New Generation Computing, 21(2003)279-295
Ohmsha, Ltd. and Springer-Verlag

NEW GENERATION COMPUTING

Invited Paper

Quantum Entanglement as a New Information Processing Resource

Jozef GRUSKA
Faculty of Informatics, Masaryk University
Botanická 68a, 60202 Brno, Czech Republic
gruska@fi.muni.cz

Received 12 November 2002
Revised manuscript received 23 April 2003

Abstract Quantum entanglement, a special correlation that can exist between subsystems of quantum multipartite systems, is increasingly seen as one of the most specific physical resources of quantum world. It is a resource that is not only behind the fact that quantum information processing can be more efficient than classical ones and that quantum communication can be both more efficient and more secure than classical one, but, and this is perhaps the main point, also behind an increasing confidence that quantum entanglement can lead to new quantum information processing technology and to a new, and deeper, understanding of important and complex (quantum) physics phenomena.

In this paper we concentrate on this new physical resource and on its various, sometimes even mysterious, consequences and impacts on computations and communications. In addition, we briefly summarize main problems and outcomes of the research concentrating on the understanding of the structure, laws and limitations of entanglement itself.

Keywords: Quantum Information Processing, Quantum Entanglement, Bound Entanglement, Quantum catalysts, Non-locality, Quantum Algorithms, Quantum Cryptography, Quantum Communication.

§1 Introduction

Informally, entanglement is a feature of quantum objects that causes particles to exhibit much closer correlations than classical objects do. For example, due to the quantum entanglement, a measurement of one of the particles of an entangled state can determine instantaneously some properties of the related entangled particles, even if they are far away. Because of that, and due to the specific features of quantum measurement, entangled particles can exhibit a certain non-locality[*1] features. This can lead, on one side, to various mysterious and paradoxical phenomena. On the other side, in spite of the fact that the above non-locality features cannot be used for direct communication, because the outcomes of quantum measurements are not uniquely determined, only their probabilities are, they can be used to create certain (instantaneous) coordination among distant parties sharing entangled states. This can have qualitative and quantitative impacts on quantum information processing, communication and cryptography.

Quantum entanglement used to be seen, practically till 1993, especially due to the accompanying non-locality impacts, as being behind various mysterious and weird phenomena of quantum world, and of interest only (mainly) to the philosophers of science (physics).

Currently, quantum entanglement is increasingly seen as important information processing resource and even as a new potential gold mine for science and technology. However, it still may be a long way to go to determine fully significance of this resource for quantum information processing and communication, because quantum entanglement is a very complex phenomenon.

It has been also increasingly often realized that quantum entanglement is at heart of quantum physics and represents perhaps its deepest departure from the classical physics. Many fundamental theoretical problems of quantum mechanics and quantum information processing and communication are related to entanglement. Moreover, perhaps the main difficulties at the implementation of real quantum information processing and communication system are connected with the need to create, store, transmit and manipulate entanglement.[*2]

Quantum entanglement is considered to be of large importance for theory and practice of quantum information processing because it allows:

- to perform tasks that are not possible without (quantum) entanglement – for example quantum teleportation;
- to speed-up computations (very much in some cases, it seems);
- to economize (even exponentially) communications;
- to increase capacity of (quantum) communication channels;
- to perform perfectly secure communications;
- to develop more general and powerful theories of computations and communications;
- to develop a new and better understanding of the key quantum phenomena and, by that, a deeper, information processing based, understanding of

[*1] It is this "quantum non-locality" which entanglement exhibits, that belongs to the most specific and controversial issues of the quantum world. A set of particles in an entangled state can therefore be seen as a special quantum channel through which outcomes of one measurement can have instantaneous impact at much distant places.

Non-locality of the physical world is not a new idea in physics. The existence of non-local phenomena has been assumed by Newton when he developed theory of gravity. It has been later rejected by Einstein when he developed theory of relativity.

Various ways to see "non-local effects" are closely related to fundamental questions concerning the nature of the physical reality and causation.

[*2] More than 45000 pages with the term "entanglement" have been found on internet.[46)]

Nature;

- to develop new information gathering methods and tools for physics and technologies.

Quantum entanglement can also be characterized and quantified as a feature of quantum system that cannot be created through local quantum operations and classical communications among the parties.

The following features and properties of quantum entanglement are of special interest and importance.

- Entanglement does not depend on a particular representation of quantum system.
- Entanglement enables and is consumed by a variety of tasks.
- Entanglement obeys a set of as yet not fully understood principles of behavior.
- Entanglement is shared according to not yet well understood laws and limitations.
- Power of entanglement as a resource is analogous to that of shared random bits in (randomized) classical computations.

