a_1^\dagger)(a_0 - a_1))}.$$

Hence FSWAP acts as follows:

$$\mathrm{FSWAP}|0,0\rangle \to |0,0\rangle, \quad \mathrm{FSWAP}|0,1\rangle \to |1,0\rangle$$
$$\mathrm{FSWAP}|1,0\rangle \to |0,1\rangle, \quad \mathrm{FSWAP}|1,1\rangle \to -|1,1\rangle$$

As a conclusion, fermionic gates are equivalent to parity preserving qubit gates modulo the so called "swap defect" operator D defined as follows:

$$D : |a,b\rangle \to (-1)^{ab}|a,b\rangle.$$

Consequently, in order to obtain a universal set of fermionic gates one needs only to find out a universal set of parity preserving qubit gates. As an example of such set of gates, due to Bravyi and Kitaev (2001) are gates:

$$\Lambda(e^{i\pi/4}), \quad \Lambda(\sigma_z), \quad \tilde{H}|a,b\rangle \to \frac{1}{\sqrt{2}}\sum_c (-1)^{bc}|a \oplus b \oplus c, c\rangle.$$

Bravyi and Kitaev (2001) have also shown that a fermion n-input gate can be simulated by n-qubit gate in $\mathcal{O}(\lg n)$ time and a qubit gate can be simulated by a fermion-circuit in constant time.

Miscellaneous

Of importance for Foch space computation and a relation between Hilbert space and Foch space are also the following operators

$$\sigma_{\pm} = \sigma_x \pm i\sigma_y$$

that relate to the annihilation and creation operators using the so-called Jordan-Wigner transformations as follows

$$\sigma_{j,+} = e^{i\pi\sum_{m=0}^{j-1} a_m^\dagger a_m} a_j^\dagger \quad \sigma_{j,-} = e^{i\pi\sum_{m=0}^{j-1} a_m^\dagger a_m} a_j.$$

Jordan-Wigner transformation therefore transforms the Pauli operators to creation and annihilation operators.

Exercise Express all Pauli operators using creation and annihilation operators only

0.1 Majorana fermions

If each fermionic mode, or site, is splitted, at least mathematically, into two halves, then these halves are called **Majorana fermions**.

By Bravyi and Kitaev (2001), since a single Majorana fermion can not interact with the environment by itself, so the decoherence can arise only from the environment-mediated interaction of two Majorana fermions. However, if we keep two halves of a qubit apart, the qubit has to be decoherence free.

The basic operators that operate on Majorana fermions are

$$c_{2k} = a_k + a_k^\dagger = \sigma_{x,k}\prod_{j=0}^{k-1}\sigma_{z,j}, \quad c_{2k+1} = \frac{a_k - a_k^\dagger}{i} = \sigma_{y,k}\prod_{j=0}^{k-1}\sigma_{z,j},$$

that satisfy the following commutation relation

$$c_j c_k + c_k c_j = 2\delta_{j,k}.$$

Using these operators one can get from a universal set of gates for fermionic computation a universal set of Majorana gates.

One such a universal set consists of the gates

$$e^{\pi/8c_0c_1}, e^{i\pi/4c_0c_1c_2c_3}$$

As observed by Bravyi and Kitaev (2001), some stabilizer codes can be described in terms of Majorana fermions.

Bosonic computations

In the case of bosonic computations, with non-interacting spin-less bosons, the basic computation space consists of a number of bosonic modes (sites), and each of them can be seen as the space spanned by infinitely many basis states $|i\rangle$, where $i \geq 0$ is an integer. (If all modes are in the state $|0\rangle$ such a state is called vacuum.) A basis state $|i\rangle$ represents i bosons. There are again two basic operators: creation and annihilation. However, in this case the following commutative (and not anticommutatives in the case of fermion) relations hold:

$$[a_i, a_j] = 0, \quad [a_i^\dagger, a_j^\dagger] = 0, \quad [a_i, a_j^\dagger] = \delta_{ij} I.$$

These operators are defined as follows:

$$a|i\rangle = \sqrt{i}|i-1\rangle \text{ if } i > 0$$
$$a|0\rangle = 0$$

$a^\dagger$ is Hermitian conjugate to a ($a^\dagger|i\rangle = \sqrt{i+1}|i+1\rangle$).

To represent qubits using bosonic modes requires mapping basic qubit states unitarily into several bosonic modes. A simple way of doing that is to encode qubits using two modes and one boson as follows:

$$|0\rangle \rightarrow |0\rangle|1\rangle, \quad |1\rangle \rightarrow |1\rangle|0\rangle$$

On the level of bosonic modes one can talk about entanglement, teleportation and so on.

For example, balanced beam splitter, whose Hamiltonian for modes 1 and 2 has the form $a_1 a_2^\dagger + a_1^\dagger a_2$ transforms two boson modes state $|1\rangle|1\rangle$ into the entangled state $\frac{1}{\sqrt{2}}(|2\rangle|0\rangle + |0\rangle|2\rangle)$ and the state $|0\rangle|1\rangle$into the state $\frac{1}{\sqrt{2}}(|1\rangle|0\rangle + |0\rangle|1\rangle)$.

7.8 Quantum computation with continuous variables

A radically new recent idea in quantum information processing is that of computation "over continuous variables" — see Lloyd and Braunstein (1999). The last term, quite a bit confusing for non-physicists, stays here for physical quantities, such a position, momentum or the amplitude of magnetic field, that can take on a continuum of possible values and also their observables have continuous spectrum of values.

It is far from clear that physical quantities with a continuum of possible values and a continuum of observables quantities, can be used to perform any discrete quantum computation and that this concept is not ill-defined.

It is also interesting to observe that the whole idea of quantum computation over continuous variables has developed in quite a different way than in the case of quantum computation over "discrete variables". It has been first shown by Braunstein and Kimble (1998) and Furusawa et al. (1998) that quantum teleportation over continuous variables is possible (and actually the first "100% teleportation" has been achieved that way (Bell measurements are more easy to implement in this case)). It has than been shown that also quantum error correcting codes over continuous variables are possible (see Braunstein, 1998). Next important step was done by Lloyd and Braunstein (1999). They have provided necessary and sufficient conditions for constructing "universal quantum computers" in the sense that it is able to perform quantum "floating point operations" on such variables. As an example they describe how such a quantum computer might be constructed for the amplitudes of electromagnetic field using such simple linear devices as beam splitter, phase shifter, squeezers and non-linear devices (as Kerr-effect fibers and atoms in optical cavities).

Nontriviality of the concept of such a quantum computer is connected with the fact that even a unitary operation over a single continuous variable requires in general an infinite number of parameters to define and therefore it cannot be in general approximated by a finite number of "basic continuous variable operations".

The way out is to consider the concept of a universal quantum computation over continuous variables for various subclasses of transformations. A set of continuous quantum operations is called universal for a set of transformations if it is possible to use a finite number of such operations to approximate arbitrarily closely any transformation in the set.

It is an open problem whether quantum computers over continuous variables could perform some computations asymptotically in a more efficient way than quantum computers over discrete variables.

7.9 Quantum Simulations

The developments in the area of quantum processors lead increasingly to beliefs that we may have (soon) quantum processors powerful enough to simulate interesting/important quantum phenomena.

In addition, it seems to be likely that in the long term such simulations can belong to the most important applications of quantum computers.

Of the growing importance seems to be therefore to characterize quantum processes and phenomena that can be efficiently and accurately simulated on quantum processors and how to make best use of quantum processors to do such simulations.

Of a special interest seems to be to find out, whether one can and how to simulate the evolution of quantum many-body systems and quantum field theories.

The existence of universal quantum simulators has been shown by Lloyd (19??).

At the practical level, quantum simulations may play important role in the development of new technologies.

At the very fundamental level, it is of importance to determine whether the recent unifying physical theories (for example M-theory which has been proposed as a unified description of all forces of Nature) can be efficiently simulated on quantum computers. Positive answers could have large impacts and so would have discoveries that such phenomena cannot be efficiently simulated even with quantum computers. This would imply that computational power of Nature is even larger than we suspect now.

Chapter 8 — Information

page 318, before Section 8.1.2 Holevo's χ-quantity

Of interest and importance is also the so called Holevo's χ-function, or Holevo's χ-quantity, introduced actually by Lebedev and Levitin (1964) and called by them *entropy defect*, defined for ensembles $\mathcal{E} = \bigoplus_{i=1}^{k}(p_i, \rho_i)$ as follows:

$$\chi(\mathcal{E}) = QS(\rho) - \sum_{i=1}^{k} p_i QS(\rho_i),$$

where $\rho = \sum_{i=1}^{k} p_i \rho_i$.

χ-quantity shows how much, on average, the system's entropy decreases if it becomes known in which subsystem ρ_i the system is and with which probability p_i. χ-quantity has several interesting properties: (1) (Levitin, 1996) $0 \leq \chi(\mathcal{E} \leq -\sum_{i=1}^{k} p_i \lg p_i$, with first inequality being equality iff all ρ_i are equal and second inequality becomes equality iff all density submatrices are orthogonal; that is $Tr\rho_i\rho_j = 0$ if $i \neq j$. (2) (Lindblad, 1975) If $\mathcal{E} = \bigoplus_{i=1}^{k}(p_i, \rho_i)$ is an ensemble and $\mathcal{F}$ is a completely positive trace-preserving mapping, then $\chi(\mathcal{F}(\mathcal{E})) \leq \chi(\mathcal{E})$, where $\mathcal{F}(\mathcal{E}) = \bigoplus_{i=1}^{k}(p_i, \mathcal{F}(\rho_i))$.

The related concept is that of Holevo capacity of a quantum channel $\mathcal{N}$ for transmitting classical information, defined by

$$\chi^*(\mathcal{N}) = \sup_{\pi,\rho} \left[QS(\sum \pi_i \mathcal{N}(\rho_i)) - \sum \pi_i QS(\mathcal{N}9\rho_i)) \right].$$

The well-known Holevo-Schumacher-Westmoreland theorem says that $\chi^*(\mathcal{N})$ is the best rate for transmission of classical information through the channel $\mathcal{N}$ when product states are used at the input.

This leads to the definition of so called *ultimate capacity of a quantum channel* for faithful transmission of quantum information (without prior entanglement) as

$$C_u(\mathcal{N}) = \lim_{n\rightarrow\infty} \frac{\chi^*(\mathcal{N}^{\otimes n})}{n}$$

The above limit exists because χ^* is superadditive, that is

$$\chi^*(\mathcal{N}_1 \otimes \mathcal{N}_2) \geq \chi^*(\mathcal{N}_1) + \chi^*(\mathcal{N}_2).$$

It is an open problem whether $C_u\mathcal{N} = \chi^*(\mathcal{N})$.

Another open problem is whether Holevo quantity is additive, that is whether $\chi^*(\mathcal{N}_1 \otimes \mathcal{N}_2) = \chi^*(\mathcal{N}_1) + \chi^*(\mathcal{N}_2)$ for all channels. Such an additivity would imply that ultimate and Holevo capacities coincide.

Additivity of Holevo quantity has been shown recently by King (2001) for the case one of the channels is so called **unital channel**, that is such channels $\mathcal{N}$ that $\mathcal{N}(I) = I$. As a consequence, for unital channels ultimate and Holevo capacities coincide.

In addition, additivity of Holevo capacity has been shown recently, by Shor (2002) also for the case one of the channels is so called **entanglement breaking channels**. They are channels which destroy entanglement with other system. More exactly, when the input state is entangled between the input space H_i and another Hilbert space H_a, then output of the channel is no longer entangled with H_a.

To entanglement-breaking channels belong the so called c-q channels and q-c-channels. Informally, c-q channels transform a classical (or classically taken) input into a quantum output and for q-c channels quantum state are transformed into classical. (More technically, a c-q channel can be expressed by the composition of a complete projection measurement and a completely-positive and trace preserving map. q-c channels are a composition of a completely positive trace preserving map with a projection measurement.

For the case that one of the channels is unital or entanglement breaking additivity has been shown also for minimum entropy output.

page 320, at the end of Section 8.1

Remark A different, and it seems that much more sound, approach to the definition of the conditional quantum entropy and quantum mutual information has been developed by L. B. Levitin (1999). Now we present the very basic ideas of his approach.

Let $\rho(A, B)$ be a density matrix of a compound quantum system $A \otimes B$.

The *conditional density matrix* (see Mityugov, 1976) of the system A, given that the result of a measurement β performed on the system B is b, is

$$\rho(A|\beta = b) = \frac{P_b\rho(A, B)P_b}{Tr_A\rho(A, B)P_b},$$

where the denominator is just the probability of β taking value b, at the measurement, observable, β. Hence

$$\sum_b (Tr_A \rho(A,B)P_b)\rho(A|\beta=b) = \rho(A).$$

In accordance with Shannon's definition of conditional entropy and the definition of quantum entropy, the conditional entropy of the system A, given the measurement β performed over B is defined by

$$QS(A|\beta) = -Tr_A\rho(A,B)P_b)\, Tr_A\rho(A|\beta=b)\lg\rho(A|\beta=b).$$

By so called Klein's Lemma, for arbitrary measurements α and β it holds $0 \leq QS(A|\beta) \leq S(\alpha|\beta)$. On this basis it is defined conditional quantum entropy

$$QS(A|B) = \inf_\beta QS(A|\beta).$$

It can be shown that from the above definition it follows

$$QS(A,B) \leq QS(B) + QS(A|B). \tag{3}$$

Example Of course, it is of interest and importance to know whether in the inequality we can have strict inequality and when such a case occurs.

The following example, due to Levitin (personal communication), shows such a case.

Let us consider the following density matrix of a bipartite system $A \otimes B$:

$$\rho = \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & \gamma \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \gamma^* & 0 & 0 & 1 \end{pmatrix},$$

where $0 \leq \gamma \leq 1$ (and $\gamma = 0$ means no entanglement - $|\gamma| = 1$ means maximal entanglement).

Since non-zero eigenvalues of the matrix ρ are $\frac{1\pm|\gamma|}{2}$, we have $QS(A,B) = h(\frac{1\pm|\gamma|}{2})$. Hence $0 \leq QS(A,B) \leq \lg 2$.

On the other hand $QS(A|B) = 0$, since the conditional density matrices are $\rho(A|\beta=0) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ and $\rho(A|\beta=1) = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$. However $\rho(B) = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, hence $QS(B) = \lg 2$. Therefore

$$QS(A,B) = h(\frac{1+|\gamma|}{2}) \leq QS(A|B) + QS(B) = \lg 2$$

and therefore the equality holds if and only if $\gamma = 0$.

More generally, the equality in holds only if all conditional density matrices in the basis β, where $QS(A|B) = QS(A|\beta)$ and the density matrix ρ commute.

Concerning *quantum mutual information* $QI(A : B)$, the basic standpoint is that for outcomes of the measurements α and β we have $I(\alpha : \beta) = S(\alpha) - S(\alpha|\beta)$. Quantum mutual information is then defined by

$$QI(A : B) = \sup_{\alpha,\beta} I(\alpha : \beta).$$

On this basis it can be shown that

$$QI(A : B) \leq QS(A) - QS(A|B).$$

Remark In addition to the Shannon approach to the definition of the (classical) information contents of an object x (as the number of bits needed to search for x in a universe), there has been developed also an approach based on Chaitin complexity (called also *self-delimiting Kolmogorov complexity*) of x — as the length of the shortest (self-delimiting) program[16] for a (reference) universal Turing machine, to generate x. This has lead to the development of the so-called *algorithmic information theory*, see Chaitin, 1987; Lee and Vitányi (1993) and also Gruska (1997). It is therefore natural to explore what would come out of a quantum version of the classical algorithmic information theory. This task has turned out not to be easy, for several reasons. For example, impossibility to copy quantum information and the fact that there are uncountably many quantum Turing machines and quantum states. This does not seem to allow to make a "straightforward quantumization" of Chaitin's algorithmic information theory as attempted first by Svozil (1996). A more worked out is the attempt of Vitányi (1999). He starts to explore two approaches to quantum Chaitin complexity. In the first approach, Chaitin complexity of a pure quantum state $|\psi\rangle$ is defined as the length of the shortest classical program (with respect to a reference universal quantum Turing machine $\mathcal{M}$) that generates or approximates $|\psi\rangle$ (in the case $\mathcal{M}$ cannot generate $|\psi\rangle$). The attempt to include such approximations makes the basic definition more complex. The second approach is through the length of the shortest qubit program generating $|\psi\rangle$.The invariance theorem, saying that the choice of the reference machines adds only a constant factor, holds for both approaches. More other technical

[16]This means that no program can be a prefix of another program.

results at Vitányi (1999) hold only for the first approach. (At the first approach, the quantum Chaitin complexity coincide with the classical case when restricted to the classical domain, it is upper bounded, it can be efficiently approximated from above and any quantum state is with high probability incompressible.)

Another attempt to come with a "proper" definition of the quantum Kolmogorov complexity is due to Berthiaume et al. (2000). They introduce several concepts of quantum Kolmogorov complexity $QK(|\phi\rangle)$ of a quantum register state (called quantum string) relative to a quantum universal Turing machine M as the length of the shortest "qubit string (state)" $|\psi\rangle$ which, given as input to M, makes M to generate $|\phi\rangle$ with sufficiently high fidelity – especially with fidelity$(\phi, M(\psi, 1^k)) \leq 1 - \frac{1}{k}$ (more exactly, Kolmogorov complexity of $|\phi\rangle$ is the smallest m such that there is an $|\psi\rangle \in H_{2^m}$ with the above property). For this concept of Kolmogorov complexity the following result have been shown: the invariance theorem, incompressibility of some strings, sub-additivity and complexity of copies of qubit strings.

In the classical case of a large importance is closely related *Minimal length description principle*, see Li and Vitányi (1993), to be used to derive a theory fitting at best a set of given (observable or experimental) data — the basic problem in many sciences. It is therefore also natural to ask whether we can develop a useful quantum version of it.

page 328, before Section 8.2.4 An important open problem is to find capacity of the noisy quantum channel, a quantum version of Shannon's noisy channel coding theorem.

A significant progress in this direction was achieved recently by Koashi and Imoto (2001).

It has been known that if we have an ensemble $\{(p_i, \rho_i)\}_{i=1}^n$ of mixed states, then the upper bound for the optimal compression rate I_p is $QS(\rho)$, where $\rho = \sum_{i=1}^n p_i\rho_i$, and so-called Holevo-Levitin lower bound is $QS(\rho) - \sum_{i=1}^n p_i SQ(\rho_i)$.

Koashi and Imoto (2001) have shown how to construct from the given ensemble $\{p_i, \rho_i\}_{i=1}^n$ another, so called reduced, ensemble $\{p_i, \sigma_i\}_{i=1}^n$, such that $I_p = QS(\sum_{i=1}^n p_i\sigma_i)$.

The protocol they use for encoding is so-called **blind protocol**. Alice gets for encoding a tensor product of states produced by the source, but not the identity of states. In such a case I_p is called **passive information**. In another scenario, Alice gets for encoding also the identity of states forming a tensor product a tensor product of the states to be compressed. Such protocols are called **visible protocols** and for them the compression rate could be better. This compression rate is not known and therefore the problem of compression rate for noisy channel has not been yet solved completely.

Reverse Shannon theorems

Shannon's noisy channel theorem establishes the ability of noisy classical channels to simulate classical noiseless channels.

Of interest and importance it seems also to explore also the reverse problem; simulation of noisy channels on noiseless channels.

Bennett et al. (2001) has shown that, surprisingly, that any classical noisy discrete memoryless channel of capacity C can be asymptotically simulated by C bits of noiseless forward communication, from the sender to a receiver, given a source R of random information shared beforehand between the sender and the receiver.

It is still an open question whether also quantum version of the reverse Shannon theorem holds in general. At QIP Shor reported on some partial results forward such a theorem.

Quantum reverse Shannon theorem conjecture can be restated as the conjecture that two quantum channels with the same quantum- entanglement assisted capacity can simulate each other with unit asymptotic efficiency.

From additivity of Holevo channel capacities to additivity of entanglement of formation

Matsumoto et al. (2002) have shown, using the Sprinstill dilation theorem that Holevo channel capacity can be expressed through entenglement of formation of states over some subspace. This formula can be used totransfer additivity results for capacities of certain channels to show additivity of entanglement of formation for certain states.

page 329, line +19 The bound presented in Theorem 8.2.19 has been improved by Nayak (1999) to $n \geq (1 - H(p))m$.

page 331, at the end A new type of quantum channel capacity has been introduced by Bennett et al. (1999a). Namely, **entanglement assisted**

classical capacity, C_E, to be defined as a quantum channel capacity for transmitting classical information with the help of pure entangled states (an unlimited amount of them) shared between sender and receiver.

The existence of superdense coding protocol, Section 6.4.4, implies that $C_E(\mathcal{N}) = 2C(\mathcal{N})$, for any noiseless quantum channel $\mathcal{N}$.

In the case of noisy quantum channels, surprisingly, $C_E(\mathcal{N})$ can be larger, comparing with $C(\mathcal{N})$, by an arbitrarily large constant factor — even in the case the channel $\mathcal{N}$ is so noisy that $QC_2(\mathcal{N}) = 0$.

By using a noisy quantum channel $\mathcal{N}$ in the superdense coding protocol one can obtain a lower bound on $C_E(\mathcal{N})$. On the other side, by using a noisy classical channel in the teleportation protocol to simulate a quantum channel $\mathcal{N}$ one can obtain an upper bound on $C_E(\mathcal{N})$. This helped to determine exactly $C_E(\mathcal{N})$ for d-dimensional de-polarizing and erasure channels, see updatings to page 332. $C_E(\mathcal{N})$ has also been determined exactly for so-called "Bell-diagonal channels" (that commute with superdense coding and teleportation, so that $Tp(Sd(\mathcal{N})) = \mathcal{N}$.

Exercise In an analogical way one can define **entanglement assisted quantum capacity**, QC_E, as the maximum rate for transmitting intact qubits with a help of borrowed entanglement and no classical communication. Determine $QC_E(\mathcal{N})$ for all channels $\mathcal{N}$.

Quite surprisingly, entanglement assisted quantum capacity seems to be the simplest to calculate. Bennett et al. (2001) have shown that QC_E of a noisy quantum channel is given by an expression similar to that for the capacity of purely classical channels: that is as the maximum, over channel inputs ρ, of the quantum entropy of the channel input plus the quantum entropy of the channel output minus their joint entropy (defined as the entropy of an entanglement purification of ρ, after half of it passed through the channel). They also calculated C_E for such channels as the amplitude dumping channels and bosonic channels.

In short $C_E(\mathcal{N}) = \max_\rho I(\rho, \mathcal{N})$, where $I(\rho, \mathcal{N})$ is so called mutual informationdefined below.

Bennett et al. (2001) also conjectured that entanglement sharing between communication parties so simplifies communication that only one parameter is needed to characterized such channels. Consequently, that if two entanglement assisted channels have the same capacity C_E, then they can mutually simulate each other with unit asymptotic efficiency.

Shor (2002) reported and Devetak (2003) has published the coding theorem for quantum capacity of quantum channels. Namely, that $Q(\mathcal{N}) = \max_\rho I_c(\rho, \mathcal{N})$, where I_c stands for accessible information, as defined below.

In the case a channel $\mathcal{N}$ has as an input a state ρ there are three entropic quantities associated with: $S(\rho)$, $S(\mathcal{N}(\rho))$ and so called **entropy exchange** $S(\rho, \mathcal{N})$ which is defined as follows:

Let $\mathcal{H}_A$ be the Hilbert space of ρ. According to a purification theorem in the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$, where $\mathcal{H}_B$ is a Hilbert space isomorphic to $\mathcal{H}$, there is a pure state $|\phi\rangle\langle\phi|$ such that $\rho = Tr_B|\phi\rangle\langle\phi|$. The entropy exchange is then defined by

$$S(\rho, \mathcal{N}) = S((\mathcal{N} \otimes I_B)(|\phi\rangle\langle\phi|)$$

that is as the entropy of the output state of the so called dilated channel $\mathcal{N} \otimes I_B$ applied to the input that is a purification of ρ. It can be shown that this definition does not depend on the choice of the purification of ρ.

