POWER OF QUANTUM ENTANGLEMENT

Jozef Gruska
*Faculty of Informatics, Masaryk University, Botanická 68a, Brno, Czech Republik**

Hiroshi Imai and Keiji Matsumoto
ERATO Quantum Computation and Information Project, Hongo 5-28-3, Bunkyo-ku, Tokyo 113-0033, Japan

Progress in theory is sometimes done by pessimists.
Progress in technology is always done by optimists.
—

Abstract Quantum entanglement is arguably the most inherently quantum feature of quantum information, computation and communication – a feature that is at heart of quantum physics. Quantum entanglement is also increasingly often considered as being behind new and surprising power quantum computations and communications exhibit – comparing to the classical computation and communication.

Quantum entanglement used to be seen, practically untill 1993, especially due to its accompanying non-locality impacts, as being behind various mysteriously looking and weird phenomena of quantum world, and of interest mainly to the philosophers of science. Since then our perception of entanglement has changed much. Currently, quantum entanglement is increasingly believed to be a resource that can be exploited to implement various quantum information processing tasks, at spatially separated locations, and to be behind new gold mine for science and technology to which the outcomes of the research in quantum information science and quantum information technology seem to pave the road.

Quantum entanglement implications are also a deep reason to attempt to develop new, quantum information processing based, foundations of quantum mechanics. To help to do that might be one of big challenges for Informatics.

* Support of GAČR grant 201/01/0413 is highly appreciated.

1. Introduction

In the last ten years, enormous progress has been made in quantum information processing and communication. In 1992, only few very theoretical results were available, with almost no indication that a rapid development and important outcomes for science and technology could follow soon. Landauer's thesis (**Information is physical**) was already known. However, on a more specific level, we had only Deutsch's (not yet fully satisfactory) model of (universal) quantum Turing machine, a very simple Deutsch's quantum algorithm, a cryptography experiment to the distance of 32cm, and with hardly anybody who could imagine to have soon implementations of quantum gates. After 10 years, we have a rapidly developing area, with about 300 papers per month. We have flourishing and increasingly broad theory, rich on deep and lasting results. We know a variety of techniques and technologies allowing some elementary experiments to be performed (and ambitious goals to be put on the agenda). We have quantum cryptography, aiming at unconditionally secure communications (with perfect detection of eavesdropping), approaching already a developing phase. (Recently, transmissions of photons through optical fibers to distance 67 km have been reported by N. Gisin and through the open air in night time to distance 23.4 km by H. Weinfurter.) Moreover, projects for ground-satellite or plane-satellite cryptography communications are under way. NMR (nuclear magnetic resonance) and quantum optics have been technologies used so far for most of the experiments. However, future seems to be in solid-state technologies, where recently quite a bit of progress has been reported in developing ways how to store, process and transform quantum information in a robust and reliable way. Shor's and Grover's algorithms made revolution in algorithmic design, and threatened to break main current cryptosystems, provided quantum computers would be available. Moreover, in the last few years, the whole field of quantum information processing and communication (QIPC) science and technology has been changing, from the theory driven to the experiments driven field. This can be seen as a positive feature, especially from the point of view of developing new quantum information technologies.

There have been several other important impacts of the developments in QIPC. Informaticians have learned that their complexity theory views of computational problems may need a change whenever a new physical theory is developed. Physicists have learned that tools of informatics, especially computational complexity concepts, methods, paradigms and results, are of the large importance for formulation and evaluation of the research goals, methods, paradigms and results, as well as for solution of physical problems. Shortly, (some) physicists have learned that (theoretical) informatics is a much needed and useful body of concepts, models, knowledge and methods that can guide their thinking and help to formulate and to solve their fundamental problems.[1] Finally, a fundamentally new view of physics started to be developed. Namely, that **physics is informational**. That is, that investigations of information processing laws and limitations of Nature may be an important new (or even the key) way to understand Nature (and, perhaps, also to develop a theory of Nature that could be used to understand both physical and biological worlds).

In general, QIPC is a rapidly developing interdisciplinary research area that encompasses many disciplines, such as physics, computer science, engineering, mathematics, chemistry and so on. It has clearly potential to revolutionize information technology, to develop Quantum Information Technology, and by that to have very broad impact on science, technology and society in large.