For a more detailed description of quantum entanglement as a resource see,[25,26], for a systematic presentation of results concerning entanglement itself see.[20,23]. For a systematic description of quantum information processing fundamentals see.[17,23,24]

§2 Basic Concepts of Quantum Entanglement

The definition of entanglement of pure bipartite states is simple and natural. A pure state $|\phi\rangle$ of a bipartite quantum system $A \otimes B$ is **entangled** if $|\phi\rangle$ cannot not be expressed as a tensor product of pure states from A and B. An example of such a state is so called *EPR state*.

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

of the quantum system $H_2 \otimes H_2$, expressed in the standard basis.[*3] Therefore, in each quantum bipartite system there are pure states for which subsystems do not have their own pure state.

The case of entanglement of the mixed states of bipartite systems seems to be slightly less natural. A mixed state ρ is entangled if ρ cannot be written as a convex combination of the products of mixed states

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

[*3] Where H_n denotes Hilbert space of dimension n. EPR-state is one of four *Bell states*

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

that form a basis in $H_2 \otimes H_2$. All Bell states are said to contain 1 *ebit* of entanglement.

where $\rho_{A,i}$ ($\rho_{B,i}$) are mixed states (density matrices) of the quantum system A (B). It can be shown that a mixed state is entangled if it cannot be represented as a convex combination of products of quantum pure states.

Example 2.1
The following one-parameter family of so called *Werner states* belong to important mixed states and these states are entangled if and only if $p > \frac{1}{3}$.

$$W_p = p|\Psi^-\rangle\langle\Psi^-| + \frac{1-p}{4}\mathbf{I}, \qquad 0 \leq p \leq 1,$$

Actually, in both definitions there is the same idea behind: a state is entangled if it cannot be created by two parties provided they perform quantum operations only on their local subsystems and at doing that they communicate only classically.

Both definitions generalize naturally to the case of multipartite systems. However, it has turned out that it is useful to consider many different types of multipartite entanglement. An entangled state of an m-partite quantum system $S_1 \otimes S_2 \otimes \ldots \otimes S_m$ is called $(\mathcal{M}_1 : \mathcal{M}_2 : \ldots : \mathcal{M}_k)$-separable, where $\mathcal{M}_1, \mathcal{M}_2, \ldots, \mathcal{M}_k$ is a partition of the set $\{1, 2, \ldots, n\}$, if it is separable with respect to the tensor product of the quantum system $S_{\mathcal{M}_i}$ that are themselves tensor products of quantum systems $\{S_j \mid j \in \mathcal{M}_i\}$.

Entanglement is only one type of non-classical correlations among particles. Quantum states of a bipartite system that are not product states (of two states of both (sub)systems) can be seen also as being quantumly correlated even if they are not entangled.

§3 Creation of Entangled States

There are various ways how to create entangled states. Some of them indicate how difficult it has to be to implement some quantum gates and to perform some measurements.

1. Experimental generation using special physical phenomena. While quite a bit of progress has been obtained in creation of bipartite entanglement, design of multipartite entanglement is still in infancy.
2. An application of some unitary operations to separable states. For example, all Bell states can be obtained if XOR operation is applied to the separable states $|\phi\rangle|a\rangle$, where $a \in \{0, 1\}$ and $|\phi\rangle$ is a suitable qubit state.
   Actually, a two-qubit gate is called **entangling** if it can create an entangled state when applied to a separable state. Entangling gates are very important. Indeed, it holds[12]: A two qubit gate forms with one-qubit gates a universal set of gates if and only if it is an entangling gate.
3. Entanglement swapping.[50] This is a transformation, by measurement only, of distant, and never-before-interacting, particles into entangled ones.
   If particles P_1 and P_2 are in the EPR-state and so are particles P_3 and P_4, then the Bell measurement of particles P_2 and P_3 makes particles P_1 and P_4

to be in the EPR-state. Entanglement swapping was already experimentally verified.[36)]

4. Measurement of separable state with respect to a basis consisting of entangled states.

§4 History of Entanglement

A brief history of entanglement can be summarized as follows:

1901 Quantum mechanics was born due to Planck.

1935 Einstein, Podolsky and Rosen[19)] pointed out non-locality aspects of entanglement (and they showed that *entanglement has counterintuitive impacts and represents the most striking departure of the quantum physics from classical one*), and Schrödinger[39)] introduced the term *Vershränkung* whose loose English translation gives the term *entanglement.*[*4]

1964 Bell[3)] derived (Bell) inequalities allowing experimentally verify non-locality impacts of entanglement (and validity of quantum mechanics).