Using the concept of entropy exchange we can define two new important entropic quantities:

Quantum mutual information is defined by

$$I(\rho, \mathcal{N}) = S(\rho) + S(\mathcal{N}(\rho)) - S(\rho, \mathcal{N})$$

Quantum mutual information is positive, concave with respect to ρ and additive for product channels. Moreover, its maximum with respect to ρ has nice operational meaning because, as discussed in Section **??**, it stands for so called entanglement assisted capacity of the channel.

Quantum accessible information is defined by

$$I_c(\rho, \mathcal{N}) = S(\mathcal{N}(\rho)) - S(\rho, \mathcal{N}).$$

Quantum accesible information is ??????. Its maximum with respect to ρ has also nice operational meaning because, as discussed in Section **??**, it stands for quantum capacity the channel.

page 332, at the end of Section 8.2.6 By Bennett et al. (1999a), d-dimensional de-polarizing channel $\mathcal{D}_p^d$ of de-polarization probability p is a channel that transmits a d-dimensional quantum state intact with probability $1-p$ and randomizes its state with probability p.

In the case of $\mathcal{D}_p^d$ it holds

$$C_E(\mathcal{D}_p^d) = 2\lg d - H_{d^2}(1 - p\frac{d^2-1}{d^2}),$$

where $H_x(q) = -q\lg q - (1-q)\lg\frac{1-p}{x-1}$.

So called **memory depolarizing channel**, with the parameter θ, is specified by the mapping $\rho \rightarrow \sum_{i=0}^{3} A_i\rho A_i^*$ where $A_0 = \frac{\sqrt{1+3\theta}}{2}I$ and $A_j = \frac{\sqrt{1-\theta}}{2}\sigma_j$ for $j = 1,2,3$. For a quantum d-dimensional erasure channel, $\mathcal{E}_p^d$ (which transmits its d-dimensional input state intact with probability $1-p$ and with probability p replace the input by a new unique state orthogonal to all input states) it holds $C_E(\mathcal{E}_p^d) = 2(1-p)\lg d$.

Of large importance are also **Pauli channels** defined by the superoperator $P(\rho) = \sum_{i=1}^{4} p_i\sigma_i\rho\sigma_i^*$, where σ_i are Pauli matrices, $\sigma_4 = I$ and $p_4 = 1 - p_1 - p_2 - p_3$. Bschorr et al. (2001) and Fischer et al. (2001) have shown a way how to estimate parameters p_i of an unknown Pauli channel. In addition, they have shown that these estimation can learn more efficiently parameters p_i if they estimate them with the help of maximally entangled states.

Another type of channels is **dephasing channel**. It is a channel that makes first measurement in standard basis and then resends the result of the measurement.

Amplitude dumping channel. It is a channel which sends states which decay with attenuation from $|1\rangle$ to $|0\rangle$, but which do not undergo any other noise. In other way, it is a channel represented by mapping

$$\mathcal{N} : \rho \rightarrow \sum_{i=1}^{2} A_j\rho A^*j,$$

where

$$A_1 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-p} \end{pmatrix} \text{ and } A_2 = \begin{pmatrix} 0 & \sqrt{p} \\ 0 & 0 \end{pmatrix}.$$

Phase dumping channel with parameter λ is defined by the mapping

$$\phi_\lambda(\rho) = \frac{1+\lambda}{2}\rho + \frac{1-\lambda}{2}\sigma_z\rho\sigma_z.$$

page 333, before Section 8.3.2 For majorization relation $X \prec Y$ between d-dimensional vectors, that play very important role in the theory of quantum state transformations, the following useful results hold, due to Marshall and Olin (1979), see also Daftaur and Klimesh (2001):

Theorem If X and Y are d-dimensional real vectors, then the following conditions are equivalent:

1. $X \prec Y$;
2. $\sum_{i=1}^{d} X_i = \sum_{i=1}^{d} Y_i$ and for all $l \in \{2, \ldots, d\}$ it holds $\sum_{i=l}^{d} X_i^{\downarrow} \geq \sum_{i=l}^{d} Y_i^{\downarrow}$;
3. $X = DY$ for some doubly stochastic d-dimensional matrix;
4. For every real number t, $\sum_{i=1}^{d} |X_i - t| \leq \sum_{i=1}^{d} \leq \sum_{i=1}^{d} |Y_i - t|$.

Nielsen's results concerning states transformations have been generalized and extended in several ways.

Bandyopathy et al. (2001) have shown that it may be the case that two state, $|\phi\rangle$ and $|\psi\rangle$ are incomparable (that is none of them can be transforms into another one by LQCC (that is with probability one), notation $|\phi\rangle \not\leftrightarrow |\psi\rangle$, but if several copies of these states are considered, then such a transformation is possible, even though this is not true for any two pairs $(|\phi\rangle, |\psi\rangle)$.

More formally, states $|\psi\rangle$ and $|\phi\rangle$ are called **k-copy LOCC incomparable** if $|\psi\rangle^{\otimes k+1}$ can be transformed into $|\phi\rangle^{\otimes k+1}$, but for $n \leq k$, $|\psi\rangle^{\otimes n} \not\leftrightarrow |\phi\rangle^{\otimes n}$. Bandyopathy et al. (2001) have shown that for any $k \geq 1$ there are incomparable states that are k-copy LOCC incomparable (and they shown a necessary condition for a given pair of states to be k-copy LOCC comparable.

For example, the following states are 5-copy LOCC incomparable

$$|\psi\rangle = \sqrt{0.4}|00\rangle + \sqrt{0.4}|11\rangle + \sqrt{0.1}|22\rangle + \sqrt{0.1}|33\rangle,$$

$$|\phi\rangle = \sqrt{0.48}|00\rangle + \sqrt{0.27}|11\rangle + \sqrt{0.25}|22\rangle.$$

Open problem Is it true that if $|\psi\rangle^{\otimes(k+1)} \rightarrow |\phi\rangle^{\otimes(k+1)}$ by LOCC, then $|\psi\rangle^{\otimes n} \rightarrow |\phi\rangle^{\otimes n}$ for all $n \geq k+2$.

They have also shown that there are pairs of states that are neither k-copy LOCC comparable for any k nor catalyzable for any k. Such pairs of states are called **strongly incomparable**. A sufficient condition is given for strong incomparability. This condition implies, for example that 3×3 incomparable states are always strongly incomparable.

Another important concept is that of **conclusive transformations** of one state to another, using SLOCC, that is with the probability greater than zero. This is related to the concept of entanglement monotones defined bellow.

Another generalization of Nielsen's results is due to Jonathan and Vedral (1999). The key concept is that of **entanglement monotones**. They are functions of quantum states (pure or mixed) that can, on average, never increase under LQCC. Entanglement monotones provide necessary conditions any local transformation on states has to satisfy.

Of importance are sets $\{\epsilon_i\}_i$ of entanglement monotones such that, if the average $\langle\epsilon_i(T(\rho)\rangle \leq \epsilon_i(\rho)$ for all i, then the transformation T is local.

An important minimal set (in the sense that none of the functions can be omitted) of entanglement monotones has been defined by Vidal (1999).

For a bipartite state $|\psi\rangle = \sum_{I=1}^{n} \sqrt{\alpha_i}|\phi_i\rangle|\psi_i\rangle$ the following set of functions constitutes a minimal set of quantum entanglement monotones.

$$E_l(|\Psi\rangle) = \sum_{i=l}^{n} \alpha_i, 1 \leq l \leq n.$$

Exercise Formulate Nielsen's theorem in the terms of the above set of entanglement monotones.

Using this set of entanglement monotones we can formulate necessary and sufficient condition for the most general transformation using LQCC on bipartite states.

Theorem Let two (distant) parties share a pure state $|\psi\rangle$ and let $\{|\theta_j\rangle\}_{j=1}^{m}$ be a set of pure bipartite states. Then a transformation T of $|\psi\rangle$ that outputs state $|\theta_j\rangle$ with probability p_j ($\sum_{j=1}^{m} p_j = 1$) can be realized using LQCC iff the above defined entanglement monotones do not increase on average, that is, iff

$$\sum_{j=1}^{m} p_j E_l(|\theta_j\rangle) \leq E_l(|\psi\rangle), \quad 1 \leq l \leq n.$$

This theorem provides a powerful tool to optimize local quantum transformations (according to a wide range of criteria) using methods of linear programming. One such application, for entanglement concentration is discussed on page 111.

Another related result due to Vidal (1999) concern the case that the source state with Schmidt decomposition $|\psi\rangle \sum_{i=1}^{n} \sqrt{\alpha_i}|i\rangle_A|i\rangle_B$ has at least as many non-zero Schmidt coefficients as the target state $|\phi\rangle = \sum i = 1^n \sqrt{\beta_i}|i\rangle_A|i\rangle_B$, (with sequences of α's and β's are non-increasing), then a conclusive transformation is possible with probability given by

$$Pr_{max}(|\psi\rangle \rightarrow |\phi\rangle) = \min 1 \leq l \leq n \frac{E_l(|\psi\rangle)}{E_l(|\phi\rangle)}.$$

Bandyopadhyay (2001) have shown that for some incomparable pairs, increasing the number of copies results in an exponential decrease in the conclusive transformation probability (i.e. $Pr_{max}(|\psi\rangle^{\otimes k} \rightarrow |\phi\rangle^{\otimes k}) \approx c^k$, $c < 1$, but for some states the optimal probability of a conclusive transformation need not be a monotonic function of the number of copies.

Several other results concerning equivalence of states with respect to some operations have been obtained:

- Two pure states can be obtained from each other with certainty by means of LOCC iff they are related by LU.
- Two bipartite pure states can be obtained from each other by SLOCC iff they have the same Schmidt number.
- Asymptotic equivalence under DLOCC – when allowing for small imperfections – allows to identify all pure bipartite entanglement with that of the EPR state.
- In three qubit systems, there are only two different equivalent classes of states that contain entangled states, so called $|W\rangle$-class and $|GHZ\rangle$-class, in case equivalence with respect to SLOCC is considered.

Transformations and equivalences of quantum operations

The problem when one quantum operation can simulate another one is of theoretical and practical importance.

For example, as pointed out by Dür and Cirac (2002), one entanglement purification scheme requires to use XOR operation that is not easy to implement. However, it can be shown that for entanglement purification it is actually sufficient a less hard to implement phase gate.

Definition A unitary operation U can simulate unitary operation $\bar{U}$ under a specific class of operations X, $U \rightarrow_X \bar{U}$, if the action of $\bar{U}$ on any input state ρ can be obtained using a sequence of operations of the kind X applied before and after a single application of U. Two such operations are equivalent under X if the two operations can simulate each other under the class of operations X.

A way to study equivalence of operators under a class of operators X, especially under SLOCC, is to assign to each operator U a state $|\psi_U\rangle$ (that is actually the state obtained by applying U to the tensor product of maximally entangled states of all parties) and then to transform the problem of operator transformations to the problem of state transformations.

For example, see Dür nd Cirac (2002), it holds that $U \rightarrow_{SLOCC} \bar{U}$ iff $|\psi_U\rangle \rightarrow_{SLOCC} |\psi_{\bar{U}}\rangle$(Dür (2001)).

Dür and Cirac (2002) showed that in the case of bipartite d-dimensional states there are at most d^2 equivalence classes of operators, but in the case of multipartite systems there are infinitely many equivalence classes.

Related problem is to determine what kind of entanglement can an operator generate from product states. For example it holds (Dür and Cirac (2002)):

Theorem Unitary operation U can generate a state $|\phi\rangle$ with non-zero probability of success iff $|\psi_U\rangle$ can be converted to $|\phi\rangle$ by means of SLOCC.

page 334, before line -8 The concept of the Werner state (introduced by Werner (1989)), has been recently generalized in several ways.

1. In the case of the tensor product of two n-dimensional Hilbert space, the generalization has the form

$$W_s = s|\Phi\rangle\langle\Phi| + \frac{1-s}{n}I,$$

where I is the identity matrix in H_{n^2} and $|\Phi\rangle = \frac{1}{\sqrt{n}}\sum_{i=0}^{n-1}|ii\rangle$.

2. In the d^n-dimensional Hilbert spaces $H = \bigoplus_{i=1}^{n} H_d$ generalization goes as follows:

$$W_s = (1-s)\frac{1}{d^n}I + s|\psi\rangle\langle\psi|,$$

where I is the identity matrix in H (and therefore $\frac{1}{d^n}I$ represents a completely random pure state in H) and $|\psi\rangle = \sum_{j=0}^{d-1}|j^{(n)}\rangle$, where $\{|0\rangle, \ldots, |d{-}1\rangle\}$ are basis vectors of the d-dimensional Hilbert space. This states find a variety of uses. A recent result due to Pittenger and Rubin (2000) says that the state W_s is fully separable as a a sum of tensor products of n density matrices of H_d if and only if $s \leq (1+d^{n-1})^{-1}$.

page 335, at the end

Practical entanglement purification

Since distribution of entangled states between distant parties seems to be of large importance for quantum communication protocols, such as quantum cryptography, quantum teleportation, ... and entanglement purification is the main way to distill highly entangled states with less entangled states or mixed states, it is of large interest to find practical entanglement purification techniques.

The techniques discussed in the book are based on the use of XOR or similar quantum gates — on tools that are far from easy to implement perfectly enough to be really useful for purification. An important task is therefore to look for other purification techniques.

One such a technique has been developed by Pan et al. (2000). This techniques requires to use only simple linear optical elements that have very high precision. It should lead to a procedure that is within the reach of current technology.

page 337, before Section 8.3.4 The Schmidt entanglement concentration method is asymptotically optimal, but requires to have many copies of the state. A different and practically important task is to perform optimal entanglement concentration for a single pure bipartite state.

Jonathan and Plenio (1999) found a way, using theorem on transformation of bipartite states from page 108, to solve the following entanglement concentration problem.

Alice and Bob share a pure bipartite state $|\psi\rangle$ with Schmidt decomposition

$$|\psi\rangle = \sum_{i=1}^{n} \sqrt{\alpha_i}|\phi_i\rangle|\psi_i\rangle,$$

whose entanglement they want to concentrate using LQCC. Consider the set of local transformations that generate the maximally entangled state $|\theta_j\rangle = \frac{1}{\sqrt{j}}\sum_{i=1}^{j}|\phi_i\rangle|\psi_i\rangle$, $1 \leq j \leq N$ with probability p_j. Since von Neumann reduced entropy of $|\theta_j\rangle$ is $\ln j$, for the average amount of distilled entanglement it holds $\langle E\rangle = \sum_{j=1}^{n} p_j \ln j$. The following theorem shows how this quantity can be maximized.

Theorem The optimal entanglement concentration procedure for a bipartite state $|\psi\rangle$ with $\alpha_1 \geq \alpha_2 \geq \ldots \geq \alpha_n > 0$ is one that produces the maximally entangled state $|\phi_j\rangle$ with probability $P_j = j(\alpha_j - \alpha_{j+1})$. The corresponding optimal average entanglement is then

$$\langle E\rangle_{max} = \sum_{j=1}^{n}(\alpha_j - \alpha - j + 1)j\ln j.$$

An interesting and important special case of the entanglement concentration problem is that of transforming a given tripartite state $|\phi\rangle$ of $H_2 \otimes H_2 \otimes H_2$ into the GHZ state $\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$. A way to do that, using local operations, that works always if such a transformation is possible, has been presented by Cen and Wang (2000).

Shor (2003) has shown that conjecture on additivity of of entanglement of formation is equivalent with other well known additivity conjectures, for example with additivity of so called Holevo quantity, strong superadditivity of entanglement of formation and additivity of minimum entropy output of quantum channels.

Deterministic entanglement concentration

The above method of entanglement concentration are probabilistic. They produce the outcome only with a certain probability. Moreover, they use collective operations on the set of states entanglement of which is to be concentrated.

A simple, elegant and deterministic method of entanglement concentrations of the states of the form

$$|\psi_i\rangle = \sqrt{a_i}|00\rangle + \sqrt{1-a_i}|11\rangle,$$

where $\frac{1}{2} < a_i < 1$ and $i = 1, 2, \ldots, n$ is due to Morikosi and Koashi (2001). This method allows to extract from such a set of states $k = \lceil -\lg(a_1 \ldots a_n) \rceil$ Bell states $|\Phi^+\rangle$.

The basic idea is very simple. On the basis of the Nelson theorem one can see easily that from two states $|\psi_1\rangle$ and $|\psi_2\rangle$ one can obtain

- if $\frac{1}{4} < a_1a_2 \leq \frac{1}{2}$, then the Bell state $|\Phi^+\rangle$ and the state $\sqrt{2a_1a_2}|00\rangle + \sqrt{1-2a_1a_2}|11\rangle$;
- if $\frac{1}{2} < a_1a_2 < 1$, then the state $\sqrt{a_1a_2}|00\rangle + \sqrt{1-a_1a_2}|11\rangle$ and the product state $|00\rangle$.

In the first case one Bell state is obtained and one partially entangled state. In the second case one new, more entangled, state is obtained.

On the basis of the above method of concentration of entanglement for two states a simple, tournament like, method of entanglement concentration for the whole set of states $|\psi_i\rangle$ is derived.

At the very beginning, let us see the whole set of states $|\psi_i\rangle$ as the *pool* of states the entanglement of which is to concentrate. Then, in a recursive process, in each step, two states are (arbitrarily) taken from the pool and the above mentioned procedure of entanglement concentration is applied. In case one Bell state is produced, this state is taken to the output. In any case, the partially entangled state that results from the process is put back to the pool. In such a way, after each step, the pool get decreased by one state.

General entanglement purification

Entanglement concentration and purification have classical analogues as pointed out by Ambainis and Yang (2001). The case that parties share copies of the same state corresponds to the classical problem of generating perfect random bits from the sequence of i.i.d. biased coin flips. Extraction of entanglement from a single copy of a known state corresponds to constructing uniform (almost uniform) random bits from a biased distribution if we know a complete description of the distribution.

A practically important and theoretically interesting problem is then to determine how much purification, and when, can be done if we have only one mixed state to purify and only local quantum operations can be used. In other words, what is the power of local purification schemes?

There are again two cases to consider:

- A complete description of to-be-purified state is known.
- No complete description of a to-be-purified state is known, only some information about its distance from maximally entangled states.

Ambainis and Yang (2001) explored the case of the entanglement of a bipartite mixed state ρ in the case that purification parties know only a lower bound on the fidelity of ρ and a maximally entangled state. In this case one cannot use methods developed for the other cases. They developed several **general entanglement purification protocols (GEPP)** working in polynomial time. Actually, they have considered development of GEPP of three types:

- **Absolutely successful GEPP** that never fail and and always output a state of very high fidelity.
- **Deterministically conditional successful GEPP** that fail with small probability, but if they do not fail they produce with certainty a state with high fidelity.
- **Probabilistic conditionally successful** that fail with small probability, but if they do not fail they produce with high probability a state with high fidelity.

Ambainis and Yang (2001) have shown:

- There are no "interesting absolutely successful" GEPP. Each of them can bring only very small increase in fidelity.
- There exist deterministically conditionally successful GEPP for states in the diagonal subspace (spanned by states of the form $\sum_i \alpha_i|i\rangle|i\rangle$). Namely, they are protocols that for an input state of fidelity $1-\varepsilon$ fail with probability less than ε, and when they do not fail they output a state of fidelity $1-\frac{\varepsilon}{L}$, where L is a parameter that can be made very large.
- There exist probabilistically conditionally successful GEPP for arbitrary states.

In their constructions Ambainis and Yang (2001) make an essential use of so called **scrambling procedures**. They are closely related to universal hash functions that play so important role in classical processes of extracting randomness.

page 337, add to line -2 Ullman (1997) have shown that every bipartite density matrix can be decomposed optimally into a mixed state – that is into the one that yields entanglement of formation for ρ, with at least $Rank(\rho)$ and at most $Rank^2(\rho)$ different pure states, where $Rank(\rho)$ is the rank of the matrix ρ. (Terhal et al. (1999),have shown two examples of separable bipartite density matrices ρ for which the length of optimal decomposition of ρ is larger than $Rank(\rho)$.)

page 338, after line +19

Remark The following properties, at which ρ and σ are density matrices of a bipartite Hilbert space $A \otimes B$ and $QS(\rho||\sigma) = Tr\sigma \lg \sigma - \sigma \lg \rho)$ is **relative entropy**, of the entanglement of relative entropy are of interest/importance (see Plenio et al., 2000).

- $E_r(\sigma) \geq \max\{QS(\sigma_A - QS(\sigma), QS(\sigma_B) - QS(\sigma\});$
- $E_r(\sigma) \geq E_f(\sigma) - QS(\sigma);$
- For pure states $|\psi\rangle \in A \otimes B$ and $\rho = |\psi\rangle\langle\psi|$, $E_r(\rho) = QS(\rho_A)$.
- If $E_r(\sigma) = QS(\sigma_A) - QS(\sigma)$ and $E_r(\rho) = QS(\rho_A) - QS(\rho)$, then $E_r(\rho \otimes \sigma) = E_r(\rho) + E_r(\sigma)$.

To prove the above properties the following inequality, due to Plenio et al. (2000) has been used:

$$QS(\sigma_A) - QS(\sigma) \leq QS(\sigma||\rho) - QS(\sigma_A||\rho_A).$$

page 338, end of Section 8.3.4 The problem of finding "proper axioms" for good measures of entanglement is a hot current research subject. There are several other, incompatible, proposals for such axioms, than those presented on page 338. For example in Bennett et al. (1999): (a) $E(\rho) = 0$ if ρ is separable; (b) invariance under local unitary operations; (c) the expectation of entanglement should not increase under LQCC; (d) additivity: $E(|\phi\rangle \otimes |\psi\rangle) = E(|\phi\rangle) + E(|\psi\rangle)$, for the case that $|\phi\rangle$ and $|\psi\rangle$ are independent bipartite states; (e) stability with respect to a transfer of a subsystem from one party to another. (In any tripartite state $|\psi\rangle$ of a system $A \otimes B \otimes C$ the bipartite entanglement of $A \otimes B$

with C should differ from that of A with $B \otimes C$ by at most the entropy of B.)

Horodeckis et al. (1999) discuss the problem of axioms for a proper measure of en entanglement in detail, and show that the inequality

$$E_d(\rho) \leq E(\rho) \leq E_t(\rho),$$

where E_t is the total entanglement, see these *Additions*, page 339, called also by Horodeckis et al. (1999) as (a regularized version of) the entanglement of formation, holds for all measures of entanglement satisfying the following set of axioms: (a) non-negativity, $E(\rho) \geq 0$; (b) $E(\rho) = 0$ if ρ is separable; (c) normalization: $E(|\Phi^+\rangle\langle\Phi^+|) = 1$; (d) monotonicity under local operations — if either of the parties sharing a pair of particles in the state ρ performs an operation leading to a state ρ_i with probability p_i, then $E(\rho) \geq \sum_i p_i E(\rho_i)$; (e) convexity: $E(\sum_i p_i \rho_i) \leq \sum_i p_i E(\rho_i)$; (f) partial additivity: $E(\rho^{\otimes n}) = nE(\rho)$; (f) continuity: if $\lim_{n\to\infty}\langle\Phi^{+\otimes n}|\rho_n|\Phi^{+\otimes n}\rangle = 0$, then also $\lim_{n\to\infty}\frac{1}{n}[E(\Phi^{+\otimes n}) - E(\rho_n)] = 0$, where ρ_n is some joint state of n pairs.

Their underlying thesis is that the entanglement of distillation is a good measure of entanglement (and therefore there is no "iff" in the axiom (b) — because the bound entanglement is not distillable).

Recently a slightly new set of axioms for measures of entanglement E, and their various modification have been formulated by Donald et al. (2001).