Quantum entanglement is often characterized and quantified as a feature of composed quantum systems that causes non-local effects, leads to pseudo-telepathy, and cannot be created through local quantum operations and classical communications among the parties.

Since the famous EPR article [EPR35], in which Einstein, Podolsky and Rosen pointed out non-locality implications of quantum entanglement, untill 1993, **entanglement was considered as a strange quantum feature**, that is behind various quantum mysteries and of interest/importance mainly only for quantum theory people and especially for philosophers of quantum physics (science). (These aspects of quantum entanglement have been well expressed by A. Peres (see [Bru01]): *Quantum entanglement allows quantum magicians to produce phenomena that cannot be imitated by classical magicians.*)

Since the discovery of the surprising power of quantum computation and of quantum teleportation, in 1993-96, **quantum entanglement is increasingly beeing considered and explored as a new and important physical resource** of (quantum) communication and computation.

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

- to perform tasks that are not possible otherwise;
- to speed-up much some computations and to economize (even exponentially) some communications;
- to increase capacity of (quantum) communication channels;
- to implement perfectly secure information transmissions;
- to develop more general and more powerful theories of computations and communications than the framework of classical physics allows;
- to develop a new, better, information based, understanding of the key quantum phenomena and of Nature.

For more details see paper [Gru00] or the book [Gru02], and its web-updatings. For more about puzzling aspects of quantum entanglement see [GI01]

2. Basics of quantum entanglement

The concept of quantum entanglement of pure states goes back to Erwin Schrödinger [Sch35], and for mixed states to Werner [Wer89].

2.1. Basic concepts

A pure state $|\phi\rangle$ of a bipartite quantum system $A \otimes B$ is **entangled** if $|\phi\rangle$ is not a tensor product of a pure state from A and a pure state from B. An example of such a state is so called *EPR state* of the Hilbert space $H_2 \otimes H_2$

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

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

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

where ρ_i^A (ρ_i^B) are mixed states of the quantum system A (B) and $\sum_{i=1}^{k} p_i = 1$.

Operationally, the same idea is behind both definitions: a state is entangled if it cannot be created by two parties if they perform quantum operations only on their subsystems and 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. For example, an entangled state $|\phi\rangle$ 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 sets $\mathcal{M}_1, \mathcal{M}_2, \ldots, \mathcal{M}_k$ form a partition of the set $\{1, 2, \ldots, m\}$, if the state $|\phi\rangle$ is separable with respect to the tensor product of the quantum system $S_{\mathcal{M}_i}$ that are themselves tensor products of quantum systems $\{S_j \mid j \in \mathcal{M}_i\}$.

Design of bipartite entangled states on demand is still experimentally a (very) difficult task, and so is any design of 3- and more-partite entangled states.

3. Quantum entanglement and quantum non-locality

As already indicated, quantum entanglement is being increasingly considered, especially due to its non-locality implications, to be the key resource for computation and communication.[2]

3.1. From Einstein's doubts through Bell's inequalities to quantum teleportation

If two particles are in the EPR state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, then, as theory says, and ever more perfect experiments strongly confirm, they can stay in that state even if they are taken much apart. Moreover, a measurement of one of the particles, with respect to the standard basis, causes that the overall state of the particles collapses, immediately and randomly, into one of the states $|00\rangle$ or $|11\rangle$. Consequently, the result of the measurement of the first (second) particle uniquely determines the result of the measurement of the second (first) particle.

In a slightly different form was this fact first observed in [EPR35]. Einstein and his colleagues did not want to accept the existence of non-local phenomena and argued that the description of the physical reality, which quantum mechanics provides, is incomplete. They suggested that such strange phenomena disappear once some hidden variables are used to complete the description of the physical reality that is missing in the Hilbert space view of states.[3]

Einstein's discovery, as well as their suggestions, caused first an uproar in physics community, but, after a while, they stopped to bother too much "working physicists" because the phenomenon they pointed out seemed to be on the philosophical level, without any visible effect on the more pragmatically oriented research in quantum mechanics, dominating at that time.