1982 Aspect[1)] performed the first convincing experimental verification of Bell inequalities.

1991 Ekert[18)] pointed out that entanglement can be used for secure cryptographic key generation.

1993 Bennett et al.[4)] discovered quantum teleportation and by that they showed that *entanglement can be a useful resource.*

1996 Zeilinger's group[8)] experimentally demonstrated quantum teleportation.

1998 **Bound entanglement** – a special not-distillable form of quantum entanglement was discovered by Horodeckis family.[27)]

§5 Classical Analogue of Quantum Entanglement

There are two reasons why it is of interest/importance to try to find and explore good classical analogues of such a key quantum concept as entanglement: (1) to find out those features of quantum entanglement that look as inherently quantum, but are actually classical (because they are in common with a classical analogue); (2) to find ways how to import some questions from quantum entanglement to classical domain and vice versa.

Collins and Popescu[15)] worked out an approach for finding a good classical analogue of quantum entanglement based on an analogy of the behavior of quantum entanglement under LOCC (local quantum operations and classical

[*4] The EPR-paper concentrated on non-locality that quantum entanglement manifests and consequently on the question of the relation between quantum theory concepts and physical reality. Schrödinger recognized profoundly non-classical correlation between the information which entangled states give us about the whole system and its subsystems.

communication) and of the behavior of secret correlations under LOPC (local classical operations and public communications). Actually, the fact that secret classical correlations are a powerful resource has already been well known and much explored in the area of classical computations.

Their overall analogy is based on the following particular basic analogies.

quantum entanglement	— — —	secret classical correlations
qubit	— — —	secret bit
ebit	— — —	secret shared bit
quantum communication	— — —	secret classical communication
classical communication	— — —	public classical communication

where by secret (classical) communication we mean communication through a channel to which an adversary has no (has some) access.

Main derived analogies are then: quantum teleportation – one-time pad cryptosystem; entanglement purification – classical privacy amplification, and so on.

The main inside coming from this analogy is that entanglement and secret classical communication are deeply related and one should not be viewed without the other.

§6 Power of Entanglement for Computation and Information Processing

It is intuitively clear that entanglement plays an important role in those quantum algorithms that exhibit much better performance than known classical algorithms for the same tasks. It is less clear how to demonstrate such intuition formally and convincingly.

In case of pure states, it is already known that without a possibility to have states with increasingly growing multipartite entanglement we cannot have with quantum algorithms an exponential speed up comparing to the classical case. This follows from the following results of Jozsa and Linden.[30)]

Definition 6.1

Given an integer p, a pure state $|\phi\rangle$ of n qubits is said to be p-blocked if no $p+1$ qubits of $|\phi\rangle$ are entangled (after tracing out the remaining qubits).

Theorem 6.1

Consider any quantum algorithm working on **pure** states (with increasing input size). Suppose there is a fixed p such that all states produced by the algorithm during computations are p-blocked. Then the algorithm can be simulated classically in polynomial time.

However, it is not clear whether the necessity of having increasingly growing entanglement can be demonstrated also for the case of computations with mixed states.

Quite surprisingly, situation is different for oracular computation problems. Indeed, for some oraculum problems one can get even more than exponential speed up, with respect to the classical algorithms and with respect to the number of queries as a complexity measure, using only quantum superposition. As shown by Meyer,[34] this is the case for the so-called Bernstein-Vazirani problem: *Given a black-box function* $f : \{0,1\}^m \to \{0,1\}$ *such that* $f(x) = a \cdot x$ *for some a, find a.*

For this problem, that requires classically $\theta(m)$ queries in the worst case there is a quantum algorithm that performs only one query and requires no entanglement.[*5]

Let us now mention some of the main success in design of quantum algorithms

1. Bernstein and Vazirani[7] gave the first example of a superpolynomial separation between probabilistic and quantum oracular computation.
2. Simon[44] gave the first example of an exponential separation between probabilistic and quantum oracular computation.
3. Shor[40] designed polynomial time quantum algorithms to factorize integers and to compute discrete logarithms — what would allow to break the RSA and other cryptosystem. For these problems no classical polynomial time algorithms are known. The key new techniques used is that of *Quantum Fourier Transform.*
4. Grover[22] showed that quantum search in an unordered database of n elements needs only $\sqrt{n}$ queries, what would allow to break the DSA cryptosystem. Classically, n queries may be needed. Key new technique used was *amplitude amplification.*
5. Childs et al.[16] showed that also using a new technique of *continuous quantum walks* an exponential speed-up in quantum algorithms can be obtained for a special graph oracular searching (reachability) problem.

However, it is also interesting to notice that quantum entanglement does not play an important role in the current theory of quantum automata (quantum finite automata, quantum Turing machines, quantum cellular automata).

On the other side, entanglement plays an important role in a surprising result[48] that PSPACE has 2-round quantum interactive proof systems. The point is that entanglement allows to create from many-rounds interactive protocols a new few-rounds protocol.

There are several other ways entanglement is of importance/interest for quantum information processing.