Let ρ and σ be states of a bipartite system $A \otimes B$. E should satisfy (most of) the following conditions:

Separability: $E(\rho) = 0$ if ρ is separable.

Normalization: $E(\rho) = 1$ if ρ is a Bell state.

Monotonicity: $E(\Lambda(\rho)) \leq E(\rho)$ if Λ is a LQCC.

Continuity: Let $\{A_i\}_i$ and $\{B\}_i$ be a sequence of Hilbert spaces and ρ_i, σ_i are density matrices of Hilbert spaces $A_i \otimes B_i$ such that $||\rho_i - \sigma_i||_1 \to 0$, then

$$\frac{E(\rho_i) - E(\sigma_i)}{1 + \lg\dim(A_i \otimes B_i)} \to 0.$$

Additivity: $E(\rho^{\otimes n}) = nE(\rho)$.

Subadditivity: $E(\rho \otimes \sigma) \leq E(\rho) + E(\sigma)$.

Regularization: The following limit exists.

$$E^{\infty}(\rho) = \lim_{n\to\infty} \frac{E(\rho^{\otimes n})}{n}.$$

Convexity: $E(\lambda\rho + (1-\lambda)\sigma) \leq \lambda E(\rho) + (1-\lambda)E(\sigma)$ for all $0 \leq \lambda \leq 1$.

Donald et al. (2001) show impact of the various modifications of the above set of axioms. They also show various dependencies among the above axioms.

They also showed the so called **uniqueness theorem** that an entanglement measure is identical with reduced von Neumann entropy on pure states if and only if it satisfies the first five axioms from the above set of axioms.

Tangle, concurrence and negativity

labelconcurrency In the case of two-qubit systems three closely related and not very intuitive measures of entanglement have turned out to be very useful for getting strong technical results. The main one is concurrence introduced by Hill and Wooters (1997).

Let ρ be a density matrix of two qubit systems and let $\tilde{\rho} = (\sigma_y \otimes \sigma_y)\rho^*(\sigma_y \otimes \sigma_y)$, where asterisk denotes complex conjugation in the standard basis and σ_y is Pauli matrix expressed in the same basis. Product $\rho\rho^*$ is not a Hermitian matrix, but it has only positive eigenvalues and let their square roots, in decreasing order, be λ_1, λ_2, λ_3 and λ_4. Then the *tangle* of ρ is defined by formula

$$\tau(\rho) = [\max\{\lambda_1 - \lambda_2 - \lambda_3 - \lambda_4, 0\}]^2.$$

If ρ is a pure state, then $\tau(\rho) = 4\det(\rho_A)$. $\tau(\rho) = 0$ if ρ is unentangled and $\tau(\rho) = 1$ if ρ is maximally entangled.

In the case ρ is a density matrix of the tensor product of three Hilbert space of dimension 2, $H = A \times B \times C$ it holds $\tau(\rho_{AB}) \leq 2(det(\rho_A) + det(\rho_B) - det(\rho_C))$.

One of the main use of this measure of entanglement is that it can help to express in a closed formula entanglement of formation of two qubit states, due to Wooters (1997). Indeed, $E_f(\rho) = H(\frac{1}{2}(1 + \sqrt{1-\tau(\rho)}))$.

Concurrence of ρ is then defined by $C(\rho) = \sqrt{\tau(\rho)})$.[17] Concurrence satisfies axioms measures of entanglement should satisfy.

Another interesting application of concurrence has been shown by Abouraddy et al. (2001). For each bi-partite state $|\phi\rangle$ of two qubits there is a unique coefficient p such that $|\phi\rangle = p|\psi_e\rangle + \sqrt{1-p^2 e^{i\alpha}}|psi_f\rangle$, where $|\psi_i\rangle$ is a maximally entangled state and $|\psi_e\rangle$ is a factorisable state orthogonal to $|\psi_e\rangle$. Namely, $p = \sqrt{C(|\psi\rangle)}$. Decomposition is not unique in terms of $|\psi_e\rangle$ and $|\psi_f\rangle$.

As pointed out by Abouraddy (1991), it has been shown by Gisin (1991), that in terms of concurrence, namely as $2\sqrt{1 + C(|\psi\rangle)^2}$, one can express the maximal violation of CHSH inequality for any bipartite two-qubit state $|\psi\rangle$.

Definition of the *negativity* of a density matrix is motivated by Peres' transposition criterion as

$$E_n(\rho) = \max\{0, -2\lambda_1(\rho^T),\}$$

where $\lambda_1(\rho^T)$ denotes the smallest eigenvalue of the matrix ρ^T.

It has been shown by Horodeckis (1996) that negativity and concurrence measures are equal on pure states. Audenaert et al. (2000) showed that concurrence is never smaller than negativity and they also characterize those states for which concurrence and negativity have the same value and also when the difference is maximal.

A related measures of entanglement is the so-called **logarithmic negativity** ????? (????), E_{ln}. For a density matrix ρ of a bipartite system $A \otimes B$,

$$E_{ln}(\rho) = \lg Tr|\rho^{T_A}| = \lg Tr|\rho^{T_B}|$$

(the logarithm of the sum of the absolute values of eigenvalues of transpositions of ρ with respect to one of the other subsystems.) The logarithmic negativity has the following properties:

- $E_{ln}(\rho) = 0$ if ρ is disentangled
- $E_d(\rho) \leq E_{ln}(\rho)$ for any density matrix ρ.
- If $E_{ln}(\rho) = 0$, then either ρ is not entangled or it is bound entangled.
- $E_{ln}(\rho) \neq 0$, then it can be the case that $E_d(\rho) = 0$.

[17] For pure states $|\phi\rangle$, it holds that $C(\phi) = |\langle\phi|\sigma_y \otimes \sigma_y|\phi^*\rangle|$ or $C(|\phi\rangle) = |\sum_{i=1}^{r} \mu_i^2|$, where μ_i are amplitudes when $|\phi\rangle$ is expressed in the magic basis.

- Logarithmic negativity is additive as a measure of entanglement.

Concurrence as a measure of entanglement keeps playing increasingly important role in various considerations concerning entanglement. It is therefore natural that there have been attempts to generalize it to bipartite systems of arbitrary dimension d and to multipartite systems.

A natural problem is how to determine experimentally concurrence and negativity of unknown quantum state.

One way would be to use "quantum tomography" and to use several copies of a given state to determine the unknown state and then compute both concurrence and negativity. A natural question is whether there is a more efficient way to proceed. P. Horodecki (2001) has shown that, indeed, there is a more efficient way, a square root improvement in comparison with a brute force approach. Namely, he has shown that in the case of qubits there is a way to estimate only 7 parameters using a collective measurement of not more than 20 copies of an unknown state.

Rungta et al. (2001) noticed that Wooters' concurrence is defined using so called "spin-flip superoperator" and generalized that to an "universal inventor" that acts on systems of any dimension. Spin-flip superoperator maps qubit density matrix in Bloch notation $\rho = \frac{1}{2}(I + \bar{r} \circ \bar{\sigma})$ into $\frac{1}{2}(I - \bar{r} \circ \bar{\sigma})$. Generalized in this way, concurrence measures entanglement of pure bipartite states in terms of the purity of their reduced density matrices.

Badziag et al. (2001) go in a different way. They argue that in the case of bipartite qudit systems concurrence should have multidimensional characterization, not by a single number, and that such a characterization should describe not only the amount of entanglement, but also its structure, for example dimensions of two subsystems, ...

Schmidt number

Let ρ be a density matrix of a bipartite system. Let us consider all possible decompositions of ρ in the terms of pure states. Namely,

$$\rho = \sum_i p_i |\phi_i^{r_i}\rangle\langle\phi_i^{r_i}|,$$

where r_i denotes the Schmidt rank of $|\phi_i\rangle$. The **Schmidt number** of ρ, $k = \min\{r_{max}\}$, where r_{max} is the maximum Schmidt rank within a decomposition, and the minimum is taken over all decompositions (see Terhal and Horodecki, 2000).

It has been shown that Schmidt number is non-increasing under LQCC (and it is therefore an entanglement monotone). In some sense it gives an information about the minimum number of the degrees of freedom which are entangled between both parties.

Entangled states can be therefore classified with respect to their Schmidt number. If we denote S_k the set of states with Schmidt number at most k, then it holds

$$S_1 \subset S_2 \subset S_3 \ldots.$$

Also for Schmidt classes S_k Sanpera et al. (2001) defined also the concept of entanglement witness. it is again an Hermitian operator W_k such that $Tr(W_k\rho) < 0$ for some $\rho \in S_k$ and $Tr(W_k\rho) \geq 0$ for all $\rho \in S_{k-1}$. Sanpera et al. (2001) developed methods how to design and optimize entanglement witnesses for Schmidt classes.

page 339, add at the end of Section 8.3.5 The discovery of the bound entanglement has been a surprise and initiated an intensive study of this phenomenon (in spite of the fact that nobody has been, till recently, really able to show that bound entanglement is useful), that has lead to several interesting concepts and results, especially in connection with the task to determine whether a state given by its density matrix has bound entanglement and how to construct such states.

It has been first shown by Horodecki et al. (1998) that if a density matrix ρ of $H_n \otimes H_m$ remains positive semidefinite under the partial transpose mapping, i.e. if $(I_n \otimes T_m)(\rho) \geq 0$, where T_m is a matrix transpose on H_m, then ρ is bound entangled.

The following interesting concept of an unextendible product basis (a basis of a Hilbert space $H = \bigotimes_{i-1}^{m} H_i$, all states of each are tensor products of states from all H_j) play an important role at the design of bound entangled states (as pointed out by DiVincenzo et al. (1998a)).

Definition *An unextendible product basis (UPB) of H is such an orthonormal set S of product states from H that the subspace H_S generated by S is a proper subspace of H and the orthogonal complement of H_S contains no product state. (An example of an unextendible product basis of $H_3 \otimes H_3$ is shown in Exercise 2.1.23.)*

Theorem (DiVincenzo et al. 1999) Let $S = \{|\phi_j\rangle\}_{j=1}^{n}$ be an unextendible product basis of H, then

1. $m \geq \sum_{i=1}^{n}(dim(H_i) - 1) + 1$.

2. The following density matrix is bound entangled:

$$\rho = \frac{1}{dim(H) - m}(I - \sum_{j=1}^{m} |\phi_j\rangle\langle\phi_j|).$$

Using the concepts of UPB DiVincenzo et al. (1999) were able to construct a family of states with bound entanglement (so called bound-entanglement states) that depends on 6 parameters (the original construction by Horodecki's family was one-parametric). Another construction of a family of bound-entanglement states with 7 parameters is due to Bruß and Peres (1999).

The goal of attempt to find explicit constructions of bound-entangled states is to help to elucidate properties of such states.

A simple bound-entangled state in $H_2 \otimes H_2 \otimes H_2 \otimes H_2$ was discovered by Smolin (2000). It is the state (let us call it Smolin's state),

$$\frac{1}{4}\sum_{i=1}^{r} |\Phi_i\rangle\langle\Phi_i|,$$

where $\Phi_i, i = 1, 2, 3, 4$ are all Bell states. The above state is bound-entangled if the corresponding particles are possessed by four non-cooperating parties (parties in "different labs") — in such a case the parties cannot distill from it Bell states. However, if we denote parties as A, B, C, D then the above state is $AB : CD$, $AC : BD$ and $AD : BC$ separable. This is an example of so-called "unlockable-state" that can be used for two of the parties to distill a Bell state provided the other two parties assist them (by performing first certain measurements on their particles).

An interesting, important and puzzling question remains whether one can make some use of bound-entangled states. In other words whether there are tasks that can be performed better with bound-entangled states than with just classically correlated states.

The first natural question is whether bound-entangled states can be of some use for quantum teleportation. Of course, they are not usable for perfect teleportation because one cannot distill form them maximally entangled pure states. In addition, Linden and Popescu (1998) have shown that with some bound-entangled states teleportation cannot be achieved with better than classical fidelity.

The first example of some use of bound-entangled states was demonstrated by Murao and Vedral (2000). They demonstrated how bound-entanglement can be used for **remote information concentration** — the reverse process to quantum teleclonning, see page 80.

In the information concentration scheme there are four parties, Alice, Bob, Charles and David and they share four particles in Smolin's state. The particles of Alice, Bob and Charles represent their input-port qubits and that of David the output-port qubit. Bob and Charles posses perfect clones of an unknown qubit state $|\phi\rangle$. At the end of the remote information concentration scheme David's particle gets into the state $|\phi\rangle$. In the protocol Alice, Bob and Charles first perform Bell measurement between their ancilla or optimal clones and their particles of the Smolin state. They communicate results of their measurement to David (who gets in total 6 bits), who then performs a product (determined uniquely by six communicated bits) of Pauli matrices on his particle to get the state $|\phi\rangle$.

Various interesting properties of bound entangled states have already been discovered.

- A BE-state remains bound entangled when subjected to LOCC.
- There is no BE-state of two qubits.
- Each PPT-state is bound entangled (or separable) and it is an open problem whether there are also BE-states that are NPT-states.
- There are multipartite BE-states that violate a multipartite Bell inequality
- Some BE-states cannot be described by a LHV theory.

Various hypothesis have emerged concerning BE-states. For example:

- BE-states exhibit non-standard (non-exponential) decay of entanglement;
- BE-states in $H_3 \otimes H_3$ have Schmidt number 2; (Sanpera et al. 2000).

Activated bound entangled states

BE-states can be *activated* (Horodeckis, 1998b) and *super-activated* (Shor et al., 2000).

Activation of bound entanglement, or the so called *quasi-distillation*, refers to the process in which a finite number of free entangled mixed states are distilled with the assistance of a large number of BE-states, but without such an assistance no useful entanglement can be distilled from these states. Or it refers to the case some BE-states can enable, with the help of some other entangled states, to carry out some tasks which could not be performed by using only these entangled states and LOCC. In a super-activation two BE-states are combined (tensored) to get a state which is not bound entangled – in other words, in this case BE-states are activated by BE-states — and therefore it can be distilled. Several examples of activation are discussed by Dürr and Cirac (2000).

- There is a three-partite bound entangled state in $A \otimes B \otimes C$ that is $AC : B$-separable, $A : BC$-separable, but not $AB : C$ separable. This implies hat neither parties A and B, nor parties A and C, nor parties B and C can alone distill some maximally entangled state.
- For any n and $1 \leq j < n$ there is a state $|\psi_{n,j}\rangle$ such that this state is distillable iff parties form two groups - one with j members and the other one with $n - j$ parties (and it does not matter which parties are in which group).
- For any n and any subset S of $|\{1, \dots, n\}$ there is a state $|\psi_{n,S}\rangle$ that is distillable iff parties with indices in S get together and all other parties also get together.
- For any n there is a state $|\phi_n\rangle$ such that once any $n - 2$ parties get together, then the remaining two parties van distill some maximally entangled state using LOCC.

On the other hand, Horodeckis (1998) have shown that bound entangled states cannot be distilled into pure entangled states even with the help of other pure entangled states as catalysts.

8.3.6 Irreversibility of entanglement formation and distillation

Vidal and Cirac (2001) have shown another surprising result, namely that irreversibility of the process of formation and distillation (in the limit case) of bipartite states is not limited to bound-entangled states.

In other words they have shown that there is a state that is distillable, but the amount of entanglement one can distill out of it is less than the amount of entanglement needed to form this state.o

On a more technical level if $E_d(\rho)$ quantifies the amount of entanglement one can distill, in limit, from the mixed state ρ, and if $E_C(\rho)$ denotes the amount of entanglement needed, in limit, to create ρ, then there is a state ρ such that $E_C(\rho) > E_D(\rho) > 0$.

In particular, they have shown that for the state $\rho(p)$ defined bellow with a parameter $p \in [0, 1]$, that $E_C(\rho(0.0015)) - E_D(\rho(0.0015)) > 0.003$.

One-parameter set of states mentioned above has the form

$$\rho(p) = (1 - p)\rho_b + |\psi\rangle\langle\psi|,$$

where $\rho_b = \Pi_b/4$ is the PPT state where Π_b is the projector to the 4-dimensional space (without product states) orthogonal to the space generated by the product states (with some amplitudes omitted): $|0\rangle \otimes (|0\rangle + |1\rangle)$, $(|0\rangle + |1\rangle) \otimes |2\rangle$, $|2\rangle \otimes (|1\rangle + |2\rangle)$, $(|1\rangle + |2\rangle) \otimes |0\rangle$, $(|0\rangle - |1\rangle + |2\rangle) \otimes (|0\rangle - |1\rangle + 2\rangle)$ and $|\psi\rangle = \frac{1}{\sqrt{6}}(|00\rangle - |01\rangle - 2|11\rangle)$ – an entangled state orthogonal to product states listed above.

The proof uses various results on upper bounds for $E_C(\rho)$ from low and $E_D(\rho)$ from above.

Open problem Is there a non-trivial example of bipartite state for which the processes of formation and distillation can be performed in a fully reversible way?

8.3.7 Operations with entanglement

Several interesting/important operations with entanglement have been discovered and explored. The first one shows how entanglement can be exchanged.

Entanglement swapping

It used to be thought that if some distant particles are in an entangled state, then some time ago they had to interact and only later they have been separated. However, it is now clear that no direct interaction is necessary in order to produce entanglement between distant quantum systems. For example, entanglement can be teleported. A so-called **entanglement swapping** protocol has been proposed by Zukowski.

The basic idea is simple. If we have two pairs of particles entangled in the Bell state (P_1 with P_2 and P_3 with P_4), Figure 2a, and a Bell measurement on particles P_2 and P_3 is performed, then we get two new entangled pairs: P_1 with P_4 and P_2 with P_3, both in a Bell state. Technically, for

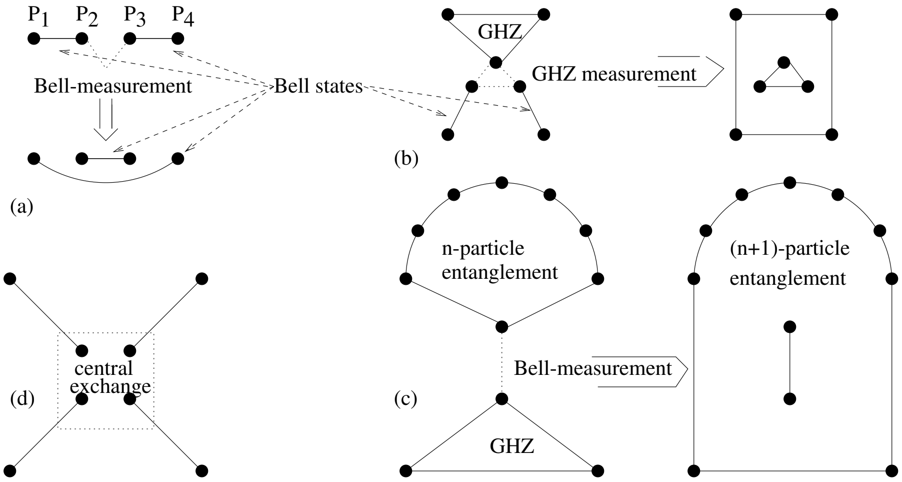

Figure 2: Entanglement swapping and its generalizations

any $a, b, c, d \in \{0, 1\}$, if a Bell operator is applied to the state

$$\frac{1}{2}(|abcd\rangle + |\bar{a}\bar{b}cd\rangle + |ab\bar{c}\bar{d}\rangle + |\bar{a}\bar{b}\bar{c}\bar{d}\rangle),$$

to its two middle qubits, then the resulting state is such that the particles P_1 and P_4, as well as P_2 with P_3, are in a Bell state.

Observe that entanglement swapping allows superluminal establishment of entanglement between two distant parties.

An elegant generalization of entanglement swapping to an arbitrary number q of quantum systems $\mathcal{S}_j$ composed from an arbitrary number m_j of qudits has been worked out by Bouda and Bužek (2000). Each of the systems $\mathcal{S}_j$ is supposed to be in a maximally entangled state of m_j qudits, while different systems are not correlated. They showed that when a set $\sum_{j=1}^{q} a_j$ of particles, with a_j particles from the system $\mathcal{S}_j$, are subjected to a generalized Bell measurement, the resulting set of particles collapses into a maximally entangled state. They also showed how to generalize results for the case of continuous variables.

Entanglement swapping for two pairs of qubits has been experimentally verified by Pan et al. (1998).

A curious modification of the entanglement swapping was developed by Peres (2000) using a simple protocol at which entanglement is produced aposteriori, after entangled particles have been measured and may no longer exists (!).

Entanglement splitting

A very natural question is whether one can split entanglement, which is as a resource in a given entangled state, in such a way that more parties can profit out of it.

The basic story is that Bob, who shares a singleton with Alice, wants to share his resource with his brother Brian, but not to give him all his resource. The question is whether he can achieve that by applying a unitary transformation on a compound state of him, Brian and of an ancilla — and not on Alice's state, therefore only locally. (In a sense the task is to create a channel bifurcation with one input (Alice) and two outputs (Bob and Brian)).

Bruß (1999a), has shown that each pure entangled bipartite state can be splitted.

8.3.10 Entanglement as a catalyst

An additional surprising use of entanglement has been discovered by Jonathan and Plenio (1999). Namely, that the mere presence of a (borrowed) entangled state can be an essential advantage when the task is to transform one quantum state into another with LQCC.

They have shown that there are pairs of pure states $(|\phi_1\rangle, |\phi_2\rangle)$ such that using LQCC one cannot transform $|\phi_1\rangle$ into $|\phi_2\rangle$, notation $|\phi_1\rangle \rightarrow |\phi_2\rangle$(LQCC)), but with the assistance of an appropriate entangled state $|\psi\rangle$ one can transfer $|\phi_1\rangle$ into $|\phi_2\rangle$ using LQCC in such a way that the state $|\psi\rangle$ is not changed in the process (and can be therefore "returned back" after the process) — notation $|\phi_1\rangle \rightarrow |\phi_2\rangle$(EQLCC) or $|\psi\rangle \otimes |\phi_1\rangle \rightarrow |\psi\rangle \otimes |\phi_2\rangle$(LQCC). In such a case, the state $|\psi\rangle$ serves as a "catalyst" for otherwise impossible transformation (reaction). To show the above result Nielsen theorem from page 333 can be used.

Example (Jonathan and Plenio, 1999) They showed that the state of the Hilbert space $H_4 \otimes H_4$

$$|\phi_1\rangle = \sqrt{0.4}|00\rangle + \sqrt{0.4}|11\rangle + \sqrt{0.1}|22\rangle + \sqrt{0.1}|33\rangle$$

cannot be transformed by LQCC into the state

$$|\phi_2\rangle = \sqrt{0.5}|00\rangle + \sqrt{0.25}|11\rangle + \sqrt{0.25}|22\rangle$$

but such a transformation can be done with the addition of the catalyst

$$\kappa\rangle = \sqrt{0.6}|00\rangle + \sqrt{0.4}|11\rangle.$$

On a more general level Plenio and Jonathan (1999) have shown that a state $|\phi_1\rangle = \sum_{i=1}^4 \sqrt{\alpha_i}|\psi_i\rangle|\theta_i\rangle$ cannot be transformed into a state $|\phi_2\rangle = \sum_{i=1}^4 \sqrt{\alpha_i'}|\psi_i'\rangle|\theta_i'\rangle$, where $\alpha_1 \geq \alpha_2 \geq \alpha_3 \geq \alpha_4 \geq 0$ and $\alpha_1' \geq \alpha_2' \geq \alpha_3' \geq \alpha_4'$ are Schmidt coefficients, by LQCC, but it can be transformed using a catalyst if

$$\alpha_1 \leq \alpha_1', \quad \alpha_1 + \alpha_2 > \alpha_1' + \alpha_2', \quad \alpha_4 \geq \alpha_4'.$$

In addition, as presented by Jensen and Schack (2000), there are bipartite states $|\phi_1\rangle$ and $|\phi_2\rangle$ such that $|\phi_1\rangle$ cannot be transformed into the state $|\phi 2\rangle$ by LQCC, but the state $|\phi_1\rangle|\phi_1\rangle$ can be transformed in to the state $|\phi_1\rangle|\phi_2\rangle$ by LQCC.