An important change in the situation came when Bell, in 1964, suggested an experimental setup that could be used to verify whether a theory of hidden variables without non-locality effects can exist. Bell derived, for results of the measurements of a Gedanken experiment, certain inequalities, which should be satisfied by physical reality provided a theory of hidden variables without non-locality is valid, and that should be violated if quantum mechanics, with non-local phenomena, is valid. In this way, the existence of the non-local phenomena stopped to be the issue only for the philosophers of quantum mechanics. Experimentalists were to resolve the dilemma.

Another important step was made by in 1993 [BBC$^+$93]. It was shown, in a way that could also be experimentally verified, that quantum entanglement can be an important resource, to teleport unknown quantum states.

3.2. From Aspect to Zeillinger

It took quite a while untill two important experimental confirmation of non-locality were made in quite a convincing, even not yet absolutely perfect, way.

From several attempts to show that Bell's inequalities[4] can be violated by bipartite entangled states, Aspect was the first to come, in 1982, with convincing results. Since then, many other experiments have been performed and a consensus has emerged that non-locality has been demonstrated even between particles quite far apart. (Experiments with more-partite states could provide even stronger tests of non-locality.) A consensus has also emerged that any local hidden variable theory that could exploit some loopholes in a way that has not been demonstrated in experiments yet, would have to be "so conspiratorial as to be almost incredible" [Ken02].

Untill 1989 it was widely believed that a quantum state is entangled if and only if it violates some Bell's inequality. However, this is not true. A state violating a Bell's inequality has to be entangled, but not vice versa, as shown first in [Wer89], for mixed states, and in [VW01], for multipartite pure states.

The next step was to demonstrate experimentally that quantum entanglement is indeed a resource that can be used to do what is impossible without it. Zeilinger's group was first to publish, in 1997, outcomes of the experiments demonstrating that quantum teleportation is possible [BPM$^+$97].

3.3. Non-locality – optimists versus pessimists

Acceptance of non-locality is such a strong departure from the former basic beliefs about Nature that it is natural, and perhaps also fortunate, that there are still pessimists who do not believe that quantum non-locality has been demonstrated beyond reasonable doubts. They try to point out, on one side, loopholes in the experiments, and/or in the conclusions made by experimentalists, or even in the hidden variable model itself. In addition, some try to offer new physical theories explaining without non-locality phenomena for which current quantum physics needs non-locality.

Experiments confirming non-locality have clearly some loopholes. Well known is the detection loophole (not sufficiently perfect detectors were used in experiments) and also the locality loophole (experiments were performed with not sufficiently far away particles). Moreover, no one seems to see a way how to close (soon) all loopholes. Detection loophole was recently closed and, almost, also locality loophole (that cannot be, in principle fully closed).

However, new loopholes are being discovered and explored again and again. For example, the *collapse locality loophole*, [Ken02], due to the fact that there may be some time between a particle enters a measuring device and the state collapse, due to the measurement, takes place. In addition, *memory loophole*, in the hidden variable model itself. Moreover, experiments are always based on some *common sense assumptions* and experimentalists from them conclude validity of some *non-common sense conclusions*, as that of non-locality. Some complain to such reasoning [Mar02], saying that correct conclusion should be to cast doubts on the assumptions.

In addition to non-locality, there are several other reasons why some believe that current quantum theory might be wrong and there might be a need to look for alternative theories: problems to understand fully quantum measurement, difficulties in matching general relativity with quantum theory and so on. For example, in so called *causal quantum theory*, measurement events that are space-like correlated do not have non-local correlations. Some versions of such theories have not been refuted yet by (Bell) experiments (due to a possibility to exploit collapse locality loophole) [Ken02].

Moreover, outcomes of QIPC seem to suggest a very new way, quantum information processing based, to build foundations of quantum mechanics, again without non-locality puzzles [Fuc02]. In any case, it seems that one of the main challenges of theoretical informatics is to help to develop such new foundations.

3.4. From particles to macroscopic objects

It used to be 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 (yet) in the macroscopic world.

One of the main task of the current experimental research in QIPC is to demonstrate that both superposition and entanglement can be witnessed not only on particles. Zeilinger's group (see [BHU$^+$02]) demonstrated superposition for special molecules, and several other experiments of this type have already been performed. It is an important open question to determine for how large molecules such superpositions can be demonstrated. Is there an upper bound? (It does not seem to be.)