- It was shown[21] that *entanglement is a computational primitive* because it is possible to realize any quantum computation by starting with some GHZ states and then performing only one qubit operations and Bell measurements. In addition, it was shown[37] that universal quantum computation is possible by starting with a proper multipartite entangled state (a sort of a computational substrate) and then performing only single-qubit measurements.

[*5] Perhaps a proper conclusion in this case is that number of queries of a black-box function is not a (physically) appropriate measure to study complexity of quantum algorithms.

- Entanglement can also serve as a *catalyst.* It can allow to perform quantum processes that are otherwise impossible, and in such a way that entanglement used during such processes, as a "catalyst," is not consumed by the processes themselves, Therefore, the entanglement that has been used can be "returned back" at the end of the process. Indeed, it was shown[29] that there are pairs of pure states $(|\phi_1\rangle, |\phi_2\rangle)$ such that using LOCC one cannot transform $|\phi_1\rangle$ into $|\phi_2\rangle$, but with the assistance of an appropriate entangled state $|\psi\rangle$, a catalyst, one can transfer $|\phi_1\rangle$ into $|\phi_2\rangle$, using LOCC, in such a way that the state $|\psi\rangle$ is not changed during the process.
Moreover, it has been shown[2] that entanglement can serve as a **super-catalyst** that not only allows to perform operations otherwise impossible, but during such a process the catalyst can even increase its entanglement.
Another surprising discovery[47] 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. This means that it s possible to *embezzle*$|\phi\rangle$ from $\mu(n)\rangle$, by removing small amount of entanglement from $|\mu(n)\rangle$, causing arbitrarily small disturbance to $|\mu(n)\rangle$.

§7 Power of Entanglement for Communication

There are four basic ways entanglement can bring new quality to communication.

Quantum teleportation: [4] Provided that two parties, say Alice and Bob, share maximally entangled pure states, Alice can teleport her new unknown state $|\phi\rangle$ in n-dimensional Hilbert space by performing local quantum operations on their particles and then sending to Bob $2\lg_2 n$ bits obtained as the classical result of a measurement. These bits are then used by Bob to choose a proper unitary operator to apply to his particles to get them into the (still unknown) state $|\psi\rangle$.

The above method of teleporting a quantum state has been generalized in many ways. Interesting and surprising results have been also obtained at the study of question what happens if the party 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, surprisingly, positive. Indeed, it has been shown[6,32] that in such a case there is a non-trivial tradeoff between the amount of ebits and bits needed.

Teleportation uses two bits to teleport one qubit. Dense coding,[4] is a dual operation to teleportation. It uses one qubit to send two bits. A very general study of quantum teleportation and dense supercoding protocols, as well as their relation to some important classical mathematical problems, has also been done.[49]

Decreasing communication complexity: While in quantum computation we merely believe that quantum tools allow exponential speed-up for some tasks, in quantum communication we can prove that quantum tools can bring exponential savings.[*6]

Indeed, for some communication tasks quantum communication complexity can be much smaller than the classical communication complexity. For example, for the following **dating problem**: *Alice and Bob have diaries for next n days specifying for each day whether they are free (1) or busy (0) that evening. How many bits they need to exchange in order to find out whether there is a day in which they could spent evening together?*

Communicating only classically, Alice and Bob need to exchange n bits in the worst case. When communicating quantumly, $\mathcal{O}(\sqrt{n}\lg n)$ bits are sufficient for them to solve the dating problem.[13]

For some other problems exponential speed-up can be obtained using quantum communication.[38]

Increasing capacity of quantum channels: If two communicating parties share some entangled states then communication capacity of their channel can be increased and there is no upper bound how big increase can be.[5]

Increasing security of communication: There are two basic ways entanglement plays a role in quantum cryptography: a positive one and negative one.

Positive is the fact that quantum entanglement allows perfectly secure transmission of information and absolutely secure generation of secret random keys.

Indeed, in case two parties share enough EPR states they can encode a state to be transmitted through a sequence of qubits and then to teleport these qubits. This is an absolutely secure way of transmission because by that no physical systems are transmitted. Moreover, by sharing n pairs of particles in the EPR state, both parties can implement quantum one-time

[*6] Let us start our discussion of quantum communication by pointing out that there have actually been good reasons to believe that quantum communication cannot be of special use. Indeed, Holevo theorem says that no more than n bits of classical information can be communicated by transmitting n qubits - unless two communicating parties are entangled, and in such a case at most twice as many classical bits can be communicated, using quantum dense coding defined above.

In addition, entanglement itself cannot be used to transmit information — otherwise faster than light communication would be possible. Our intuition therefore says that there should be negative answers to the following fundamental questions:[10]

- Can entangled parties make better use of communication channels than non-entangled parties?
- Can entangled parties benefit from their entanglement even if they are not allowed any form of direct (classical or quantum) communication?