This is true for example for the states:

$$|\phi_1\rangle = \sqrt{0.31}|00\rangle + \sqrt{0.31}|11\rangle + \sqrt{0.3}|22\rangle + \sqrt{0.04}|33\rangle + \sqrt{0.04}|44\rangle$$

and

$$|\phi_2\rangle = \sqrt{0.48}|00\rangle + \sqrt{0.24}|11\rangle + \sqrt{0.14}|22\rangle + \sqrt{0.14}|33\rangle.$$

The above result about the power of entanglement has been generalized by Eisert and Wilkens (2000), as follows:

1. There are density matrices (mixed states) σ_1 and σ_2 that correspond to genuinely mixed states such that $\sigma_1 \not\twoheadrightarrow \sigma_2$(LQCC), but $\sigma_1 \rightarrow \sigma_2$(ELQCC). That is there is an entangled density matrix ρ such that $\rho \otimes \sigma_1 \rightarrow \rho \otimes \sigma_2$(ELQCC).
2. The proportion of a pure state in a mixed state can be more efficiently increased with EQLCC operations than using LQCC operations in the following way:

   There is a density matrix σ, corresponding to a genuinely mixed state, and a pure state $|\phi\rangle\langle\phi|$ such that the maximal average obtainable value of the fidelity under ELQCC

$$F_{\text{EQLCC}}(\sigma, |\phi\rangle\langle\phi| = \sup_{\rho \in S^{\sigma}_{\text{EQLCC}}} \langle\phi|\rho|\phi\rangle$$

is larger than the maximal fidelity obtained under LQCC is:

$$F_{\text{QLCC}}(\sigma, |\phi\rangle\langle\phi| = \sup_{\rho \in S^{\sigma}_{\text{QLCC}}} \langle\phi|\rho|\phi\rangle$$

where S^{σ}_{LQCC} ($S^{\sigma}_{\text{ELQCC}}$) is the set of states that can be obtained by applying LQCC (ELQCC) on σ.

However, there are also limitations concerning the power of EQLCC. For example, for every pure state $|\phi\rangle$ there exists a $\delta_{\phi} > 0$ such that if $|\phi\rangle \nrightarrow |0\rangle$(EQLCC), then $|\phi\rangle \nrightarrow |\psi\rangle$(ELQCC) for any sufficiently close state $|\psi\rangle$ such that $|\langle\psi|\phi\rangle|^2 > 1 - \delta_{\phi}$.

Bandyopadhyay and Roychowdhury (2001) showed the following result that allows to determine whether for a given pair of $n \times n$-dimensional incomparable states and a given integer k, there is a $k \times k$-dimensional catalyst.

Theorem The set of all $k \times k$ catalytic states for any given pair of $n \times n$ incomparable states is either empty or a union of a finite number of polyhedra in dimension $\leq k - 1$.

It is an open problem whether there is an efficient procedure to construct catalytic states.

An elegant way to study catalysts was introduced and explored by Daftuar and Klimesh (2001) using the so called **trumping relation**. We say for two d-dimensional vectors X and Y that X is **trumped by** Y, notation $X \prec_T Y$ if there is a vector$Z$, called catalyst, such that $x \otimes z \prec y \otimes z$.

By Nielsen theorem a bipartite state $|\psi\rangle$ in $A \otimes B$ with Schmidt decomposition $|\psi\rangle = \sum_{i=1}^{d} \sqrt{\alpha_i}|i_A\rangle|i_B\rangle$ can be transformed, using LOCC, into a bipartite state $|\phi\rangle = \sum_{i=1}^{d} \sqrt{\beta_i}|i'_A\rangle|i'_B\rangle$ iff $\alpha = (\alpha_1, \ldots, \alpha_d) \prec (\beta_1, \ldots, \beta_d)$.

In a similar way as majorization relation allowed to study transformation of states, trumping relation allows to study catalyst.

In order to formulate some problems and results let us introduce some notation.

- For a d-dimensional vector Y let $S(Y) = \{X \in \mathbf{R}^d \,|\, X \prec Y\}$;
- For a d-dimensional vector Y let $T(Y) = \{X \in \mathbf{R}^d \,|\, X \prec_T Y\}$;
- or a d-dimensional vector Y let $T_k(Y) = \{X \in \mathbf{R}^d \,|\, X \prec_T Y \text{ and there is a probabilistic vector } Z \text{ such that} X \otimes Z \prec Y \otimes Z\}$.;

Some natural problems to investigate

- What are necessary and sufficient conditions for probabilistic vectors X and Y that $X \prec Y$ iff $X \prec_T Y$? (In other words, for which states catalysts can be useful. For example if $Y = (\frac{1}{d}' \ldots, \frac{1}{d})$, then for any X, $X \prec Y$ iff $X \prec_T Y$.);
- Given Y, is it possible to find a k such that $T_k(Y) = T(Y)$? (In other words, for which states we can have catalysts of arbitrarily high dimension?)

Daftuar and Klimesh (2001) have shown that almost for all states $|\phi\rangle$ a catalyst can be useful to produce $|\phi\rangle$, Namely, they have shown that for almost all Y of four-dimension and more, $S(Y) \neq T(Y)$. Moreover they have shown that for most Y, there is no k such that $T(Y) = T_k(Y)$. (In other words, for most of the states there is no limit to the dimension of catalyst that must be considered if trying to determine which vectors are trumped by a given vector Y.

Another interesting question Daftuar and Klimesh (2001) explored is which states are potentially useful as catalysts. Surprisingly, maximally entangled states are not. However, practically all other states are useful as catalyst. Namely, it holds

Theorem Let Z be a non-uniform probability vector. Then there are 4-dimensional probability vectors X, Y such that $X \not\prec Y$, but $X \otimes Z \prec Y \otimes Z$.

Supercatalyst

An interesting/important generalization of the concept of catalyst, the so called **super-catalyst**, is due to Bandyopadhyay and Roychowdhury (2001). For a pair of incomparable states $|\phi\rangle$ and $|\psi\rangle$ a supercatalyst is a pair of states $|\chi\rangle$ and $|\omega\rangle$ such that the state $|\phi\rangle \otimes |\chi\rangle$ is transformable to $|\psi\rangle \otimes |\omega\rangle$ and, and this is the point, the entanglement of $|\omega\rangle$ is larger than that of $|\chi\rangle$. In other words, a supercatalyst not only allows to make transformation of a state that is otherwise not possible with LOCC, but, in addition, LOCC allow to increase entanglement of the catalyst state.

It can happen for three incomparable states $|\phi_1\rangle$, $|\phi_2\rangle$ and $|\phi_3\rangle$ that a catalyst $|\psi\rangle$ can help to transform $|\phi_1\rangle$ to $|\phi_2\rangle$, but it is not strong enough to transform $|\phi_2\rangle$ into $|\phi_3\rangle$. However, it is possible to transform $|\phi_1\rangle \otimes |\psi\rangle$ into $|\phi_1\rangle \otimes \psi_1\rangle$ in such a way that $|\phi_2\rangle \otimes |\psi_1\rangle$ can then be transformed into $|\phi_3\rangle \otimes \psi_2\rangle$ by LOCC.

Embezzling entangled quantum states

Another surprising discovery, due to van Dam And Hayden (2002), is that there is an infinite family of bipartite states $\{|\mu(n)\rangle\}_{i=1}^{\infty}$ such that, for any $\varepsilon > 0$ and any bipartite state $|\phi\rangle$, the transformation

$$|\mu(n)\rangle \rightarrow |\mu(n)\rangle \otimes |\phi\rangle$$

can be obtained with fidelity better than $1-\varepsilon$ for all sufficiently large n without any communication, neither quantum nor classical.

Therefore, one can **embezzle** $|\phi\rangle$ from a $|\mu(n)\rangle$ by removing a small portion of entanglement from $|\mu(n)\rangle$, while causing only small disturbance to $|\mu(n)\rangle$.

This can be done using

$$|\mu(n)\rangle = \frac{1}{C(n)}\sum_{j=1}^{n}\frac{1}{\sqrt{j}}||||j\rangle_A|j\rangle_B,$$

where $C(n) = \sum_{j=1}^{n}\frac{1}{j}$.

Embezzling protocol is actually very simple.

As a consequence, in the presence of arbitrary catalyst, any pure bipartite entangled state can be converted into any other to unlimited accuracy without the use of any communication, quantum or classical.

8.3.11 Detection of entanglement

It is fairly easy to determine whether a given pure bipartite state is entangled. On the other hand, to determine whether a given density matrix is entangled seems to be a very nontrivial problem. Non-triviality of the problem is due to the fact that in the density matrices quantum correlations are weak and a manifestation of quantum entanglement can be very subtle (see Horodeckis, 2001).

Separability criteria

By a **separability criterion** we call a condition for density matrices that is satisfied by all separable density matrices and it is not satisfied by all density matrices. More of entangled density matrices do not satisfy a separability criterion, stronger this criterion is.

For example, all Bell inequalities (that are always satisfied by separable states) represent an interesting set of (not very strong) separability criteria.[18] As pointed out by Werner (1998), separable states satisfy all possible Bell inequalities and some entangled states also satisfy standard Bell inequalities. Another set of (not too strong) separability criteria are inequalities

$$QS(\rho_A) \leq QS(\rho), \quad QS(\rho_B) \leq QS(\rho),$$

for Reneýi quantum entropies $S_i = (1-i)^{-1} \lg Tr(\rho^i)$, $i = 0,1,2,3$ (Horodeckis, 2001).

For each pure entangled state there is a set of separability criteria that allow to detect its entanglement.

Operational separability criteria

They are criteria that allow with well specified computations to determine whether a given state of a bipartite system $A \otimes B$, is entangled.

In the case of pure bipartite states it is an easy operational criterion for separability. Each such state $|\phi\rangle$ can be easily put into the Schmidt normal form

$$|\phi\rangle = \sum_{i=1}^{r} a_i |e_i\rangle |f_i\rangle,$$

where $a_i > 0$, $\sum_{i=1}^r a_i^2 = 1$, and the following sets of states are mutually orthogonal: $\{|e_i\rangle\}_{i=1}^r$ and $\{|f_i\rangle\}_{i=1}^r$. $|phi\rangle$ is entangled if and only if $r > 1$.

PPT criterion

A simple, but powerful, separability criterion for mixed states, the so called **positive partial transposition criterion** (PPT-criterion or Peres-Horodecki criterion) is due to Peres (1996). It is based on the observation that if a density matrix ρ of a composed (bipartite) quantum system $A \otimes B$ is separable, then its *partial transpose* $\bar{\rho}$ has to have positive eigenvalues.

[18]The so called Bell-CHSH inequalities are inequalities of the form $Tr(\rho B) \leq 2$, where B are matrices of the form $B = \bar{r}_1\sigma \otimes (\bar{r}_2 + \bar{r}_3)\sigma + \bar{r}_4\sigma \otimes (\bar{r}_2 - \bar{r}_3)\sigma$, where $\bar{r}$'s are unit real vectors and if $\bar{r} = (r_1, r_2, r_3)$, then $\bar{r}\sigma = r_1\sigma_x + r_2\sigma_y + r_3\sigma_z$, where $\sigma_x, \sigma_y, \sigma_z$ are Pauli matrices.

A partial transpose $\bar{\rho}$ of ρ is obtained from ρ by making a transposition in ρ with respect to only one of the subsystems.

Formally, if both A and B are n-dimensional Hilbert space and a density matrix ρ of $A \otimes B$ is decomposed into $n \times n$ submatrices, then the transposition of ρ, is obtained just by making transposition of submatrices as follows:

$$\rho = \begin{pmatrix} A_{11} & \dots & A_{1n} \\ \vdots & \ddots & \vdots \\ A_{n1} & \dots & A_{nn} \end{pmatrix}, \quad \bar{\rho} = \begin{pmatrix} A_{11}^T & \dots & A_{1n}^T \\ \vdots & \ddots & \vdots \\ A_{n1}^T & \dots & A_{nn}^T \end{pmatrix}$$

For example, the density matrix ρ of the Bell state Ψ^+ and its transpose $\bar{\rho}$ have the form

$$\rho = \frac{1}{2}\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad \bar{\rho} = \frac{1}{2}\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix},$$

and $\bar{\rho}$ has $-\frac{1}{2}$ as one of the eigenvalues.

In other way partial transpose ρ_T of a separable state

$$\rho = \sum_i p_i |\phi_i\rangle\langle\phi_i| \otimes |\psi_i\rangle\langle\psi_i|$$

has the form

$$\rho^T = \sum_i p_i (|\phi_i\rangle\langle\phi_i|)^T \otimes |\psi_i\rangle\langle\psi_i|$$

and since $(|\phi_i\rangle\langle\phi_i|)^T$ is again a density matrix,it has to be $\rho^T \geq 0$.

Peres' criterion was shown by Horodeckis (1996) to be a necessary and sufficient condition for density matrices of the bipartite systems of dimension 2×2 and 2×3 to be entangled.

A state ρ is called **PPT-state** (**NPT-state**) if its partial transpose is positive (is not positive). Quite a bit of effort in the last years has been given to the understanding of PPT-states and to the development of methods how to construct PPT-states (see Horodeckis (2001) for an overview).

Reduction criterion

According to this criterion, due to M. Horodecki and P. Horodecki (1999), if ρ is separable, then

$$I \otimes \rho_B - \rho \geq 0, \qquad \rho_A \otimes I - \rho \geq 0$$

Similarly as in the case of PPT criteria, reduction criterion is necessary and sufficient for density matrices of degree $2 \otimes 2$ or $2 \otimes 3$; otherwise this is only a necessary condition.

0.1.1 Majorization criterion

According to this criterion, due to Nielsen and Kempe (2000) if a mixed state ρ is separable, then the following conditions have to be satisfied

$$\lambda_\rho^\downarrow \prec \lambda_{\rho_A} \text{ and } \lambda_\rho^\downarrow \prec \lambda_{\rho_B},$$

where $\lambda_\rho^\downarrow$ is the vector of the eigenvalues of ρ in decreasing order. Notation $x^\downarrow \prec y^\downarrow$ means that the vector $x^\downarrow$ is majorized by a vector $y^\downarrow$, when $\sum_{i=1}^k x_i^\downarrow \leq \sum_{i=1}^k y_i^\downarrow$ holds for $k = 1, 2, \ldots, d-1$, where d is the dimension of the vectors, and $\sum_{i=1}^d x_i^\downarrow = \sum_{i=1}^d y_i^\downarrow$.

The following ordering holds between the above separability criteria. A density matrix ρ is separable

$\Rightarrow$ ρ satisfies PPT criterion;

$\Rightarrow$ ρ satisfies reduction criterion;

$\Rightarrow$ ρ satisfies the Majorization criterion.

However, for matrices of degree 2×2 and 2×3 PT and reduction criteria are equivalent with separability condition for density matrices.

Non-operational criteria separability

The two criteria discussed bellow are necessary and sufficient, but provide no easily to be used method to verify separability.

Entanglement witnesses and separability

A very interesting and useful approach to the detection of entanglement is based on the concept of **entanglement witness** introduced by Horodeckis (1996) and coined by Terhal (2000).

An entanglement witness for density matrices of a Hilbert space H of the dimension n is any matrix W of dimension n such that

- $Tr(W\rho) \geq 0$ if $\rho \in H$ is a separable density matrix.
- There is an entangled density matrix $\rho \in H$ such that $Tr(W\rho) < 0$.

In other words an entanglement witness can detect entanglement in some density matrices.

The Hahn-Banach Theorem[19] actually implies that a state ρ is entangled if and only if there exists an entanglement witness that detects it.

Swapping (or flipping) operator V defined by $V(|\phi\rangle \otimes |\psi\rangle) = |\psi\rangle \otimes |\phi\rangle$ is an example of an entanglement witness.

Since an entanglement witness can fail to discover entanglement a natural question is to find as best as possible entanglement witnesses. Namely, such that do not fail at all or fail very rarely to detect entanglement.

An entanglement witness W is called **optimal**, see Lewenstein et al. (2000), if there is no other entanglement witness that detects the same entanglement as W and more. Lewenstein et al. (2000) also found a way to design optimal witnesses. This allows well experimentally detect quantum entanglement. For example, the optimal entanglement witness for the state $\cos\theta|00\rangle + \sin\theta|11\rangle$ has the form

$$W = \frac{1}{2}(|01\rangle\langle 01| + |10\rangle\langle 10| - |00\rangle\langle 11| - |11\rangle\langle 00|).$$

The concept of entanglement witness may seem to be quite puzzling at first sight. However, it is quite natural once we realize that in the Hilbert space of Hermitian operators $Tr(W\rho)$ is actually inner-product of W and ρ and therefore W separates non-separable density matrices by a hyperplane from separable ones.

[19]Hahn-Banach theorem says that if S is a convex and compact set and $\rho \notin S$, then there exists a hyper-plane that separates ρ from S.

Separability and positive maps

A detailed overview of the results related to the question whether a given density matrix of a bipartite mixed state is entangled is given by Horodeckis (2001) and Terhal (2001). For example, they well demonstrate the role of positive maps for characterization of separable states.

Let $\mathcal{L}(H_1, H_2)$ denote the set of linear maps from a Hilbert space H_1 to a Hilbert space H_2. A map $\Lambda \in \mathcal{L}(H_1, H_2)$ is called **positive map**, if it maps positive operators into positive. Λ is called **completely positive map** (CP-map), if it is positive and, for each n, the induced map Λ_n : $\Lambda \otimes I_n$ is also positive, where I_n is the identity map on the n-dimensional Hilbert space.

Transposition is an example of a map that is positive, but not completely positive.

The following theorem (see Horodeckis, 2001) yields a characterization of the separable states in terms of positive maps.

Theorem Let ρ be a density matrix of the Hilbert space $H_1 \otimes H_2$. Then ρ is separable if and only if, for any positive map, $\Lambda \in \mathcal{L}(H_2, H_1)$ the operator $(I \otimes \lambda)\rho$ is positive.

Theorem is nice, but it actually requires to find characterization of all positive maps and this is a big problem.

Actually, it has been on the basis of this theorem, that it has been shown that a density matrix ρ of a 2×2 or 2×3 dimensional bipartite quantum system is separable if and only if its partial transposition is a positive operator.

The above theorem also allows to deduce, if we take $\Lambda(A) = (Tr(A)I - A)$, see Horodecki and Horodecki (1999) and Cerf et al. (1999), a simple separability criterion, called **reduction criterion**, represented by inequalities

$$I \otimes \rho_B - \rho \geq 0, \qquad \rho_A \otimes I - \rho \geq 0$$

that are satisfied by all separable states and not by all states.

Interesting enough, there is an isomorphism between entanglement witnesses and positive maps that are not completely positive (Jamiolkowski, 1972). It holds that

$$W = (\mathbf{I} \otimes \Lambda)P_+,$$

where, see Bruß2001,

$$P_+ = \frac{1}{d}(\sum_{i=1}^{d} |ii\rangle 0(\sum_{i=1}^{d} \langle jj|)$$

is the projection onto the maximally entangled state.

8.3.12 Entanglement invariants

A common feature of entangled states is that their non-local properties do not change under local unitary transformations – under local transformations acting on each of the subsystems. It is therefore natural to call **entanglement invariant** that any quantity of quantum states that is invariant with respect to local unitary transformations. Consequently, since any good measure of entanglement has to be invariant under local unitary transformations, it has to be a expressed in terms of entanglement invariants.

Importance of the invariants of multipartite states is also due to the fact that the finest discrimination between different types of entanglement. For example, Grassl et al. (1998) have shown two density matrices of degree 4 that are conjugated to each other, have the same eigenvalues, their reduced density matrices are also the same, and, in addition, all polynomial invariants up to degree five evaluate to the same number. However, for invariants of degree six these two density matrices evaluate differently. On this basis on can conclude that these two density matrices are not locally invariant.

A general theory of invariants of mixed multipartite states has been introduced by Rains (1997). Grassl et al. (1998) showed a more efficient way to determine polynomial invariants. They established a connection between polynomial invariants of quantum systems and permutations. Consequently, invariants of n-partite systems can be computed directly and efficiently from n-tuples of permutations.[20] In the case of qubit systems permutations derived from binary trees are sufficient to consider.[21]

Invariants of entanglement can be of various types. Of a special interest are the so called **polynomial invariants** – polynomial functions of the

[20]The method of Grassl et al. (1997) can also be used to study non-local properties of other objects, for example, of unitary transformations.

[21]Grassl et al. (1997) presented a set of polynomials that generate, for a system of two qubits, all invariants up to degree 23.

amplitudes of quantum state. Rains (1997) has shown that in principle all polynomial invariants can be computed.

For mixed states of two qubits Makhlin (2000) gave a complete set of (18) invariants. For mixed-states of three qubits Sudbery (2000) exhibit a set of six independent invariants.

For pure states

$$|\psi\rangle = \sum_{ij}^{n} \alpha_{ij}|e_i\rangle|e_j\rangle,$$

with $\sum_{ij}^{m} \alpha_{ij}\alpha_{ij}^* = 1$, of an $n \times n$ bipartite system $A \otimes B$, the reduced density matrix has the form $\rho_0 = AA^*$, where $A = \{\alpha_{ij}\}$. Of importance are the following polynomial invariants (Linden and Popescu (1998), Albeverio and Fei (2001))

$$I_k = Tr((AA^*)^{k+1}), k = 0, 1, \ldots, n.$$

In the case

$$|\psi\rangle = \sum_{i=1}^{n} \sqrt{\lambda_i}|e_i\rangle|e_i\rangle,$$

$$I_k = \sum_{i=1}^{n} \lambda_i^{k+1},$$

that is the entanglement invariants of bipartite states are the symmetric functions of the Schmidt coefficients.

In the case of three-qubit states $|\psi\rangle$, of the three-partite systems $A\otimes B\otimes C$ and $\rho = |\psi\rangle\langle\psi|$, four linearly independent quartic invariants are

$$\langle\psi|\psi\rangle,\ Tr_{AB}\rho,\ Tr_{AC}\rho,\ Tr_{BC}\rho.$$

Since linear combinations and products of invariant polynomials are again invariant polynomials, any polynomial of invariant polynomials is again an invariant polynomial.

One of the tasks is to find a set of fundamental polynomials such that any polynomial invariant can be expressed as a polynomial of the fundamental polynomials.

It is sufficient to study homogeneous polynomials because each homogeneous polynomial of degree k remains homogeneous of the same degree under unitary operations and every polynomial can be decomposed additively into its homogeneous components.

8.3.13 Entanglement monotones

A more general concept than that of entanglement invariants is that of (non-increasing) **entanglement monotones** – see Vidal (1998). Informally, they are those functions on multipartite mixed states that do not increase, on average, under LOCC.[22]

The importance of entanglement monotones steams from the observation that non-local resources of quantum states do not increase under LOCC. Consequently, the most natural requirement (and actually the only very natural requirement) for a measure of entanglement is that it is an entanglement monotone.

The main goal of the entanglement monotones investigations is to get a deeper insight into the nature of entanglement.

On a more technical level a functions μ on mixed states is an entanglement monotone if the following two conditions are satisfied:

C1 For any ρ and any superoperator $\mathcal{E}_{i,k}$ performed by the party i, with outcomes labeled by k

$$\mu(\rho) \geq \sum_k p_k \mu(\mathcal{E}_{i,k}(\rho_k)),$$

where

$$p_k = Tr[\mathcal{E}_{i,k}(\rho)]; \quad \rho_k = \frac{1}{p_k}\mathcal{E}_{i,k}(\rho).$$

C2 For any ensemble $\{q_k, \rho_k\}$ of mixed states

$$\sum_k q_k \mu(\rho_k) \geq \mu(\rho).$$

Condition C1 assures monotonicity, on average, under any local QOCC individually. Condition C2 assures that monotonicity is preserved even if some information about actual performance and results is not made available during the local transformation.