Most of the experiments demonstrating entanglement did that for states of light. For storage and processing of quantum information, entanglement of material particles seems to be of larger importance. Polzik's group (see [JKP01]), has demonstrated (robust with respect to quantum standards) entanglement of two objects consisting of about 10^{12} atoms.

4. Quantum teleportation

Discovery of quantum teleportation has been so far one of the major demonstrations of the power of entanglement as an information transmission resource.

Indeed, let us assume that two parties, called in quantum computing usually Alice and Bob, share two particles in the EPR state, and Alice gets another particle, in an unknown state $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$, to teleport. The total state of the system is then, after a proper rearrangement of terms,

$$\begin{aligned} |\phi\rangle|EPR\rangle &= \frac{1}{2}|\Phi^+\rangle(\alpha|0\rangle + \beta|1\rangle) + \frac{1}{2}|\Psi^+\rangle(\beta|1\rangle + \alpha|0\rangle) \\ &\quad + \frac{1}{2}|\Phi^-\rangle(\alpha|0\rangle - \beta|1\rangle) + \frac{1}{2}|\Psi^-\rangle(-\beta|0\rangle + \alpha|1\rangle), \end{aligned}$$

where

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

are so called Bell states (that form the (Bell) basis in H_4). If Alice performs a measurement on her two particles with respect to the Bell basis, then Bob's particle state collapses, with equal probability, into one of the states

$$\alpha|0\rangle + \beta|1\rangle, \;\; \alpha|1\rangle + \beta|0\rangle, \;\; \alpha|0\rangle - \beta|1\rangle, \;\; -\alpha|1\rangle + \beta|0\rangle$$

and Alice gets information, 2 bits, which of the four potential outcomes of the measurement has been obtained. If Alice then sends these two bits, using a public classical channel, to Bob, then he can achieve that his particle gets into the state that was teleported, by just performing on his particle, depending on two bits received, one of the following Pauli operators

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, i\sigma_y = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

An inverse process, in a sense, to quantum teleportation, in which one qubit is used to send two bits, is called **superdense quantum coding**.

Quantum teleportation is still one of the most studied subjects of QIPC. On the theoretical level, various its generalizations are being explored and also their relations to other problems [Wer00]. On the experimental level, a big challenge is to increase reliability and distance at teleportation.

5. Power of entanglement

There are several ways power of entanglement has been demonstrated.

5.1. Speeding-up quantum computations

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

In case of pure states, it is already known that without processing with increasingly growing multipartite entanglement, we cannot have an exponential speed-up, compared with the classical case. This follows from the results in [JL02], presented bellow.

Definition For a given integer p, a pure state of n qubits is p-blocked, if none of its $p+1$ qubits are entangled (after tracing out the remaining qubits).

Theorem Consider any quantum computational process on *pure* states with an increasing input size. Suppose there is a p such that at every stage of the computation the states produced by the process are p-blocked. Then such a computation process can be classically simulated in polynomial time.

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

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

- Shor designed, in 1994, polynomial time quantum algorithm to factorize integers [Sho97]— which would allow to break the RSA cryptosystem – no classical polynomial time algorithm for factorization is known. (Shor and other showed that quantum computers could break also other well known public-key cryptosystems.)

- Grover [Gro97] showed that quantum search in an unordered database of n elements can be done with $O(\sqrt{n})$ queries — that would allow to break the DSA cryptosystem – while classically n queries may be needed.

- Shor's result has been generalized to show that polynomial time algorithms exist for all *Hidden subgroups problem* for abelian groups.[5]

- For several other computational and simulation problems, for which no classical polynomial time algorithm is known, polynomial time quantum algorithms exist. For example, for solving so called Pell equation, $x^2 - dy^2 = 1$, with d as the parameter (Hallgren in 2002).

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

- It was shown [GC99] that entanglement is a computational primitive. Indeed, it is possible to realize any quantum computation by starting with some GHZ states $\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$, and then performing one qubit operations and Bell measurements.

  Moreover, it was shown [RB00] that universal quantum computation is possible by initializing a proper multipartite entangled state (a sort of a computational substrate) and then performing only one qubit measurements.

- Entanglement can also serve as a catalyst. Indeed, it was shown [JP99] that there are pairs of pure states $(|\phi_1\rangle, |\phi_2\rangle)$ such that, using local quantum operations and classical communications (LOCC), one cannot transform $|\phi_1\rangle$ into

$|\phi_2\rangle$, but with the assistance of an appropriate entangled state $|\psi\rangle$, as 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 in the process.