However, such views turned out to be wrong.

pad cryptosystem without a need to share a classical key.[9] Again, this is absolutely secure way of transmission.

There is also an easy and unconditionally secure way for two parties, Alice and Bob, to make use of entanglement to generate a random binary key.

Indeed, let Alice and Bob share n pairs of particles, each pair in the entangled EPR-state. If both parties measure their particles in the standard basis (and it does not matter in which order), they receive, as the result of their measurement, the same random binary string of length n. This way of binary key generation is absolutely secure, because, again, no information is transmitted.

Negative impact has entanglement on security of such basic quantum protocols as for *bit commitment*. It can be shown that, due to the fact that by using entanglement one party can always cheat, no unconditionally secure bit commitment is possible[33] (in non-relativistic physical setting).

There are also other ways quantum entanglement is used in cryptography: for quantum authentication protocols, quantum secret sharing and so on.

§8 Entanglement as a Main Tool to Fight Decoherence

Till 1995 there was strong pessimism whether meaningful quantum information processing would eventually be possible. The main reason behind was *quantum decoherence* – the fact that due to unavoidable entanglement of any real computational quantum system with its environment, fragile quantum superpositions, that are behind powerful quantum parallelism, get exponentially fast destroyed.

In addition, it has been believed that efficient quantum error-correcting codes cannot exist because: (a) number of quantum errors seemed to be infinite; (b) quantum copying, needed to create redundancy, so vital for classical error-correcting codes, is impossible; (c) measurement of an erroneous state would, in general, irreversibly destroy the state. However, Shor[41,42] have shown that not only quantum error-correcting codes, but also quantum fault-tolerant computations, are possible. (The main idea is to use multipartite entanglement to fight, in polynomial time, exponentially fast growing decoherence – caused actually by the entanglement of the system with its environment.)

§9 Entanglement versus Energy

For a long time energy used to be arguably the main resource to consider at the study of physical systems. Once entanglement is seen as a resource, it is natural to ask about the relation and analogies between energy and entanglement.

The thesis that information is physical, and that the role of information in physics is analogous to that of energy in thermodynamics, leads naturally to the search for information processing principles and laws, especially for principles and laws analogous to those in thermodynamics. It is only natural that quantum entanglement is expected to play the key role in such principles and laws. One such principle, the counterpart of second principle of thermodynamics, seems to be *no-increasing of entanglement principle* — under LOCC.

The counterpart to the first principle of thermodynamics is the preservation of (quantum) information in closed quantum systems: *Entanglement of composed system does not change under unitary processes on one of the subsystems.*

9.1 Thermodynamics and Entanglement

The above entanglement processing principles are connected with a belief, of some, that there are laws governing entanglement processing that are analogous to those of thermodynamics and that exploration of these analogies can be very useful for understanding basic laws of entanglement processing. The entanglement is then considered[28)] to play the role of energy[*7] (and distillation of pure entanglement to drawing work). This entanglement-energy analogy has been explored recently[28)] and it was postulate that

- entanglement is a form of quantum information corresponding to internal energy;
- sending of qubits corresponds to a work.

One of the key obstacles for attempts to develop a "thermodynamic of entanglement" is irreversibility of entanglement processing. It is an open problem how to get around this difficulty and to develop a really deep and useful entanglement-energy analogy.

§10 How Far beyond Usual Borders Can We Get with Entanglement?

Once entanglement is seen and demonstrated as a new resource, it is natural to ask how much can entanglement help to understand some of the very fundamental and exciting challenges of current science:

- Can entanglement help to understand our universe and its creation?
- Can entanglement help to understand brain?
- Can entanglement help us to get beyond Turing?

There have been recently a variety of papers on these subjects, seen often as controversial, but hardly some generally accepted "hard-core" results.

§11 Basic Problems Concerning Entanglement

Since entanglement is such an important and puzzling resource, a much deeper exploration of entanglement is needed to make a better and broader use of this resource.

A better understanding of quantum entanglement, of ways it is characterized, created, detected, stored, manipulated, transformed (from one form to another), transmitted, shared and consumed (to do some useful work), as well as of various types and measures of entanglement, is theoretically perhaps the

[*7] Pure state entanglement can be seen as analogous to mechanical energy and mixed state entanglement as analogous to energy that must be partly accumulated in the form of heat.

most basic task of the current quantum information processing research. In short, quantitative and qualitative theory of the entanglement is much needed.

It is interesting also to observe that the whole field of quantum information theory, and especially of quantum entanglement, is currently mainly *theory driven.* It did not arise because of observations from some experiments or from specific needs of some applications.

Basic problems concerning entanglement itself can be summarized as follows.