Observe that monotonicity in both conditions has statistical character. It says that LOCC cannot be used to increase entanglement systematically,

[22]Sometimes the concept of entanglement monotone is defined in a more general way. Namely as those functions that do not increase (or do not decrease) under LOCC. However, if μ is a non-decreasing entanglement monotone, then $-\mu$ is a non-increasing entanglement monotone. That is why by an entanglement monotone we will consider here mainly non-increasing entanglement monotones.

since, on average, μ will be at most conserved. (However, it may happen that $\mu(\rho_k) < \mu(\rho)$ for some k.)

As the first application of the concept of entanglement monotones a characterization the optimal probability with which a given mixed state ρ can be transformed into another given mixed state ρ' using LOCC.

Theorem (Vidal, 1998) The maximal probability $Pr(\rho \leftarrow \rho')$ of the success in the transformation of ρ into ρ' that can be achieved by LOCC is given by

$$Pr(\rho \leftarrow \rho') = \min_{\mu \in \mathrm{EM}} \frac{\mu(\rho)}{\rho')},$$

where the minimization is to be performed over the set of all entanglement monotones (EM).

Therefore, there is an intimate relation between entanglement transformations and entanglement monotones.

n the case of bipartite systems, when evaluated on a pure state $|\phi\rangle$, any entanglement monotone depends only on Schmidt coefficients of $|\phi\rangle$, or, equivalently, on its partial trace $Tr(|\phi\rangle\langle\phi|)$, through an entanglement invariant. It holds

Theorem (Vidal, 1998) Entanglement monotones for pure bipartite states is given by a unitarily invariant concave function of the partial trace $Tr(|\phi\rangle\langle\phi|)$.

An important example of entanglement monotones are so called α-entropies of entanglement[23] (Vidal, 1998).

$$E_\alpha(\phi) = \frac{1}{1-\alpha} \lg Tr(|\phi\rangle\langle\phi|) = \frac{1}{1-\alpha} \lg \sum_{i=1}^{n} \alpha_i^\alpha.$$

8.3.14 Multipartite entanglement

Understanding, characterization, classification and quantification as well as manipulation of multipartite entangled states is a very important and difficult problem, perhaps the main current challenge in quantum information theory, that needs to be explored in order to get more insights into the possibilities of distributed quantum computing and networks.

[23] For $k = 1$ we have to take a limit from left.

The problem is also of special interest outside of QIP, for physics in general.

Error correcting codes are an example of an important area where multi-particle entanglement plays crucial role and where quite a few insights have been obtained about it.

A state $|\phi\rangle$ of a m-partite quantum system represented by the Hilbert space $H^{(1)} \otimes H^{(2)} \otimes \ldots \otimes H^{(m)}$ is called separable if it can we written in the form

$$\sum_{i=1}^{n} \lambda_i \rho_{i,1} \otimes \rho_{i,2} \otimes \ldots \rho_{i,m},$$

where $\rho_{i,j}$ is a density matrix of $H^{(j)}$. Otherwise $|\phi\rangle$ is called inseparable or entangled. Such a state cannot be created by m parties if the i-th party works with a quantum system corresponding to the Hilbert space $H^{(i)}$ and uses only local operations.

If an m-partite state is entangled it can be separable if some of the parties get together and can perform global operation on the corresponding composition of the quantum systems, For example, if $I_1, I_2, \ldots I_k$ is a partition of the set $\{1, 2, \ldots, m\}$, then an m-partite state $|\rho\rangle$ is $I_1 : I_2 : \ldots I_k$ separable if it is separable on the Hilbert space $H(I_1) \otimes H^{(I_2)} \otimes H^{(I_m)}$, where $H^{(I_s)}$ is a tensor product of Hilbert spaces $\{H^{(i)} \,|\, i \in I_s\}$.

For example the so-called Smolin state

$$\frac{1}{4} \sum_{i=1}^{4} |\Phi_i\rangle,$$

where $|\Phi_i\rangle \,|\, i \in \{1, 2, 3, 4\}$ are all Bell states, is entangled in the Hilbert space $H_2 \otimes H_2 \otimes H_2 \otimes H_2$, but is $AB : CD$, $AC : BD$ and $AD : BC$ separable if parties are denoted as A, B, C, D.

Creation of multipartite states.

There are several techniques how to create multipartite entangled states. A simple idea is due to Bose et al. (1997), as a generalization of the procedure of entanglement swapping. In the generalized entanglement swapping one deals with generalized n-partite Bell states of the form

$$\frac{1}{\sqrt{2}}(|x\rangle + |\bar{x}\rangle),$$

where $x \in \{0,1\}^n$ and $\bar{x}$ is a bitwise complement of x. Let us assume that we have N sets of entangled particles, each one in a generalized Bell state. Let from the ith set p_i particles are brought together and a joint Bell measurement is performed on them. (Observe that all sets of Bell states of p particles form an orthogonal basis.) In such a case all measured particles get into a Bell state and the same is true for the rest of particles.

Figure 2b shows the case of one GHZ state and two bipartite Bell states. The result of the measurement is one GHZ state and one 4-partite Bell state.

A generalization of entanglement swapping can also be used to create from an m -partite Bell state and from one GHZ state an $(m+1)$-partite Bell state by simply performing a Bell measurement on one particle of the m-partite state and one particle of the GHZ state, see Figure 2c.

Sometimes a flexibility is needed to create "on demand" a generalized Bell state for a group of particles. In such a case the following method can be used, see Figure 2d. Each party involved share a singlet with a center $\mathcal{O}$. If a set of parties wants to share an multipartite state, then the center performs a generalized Bell measurement of its share of singlets to make the corresponding second particles of parties to get into a generalized Bell state.

Schmidt decomposition of multipartite states

For the study of bipartite states of large importance is the fact that for each bipartite state there is a unique Schmidt decomposition. This is not true for more than two partite states. The absence of Schmidt decomposition for multipartite states means that on one hand one cannot use for the study of n-partite entanglement, for $n > 2$, techniques developed for bipartite states. On the other hand this means that one can expect that those multipartite states that are not Schmidt decomposable will have various interesting properties.

An n-party state $|\phi\rangle$ is said to be Schmidt decomposable if it can be written in the form

$$|\phi\rangle = \sum_i a_i |i_1\rangle|i_2\rangle \dots |i_n\rangle,$$

where $\{|i_k\rangle\}_i$ is a basis of the i-th Hilbert space of $|\phi\rangle$.

Thapliyal (1999) has shown that n-partite states with Schmidt decomposition have an interesting property. Namely that an n-partite state has a Schmidt decomposition if and only if each density matrix obtained from the state by tracing out a party is separable.[24]

Measures of entanglement of multipartite systems

One of the key problems concerning multipartite entanglement is how to measure it. How to define appropriate measures of entanglement of multipartite quantum states.

The problem seems to be quite complex. In the case of bipartite systems of two qubits a natural measure of entanglement is the number of Bell states that can be distilled from a given state. However, it is not yet clear whether entanglement of multiparticle states can be defined in terms of such a standard currency.

One natural approach to explore is to generalize measures of entanglement for bipartite systems to multipartite systems.

An attempt to do such generalization for the entanglement of formation is presented in Wang (2000). Especially entanglement of formation of three-particle systems is studied in depth. Entanglement of a mixed state ρ of a three-partite system $A \otimes B \otimes C$ is defined by

$$E_f(\rho) = \frac{1}{6}[E_f(\rho_{AB}) + QS(\rho_{AB}) + E_f(\rho_{AC}) + QS(\rho_{AC}) + E_f(\rho_{BC})] \quad (4)$$

$$+\frac{1}{6}[QS(\rho_A) + QS(\rho_B) + QS(\rho_C)]. \quad (5)$$

A generalization of the entanglement of relative entropy has been developed by Plenio and Vedral (2000) and Wang (2000a).

Generalized concurrence

Albeverio and Fei (2001) introduced a generalization of concurrence measure for multipartite states based on the concept of entanglement invariant. The basic idea is the following one.

[24]Actually, if these density matrices are separable then they are also eigenseparable, that is they have separable eigenvectors.

If $|\psi\rangle = \sum_{ij=1}^{n} a_{ij} e_i \otimes e_j$ is a bipartite pure state of two n-dimensional systems $H_1 \otimes H_2$, with $\sum_{i,j=1}^{n} a_{ij} a_{ij}^* = 1$, and $A = \{a_{ij}\}$, then $\mathrm{Tr}_{H_1}(|\psi\rangle\langle\psi|) = AA^*$.

It has been shown by Linden and Popescu (1998) and by Albeverio and Fei (2001), that the following quantities are entanglement invariants $I_\alpha = \mathrm{Tr}(AA^*)^{\alpha+1}$, for $alpha = 0, 1, \ldots, n-1$.

More exactly,

$$I_0 = \sum_{ij=1}^{n} a_{ij} a_{ij}^*, I_1 = \sum_{ijkm=1}^{n} a_{ik} a_{im}^* a_{jm} a_{jk}^*.$$

Polynomials in I_0 and in I_1 are also invariants. Albeverio and Fei (2001) used this fact to define **generalized concurrence** as follows

$$C_n(|\psi\rangle) = \sqrt{\frac{n}{n-1}(I_0^2 - I_1)} = \sqrt{\frac{n}{2(n-1)} \sum_{ijkm=1}^{n} |a_{ik} a_{jm} - a_{im} a_{jk}|^2}.$$

It can be shown that $C_n(|\psi\rangle) = 0$ if $|\psi\rangle$ is factorisable and $C_n(|\psi\rangle) = 1$ if $|\psi\rangle$ is maximally entangled state. Moreover, C_2 is equal to the usual concurrence measure.

C_n satisfies the very basic requirements for an entanglement measure. However, it does not seem to be the case that in general this measure of entanglement can specify entanglement of formation as it is for the original measure concurrence. In a special case, if the matrix AA^* has exactly two non-zero eigenvalues. then the entanglement of formation is a monotonically increasing function of C_n.

Natural generalizations of invariants I_0 and I_1 for the case of multipartite systems was used by Albeverio and Fei (2001), to a natural generalization of the measure C_n defined above.

Incomparable forms of quantum entanglement

In the case of bipartite systems one of the fundamental results concerning entanglement is that all entangled states are mutually inter-convertible by LQCC (asymptotically, with respect to the number of copies available). Nothing similar is true for multipartite entanglement. It seems that in the case of m-partite systems there are at least $2^m - m - 1$ kinds of asymptotically inequivalent entanglement. (This corresponds, for $n = 2, \ldots, m$, to all $\frac{m!}{n!(m-n)!}$ ways different subsets of n parties can be chosen.) Actually, the understanding of inequivalent ways in which subsystems of a multipartite composite system can be entangled is one of the central problems not only of multipartite entanglement, but of all quantum information theory.

The study of entanglement of multipartite systems is at the very beginning even if they are exactly those quantum systems from which one expects the most significant applications — for example for distributed computing, quantum networks or even for understanding of the behavior of strongly-coupled many-body systems.

Some of the basic problems to deal with are easy to formulate, but usually difficult to solve. For example: How to detect entanglement of multipartite systems? What is the structure of the set of n-partite pure (mixed) entangled states? How many inequivalent types of entanglement we have in multipartite systems? Which sets of entangled states are inter-convertible by LQCC (exactly and asymptotically)? Which types of entanglement we have in such multipartite systems (for example what are properties of bound entangled states)? What are the laws entanglement can be shared among n parties? What are proper axioms for measures of entanglement of multipartite systems? Which measures of entanglement of multipartite systems are useful and what are the relations between them? In general, quantitative and qualitative theory of multipartite entanglement is needed.

Concerning multipartite entanglement detection, a variety of results have been generalized for multipartite systems, see Horodeckis (2001), Terhal (2001). For example, the concept of entanglement witness.

So far only very partial results are known, but they well demonstrate complexity of the task.

For example, Dürr et al. (2000) have shown that in an n-partite system, with $n \geq 4$ if two pure states are chosen randomly, then they are *stochastically incomparable* in the sense that neither state can be produced from other by SLQCC. Moreover Bennett et al. (1999) have shown that two GHZ states are LQCC-incomparable with three EPR states. On a more general level they have shown that two multipartite states whose marginal one-party entropies agree are either locally unitarily equivalent or they are not LQCC-comparable.

Reversible transformations of multipartite states and entropies

In order to study various types of multipartite entanglement the basic question is for which pairs of (sets of) states S and R we can transform S into R in a reversible way using transformations based on LQCC.

For example one GHZ-state can be transformed into one singlet (but not reversibly), and two singlet into one GHZ state (but again not reversibly).

One way to show that some reversible transformations do not exist is to consider how various types of entropies are changed by a transformation process.

It is clear that entropy must be constant during a reversible process, because entropy cannot get increased by such a process.

A useful tool to study reversible transformations has been developed by Linden et al. (1999). They have shown that at any reversible transformations based on LQCC the average relative entropy of entanglement of any pair of parties must be constant. This allowed them to show it is not possible to convert $2n$ GHZ-states into $3n$ singlets, even asymptotically.

An interesting open problem is whether any entangled three-partite state can be transformed in a reversible way into GHZ states and singlets.

Three qubit systems

This type of three-partite systems is a natural next target to explore in details.

Three-qubit pure states

By Acid et al. (2000) each three qubit state can be expressed in the following form with 5 entanglement parameters

$$|\phi\rangle = \lambda_1|000\rangle + \lambda_2 e^{i\theta}|100\rangle + \lambda_3|101\rangle + \lambda_4|110\rangle + \lambda_5|111\rangle,$$

where $0 \leq \theta \leq \pi$ and $\lambda_i \geq 0$, $\sum_{i=1}^{5} \lambda_i^2 = 1$.

There are four types of pure three-qubit entanglement states:

beginitemize

Separable states that are tensor products of three qubit states.

Bi-separable states, that is $AB : C$ or $AC : B$ or $A : BC$ separable states.

Fully correlated states with genuine entanglement of all three parties. As shown by Dürr et al. (2000) each such states can be transformed by local reversible operations to one of the following states:

- W-states – states that can be transformed by LOCC to the state (Dürr et al. (2000)

$$\frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle)$$

- GHZ-states – states that can be transformed by LOCC into the GHZ state.

It has been shown, see Dürr et al (2000), that all these four classes are different and therefore there are four different types of fully entangled pure three-qubit states.

Another interesting question concerning three-partite states is of what type can be density matrices obtained by tracing out one party.

Two results along these lines have been obtained by Thapliyal (1998). For example, if $|\phi_{abc}\rangle$ is a three-partite state such that density matrices ρ_{ab} and ρ_{ac} are PPT-states, then the state $|\phi\rangle$ is Schmidt decomposable.

Another result due to Thapliyal (1998) says that if $|\phi\rangle$ is such that ρ_{ab} is a PPT-state and ρ_{bc} is separable, then also ρ_{ab} is also separable.

Open problem (1) Are there three-partite states such that by tracing out any party one gets a bound-entangled PTT state.

2) Are there three partite states such that by tracing out one party we get one separable state and two bound-entangled PTT states.

Mixed three-partite states

The case of mixed states, or, better, of density matrices over H has been investigated by Acin et al. (2001). They have defined four types of density matrices:

- The class S of separable density matrices – those that can be expressed as convex sums of projectors onto product states.

- The class B of Biseparable density matrices – those that can be expressed as convex sums of projectors onto product and bipartite entangled states.
- The class W of so-called W-states – those that can be expressed as convex sums of projectors onto product, biseparable and W-states of the form

$$\lambda_0|000\rangle + \lambda_1|100\rangle + \lambda_2|101\rangle + \lambda_3|100\rangle$$

.

- The class GHZ of all three-partite qubit density matrices.

It has been shown that all these four classes are convex and compact and it holds

$$S \subset B \subset W \subset GHZ.$$

In addition, these classes are invariant under local unitary and reversible non-unitary quantum operations.

Next natural question is how to determine to which class a density matrix belong. Acin et al. (2001) extended to the three-partite qubit systems the concept of entanglement witness. Any GHZ-witness (W-witness) has the canonical form $W = Q - \varepsilon I$, where Q is a positive operator which has no W-type (B-type) vectors in its kernel. They and Bruß(2001),also showed specific examples of such witnesses.

An example of a GHZ witness is the matrix

$$W_{GHZ} = \frac{3}{4}\mathbf{I} - P_{GHZ},$$

where P_{GHZ} is the projector into the GHZ state.

An example of W-witness is the matrix

$$W_W = \frac{2}{3}\mathbf{I} - P_W,$$

where P_W is the projector into the W-state.

Acín et al. (2001) obtained several interesting results about the entanglement of three-partite states utilizing the concept of entanglement witness. For example, they have shown that the class $W - B$ of mixed states has non-zero measure and that the class GHZ-W does not contain bound entangled states.

MREGS

For each m, m-MREGS are sets of m-partite states, of minimal cardinality, sufficient to generate all m-partite pure states by asymptotically reversible SLQCC.

Not too much is known about MREGSs for different m.

For bipartite states such a MRGES exists and consists of the single EPR state.

Open problem Do there exist finite MREGSs for n-partite pure states for $n \geq 3$?

0.1.2 Partial results

Wu and Zhang (2000) have shown that not all 4-partite states can be generated, in the asymptotic way, reversibly from all 2-, 3- and 4-partite cat states.

Acin et al. (2002) have shown that not all 3-partite states can be generated, in the asymptotic way, reversibly from all 2- and 3-partite cat states.

Proof technique: To show, for a specific state $|\psi\rangle$ that conversation law for relative entropy would have to be violated if $|\psi\rangle$ would be derived from such states in a reversible way.

Sharing of entanglement

Another basic question concerning multipartite entanglement that has already been investigated is the following one: to what extend does entanglement between some particles restrict their entanglement with other particles?

In the case of classical correlations, arbitrarily many classical systems can be perfectly correlated with each other. In the case of quantum correlations this is no longer true and this another essential difference between classical and quantum correlations.

For example, if two qubit-particles are maximally entangled, then they cannot be entangled with other particle (this property of entanglement is usually called *monogamy*). One can therefore expect, in general, that if two particles are entangled, then they can have only limited entanglement with other particles. Let us now discuss several results that have been obtained recently on sharing of entanglement.

Coffman et al. (1999) considered the following problem: given a pure state of three qubits, say A, B, C, how is tangle between A and B, notation τ_{AB}, related to tangle between A and C, notation τ_{AC}. They showed that

$$\tau_{AB} + \tau_{AC} \leq 4 \det \rho_A.$$

what can be interpreted that tangle between A and B, plus tangle between A and C, cannot be greater than tangle between A and the pair BC.[25]

Bounds on the achievable nearest neighbors entanglement have been obtained also for the case qubits form a bi-infinite translationally invariant linear chain or a finite ring. (Translational equivalence in these cases means that global states to consider are invariant under all shifts of qubits. As a consequence of the translational equivalence, the degree of entanglement between neighbors has to be constant through the chain or ring.) Wooters (2000) has shown that in the case of bi-infinite chains it is possible to achieve an entanglement of formation equal to 0.285 ebits between neighbors and this is the best possible under certain assumptions. Actually, his main result is formulated in terms of concurrence as a measure of entanglement. For the case of rings, O'Connor and Wooters (2000) derived, under certain assumptions, formulas for the maximum possible nearest-neighbor entanglement measured by concurrence.

Sharing of entanglement between n qubits in the case that all pairs of qubits are correlated in the same way, and therefore one can say that entangled pairs of qubits form a complete graph, was investigated by Koashi et al. (2000) and Dürr et al. (2000). They showed that under the above assumptions the maximal entanglement between any pair of qubit, measured in terms of concurrence, is $\frac{2}{n}$.

An interesting general question concerning entanglement sharing was raised by Dennison and Wooters (2001). For the case of the states of n-partite d-dimensional quantum systems they denote by $E_{max}(n,d)$ maximum of the minimal entanglement of formation in any two subsystems.

It is easy to see that $E_{max}(2,d) = \lg d$. Dürr et al. (2000) have shown that$E_{max}(3,2)$ (and that the optimal pairwise entanglement is for the

[25]It make sense to speak of the tangle between A and BC, because, even if the state space of BC is four-dimensional, only two of these dimensions are necessary to express pure state of ABC.

state $\frac{1}{\sqrt{3}}(|100\rangle + |010\rangle + |001\rangle)$. From the results of Koashi et al. (2000) it follows that $E_{max}(n,2) \geq H(\frac{1}{2}(1+\sqrt{1-4/n^2}))$, where H is the binary entropy function. Dennison and Wooters (2001) have shown that $E_{max}(d,d) \geq 1$ for any d. (The very basic idea is simple. They consider the state $\frac{1}{\sqrt{d!}}\sum_{i_1,\ldots,i_d}\varepsilon_{i_1,\ldots,i_d}|i_1\ldots i_d\rangle$, where $i_1,\ldots i_d$ is a permutation on $\{1,\ldots d\}$, $\varepsilon_{i_1,\ldots,i_d}$ is completely antisymmetric and $\varepsilon 1,2,\ldots,d = 1$. In such a case the reduced density matrix of each pair of subsystems is $\rho = \frac{1}{d(d-1)}(I-F)$, where F is the swapping operator $F = \sum_{ij}|ij\rangle\langle ij|$. It follows from results of Vollbrecht and Werner (2001) that entanglement of formation of such states is 1.)

Observe that in a system of three qutrits the entanglement (of formation) of each pair can be larger than in the case of three qubits – 1: 0.550.

Open problem To determine values of the function $E_{max}(n,d)$ for other values of parameters and for other measures of entanglement.

Entangled graphs - distribution of bipartite entanglement in multi-qubit systems

Peschl and Bužek (2002) have shown that for any graph G of n-vertices there is A pure state $|\phi_G\rangle$ state in H_{2^n} such that its ith and jth qubit are entangled, after tracing out all other qubits, if and only if (i,j) is an edge of G.

Solution is actually simple, but proof requires carefull computations. the state $|\psi_G\rangle$ of the form $|\psi_G\rangle = \alpha|0^{(n)}\rangle + \beta|1^{(n)}\rangle + \frac{\gamma}{\sqrt{k}}\sum_{(i,j)\in E_G}|1\rangle_i|1\rangle_j|0\ldots 0\rangle_{\bar{i}\bar{j}}$, where E_G is the set of k edges of G and $|\alpha|^2+|\beta|^2+|\gamma|^2 = 1$ satisfies the above conditions if

$$|\gamma|^2 k \leq 4|\alpha|^2, \quad |\alpha\beta|^2 \geq |\gamma|^4.$$

A solution is therefore a supperposition of states from the subspace dimension of which grows at most quadratically with the number of edges of the underlying graph G.

Peschl and Bužek (2002) posed also a new interesting/important question concerning the distribution of bipartite entanglement and classical correlations in multi-qubit states.

Let us assume that an n node graph G is given in which each edge is labelled by e (quantum correlation) or by c (classical correlation). The question now is whether there exists a quantum state $\phi_G\rangle$ such that two its qubits i and j are entangled (classically correlated) if and only if graph G has edge (i, j) and it is labelled by e (by c).

They have shown that not for all 3 qubits graphs of above types there is correpsonding pure state. To determine in which cases such graph exists is an interesting open problem.

8.3.15 Disentanglement

Disentanglement of entangled states is another interesting subject. If ρ is an entangled bipartite state, then $\rho_p = Tr_B(\rho) \otimes Tr_A(\rho)$ is called *disentanglement of ρ to the product state* and $\rho_s = \sum_i p_i \rho_i^A \otimes \rho_i^B$, where $Tr_A(\rho) = Tr_A(\rho_s)$, $Tr_B(\rho) = Tr_B(\rho_s)$ and ρ_i^A (ρ_i^B) is the density matrix of the subsystem A (B), is called *disentanglement of ρ into separable states*. It has been shown that an unknown bipartite state cannot be disentangled neither to product state nor

to separable states (Terro (1999), Mor (1998)). A related problem is disentanglement of an unknown state randomly chosen from a known set of states. By Mor and Terro (1999), any set of distinguishable states or of the states with identical density matrices can be disentangled into the product states and any set of states such that a reduced density matrices of one of the parties commute can be disentangled into separable states.

page 339, add at the end The above principles are connected with a belief of some that there are laws of governing entanglement processing that are analogous to those of thermodynamics. The entanglement is considered then to play the role of energy. This entanglement-energy analogy has been farther explored recently by Horodeckis (2000). They postulate that

- Entanglement is a form of quantum information corresponding to internal energy;
- Sending qubits corresponds to work.