1. To develop ways how to create reliably, and on demand, pure entangled states?
2. To find out how to distill efficiently pure entanglement from mixed states?
3. To determine which macroscopic objects can be entangled?
4. To develop methods to determine whether a given state is entangled?
5. To explore relations between entanglement and non-locality.
6. To study entanglement monotones and invariants.
7. To create and explore good measures of entanglement.
8. To discover laws and limitations of entanglement transformation.
9. To explore how to detect and utilize bound entanglement.
10. To study different types of multipartite entanglement.
11. To study laws and limitations of entanglement sharing.
12. To explore how robust and how frequent is entanglement in Nature.

In the following we will deal briefly with some of the above problems.

11.1 Entanglement of Macroscopic Objects

It is often said that one of the puzzling facts about Nature is that two key features of the microscopic quantum world, superposition and entanglement, have not been (much) seen in the macroscopic world.

One of the main tasks of the current experimental research in quantum information processing and communication is to demonstrate that both superposition and entanglement can be witnessed not only on particles.

There are already significant results along these lines that indicate that research in this direction can have far reaching impacts on future quantum information processing technologies and even far beyond that.

- Zeilinger's group,[11)] demonstrated superposition for special molecules.
- Polzik's group,[31)] has demonstrated robust entanglement of two objects consisting of about 10^{12} atoms.

11.2 Bound Entanglement

Some of the key applications of entanglement require that communicating or cooperating parties, say Alice and Bob, share maximally entangled pure states. This is practically very difficult to achieve.· A way out is that parties share copies of a mixed entangled state and then use LOCC to distill out of them some pure maximally entangled states. Several procedures for doing that are known. It has been therefore assumed that mixed entangled states are so much useful how much of pure entangled states one can distill out of them. Discovery, that there are so called ***bound entangled states***, (*BE-states*), a resource, from which no useful (pure) entanglement, a real resource, can be distilled, if all parties work quantumly only locally, has been very surprising.[27)]

A simple example of a multipartite BE-state is the state[45)]

$$\rho_s = \frac{1}{4}\sum_{i=1}^{4} |\Phi_i\rangle\langle\Phi_i| \otimes |\Phi_i\rangle\langle\Phi_i|, \tag{1}$$

where $|\Phi_i\rangle, i = 1, 2, 3, 4$, are all Bell states.

The existence of BE-states has been seen as a puzzling phenomenon. Such states cannot be used at many important applications of entanglement, such as teleportation, where maximally entangled pure states are needed. Of interest and importance has therefore been to find out whether we can make any use at all of BE-states. There are now several results showing that this is indeed the case.

First of all, in case of multipartite systems, a BE-state can be distillable if some groups of parties "get together." Indeed, if we denote parties as A, B, C, D, then the state (1) is $\{A, B\} : \{C, D\}-$, $\{A, C\} : \{B, D\}-$ and $\{A, D\} : \{B, C\}-$separable.

Secondly, BE-states can be *activated*,[27)] and *super-activated*.[43)] In addition, a protocol has been developed, so called *remote information concentration protocol*,[35)] that that can make essential use of BE-states.

Activation of bound entanglement, or 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. 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 one can distill entanglement out of them.

11.3 Quantum Correlations and Non-locality

There is already quite a bit of understanding of quantum non-locality, due to quantum correlations, of simple bipartite systems in $H_2 \otimes H_2$, but situation is quite different in the case of quantum systems of higher dimensionality or for many-partite systems – even though such an understanding could be of large importance for getting deeper and new insights into how and why quantum mechanics differ from the classical mechanics.

In order to get a better understanding of quantum non-locality, that is behind the fact that quantum entanglement is such an important information processing resource, it is of large importance to study the following questions:

- which are good measures of non-locality;
- how much classical communication is required to create quantum correlations;
- how non-locality scales with the number of parties involved.

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[14)] 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 correlations 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 $O(1/n)$.[*8]

11.4 Volume and Frequency of Entanglement

Once it has been discovered that there are various types of quantum states it is natural to try to get some insight into how many of different types of states we have.

In case of separable and entangled states, in behind is actually a very natural question: is the world more classical than quantum or not — do we have more entangled or more separable states?

Questions concerning volume and frequency of certain types of states are also of large interest for implementation considerations and for numerical simulation and analysis tasks as well as for quantum computation and communication.

In this connection there are three natural questions to ask for any type $\mathcal{T}$ of states.

- Given a state $|\phi\rangle$ of type $\mathcal{T}$, is there always a ball, in some reasonable distance measure, around $|\phi\rangle$ such that all states in that ball are of the same type $\mathcal{T}$?
- Are there states of the type $\mathcal{T}$ such that some ball of non-zero radius contains only states of the type $\mathcal{T}$?
- Is it true that in any ball there is a state of the type $\mathcal{T}$?

It has been shown[51)] that there are separable, entangled and bound entangled states such that a ball around them contains the same type of states. Volume of these sets of states is therefore non-zero (for a chosen distance measure and volume).