They have also shown that in closed bipartite quantum communication systems information is conserved and so is in deterministic distillation protocols.

In order to consider balance of quantum information they introduce, in addition to the concept of physical work, the concept of **useful logical work** in quantum communication to be the amount of qubits transmitted without decoherence.

8.3.16 A classical analogue of entanglement

Since entanglement seems to be the most deep departure of quantum mechanics from classical physics of interest is also to look for some reasonable classical analogues of it. There are two reasons for such a search: (1) Such an analogy could help to see those aspects of entanglement that are actually classical, but that are often considered as quantum; (2) An analogy could help to transfer questions from quantum domain into classical one and vice versa that could be beneficial for both sides.

A recent attempt to develop such an analogy has been due to Collins and Popescu (2001). Their analogy is summarized in the following table

quantum entanglement	secret classical correlation
quantum communication	secret classical communication
classical communication	public classical communication
local actions	local actions

Here secret (public) communications are such that an eavesdropper cannot (can) have the access to the communication.

The basis of the analogy is the similar behavior of secret correlations and quantum entanglement under LOPC (local operations and public communication) and LOCC.

As a classical analogue of a pair of entangled particles they see two secret, correlated, random variables – one at each of the remote parties.

Some other analogies they see: ebit – shared secret bit; qubit – secret bit; classical bit – public classical bit.

Derived analogies: teleportation – one-time pad;[26] entanglement concentration – secret correlation concentration; entanglement dilution – secret correlation dilution; entanglement purification – classical privacy amplification; catalytic transformations – LOCC - LOPC; catalytic transformations – catalytic transformations; ….

Other analogies: environment - eavesdropper.

On a more technical part their basic analogy, quite nontrivial one, is derived as follows.

If Alice and Bob own particles in the state $|\psi\rangle$ of a bipartite system $A \otimes B$, that can be written in the Schmidt basis as

$$|\psi\rangle = \sum_i \sqrt{p_i}|i_A\rangle|i_B\rangle.$$

[26] they did not find any analogue to quantum superdense coding.

Then for the random variables X_A and X_B, for measurement results, in the Schmidt basis, it holds that $Pr(X_A = i, X_B = j) = \delta ijp_i$. In addition, the values of X_A and X_B are secret, not known to some third party E.

On this base Collins and Popescu (2001) proposed the following classical analogue. A bipartite classical state is such a distribution that

$$Pr(X_A = i, X_B = j, X_E = k) = \delta_{ij} p_i \bar{P}r(E_k),$$

where $\bar{P}r(E_k)$ is the distribution of eavesdropper's variable X_E and it is completely irrelevant, except for the fact that it is uncorrelated with distributions X_A and X_B. (The role of the third party can be puzzling here. The point is that in the quantum case if we know a (mixed) state – density operator – of two parties, we can find out of it whether they are entangled with some other party. This is not so in the classical case and therefore the third party has to be involved very explicitly.)

Their final point is the following fundamental one: quantum entanglement and shared secret correlations are so deeply related that "one should never be viewed without the other".

The approach of Collins and Popescu (2001) seems to show again a deep relation between quantum communication and secret communication.

8.3.17 Generalized approach to entanglement

The usual approach to entanglement assumes at least two distinguishable quantum systems and it is expressed in terms of subsystems.

It has turned out that for several reasons a more general approach to entanglement is needed, possible and stimulating.

First of all, it is known that also a single particle can be seen as being entangled. For example, letus consider the state of one photon in two copled cavities. Since each cavitis a quantum system, the state where the photon is is an equally weighted superposition of being in either cavity what can be represented by a Bell state.

Entanglement-like concepts for bosons, fermions and anyons have also a special form.

Based on the idea that entanglement is a relative concept and that the presence or absence of entanglement depends the physically relevant point of view,[27] Barnum et al. (2002) develop an approach to study entanglement-like properties in a more general setting of partially ordered families of Lie algebras and even of convex cones of states[28]. This allows to study certain feautures of entanglement without refereing to subsystems. They show that one can study such concepts as entanglement, separability and product states without reference to subsystems.

One goal is to get a better insight into ...... The second reason is to get a better understanding of entnaglement-like concepts in condense matter.

Barnum et al. (2002) showed that a more general theory based on Lie algebras exhibits most of the features as bipartite entanglement does and that many of these feautures can be found even in the convex cone setting. They also show how their general approach applies to fermions, bosons, and anyons.

Another general goal of their generalizations is to connect the theory of entanglement and the theory of coherent states. Their main conclusion is that the usual entanglement theory is a special case of a more general theory that has also other applications. Another conclusion is that entenglement is a relative concept and that states that are mixed from one perspective can be pure from another, more powerful perspective.

page 340, an addition 8.4.3 Information as a resource in distributed quantum systems

Horodecki et al. (2002) suggested to consider **information** as an important additional resource for distributed quantum computing and started to develop basics of a theory of information manipulation that parallel that of entanglement manipulation.

Starting from the purely operational point of view, namely, that *information*, whatever it is, cannot increase under noisy operations, cannot be created and can only be manipulated and lost, they derive the following measure for the amount of information in a mixed state ρ of a bipartite system of the total number of qubits N:

$$I(\rho) = N - QS(\rho).$$

[27]In particular, that how much entanglement is present depends on the observables to measure the system and describe its state.

[28]States when seen as linear functionals on on observables form a convex cone

They expect that a theory that will consider such an information as a resource can contribute to our understanding of the irreversibilities (due to information loses) in entanglement manipulations.

They show that in order to study information as a resource modifications of concepts and methods used to study entanglement manipulation are useful. For example instead of LOCC they consider so called NLOCC which differ from LOCC in that that addition of only noisy ancillas is allowed.

As a parallel of the entanglement distillation problem they consider problem of distillation of product states and the task of concentration of information is formulated as optimal distillation of product states. Technically, the question is: *how many pure product states can one distill from a given mixed state ρ?* They see this as a way to quantify *quantum correlations* taken the position that the amount of information that cannot be concentrated, into pure product states, must be quantum. That is why they define the **classical information contents** I_l of a state ρ (or the amount of concentratable information) as the optimal rate $\frac{2n}{m}$, where n is the number of copies of the state ρ and m is the number of two-qubit pairs output into pure product states. On this basis they define the contents of quantum correlations in a state ρ as

$$\Delta(\rho) = N - QS(\rho) - I_l(\rho).$$

Horodecki et al. (2002) show some upper bounds on $I_l(\rho)$ and $\Delta(\rho)$ and conjecture that

$$I_l(\rho) = N - QS(\rho) - D^{\infty}(\rho),$$

where $D^{\infty}(\rho)$ is regularized relative entropy distance from the set of IPB states[29]

Chapter 9 - Appendix

page 352, before Section 9.1.5 Several additional types of measurements seem to be of growing interest for QIP.

- **Weak measurements.** In a single such measurement of any observable A the disturbance caused to the system is minimized at the expense of precision of the measurement. However, for a large number of measurements one can determine some statistical averages, for example the expectation value of A.

[29]IPB stands for *Implementable Product Basis* – it is basis that can be obtained from the standard basis by means of reversible NLOCC.

- **Interaction-free measurements** are usually defined as the ones that determine the presence or absence of an object by means of a test particle even though no "interaction" may have occurred between the object and the particle. (IFM is a special case of counterfactual effects, see page 156.)

  However, more exactly, they are measurements at which no energy is exchanged between the measurement device (probe) and the object, but the presence of the object is determined. (However, the fact that no energy is exchanged between the probe does not preclude the possibility of other quantum number being exchanged and therefore the term "interaction-free" is quite misleading.)

page 357, at the end of section 9.1.5 Another puzzling phenomenon that has been recently explored in connection with the quantum computing are so-called **counter-factual effects**.[30] An event can have an impact if it could happen even if it did not happen.

A well-known and much studied recently example of such a phenomenon are **interaction-free measurements** (IFM).

Another interesting example of the counter-factual phenomenon are **counter-factual computations** at which the result of a computation may be obtained without running the computation — provided such a computation is possible even though the computation is not performed. Mitchison and Jozsa (1999) study the potentials and limitations of protocols for counterfactual solution of decision problems.

page 362, at the end

Hardy's axioms for quantum theory

Hardy (2001) has shown that the mathematical structure of quantum mechanics can be derived from 5 simple axioms.

His basic setting is that an experimentator has a preparation device, a transformation device and a measurement device and a quantum state is a property of a preparation device. In usually way he then defines probabilities of measurement based on frequency of outcomes of measurements, A minimum number, K, of appropriately chosen probability measurements that completely specify the state of the system is called

[30]The term *counter-factual* comes from philosophy/logic and is used for events that cause subsequent events even if they do not happen.

the number of degrees of freedom of the system. The *dimension* N of a system is defined as the maximum number of states that can be distinguished reliably in one measurement. Hardy's axioms have now the form:

Axiom 1 (probabilities): Relative frequencies (measured by taking the proportion of times a particular outcome is observed) tend to the same value (which we call probability) for any case where a given measurement is performed on a ensemble of n systems prepared by some given preparation in the limit as n becomes infinite.

Axiom 2 (simplicity) K is detrmined by a function of N, where $N = 1, 2\ldots$ and where, for each given N, K takes the minimum value consistent with the axioms.

Axiom 3 (subspaces): A system whose state is constrained to belong to an M dimensional subspace (i.e. have support on only M of a set of N possible distinguishable states) behaves like a system of dimension M.

Axiom 4 (composite systems): A composite system consisting of subsystems A and B satisfies $N = N_A N_B$ and $K = K_A K_B$.

Axiom 5 (continuity): There exists a continuous reversible transformation on a system between any two pure states of that system.

Shack (2002) has shown that the first axiom is superflous if for probabilities Bayesian view is taken at which probabilities are not objective states of nature, but rather degrees of belief that determine an agent's decisions in the face of uncertainity. In this approach a quantum state represents a state of belief (and therefore no physical collapse happens at a measurement).

Information processing axioms for quantum theory

One of the most fascinating ideas that has recently came up in QIPC is whether one can derive mathematical framework of quantum theory from some natural laws or limitations of quantum information processing. As quoted by Clifton et al. (2002), this corresponds to very short and basic question of David Deutsch, namely *can we get* **it from qubit**?

Clifton et al. claim/believe that quantum theory can be derived from the following three axioms – laws of nature – that at the same time represents three fundamental results, three "no-go" theorems, of QIPC:

- The impossibility of superluminal information transfer between two physical systems by performing measurement on one of them.
- The impossibility of perfectly broadcasting the information contained in an unknown physical state.
- The impossibility of unconditionally secure bit commitment.

page 364, at the end

Remark Werner and Wolf (2001) present a broad overview of basic problems and results concerning Bell inequalities and their relations to the entanglement problem. They discuss also Bell inequalities in the framework of Algebraic Quantum Field Theory.

Remark Vaidman (2001) points out that in spite of the remarkable recent progress in the tests of Bell inequalities, a decisive experiment that would ruled out any local variable theory has not been performed yet. In additions he shows that some experiments do not justify conclusions authors make (for example due to the fact that they exclude only certain types of local variables theories or close some loopholes for the price of opening a new one).

Vaidman (2001) also points out that "instead of showing that the quantum correlations cannot be explained by local theories, it is more important to show that the quantum correlations can be used". For example, he suggest that in order to illustrate that Nature has non-locality features entanglement implies it would be sufficient to show that for some games, as "Guess my number game", players using quantum features could perform better that players using only classical tools. Vaidman (2001) also points out that in spite of the remarkable recent progress in the tests of Bell inequalities, a decisive experiment that would ruled out any local variable theory has not been performed yet. In additions he shows that some experiments do not justify conclusions authors make (for example due to the fact that they exclude only certain types of local variables theories or close some loopholes for the price of opening a new one).

Vaidman (2001) suggest also a new game, the so called "Impossible necklace game' '. Two parties, that cannot communicate, want to persuade the third one that they have copies of a necklace with an even number n of beads of the two color beads, such that all neighboring beads are of different colors, with the exception of the first and the last one. The interrogator is allowed to ask them to let him to know colors of any two neighboring beads.

Classically, the probability that they pass the test $5n$ times is $(1-\frac{1}{n})^{5n} \approx e^{-5} \approx 0.01$. However, in case if for each pair of neighboring beads players share an EPR state, and they answer questions due to the outcomes of some quantum projection measurements, then the probability of errors can be reduced to $e^{-\frac{5\pi^2}{4n}}$.

Vaidman (2001) suggest also a new game, the so called "Impossible necklace game". Two parties, that cannot communicate, want to persuade the third one that they have copies of a necklace with an even number n of beads of the two color beads, such that all neighboring beads are of different colors, with the exception of the first and the last one. The interrogator is allowed to ask them to let him to know colors of any two neighboring beads.

Classically, the probability that they pass the test $5n$ times is $(1-\frac{1}{n})^{5n} \approx e^{-5} \approx 0.01$. However, in case if for each pair of neighboring beads players share an EPR state, and they answer questions due to the outcomes of some quantum projection measurements, then the probability of errors can be reduced to $e^{-\frac{5\pi^2}{4n}}$.

Remark Volovich (2000) seems to bringing up new important points concerning Bell theorem.

His main point is that the space part of the wave function was neglected in the Bell theorem even it is exactly this part that is crucial for consideration of property of locality of quantum systems. As he pointed out, the space part of the wave function leads to an extra factor in quantum correlations and as the result the ordinary proofs of Bell theorem fail. (Actually, the very formulation of the locality problem in quantum mechanics is based on ascribing a special role to the position in Euclid three-dimensional space.)

Volovich (2000) argues that predictions of quantum mechanics for Gaussian wave functions can be consistent with Bell's inequalities and hence Einstein local realism is restored in this case.

Volovich admits that he did only a rough estimate and it would be interesting to investigate whether one can prepare a reasonable wave function for which the usual condition of non-locality is satisfied for a pair of the well separated regions. However, he suspects that in order to establish such a localization one has to destroy the original entanglement because it was created far away from detectors.

To illustrate that his new view of Bell theorem are not only philosophical Volovich (2000a) shows that, form his new point of view, the proof of security of Ekert's 91 quantum key generation protocol, see Section 6.2.5 in the book, is not correct.

There has been recently significant progress in closing some loopholes. Rowe (2001) is believed to close the efficiency loophole and Weihs et al. (1998) seem to close the locality loophole. On the other hand there does not seem to be a way feasible to close currently both loopholes in a single experiment. **9.1.9 Bell inequalities and quantum entanglement**

A fundamental problem is to determine relation between entanglement and Bell inequalities.

So called Gisin's theorem (Gisin (1991)) says that each bipartite pure entangled state violates the CHSH -inequality.

It has been believed, till recently, that the same is true for all pure entangled states – that each of them violates some Bell inequality.

However, Zukowski et al. (2001), have shown that there is a family of multipartite pure states that do not violate any Bell inequality. Namely, it is the family of states

$$|\psi\rangle = \cos\alpha|0(n)\rangle + \sin\alpha|1^{(n)}\rangle,$$

with $0 \leq \alpha\pi/4$. Indeed, if $2\alpha \leq \frac{1}{\sqrt{2^{n-1}}}$, then these states violate so called Mermin-Ardehali-Bielinski-Klysko inequality.

To show that, they used the result from Zukowski and Brukner (2001), that there is a single general Bell inequality, which is a necessary and sufficient condition "for the correlation function for n particles to be describable in a local and realistic picture, for the case where measurements on each particle can be chosen between two arbitrary dichotomic observables".

It is still an interesting and important open problem to determine fully which pure entangled states do not violate any Bell inequality.

The case of mixed entangled states is even less clear.

Werner (1989) showed for certain class of entangled mixed states that they do not violate any Bell inequality. (However, Popescu (1995) showed that some of these Werner's states exhibit so-called "hidden non-locality". Dürr (2001) showed that there are multipartite bound entangled states that violate a (multipartite) Bell inequality (and therefore they cannot be described by a LHV theory).

9.1.10 Special quantum phenomena

In this section we present briefly various special quantum phenomena that are being more intensively explored and/or utilized in QIP.

Quantum Zeno effect (another (older) name is a "watchdog effect") refers to the observation that if a coupling of a quantum system with environment is very strong (what can be caused also by (very) frequent measurements), then internal dynamics of the system may be slowed down, or even frozen.

9.1.11 Limitations of quantum mechanics?

A variety of puzzling, mysterious and paradoxical phenomena of quantum mechanics naturally arise questions about the proper scope of quantum mechanics.

For example, Bell mentions the possibility that quantum mechanics is of limited validity and applies only when "the setting of instruments are made sufficiently in advance to allow them to reach some mutual rapport by exchanging of signals with velocity less than or equal to that of light".

page 374, at the end

Remark 0.2 (DiVincenzo et al. 1999) Various concepts of superoperators are used in QIP literature. The most general one is that of a completely positive map that does not increase trace. Such maps, say $\mathcal{L}$, can be written as $\mathcal{L}(\rho) = \sum_{i\in I} L_i\rho L_i^*$, where $\sum_{i\in I} L_iL_i^* \leq I$, with the equality holding for trace-preserving superoperators. They correspond to "non-selective dynamics". Trace decreasing superoperators correspond to "selective dynamics" — e.g. a measurement that then discards some outcomes.

A superoperators is said to be separable if L_i are tensor products of local operators, each on the corresponding subspace from which the total space is composed. A superoperator is a multilocal superoperator if it can be implemented locally using classical communications between the parties.

Characterization results for density matrices

Two characterization results concerning mixed state representation of density matrices and of the probability distributions are of interest and importance.

The first result (Hughston et al. 1993) characterizes mixed states $[\phi\rangle$ such that $\rho_{[\phi\rangle} = \rho$ for a given density matrix ρ.

Theorem If ρ is a density matrix, then $\rho_{[\phi\rangle} = \rho$ for a mixed state $\bigoplus_{i=1}^{k}(p_i, |\psi_i\rangle)$, if and only if there exists a unitary matrix $U = \{u_{ij}\}$ such that $\sqrt{p_i}|\psi_i\rangle = \sum_j u_{ij}|e_j\rangle$, where $|e_j\rangle$ are eigenvectors of ρ such that $\langle e_j \mid e_j\rangle$ are the corresponding eigenvalues.[31]

The second result (Nielsen, 1999a) characterizes probability distributions consistent with a given density matrix.

Theorem If ρ is a density matrix and $p = (p_1, \ldots, p_n)$ a probability distribution, then there are pure states $|\phi_i\rangle$ such that $\rho = \bigoplus_{i=1}^{n}(p_i, |\phi_i\rangle)$ if and only if $p \prec \lambda_\rho$, where λ_ρ is the vector of eigenvalues of ρ and $\prec$ stands for the majorisation relation defined on page 333.[32]

page 390, at the end of Section 9.3.3 Remark 0.3 Surprising are recent de-randomization results in the study of the power of randomness. For example, Impagliazzo and Wigderson (1999) have shown that if **BPP** $\neq$ **EXP**, then every problem in **BPP** can be solved deterministically in subexponential time on almost every input. This result maybe interpreted that either **P** = **BPP** or **BPP** = **EXP**, what is really hard to believe. This interpretation is correct in the spirit even if not quite technically. The above result indicates that our intuition that randomness is a resource basically not comparable with time is wrong. The result that either there is a non-trivial deterministic simulation of **BPP** or **BPP** = **EXP** shows that either time can non-trivially substitute for randomness, or randomness can non-trivially substitute for time (Impagliazzo and Wigderson, 1999). (On the basis of this result one can wonder what a study of dequantumization can tell us.)

Chapter 9 - Historical remarks

page 399, addition to the end of line -2 Cleve and DiVincenzo's algorithm requires $\Omega(n^3)$ elementary quantum operations. A more efficient algorithm, presented by Reif (1998a), requires $\mathcal{O}(n \lg^4 n \lg\lg n)$ elementary quantum operations for asymptotically optimal noiseless quantum compression and decompression. Jozsa et al. (1998) generalized the Schumacher compression to the case that the compressor does not need to known the quantum source. i.e. its density matrix (what was assumed

[31]It is here understood that in the case there are more pure states $|\psi_i\rangle$ than eigenvectors $|e_j\rangle$, one should append extra zero vectors to the list of eigenvectors until both lists have the same number of elements.

[32]It is again assumed that if the probability vector is longer than that of eigenvalues then the second one is appended by zeroes to have both of the same length.

in Schumacher's result), only its quantum entropy, and they have provided the first asymptotically optimal universal quantum compression algorithm).

The result of Jozsa et al. (1998) can be formulated as follows

Theorem For any ε, δ there is an $n = n(\varepsilon, \delta)$ such that for any entropy bound S there is an encoding scheme that works for any source (mixed state, density matrix) $\rho = \sum_{i=1}^{k} p_i |\phi_i\rangle\langle\phi_i|$, with all $|\phi_i\rangle \in H_d$ for some d and $QS(\rho) \leq S$, in such a way that:

- Each $|\phi_i\rangle$ can be encoded by a codeword σ_i of length $\leq S + \delta + \frac{1}{n}(d^2 \lg(n+1))$
- For each i fidelity $F(\phi_i, \sigma_i) \geq 1 - \varepsilon$.

page 400, addition to line -8 From new overview and survey papers see: Cleve (1999) — quantum complexity (especially relations between computational complexity, query complexity and communication complexity); Bennett and Shor (1998) — quantum information theory; Gruska (1999a) — quantum automata; Gruska (1999b), Gruska (2000), Gruska (2000a); Plenio and Vedral (1998) — quantum entanglement; Gruska and Imai (2001) – quantum entanglement, Pellizari (1998) — principles and the initial developments in trapped ions and QED quantum computing technology; Chuang (1998) — principles and initial developments in NMR quantum computing technology; Tittel and Weihs (2001) — Photonic entanglement.

page 400, addition to line -5 The book by editors Lo et al. (1998) contains a collection of overview papers on a variety of subjects of quantum computing and information processing. Proceedings "Quantum computing and quantum communication" edited by Williams (1999) contains full versions of papers presented at the 1st NASA International Conference on Quantum Computing & Quantum Communication. The book by Chuang and Nielsen (2000) deals with quantum computing from physics point of view; Hirvensalo (2001) presents in details Shor's and Grover's algorithms.

page 400, additions to line -1 before final dot ", 1999 (106), 2000 (13?), first half of 2001 (156?)"

BIBLIOGRAPHY

page 409, item 189 Paper has already appeared in "Journal of Computer and System Sciences", 59(2):240-252, 1999.

page 411, item 229 Paper has appeared in "Physical Review Letters", V80 (2), 5239-5242, 1998.

page 414, item 312 Paper has appeared under the new title: "Conditions for a class of entanglement transformation" in "Physical Review Letters", V83 (2), 436-439, 1999.

References

[1] Sergip Aalbeverio and Shao-Ming Fei. Teleportation of general finite dimensional quantum systems. Technical report, quant-ph/0012035, 2000.

[2] Scott Aaronson. Quantum lower bound for the collision problem. Technical report, quant-ph/0111102, 2001.

[3] Scott Aaronson. Multilinear formulas and skepticism of quantum computing. 2003.

[4] Ayman F. Abouraddy, Bahaa E. A. Saleh, and Alexander V. Sergienko. Degree of entanglement for two qubits. Technical report, quant-ph/0109081, 2001.

[5] A. Acin, Gerard Vidal, and J. I. Cirac. On the structure of a reversibe entanglement generating set for three-partite states. Technical report, quant-ph/0202056, 2002.

[6] D. Aharonov, A. Ta-Shna, Umesh Vazirani, and A. Yao. Quantum bit escrow. In *Proceedings of 32th STOC*, pages ???–???, 2000.

[7] Dorit Aharonov, Andris Ambainis, Julia Kempe, and Umesh Vazirani. Quantum walks on graphs. Technical report, quant-ph/0012090, 2000. Proc. of 33th STOC, 50-59.

[8] J. Ahn, T. C. Weinacht, and P. H. Bucksbaum. Information storage and retrieval through quantum phase. *Science*, 287:463–465, 2000.

[9] Sergio Albeverio and Shao-Ming Fei. A note on invariants and entanglement. Technical report, quant-ph/0109073, 2001.

[10] Masami Amano and Kazuo Iwama. Undecidability on quantum finite automata. In *Proceedings of the 31st ACM STOC*, pages 368–375. ACM, 1999.

[11] Andris Ambainis. Quantum lower bounds by quantum arguments. Technical report, quant-ph/0002066, 2000.

[12] Andris Ambainis, E. Bach, A. Nayak, A. Vishwanath, and J. Watrous. One-diemsional quantum walks. 2001.

[13] Andris Ambainis, Richard Bonner, Rūsiņš Freivalds, and Arnolds Kikusts. Probabilities to accept languages by quantum finite automata. Technical report, quant-ph/9904066, 1999.

[14] Andris Ambainis and Ronald de Wolf. Average-case quantum query complexity. Technical report, quant-ph/9904079, 1999.

[15] Andris Ambainis and Arnolds Kikusts. Exact results for acceepting probabilities of quantum automata. In *Proceedings of ????, LNCS 2136, 135-147*, pages 135–147, 2001.

[16] Andris Ambainis and John Watrous. Two-way finite automata with quantum and classical states. Technical report, quant-ph/9911009, 1999.

[17] Andris Ambainis and Ke Yang. Extracting quantum enetanglement (general entanglement purification protocols. Technical report, quant-ph/0110011, 2001.

[18] Arwind and N. Mukunda. A two-qubit algorithm involving quantum entanglement. Technical report, quant-ph/0006069, 2000.

[19] Alexei Ashikhmin, Alexander Barg, Emanuel Knill, and Simon Litsyn. Quantum error detection I: Statement of the problem. Technical report, quant-ph/9906126, 1999.

[20] Alexei Ashikhmin, Alexander Barg, Emanuel Knill, and Simon Litsyn. Quantum error detection II: Bounds. Technical report, quant-ph/9906131, 1999a.

[21] D. V. Averin. Adiabatic quantum computation with cooper pairs. *Solid State Communications*, 105:659–664, 1998.

[22] Somshubhro Bandyopadhyay, Vwani P. Roychowdhury, and Ujjwal Sen. A classification of incomporable states. Technical report, quant-ph/0103131, 2001.

[23] Howard Barnum. Quantum secure identification using entanmglement as catalyst. Technical report, quant-ph/9910072, 1999.

[24] H. Bechmann-Pasquinucci and Asher Peres. Quantum cryptography with 3-state systems. *Physics Review Letters*, 85:3313–3316, 2000.

[25] H. Bechmann-Pasquinucci and W. Tittel. Quantum cryptography using larger alphabet. *Physics Review A*, 61:???–???, 2000.

[26] S. C. Benjamin. A comment on "quantum approach to static games of complete information". Technical report, quant-ph/0008127, 2000.

[27] S. C. Benjamin and P. M. Hayden. Comment on "quantum games and quantum strategies". Technical report, quant-ph/0003036, 2000.

[28] Charles Bennett, Peter W. Shor, John A. Smolin, and Ashish V. Thaliyal. Entenglement assisted capacity of a quantum channel and the reverse Shannon theorem. Technical report, quant-ph/0106052, 2001.

[29] Charles H. Bennett, David P. DiVincenzo, C. A. Fuchs, T. Mor, E. Rains, Peter W. Shor, John A. Smolin, and W. K. Wooters. ??????? Technical report, quant-ph/98040053, 1998. Phys. Rev. A V59, 1070-???

[30] Charles H. Bennett, Sandu Popescu, Daniel Rohrlich, John A. Smolin, and Ashish V. Thapliyal. Exact and asymptotic measures of multipartite pure state entanglement. Technical report, quant-ph/9908073, 1999.

[31] Charles H. Bennett and Peter W. Shor. Quantum information theory. *IEEE Transactions on Information Theory*, 44:2724–2742, 1998.

[32] Charles H. Bennett, Peter W. Shor, John A. Smolin, and Ashish V. Thapliyal. Entanglement-assisted classical capacity of noisy quantum channels. Technical report, quant-ph/9904023, 1999a.

[33] Janos A. Bergou, Mark Hillery, and Yuqing Sun. Non-unitary transformations in quantum mechanics: an optical realization. *Journal of Modern Optics*, 47:487–497, 2000.

[34] André Berthiaume, Wim van Dam, and Sophie Laplante. Quantum Kolmogorov complexity. Technical report, quant-ph/0005018, 2000.

[35] Aija Berzina, Richard Bonner, and Rūsiņš Freivalds. Parameters in Ambainis-Freivalds algorithm. In *Proceedings of the International Workshop on Quantum Computing and Learning, Sundbyhols Slott, Sweden, May 2000*, pages 101–109, 2000.

[36] Thomas Beth and Markus Grassl. The quantum Hamming and hexacodes. *Fortschritte Phys.*, 46:459–491, 1998.

[37] Eli Biham, Michel Boyer, P. Oscar Boykin, Tal Mor, and Vwani Roychowdhury. A proof of the security of quantum key distribution. Technical report, quant-ph/9912053, 1999.

[38] Richard Bonner, Rūsiņš Freivalds, and Maxim Kravtsev. Quantum versus probabilistic one-way finite automata with counter. In *Proceedings of the International Workshop on Quantum Computing and Learning, Sundbyholms Slott, Sweden, May 2000*, pages 80–88, 2000a.

[39] Richard Bonner, Rusins Freivalds, and Madars Rikards. Undecidability on quantum finite- one-counter automata. In *Proceedings of the International Workshop on Quantum Computing and Learning, Sundbyholms Slott, Sweden, May 2000*, pages 65–71, 2000.

[40] Sugato Bose and Vlatko Vedral. Mixedeness and teleporattion. Technical report, quant-ph/9912033, 1999.

[41] Sugato Bose, Vlatko Vedral, and Peter L. Knight. A multiparticle generalization of entanglement swapping. Technical report, quant-ph/9708004, 1997.

[42] Jan Bouda and Vladimír Bužek. Entanglement swapping between multiqudit systems. Technical report, Tech. Report, Faculty of Informatics, Masaryk University, 2000.

[43] Charles M. Bowden, Goong Chen, Zijian Diao, and Andreas Kalppenecker. The universalilty of the quantum fourier traqnsform in forming the basis of quantum computing algorithms. Technical report, quant-ph/0007122, 2000.

[44] P. Oscar Boykin, Tal Mor, Matthew Pulver, Vwani Roychowdhury, and Farrokh Vatan. On universal and fault-tolerant quantum computing. Technical report, quant-ph/9900054, 1999.

[45] P. Oscar Boykin and Vwani Roychowdhury. Optimal encryption of quantum bits. Technical report, quant-ph/0003059, 2000.

[46] Martin B.Plenio and Vlatko Vedral. Teleporatation, entanglement and thermodynamics inthe quantum world. Technical report, quant-ph/9804075, 1998.

[47] Gilles Brassard, Peter Hoyer, Michele Mosca, and Alain Tapp. Quantum amplitude amplification and estimation. Technical report, quant-ph/0005055, 2000.

[48] Samuel L. Braunstein and Jeff H. Kimble. Teleportation of continuous quantum variables. *Physical Review Letters*, 80:869–872, 1998.

[49] Shamuel L. Braunstein and H. Jeff Kimble. Exprimental quantum teleportation. *Nature*, 394:840–841, 1998.

[50] M. J. Bremner, Ch. M. Dawson, J. L. Dodd, A. Gilchris, A. W. Harrow, D. Mortimer, M. A. Nielsen, and T. J. Osborne. A oractical scheme for quantum computation with any two-qubit entangling gate. Technical report, quant-ph/0207072, 2002.

[51] Björn Brezger, Lucia Hackermüller, Stefan Uttenthaler, Julia Petschinka, Markus Arndt, and Anton Zeilinger. Matter-wave interferometer for large molecules. Technical report, quant-ph/0202158, 2002.

[52] Todd . Brun, Hilary A. Carterer, and Andris Ambainis. The quantum to classical transition for random walks. Technical report, quant-ph/0208195, 2002.

[53] Dagmar Bruß. Entanglement splitting of pure bipartite quantum states. Technical report, quant-ph/9902023, 1999a.

[54] J.-L. Brylinski and R. Brylinski. Universal quantum gates. Technical report, quant-ph/0108062, 2001.

[55] Harry Buhrman, Richard Cleve, Ronald de Wolf, and Christof Zalka. Bounds for small-error and zero-error quantum algorithms. Technical report, quant-ph/9904019, 1999.

[56] Harry Buhrman and Ronald de Wolf. Complexity measures and decision tree complexity. Technical report, cs.CC/9910010, 1999.

[57] Harry Buhrman, Christoph Dürr, Mark Heiligman, Peter Hoyer, Fréderic Magniez, Miklos Santha, and Roland de Wolf. Quantum algorithms for element distinctness. Technical report, quant-ph/0007016, 2000.

[58] Harry Buhrman, Serge Massar, and Hein Röhrig. Combinatorics and quantum non-locality. Technical report, quant-ph/0209052, 2002.

[59] William T. Buttler, Richard J. Hughes, Steve K. Lamoreaux, George L. Morgan, Jane E. Nordholt, and C. G Peterson. Daylight quantum key distribution over 1.6 km. Technical report, quant-ph/0001088, 2000.

[60] Cristian S. Calude and Boris Pavlov. Coins, quantum measurements, and turing's barrier. Technical report, quant-ph/0112087, 2001.

[61] A. Carlini and A. Hosoya. Quantum computers and classical randomized algorithms. Technical report, quant-ph/9907020, 1999.

[62] S. C.Benjamin and P. M. Hayden. Multi-player quantum games. Technical report, quant-ph/0007038, 2000.

[63] Li-Xiang Cen and Shun-Jin Wang. Distilling a Grenberger-Horne-Zeilinger state from an arbitrary pure state of three qubits. Technical report, quant-ph/0012022, 2000.

[64] Gregory J. Chaitin. *Algorithmic information theory*. Cambridge University Press, 1987.

[65] Andrew M. Childs, Richard Cleve, Enrico Deotto, Edward Farhi, Sam Gutmann, and Daniel A. Spielman. Exponential algorithmic speedup by quantum walks. Technical report, quant-ph/0209131, 2002.

[66] Andrew M. Childs, Edward Farhi, and Sam Gutmann. An example of the difference between quantum and classical random walks. Technical report, quant-ph/0103020, 2001.

[67] Andrew M. Childs, John Preskill, and Joseph Renes. Quantum information and precission measurement. Technical report, quant-ph/9904021, 1999.

[68] Isaac I. Chuang and Michael A. Nielsen. *Quantum information processing*. Cambridge University Press?, 2000.

[69] Isaac L. Chuang. *Introduction to quantum computation and information*, chapter Quantum computation with nuclear magnetic resonance, pages 311–339. World Scientific, 1998.

[70] Richard Cleve. An introduction to quantum complexity theory. Technical report, quant-ph/9906111, 1999.

[71] Richard Cleve. The query complexity of order-finding. Technical report, quant-ph/9911124, 1999.

[72] Richard Cleve and Daniel Gottesman. Efficient computations of encodings for quantum error correction. *Physics Review A*, 56:76–82, 1997.

[73] Richard Cleve and John Watrous. Fast parallel circuits for the quantum Fourier transform. Technical report, quant-ph/0006004, 2000.

[74] Bob Clifton, Jeffery Bub, and hans Halverson. Characterizing quantum theory in terms of information-theoretic constraints. Technical report, quant-ph/0210089, 2002.

[75] Valerie Coffman, Joydip Kundu, and William K. Wootters. Distributed entanglement. Technical report, quant-ph/9907047, 1999.

[76] Daniel Cory, Amr Fahmy, and Timothy F. Havel. ??? *Physica D*, 82:???–???, 1998a.

[77] Sumit Daftaur and Matthew Klimesh. The trumping relation and the structure of the bipartite entangled states. Technical report, quant-ph/0104058, 2001.

[78] G. M. D'Ariano, C. Macchiavello, and M. F. Sachi. Joint measurements via quantum clonning. *Journal of Optics*, B3, 2001.

[79] J. Niel de Beaudrap, Richard Cleve, and John Watrous. Quantum Fourier transforms for extracting hidden linear structures in finite fields. Technical report, quant-ph/0011065, 2000.

[80] Ronald de Wolf. Characterization of non-deterministic quantum query and quantum communication complexity. Technical report, quant-ph/0001014, 2000.

[81] F. DeMartini, V. Mussi, and F. Bovino. Schrödinger cat states and optimum universal quantum cloning by entangled parametric amplification. *Optics communication*, 179:2000, 2000.

[82] I. Devetak. The private classical information capacity and quantum information capacity of a quantum channel. quant-ph/0304127, 2003.

[83] David P. DiVincenzo, Tal Mor, Peter W. Shor, John A. Smolin, and Barbara M. Terhal. Unextendible product bases, uncompletable product bases, and bound entanglement. Technical report, quant-ph/9908070, 1999.

[84] David P. DiVincenzo, Peter W. Shor, John A. Smolin, Barbara M. Terhal, and Ashish V. Thapliyal. Evidence for bound entangled states with negative partial transpose. Technical report, quant-ph/9910026, 1999.

[85] Jiangfeng Du, Hui Li, Xiaodong Xu, Mingjun Shi, Xianyi Zhou, and Rongdian Han. Entanglement enhanced multiplayer quantum games. Technical report, quant-ph/0110122, 2001.

[86] Jiangfeng Du, Xiaodung Xu, Hui Lu, Mingjun Shi, Xianyi Zhou, and Rongdian Han. Nash equilibrium in quantum games. Technical report, quant-ph/0001050, 2000.

[87] Jiangfeng Du, Xiaodung Xu, Hui Lu, Mingjun Shi, Xianyi Zhou, and Rongdian Han. Quantum strategies without entanglemnet. Technical report, quant-ph/0011078, 2000.

[88] W. Dür and J. I. Cirac. Equivalence classes of non-local unitary operations. Technical report, quant-ph/0201112, 2002.

[89] W. Dürr and J.I. Cirac. Multipartite entanglement and its experimental detection. Technical report, quant-ph/0011025, 2000.

[90] J. Eisert, Martin Wilkens, and M. Lewenstein. ???? *Physical Review Letters*, 83:3077–30??, 1999.

[91] Jens Eisert and M. Wilkens. ???/? *Physics Review Letters*, 85:437–4??, 2000.

[92] N. J. Cerf et al. ???? *Physics Review A*, 57:1477–14??, 1998.

[93] G. Etesi and I. Németi. Non-Turing computations via Malament-Hogarth space-times. Technical report, quant-ph/0104023, 2001.

[94] E. Farhi and S. Gutmann. Quantum computation and decision treees. Technical report, quant-ph/9706062, 1997.

[95] S. A. Fenner and Y. Zhang. Universal quantum computation with two- and three-qubit projective measuremnts. Technical report, quant-ph/0111077, 2001.

[96] Richard Fitzgerald. What really gives a quantum computer its power. *Physics Today*, pages 20–22, January 2000.

[97] Lance Fortnow and John Rogers. Complexity limitations on quantum computation. *Journal of Computer and System Sciences*, 59:240–252, 1999.

[98] Rusins Freivalds and Andreas Winter. Quantum finite state transducers. Technical report, quant-ph/0011052, 2000.

[99] A. Furusawa, J. Sorenson, Shamuel L. Braunstein, Christopher A. Fuchs, H. Jeff Kimble, and E. S. Polzik. ???? *Science*, 282:706–707, 1998.

[100] S. Ghosh, G. Kar, A. Roy, A. Sen, and U. Sen. ??? Technical report, quant-ph/0106148, 2001.

[101] N. Gisin. Bell inequality holds for all non-product states. *Physical Letters*, 154:201–202, 1991.

[102] Nicolas Gisin and S. Masar. Optimal quantum cloning machines. *Physics Review Letters*, 79:2153–21??, 1997.

[103] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. Quantum cryptography. Technical report, quant-ph/0101098, 2001.

[104] Lior Goldenberg and Lev Vaidman. Quantum cryptography based on orthogonal states. *Physical Review Letters*, 75:1239–12??, 1995.

[105] Lior Goldenberg, Lev Vaidman, and Stephen Wiesner. Quantum gambling. *Physical Review Letters*, 82:3356–3359, 1999.

[106] Marats Golovkins. On quantum pushdown automata. In *Proceedings of the International Workshop on Quantum Computing and Learning, Sundbyhols Slott, Sweden, May 2000*, pages 41–51, 2000.

[107] V. N. Gorbachev and A. I. Trubilko. Quantum teleportation of EPR pair by three-particle entanglement. Technical report, quant-ph/9906110, 1999.

[108] Daniel Gottesman. Theory of quantum entanglement. Technical report, quant-ph/9910067, 1999.

[109] Daniel Gottesman and Isaac Chuang. Quantum digital signature. Technical report, quant-ph/0105032, 2001.

[110] Daniel Gottesman and Isaac L. Chuang. Quantum teleportation is a universal computational primitive. Technical report, quant-ph/9908010, 1999.

[111] Daniel Gottesman and Hoi-Kwang Lo. Proof of securitu of quantum key distribution with two-way classical communication. Technical report, quant-ph/0105121, 2001.

[112] Markus Grassl and Thomas Beth. Cyclic quantum error-correcting codes and quantum shift registers. Technical report, quant-ph/9910061, 1999.

[113] Markus Grassl and Thomas Beth. Quantum BCH codes. Technical report, quant-ph/9910060, 1999.

[114] Markus Grassl, Willi Geiselmann, and Thomas Beth. Quantum Reed-Solomon codes. Technical report, quant-ph/9910059, 1999.

[115] Markus Grassl, Martinn Rötler, and Thomas Beth. Computing local invariants of qubit systems. Technical report, quant-ph/9712040, 1997.

[116] Frederic Green, Steven Homer, and Christopher Pollet. On the complexity of quantum **acc**. Technical report, quant-ph/0002057, 2000.

[117] Lov K. Grover. Rapid sampling through quantum computing. Technical report, Bell Labs, 1999.

[118] Jozef Gruska. Quantum challenges. In *Proceedings of SOFSEM'99*, pages 1–28, 1999.

[119] Jozef Gruska. Quantum challenges for descriptional complexity. In *Proceedings of the International Workshop on Descriptional Complexity of automata, Grammars and Related Structures*, pages 23–38, 1999a.

[120] Jozef Gruska. Descriptional complexity issues in quantum computing. *Journal of Automata and Combinatorics*, 5:191–218, 2000.

[121] Jozef Gruska. *Mathematics unlimited, 2001 and beyond*, chapter Quantum computing challenges, pages 529–563. Springer-Verlag, 2000a.

[122] Jozef Gruska and Hiroshi Imai. Power, properties and mysteries of quantum entanglement. In *Proceedings of MUC'01*, pages 25–69, 2001.

[123] Lisa Hales and Sean Hallgren. An improved quantum Fourier transform algorithm and application. In *Proceedings of 41th IEEE FOCS*, pages ??–??, 2000.

[124] K. Hammerer, G. Vidal, and J. I. Cirac. Characterization of non-local gates. Technical report, quant-ph/0205100, 2002.

[125] L. Hardy. Quantum theory from five reasonable axioms. Technical report, quant-ph/0101012, 2001.

[126] Lucien Hardy. Disentangling nonlocality and teleportation. Technical report, quant-ph/9906123, 1999.

[127] Lucien Hardy and Adrian Kent. ?????? Technical report, quant-ph/9911043, 1999.

[128] Lucien Hardy and David D. Song. Universal manipulation of a single qubit. Technical report, quant-ph/0008011, 2000.

[129] Aram W. Harrow, Benjamin Recht, and Isaac L. Chuang. Tight bounds on discrete approximations of quantum gates. Technical report, quant-ph/0111031, 2001.

[130] Mark Hillery. Quantum cryptography with squeezed states. *Physical Review A*, 61:????–????, 2000.

[131] Tohya Hiroshima. Optimal dense coding with mixed state entanglement. Technical report, quant-ph/0009048, 2000.

[132] Mika Hirvensalo. *Quantum computing.* Springer Verlag, 2001.

[133] Michal Horodecki, Karol Horodecki, Pawel Horodecki, Jonathan Oppenheimer, Aditi Sen, and Ujiwal Sen. Information as a resource in distributed quantum systems. Technical report, quant-ph/0207168, 2002.

[134] Michal Horodecki, Pawel Horodecki, and Ryszard Horodecki. Limits for entanglement measures. Technical report, quant-ph/9908065, 1999.

[135] Michal Horodecki, Pawel Horodecki, and Ryszard Horodecki. On balance of information in bipartite quantum communication systems: entanglement-energy analogy. Technical report, quant-ph/0002021, 2000.

[136] Michal Horodecki, Pawel Horodecki, and Ryszard Horodecki. Mixed-state enatnglement and quantum communication. Technical report, in print, 2000a.

[137] Michal Horodecki, Aditi Senand Ujjwal Sen, and Karol Horodecki. Local indistinguishability and LOCC monotones. Technical report, quant-ph/0204116, 2002.

[138] Pawel Horodecki. How to measure amount of entanglement contained in unknown state. Technical report, quant-ph/0111082, 2001.

[139] Peter Hoyer and J. Neerbeck. Bounds on quantum order searching. Technical report, quant-ph/0009032, 2000.

[140] Peter Hoyer, Jan Neerbeck, and Yaoyun Shi. Quantum complexities of order searching, and element distinctnss. Technical report, quant-ph/0102078, 2001.

[141] Y-F. Huang. Optical realization of universal quantum cloning. *Phycics Review A*, 64:????, 2001.

[142] S. F. Huelga, J. A. Vaccaro, A. Chefles, and Martin Plenio. Quantum remote control: teleportation of unitary operations. Technical report, quant-ph/0005061, 2000.

[143] Lane P. Hughston, Richard Jozsa, and Wiliam K. Wooters. A complete classification of quantum ensembles having a given density matrix. *Physics Letters A*, 183:14–18, 1993.

[144] Bruno Huttner, N. Imoto, Nicolas Gisin, and Tal Mor. Quantum cryptography with coherent states. *Physical Review A*, 51:1863–1869, 1993.

[145] Russell Impagliazzo and Avi Wigderson. Randomness vs. time: derandomization under a uniform assumption. In *Proceedings of the ??th IEEE Computational Complexity Conference*, pages ???–???, 1999.

[146] H. Inamori. Security of EPR-based quantum key distribution. Technical report, quant-ph/0008064, 2000.

[147] A. Jamiolowski. ????? *Rep. Math. Phys*, 3:72, 1972.

[148] Dominik Janzig and Thomas Beth. Remark on multi-particle observables and entangled states with constant complexity. Technical report, quant-ph/0003117, 2000.

[149] Dominic Janzing, Pawel Wocjan, Robert M. Zeieer, R. Geiss, and Thomas Beth. The thermodynamic cost of reliability and low temperatures: tightening Landauer's principle and the Second law. Technical report, quant-ph/0002048, 2000.

[150] T Jennewein, C. Simon, G. Weihs, Harald Weinfurter, and Anton Zeilinger. A quantum cryptography with entangled photons. *Physics Review Letters*, 84:4729–4732, 2000.

[151] Jens G. Jensen and Rüdiger Schack. Quantum authentication and key distribution using catalysis. Technical report, quant-ph/0003104, 2000.