Concerning frequency, numerical results[51)] show that ratio of the volume of separable states and also of bound entangled states to the volume of all states goes down exponentially with the dimension of the system.

These results also show that a pure state is more likely to be entangled, and a mixed state is more likely to be separable.

[*8] 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). (As already discussed in Section 5, shared random bits are actually classical analogue of quantum entanglement.)

Acknowledgements

This is to acknowledge support of the grant GAČR number 201/01/0413 and VEGA grant 1/0172/03.

References

1) Aspect, A., Dalibard, J. and Roger, G., "Experimental Tests of Bell's Inequalities Using Time-varying Analyzers," *Phys. Rev. Lett. 49*, pp. 1804–1807.

2) Bandyopadhyay, S. and Roychowdhury, V. P., "Supercatalyst," quant-ph/0107103.

3) Bell, J. S., "On the Einstein-Podolsky-Rosen paradox," *Physics 1*, pp. 195–200, 1964.

4) Bennett, Ch. H., Brassard, G., Crépeau, C., Jozsa, R., Peres, A. and Wooters, W. K., "Teleporting an Unknown Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels," *Phy. Rev. Lett. 70*, pp. 1895–1899, 1993.

5) Bennett, Ch. H., Shor, P. W., Smolin, J. A. and Thapliyal, A. V., "Entanglement-assisted Classical Capacity of Noisy Quantum Channels," quant-ph/9904023.

6) Bennett, Ch. H., DiVincenzo, D., Smolin, J., Terhal, B. and Wooters, W., "Remote State Preparation," quant-ph/0006044.

7) Bernstein, E. and Vazirani, U., "Quantum Complexity Theory," in *Proc. of* 25*th ACM STOC*, pp. 11–20, 1993.

8) Bowmeesteretal, D., Pan, J-W., Mattle, K., Eibl, M., Weinfurter, H. and Zeilinger, A., "Experimental Quantum Teleportation," *Nature, 390, 6600*, pp. 575–579, 1997.

9) Boykin, P. O and Roychowdhury, V., "Optimal Encryption of Quantum Bits," quant-ph/0003059.

10) Brassard, G., "Quantum Communication Complexity," quant-ph/0101005.

11) Brezger, B., Hackermüler N., Uttenhalter, S., Sampera, A. and Lewenstein, M., "Matter-wave Interferometer for Large Molecules," quant-ph/0202158.

12) Brylinski, J.-L. and Brylinski, R., "Universal Quantum Gates," quant-ph/0108062.

13) Buhrman, H., Cleve, R., and Widgerson, A., "Quantum vs. Classical Communication and Complexity," in *Proc. of* 30*th ACM STOC*, pp. 63–68, 1999.

14) Buhrman, H., Massar, S., and Röhrig, H., "Combinatorics and Quantum Nonlocality," quant-ph/0209052.

15) Collin, D. and Popescu, S., "Classical Analogue of Quantum Entanglement," quant-ph/0107082.

16) Childs, A. M., Cleve, R., Detto, E., Farhi, E., Gutmann, S. and Spielman, D. A., "Exponential Algorithmic Speedup by Quantum Walks," quant-ph/0209131.

17) Chuang, I. I. and Nielsen, M. A., *Quantum information processing*, Cambridge University Press, 2000.

18) Ekert, A. K., "Quantum Cryptography Based on Bell's Theorem," *Phys. Rev. Lett., 67*, pp. 661–663, 1991,

19) Einstein, A., Podolsky, B. and Rosen, N., "Can Quantum Mechanical Description of Physics Reality be Considered Complete?" *Phys. Rev., 47*, pp. 777–780, 1935.

20) Eisert, J., "Entanglement in Quantum Information Theory," PhD thesis, University of Potsdam, 2001.

21) Gottesman, D. and Chuang, I. L., "Quantum Teleportation is a Universal Computational Primitive," quant-ph/9908010.

22) Grover, L. K., "Quantum Mechanics Helps in Searching for a Needle in a Haystack." *Phys. Rev. Lett. 78*, pp. 325–328, 1997.

23) Gruska, J., *Quantum Computing,* McGraw-Hill, London. For web extension see http://www.mcgraw-hill.co.uk/gruska, 1999.

24) Gruska, J., "Quantum Computing Challenges," *Mathematics unlimited, 2001 and beyond, Springer* (Enquist B and Schmid W. eds.), pp. 529–564, 2000.

25) Gruska, J and Imai, H., "Puzzles, Mysteries and Power of Quantum Entanglement," in *Proc. of MCU'01, Ciseneu, Springer, LNCS 2055*, pp. 25–69, 2001.