[152] I. D. Jonathan and Martin B. Plenio. Entanglement-assisted local manipulation of pure quantum states. Technical report, quant-ph/99?????, 1999. See also Phys. Rev. Lett., 83, 3566-35??, 1999.

[153] Jonathan A. Jones, R. H. Hansen, and Michael Mosca. Quantum logic gates and nuclear magnetic resonance pulse sequence. Technical report, quant-ph/9805070, 1998.

[154] Brian Julsgaard, Alexander Kozhekin, and Eugene S. Polzik. Experimental long-lived entanglement of two macroscopic objects. Technical report, quant-ph/00?????, 2000.

[155] Elham Kashefi, Adrian Kent, Vlatko Vedral, and Konrad Banaszek. On the power of quantum oracles. Technical report, quant-ph/0109104, 2001.

[156] Julia Kempe. Quantum random walks hit eponentially faster. Technical report, quant-ph/0205083, 2002.

[157] Adrian Kent. Unconditional secure bit commitment. *Physical Review Letters*, 83:1447–1450, 1999.

[158] Adrian Kent. Secure classical bit commitment over finite channels. Technical report, quant-ph/9906103, 1999a.

[159] Adrian Kent. Unconditionally secure commitment of a certified classical bit is impossible. Technical report, quant-ph/9910087, 1999b.

[160] Adrian Kent. Founding mistrustful quantum cryptography on coin tossing. Technical report, quant-ph/0111097, 2001.

[161] Adrian Kent. Quantum bit string commitment. Technical report, quant-ph/0111099, 2001a.

[162] Tien D. Kieu. Gödel's incompleteness, Chaitin's ω and quantum physics. Technical report, quant-ph/0111062, 2001.

[163] Tien D. Kieu. Quantum algorithm for the Hilbert's tenth problem. Technical report, quant-ph/0110136, 2001.

[164] Tien D. Kieu. Computing the noncomputable. Technical report, quant-ph/0203034, 2002.

[165] Tien D. Kieu. Quantum principles and mathematical computability. Technical report, quant-ph/0205093, 2002a.

[166] Arnolds Kikusts and Zigmars Rasščevskis. On the accepting probabilities of 1-way quantum finite automata. In *Proceedings of the International Workshop on Quantum Computing and Learning, Sundbyholms Slott, Sweden, May 2000*, pages 72–79, 2000.

[167] Christopher King. Additivity for unital qubit channels. Technical report, quant-ph/0103156, 2001.

[168] Alexei Kitaev and John Watrous. Parallelisation, amplification, and exponential time simulation of quantum interactive proof systems. In *Proceedings of 32th ACM STOC*, pages ??–??, 2000.

[169] Hartmut Klauck. On rounds in quqantum communication. Technical report, quant-ph/0004100, 2000.

[170] E. Knill, R. Laflamme, R. Martinez, and C. Negrevergne. Implementation of five qubit error correcting benchmark. Technical report, quant-ph/0101034, 2001.

[171] Emanuel Knill, R. Laaflame, R. Martinez, and C.-H. Tseng. An algorithmic beanchmark for quantum information processing. *Nature*, 404:368–370, 2000.

[172] M. Koashi and N. Imoto. Quantum cryptography based on split transmission of one-bit information in two steps. *Physical Review Letters*, 79:2383–2386, 1997.

[173] Masato Koashi, Vladimír Bužek, and Nobuyuki Imoto. Tight bounds for symmetric sharing of entanglement among qubits. Technical report, quant-ph/0007086, 2000.

[174] Hirotada Kobayashi and Keiji Matsumoto. Quantum multi-prover interactive proof systems and quantum characterizations of **nexp**. Technical report, quant-ph/0102013, 2001.

[175] Hideo Kosaka, Akihisi Tomita, Yoshihiro Nambu, Tadamasa Kimura, and Kazua Nakamura. Single photon experiment over 100km for quantum cryptography system using a balanced gate mode detector. Technical report, quant-ph/0306066, 2003.

[176] Maksim Kravcev. Quantum finite one-counter automata. Technical report, quant-ph/9905092, 1999.

[177] P. G. Kwiat, J. R. Mitchell, P. D. D. Schwwindt, and A. G. White. ?????? Technical report, quant-ph/9905086, 1999.

[178] Chiu Fan Lee and Neil F. Johnson. Theory of quantum gates. Technical report, quant-ph/0207012, 2002.

[179] Debbie W. Leung. Quantum Vernam cipher. Technical report, quant-ph/0012077, 2000.

[180] Debbie W. Leung. Two-qubit projective measurements are universal for quantum computation. Technical report, quant-ph/0111122, 2001.

[181] Leonid Levin. The tale of one-way function. *Problems of information transmission*, 39(1):???–???, 2003.

[182] Lev B. Levitin. Conditional entropy and information in quantum systems. *Chaos, Solitons and Fractals*, 10(10):1651–1656, 1999.

[183] Mang Li and Paul Vitányi. *An introduction to Kolmogorov complexity and its applications*. Springer-Verlag, 1993.

[184] Göran Lindblad. Completely positive maps and entropy inequalities. *Communications in Mathematical Physics*, 40:147–151, 1985.

[185] Noah Linden and Sandu Popescu. Bound entanglement and teleportation. Technical report, quant-ph/9807069, 1998.

[186] Noah Linden, Sandu Popescu, Ben Schumacher, and M. Westmoreland. Reversibility of local transformations of multiparticle entanglement. Technical report, quant-ph/9912039, 1999.

[187] Seth Lloyd. Quantum search without entanglement. Technical report, quant-ph/9903057, 1999.

[188] Seth Lloyd. Ultimate physical limits to computation. Technical report, quant-ph/9908043, 1999.

[189] Seth Lloyd. Computational capacity of the universe. Technical report, quant-ph/0110141, 2001.

[190] Seth Lloyd and Samuel L. Braunstein. Quantum computation over continuous variables. *Physical Review Letters*, 82:1784–1787, 1999.

[191] Seth Lloyd and Jean-Jacques E. Slotine. ??? *Physical Review Letters*, 80:4088–4091, 1998.

[192] Hoi-Kwang Lo. Will quantum cryptography ever become a successful technology in the marketplace. Technical report, quant-ph/9912011, 1999a.

[193] Hoi-Kwong Lo. A simple proof of the unconditional security of quantum key distribution. Technical report, quant-ph/9904091, 1999.

[194] Hoi-Kwong Lo, Sandu Popescu, and Tom Spiller. *Introduction to quantum computation and information*. World scientific, 1998.

[195] I. Marcikic, H. de Riedmatten, W. Tittel, H. Zbinden, and N. Gisin. Long distance quantum teleporattion of qubits from photons at 1300 nm to photons at 1550 nm wavelength. Technical report, quant-ph/0301178, 2003.

[196] L. Marinatto and T. Weber. ??? *Physical Review Letters A*, 272:291–???, 2000.

[197] R. Marx, A. F. Fahmy, John M. Myers, W. Bermel, and S. J. Glaser. Realization of a 5-bit NMR quantum computer using a new molecular architecture. Technical report, quant-ph/9905087, 1999.

[198] Keiji Matsumoto, Toshiyuki Shimono, and Andreas Winter. Remarks om additivity of the Holevo channe; capacity and of the entanglement of formation. Technical report, Pre-proceedings of EQIS'02, 2002.

[199] Dominic Mayers, Louis Salvail, and Yoshie Chiba-Kohno. Unconditionally secure quantum coin tossing. Technical report, quant-ph/9904078, 1999.

[200] David A. Meyer. From quantum cellular automata to quantum lattice gas automata. *Journal of Statistical Physics*, 85:551–574, 1996.

[201] David A. Meyer. Quantum strategies. Technical report, quant-ph/9804010, 1998.

[202] David A. Meyer. ??? *Physical Review Letters*, 82:1052–10??, 1999.

[203] David A. Meyer. Quantum game and quantum algorithms. Technical report, quant-ph/0004092, 2000.

[204] David A. Meyer. Quantum computing classical physics. Technical report, quant-ph/0111069, 2001.

[205] Graeme Mitchison and Richard Jozsa. Counterfactual computation. Technical report, quant-ph/9906026, 1999.

[206] V. V. Mityugin. *Physical Principles of Information Theory.* Sovietskoye Radio, Moscaw, 1976.

[207] C. Moore and A. Russel. Quantum walks on the hypercube. Technical report, quant-ph/0104137, 2001.

[208] Christopher Moore and Alexander Russel. Quantum walks on the hypercube. Technical report, quant-ph/0104137, 2001.

[209] Tal Mor. On the disentanglement of states. Technical report, quant-ph/9812020, 1998.

[210] Tal Mor and Daniel R. Terno. Sufficient conditions for a disentanglement. Technical report, quant-ph/9907036, 1999.

[211] Norman Morgolus and Lev B. Levitin. The maximum speed of dynamical evolution. *Physica D*, 120:188–195, 1998.

[212] F. Morikoshi and M. Koashi. ????? *Physical Review A*, 64:???–???, 2001.

[213] Michele Mosca, Alain Tapp, and Roland de Wolf. Private quantum channels and the cost of randomizing quantum information. Technical report, quant-ph/0003101, 2000.

[214] M. Murao and etal. ??? *Physics Review A*, 59:156–1??, 1999.

[215] Mio Murao and Vlatko Vedral. Remote information concentration using a bound entagled state. Technical report, quant-ph/0008078, 2000.

[216] D. S. Naik, C. G. Peterson, A. G. White, A. J. Berlung, and P. G. Kwiat. Entangled state quantum cryptography: eavesdropping on the Ekert protocol. *Physics Review Letters*, 84:4737–4740, 2000.

[217] Ahmad Nawaz and A. H. Toor. Worst-case payoffs in quantum battle of sexes game. Technical report, quant-ph/0110096, 2001.

[218] Ashwin Nayak. Optimal lower bounds for quantum automata and random access codes. Technical report, quant-ph/9904093, 1999.

[219] Ashwin Nayak and Asvin Vishwanath. Quantum walks on the line. Technical report, quant-ph/0010117, 2000.

[220] M. A. Nielsen, Ch. M. Dawson, J. L. Dodd, A. Gilchrist, D. Mortimer, T. J. Osborne, M. J. Bremner, A. W. Harrow, and A. Hines. Quantum dynamics as a physical resource. Technical report, quant-ph/0208077, 2002.

[221] Michael Nielsen. Probability distributions consistent with a mixed state. Technical report, quant-ph/9909020, 1999a.

[222] Michael A. Nielsen and J. Kempe. Separable states are more disordered globally than locally. Technical report, quant-ph/0011117, 2000.

[223] Michal A. Nielsen. Universal quantum computation using only projective measurement, quantum memory and preparation of 0 state. Technical report, quant-ph/0108020, 2001.

[224] Harumichi Nishimura and Masanao Ozawa. Computational complexity of uniform circuit families and quantum Turing machines. Technical report, University Osaka, 1999.

[225] Harumichi Nishimura and Masanao Ozawa. Quantum oracles and computational complexity. Technical report, quant-ph/00030??, 2000.

[226] Kevin M. O.Connors and William K. Wooters. Entangled rings. Technical report, quant-ph/0009041, 2000.

[227] Tatsuaki Okamoto and Keisuke Tanaka. Graph non-isomorphism has a succinct quantum certificate. Technical report, NTT Laboratories and Tokyo Institute of Technology, 2001.

[228] Tatsuaki Okamoto, Keisuke Tanaka, and Shigenori Uchiyama. Quantum public-key cyptosystem. In *Proceedings of CRYPTO 2000*, pages 147–165, 2000.

[229] Jian W. Pan, Dik Bouwemester, Harald Weinfurter, and Anton Zeilinger. Experimental entanglement swapping: entangled photons that never interacted. *Physical Review Letters*, 80:3891–3894, 1998.

[230] Jian-Wei Pan, Christoph Simon, Časlav Bruknwer, and Anton Zeilinger. Feasible entanglement purification for quantum communication. Technical report, Institut für Experimentalphysik, Universität Wien, 2000.

[231] S. Parker and Martin B. Plenio. Efficient factorization with a single pure qubit. Technical report, quant-ph/0001066, 2000.

[232] Arun K. Pati and Samuel L. Braunstein. ????? *Nature*, 404:164–16?, 2000.

[233] Arun Kumar Pati. Minimum classical bit for remote preparation and measurement of a qubit. Technical report, quant-ph/9907022, 1999. See also Phys. Rev. A Vol 63 (2001) 014302.

[234] Arun Kumar Pati. Impossible and possible operations in quantum information. Technical report, quant-ph/0111153, 2001.

[235] Arun Kumar Pati and Samuel Braunstein. Quantum no-deleting principle and some of its applications. Technical report, quant-ph/0007121, 2000a.

[236] Thomas Pelliziari. *Introduction to quantum computation and information*, chapter Quantum computers, error-corection and metworking, pages 270–310. World Scientific and Tim Spiller, 1998.

[237] Asher Peres. Delayed choice for entanglement swapping. *Journal of Modern Optics*, 47:139–143, 2000.

[238] Arthur O. Pittenger and Morton H. Rubin. Note on separability of the Werner states in arbitrary dimensions. Technical report, quant-ph/0001110, 2000.

[239] Martin Plenio and Vlatko Vedral. ?????? Technical report, quant-ph/0010080, 2000.

[240] Martin Plesch and ır Buˇ zek Vladim˙ Entangled graphs: bipartite entanglement in multiqubit systems. Technical report, Pre-procedings of EQIS'02, 2002.

[241] John Preskill. Quantum information and physics: some future directions. Technical report, quant-ph/9904022, 1999.

[242] T. Ralph. Security of continuous variable quantum cryptography. Technical report, quant-ph/9907073, 1999.

[243] Robert Raussendorf and Hans J. Briegel. Quantum computing with measurement only. Technical report, quant-ph/0010033, 2000.

[244] Robert Raussendorf, Daniel E. Browne, and Hans J. Briegel. The one-way quantum computer - a non-network model of quantum computation. Technical report, quant-ph/0108118, 2001.

[245] Ran Raz. Exponential separation of quantum and classical communication complexity. In *Proceedings of* 31*st ACM STOC*, pages 358–367, 1999.

[246] John Reif. Alternative computational models: a comparison of biomolecular and quantum computing. In *Proceedings of 18th International Conference on Foundations of Software technology and Theoretical Computer Science*, pages 102–121, 1998. For an extended version see http://www.cs.duke/r̃eif/paper/altcomp.ps.

[247] John Reif. Efficient quantum compression. Technical report, http://www.cs.duke.edu/ reif/paper/qcompress.ps, November 1998a.

[248] Terry Rudolph and Lov Grover. A 2 rebit gate universal for quantum computating. Technical report, quant-ph/0210187, 2002.

[249] A. Saito, K. Kioi, Y. Akagi, N. Hashizume, and K. Ohta. Actual computational time-cost of the Quantum Fourier Transform in a quantum computer using nuclear spins. Technical report, quant-ph/0001113, 2000.

[250] Anna Sampera, Dagmar Bruß, and Maciej Lewenstein. Schmidt number witness and bound entanglement. Technical report, quant-ph/0009109, 2000.

[251] A. Sanpera, Dagmar Bruß, M. Lewenstein, and A. Sanpera. Classification of mixed three-partite states. Technical report, quant-ph/0103025, 2001.

[252] Rüdiger Schack. Quantum theory from four of hardy's axioms. Technical report, quant-ph/0210017, 2002.

[253] Yaoyun Shi. Quantum lower bound for sorting. Technical report, quant-ph/0009091, 2000.

[254] Yaoyun Shi. Quantum lower bound for the collision and the element distinctness problems. Technical report, quant-ph/0112086, 2001.

[255] A. Shirman, G. Schön, and Z. Herman. Quantum manipulation of small Josephson junction. *Physical Review Letters*, 79:2371–2374, 1998.

[256] Peter Shor and John Smolin an A. Thapliyal. Superactivation of bound entanglement. Technical report, quant-ph/0005117, 2000.

[257] Peter Shor and John Preskill. Simple proof of security of the bb84 quantum key distribution protocol. Technical report, quant-ph/0003004, 2000.

[258] Peter W. Shor. Additivity of the classical capacity of entanglement-breaking quantum channels. Technical report, quant-ph/0201149, 2002.

[259] Peter W. Shor. Equivalence of additivity questions in quantum information theory. quant-ph/0305035, 2003.

[260] C. Simon, G. Weihs, and Anton Zeilinger. Optimal quantum cloning via stimulated emission. *Physics Review Letters*, 84:2993 – ????, 2000.

[261] Christoph Simon and Vladimír Bužek amd Nicolas Gisin. No-signaling condition and quantum dynamics. *Physical Review Letters*, 87(17):???–???, 2001.

[262] John A. Smolin. A four-party unlockable bound-entangled state. Technical report, quant-ph/0001001, 2000.

[263] Anthony Sudbery. On local invariants of pure three-qubit states. Technical report, quant-ph/0001116, 2000.

[264] Barbara M. Terhal, David P. DiVincenzo, and Debbie W. Leung. Hidding bits in Bell states. Technical report, quant-ph/0011042, 2000.

[265] Daniel R. Terno. Nonlinear oerations in quantum information theory. *Physical Review A*, 59:3320–3324, 1999.

[266] Ashish V. Thapliyal. On multipartite pure-state entanglement. Technical report, quant-ph/9811091, 1998.

[267] Gerard t'Hooft. Quantum gravity as a dissipative deterministic systems. *Classical and quantum gravity*, 16:3263–3279, 1999.

[268] Wolfgang Tittel, T. Brendel, Hugo Zbinden, and Nicolas Gisin. Quantum cryptography using entangled photons in energy-time Bell states. *Physics Review Letters*, 84:4737–4740, 2000.

[269] Wolfgang Tittel, Hugo Zbinden, and Nicolas Gisin. Quantum secret sharing using pseudo-ghz states. Technical report, quant-ph/9912035, 1999.

[270] Robert R. Tucci. A rudimentary quantum compiler. Technical report, quant-ph/9902062, 1999.

[271] Lev Vaidman. Teleportation: dream or reality? Technical report, quant-ph/9810089, 1998.

[272] Māris Valdats. The class of languages recognizable by 1-way quantum finite automata is not closd under union. Technical report, quant-ph/0001105, 2000.

[273] Wim van Dam and Sean Hallgren. Efficient quantum algorithms for shifted quadratic character problems. Technical report, quant-ph/0011067, 2000.

[274] Wim van Dam, Frédéric Magniez, Michele Mosca, and Miklos Santha. Self-testing of universal and fault-tolerant sets of quantum gates. Technical report, quant-ph/99?????, 1999.

[275] Wim van Damm and Patrick Hayden. Embezzling entangled quantum states. Technical report, quant-ph/0201041, 2002.

[276] Geofré Vidal. ??? *Physical Review Letters*, 83:406, 1999.

[277] Guifré Vidal and J. I. Cirac. When only two thirds of the entanglement can be distilled. Technical report, quant-ph/0107051, 2001.

[278] Guifré Vidal, W. Dür, and Juan I. Cirac. Reversible combination of inequivalent kinds of multipartite entanglement. Technical report, quant-ph/0004009, 2000.

[279] David Di Vincenzo, Barbara M. Terhal, and Ashish V. Thapliyal. Optimal decomposition of barely separable states. Technical report, quant-ph/9904005, 1999.

[280] Paul Vitányi. Two approaches to the quantitative definition of information in an individual pure quantum state. Technical report, quant-ph/9907035, 1999.

[281] Igor V. Volovich. Bell theorem and locality in space. Technical report, quant-ph/0012010, 2000.

[282] Igor V. Volovich. An atgtack on quantum cryptography from space. Technical report, quant-ph/0012054, 2000a.

[283] Rutger Vrijen, Eli Yablonovitch, Kang Wang, Hong Wen Jiang, Alex Balandin, Tal Mor, and David DiVincenzo. Electron spin resonance transistors for quantum computing in silicon-germanium heterostructures. Technical report, quant-ph/9905096, 1999.

[284] J. Walgate, A. J. Short, L. Hardy, and V. Vedral. Local distinguishability of multipartite orthogonal quantum states. Technical report, quant-ph/0007098, 2000.

[285] An Min Wang. Generalization of the entanglement of formation for multi-party systems. Technical report, quant-ph/0011040, 2000.

[286] An Min Wang. Improved relative entropy of entanglement for multi-party systems. Technical report, quant-ph/0012029, 2000.

[287] Andris Watrous, E. Bach, A. Nayak, a. Vishvanath, and John Watrous. One-dimensional quantum walks. In *Proceedings of 33th ACM STOC*, pages 37–49, 2001.

[288] John Watrous. Quantum simulations of classical random-walks and undirected graph connectivity. Technical report, quant-ph/9812012, 1998.

[289] John Watrous. PSPACE has 2-round quantum interactive proof system. Technical report, quant-ph/9901015, 1999.

[290] John Watrous. On quantum and classical space-bounded processes with algebraic transition amplitudes. Technical report, quant-ph/9911008, 1999a.

[291] John Watrous. Space-bounded quantum complexity. *Journal of Computer and System Sciences*, 59(2):281–326, 1999b.

[292] John Watrous. Quantum algorithms for solvable groups. Technical report, quant-ph/0011023, 2000.

[293] John Watrous. Quantum statistical zero-knowledge. Technical report, quant-ph/0202111, 2002.

[294] R. F. Werner. Optimal quantum cloning of pure states. *Physics Review A*, 58:1827–, 1998.

[295] Reinhard F. Werner. Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model. *Physics Review A*, 40:4277–4281, 1989.

[296] Reinhard F. Werner. All teleportation and dense coding schemes. Technical report, quant-ph/0003070, 2000.

[297] Collins P. Williams. *Quantum computing and communication*. Springer-Verlag, LNCS 1509, 1999. Proceedings of the 1st NASA Conference on Quantum Computation and Communication, Edited by C.P. Williams.

[298] A. W.Marshall and I. Olkin. *Inequalities: Theory of majorization and its applications*. Academic Press, New York, 1979.

[299] S??? Wolfram. *A new kind of science*. Wolfram Media, 2002.

[300] William K. Wootters. Entangled chains. Technical report, quant-ph/0001114, 2000.

[301] S. Wu and Y. Zhang. ???? Technical report, quant-ph/0004020, 2000.

[302] Tomohiro Yamasaki, Hirotada Kobayashi, and Yuuki Tokunaga nd Hiroshi Imai. Two-way quantum one-counter automata. Technical report, Tech. Report, ERATO project, University of Tokyo, 2001.

[303] Tomohiro Yamasaki, Hirotada Kobayashi, Yuuki Tokunaga, and Hiroshi Imai. One-way probabilistic reversible and quantum finite one-counter automata. Technical report, Department of Information Science, University of Tokyo, 2000. yamasaki@is.s.u-tokyo.ac.jp.

[304] Hao-Sheng Zeng and Le-Man Kuang. Preparation of GHZ states via Grover's search algorithm. Technical report, quant-ph/0005002, 2000.

[305] Yong-Sheng Zhang, Chuan-Feng Li, and Guang-Can Guo. Quantum authentication using enetngeled states. Technical report, quant-ph/0008044, 2000.

[306] M. Ziman, P. Štelmachovič, V. Bužek, M. Hillery, V. Scarani, and N. Gisin. Quantum homogenization. Technical report, quant-ph/0110164, 2001.

[307] Marek Zukowski and Caslav Brukner. Bell's theorem for general n-qubit state. Technical report, quant-ph/0102039, 2001.

[308] Marek Zukowski, Caslav Brukner, Wieslaw Laskowski, and Marcin Wiesniak. Gisin's theorem cannot be generalized to all multipartite states. Technical report, quant-ph/0110095, 2001.

[309] Marek Žukowski, Anton Zeilinger, Michael A. Horne, and Aarthur K. Ekert. "Event-ready-detectors"; Bell experiments via entanglement swapping. *Physical Review Letters*, 71:4287–4290, 1993.