26) Gruska, J., Imai, H. and Matsumoto, K., "Power of Quantum Entanglement," in *Proc. of IFIP World Computer Congress 2002, Kluwer Academic publisher, Montreal*, pp. 3–22, 2002.

27) Horodecki, M., Horodecki, P. and Horodecki, R., "Mixed-state Entanglement and Distillation: Is There a "Bound-entanglement" in Nature?" quant-ph/9801069.

28) Horodecki, P, Horodecki, M. and Horodecki, R., "Entanglement and Thermodynamical Analogies," *Acta Phys. Slovaca, 47*, pp. 141–156, 1998.

29) Jonathan, I. D. and Plenio, M. B., "Entanglement-assisted Local Manipulation of Pure Quantum States," *Phys. Rev. Lett. 83*, pp. 3566–35??, 1999.

30) Jozsa, R. and Linden, N., "On the Role of Entanglement in Quantum Computational Speed-up," quant-ph/0201145.

31) Julsgaard, B., Kozhekin, A. and Polzik, E. S., "Experimental Long-lived Entanglement of Two Macroscopic Objects," quant-ph/0106057.

32) Lo, H-K., "Classical Communication Cost in Distributed Quantum Information Processing – a Generalization of Quantum Communication Complexity," quant-ph/9912009.

33) Mayers, D. M., "Unconditionally Secure Quantum Bit Commitment Is Impossible," *Phys. Rev. Lett., 78*, pp. 3414–3417.

34) Meyer, D. A., "Sophisticated Quantum Search without Entanglement," quant-ph/0007070.

35) Murao, M. and Vedral, V., "Remote Information Concentration using a Bound Entangled State," quant-ph/0008078.

36) Pan, J. W., Bouwmeester, D., Weinfurter, H. and Zeilinger, A., "Experimental Entanglement Swapping; Entangled Photons that Never Interacted," *Phys. Rev. Lett, 89*, pp. 3891–3894, 1998.

37) Raussendorf, R. and Briegel, H. J., "Quantum Computing with Measurement Only," quant-ph/0010033.

38) Raz, R., "Exponential Separation of Quantum and Classical Communication," in *Proc. of* 31*st ACM STOC*, pp. 358–467, 1999.

39) Schrödinger, E., "Die Gegenwartige Situation in der Quantenmechanik," *Natürwissenschaften, 23*, pp. 807–812, 823–828, 844–840, 1936.

40) Shor, P. W., "Algorithms for Quantum Computation: Discrete Log and Factoring," in *Proc. of* 35*th IEEE FOCS*, pp. 124–134, 1994.

41) Shor, P. W., "Scheme for Reducing Decoherence in Quantum Computer Memory," *Phy. Rev. A, 52*, pp. 2493–2496, 1995.

42) Shor P. W., "Fault-tolerant Quantum Computation," in *Proc. of* 37*th IEEE FOCS*, pp. 56–65, 1996.

43) Shor, P. W., Smolin, J. and Thapliyal, A., "Superactivation of Bound Entanglement," quant-ph/0005117.

44) Simon, D. R., "On the Power of Quantum Computation," in *Proc. of* 35*th IEEE FOCS*, pp. 116–123, 1994.

45) Smolin, D. R., "A Four-party Unlockable Bound-entangled State," quant-ph/0001001.

46) Tittel, W. and Weihs, G., "Photonic Entanglement for Fundamental and Quantum Communication," *Quantum Information and Communication, 1*, pp. 1–43, 2001

47) van Dam, W. and Hayden, P., "Embezzling Entangled Quantum States," quant-ph/0201041.

48) Watrous, J., "PSPACE Has 2-round Quantum Interactive Proof System," quant-ph/9901015.

49) Werner, R., "All Teleportation and Dense Coding Schemes," quant-ph/0003070.

50) Žukowski, M., Zeilinger, A., Horne, M. A. and Ekert, A. K., "Event-ready-detectors; Bell Experiments via Entanglement Swapping," *Phys. Rev. Lett., 71* pp. 4287–4290, 1993.

51) Zyckowski, K., Horodecki, P., Sampera, A. and Lewenstein, M., "On the Volume of Mixed Entangled States," quant-ph/9804024.

Jozef Gruska, Ph.D.: Professor of Informatics at Masaryk University, Brno. Graduated in 1958 in mathematics from Commenius University, and received PhD in computer science in 1995 in Bratislava. His research has progressed from descriptional complexity to parallel automata and to foundations of computing and to quantum computing and culminated by books: Foundations of computing (1997) and Quantum computing (1999). Awarded by IEEE as "Computer Pioneer". He spent more than 15 years at universities abroad. Founder of four already established international conferences in computing. Founding head of Theoretical Computer Science at IFIP (1989). He likes to explore relations between foundations of computing and of physics. He collects art and makes regular exhibitions of large collection of nativity sets from more than 60 countries.