Moreover, as shown in [BR01], 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.

5.2. Making communication more efficient

There are five basic ways entanglement can provide a new quality for communication. One of them, quantum teleportation, has already been discussed. Three other are analyzed in this section. The last one, concerning security of communication, is discussed in Section 10.

Decreasing communication complexity: While in quantum computation we merely believe that quantum mechanics allows exponential speed-up for some computational tasks, in quantum communication we can prove that quantum tools can provide exponential savings. And not only that. It can be shown that

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

In the so called *entanglement-enhanced quantum communication model*, only classical bits are communicated, but communication is facilitated by an a priori distribution of entangled qubits among the communicating parties.

An exponential gap between the bounded-error classical and quantum entanglement-enhanced communication complexity has been shown in [Raz99], for a *promise problem*. This seems to be so far the strongest separation result for communication complexity

Proving lower bounds is notoriously hard. One of the main recent results in this direction has been a complete characterization, up to a logarithmic factor, of the bound-error quantum communication complexity for every symmetric predicate $f(x, y), x, y \in \{0,1\}^n$, depending only on $|x \cap y|$; that is if $f(x, y) = D(|x \cap y|)$ for some $D \in \{1, 2, \ldots, n\} \to \{0, 1\}$. Lower bound was shown in [Raz02], even for the model with preshared entanglement, in the form $\sqrt{nl_0(D,n)} + l_1(D,n)$ for certain functions l_0 and l_1. In two special cases, $D(s) \equiv (s = 0)$ and $D(s) \equiv s \pmod 2$, one gets lower bounds for much studied communication problems of disjointness and of inner product.

Concerning "communication without communication", we say, see [BCT99], that a *spooky communication* or *pseudo-telepathy* takes place, if a task cannot be done using classical communication only, but it can be done once parties share entanglement. **Spooky communication complexity** of the task is then defined as the amount of entanglement required to perform the task.

It has been shown, for a certain relation, that the number of bits to compute the relation classically is exponentially larger than the number of entangled pairs shared by the parties at the spooky communication (and therefore that spooky communication can be exponentially more efficient).

Increasing capacity of quantum channels: If two communicating parties share entangled states, then classical communication capacity of their noisy quantum channel can be increased, with respect to the best achievable capacity without preshared entanglement, by arbitrarily large constant factor [BSST99]. Surprisingly, from several capacities that have been defined for quantum channels with quantum inputs and outputs, entanglement-assisted capacity of noisy quantum channels is the only one that we already know how to compute.

Fighting decoherence: Untill 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 the unavoidable entanglement of any computational quantum system with its environment, fragile quantum superpositions, that are behind powerful quantum parallelism, can get exponentially fast destroyed. In addition, it had 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 could, in general, irreversibly destroy the state to be corrected. However, Shor [Sho96] showed, that not only quantum error-correcting codes, but also quantum fault-tolerant computations, are possible. (The main new and ingenious idea was to use multipartite entanglement to fight, in polynomial time, exponentially fast growing decoherence (caused, actually, by entanglement itself).)

6. Basic approaches to study entanglement

Two main approaches to develop qualitative and quantitative theory of entanglement have been pursued so far. They are related to the fact that in order to understand entanglement as a resource, we need to understand laws and methods how entanglement can be transformed, from one form to another, and also how to quantify entanglement.

6.1. Investigation of (reversible) transformations of states

Entanglement may appear in a form not suitable for a specific application. Therefore, it is of importance to understand how and when one can transform entanglement from one form into another form. The basic problem is to determine, when we can transfer one given state (or several copies of it), into some other given state (or several copies of it), using certain quantum and classical tools. Of special importance are the cases when the transformations allowed are from the following three classes.

LOCC This stands for the case that parties can perform only local quantum operations and classical communication.

SLOCC Operations are as in the LOCC case, but this time it is enough if the result is obtained with some non-zero probability.

EALOCC As above, but communicating parties are allowed to share some entanglement – these are *entanglement-assisted LOCC*.

Of a special importance are the following problems.

Entanglement concentration: How to obtain, from n copies of a non-maximally entangled pure state $|\phi\rangle$, using LOCC, as many as possible (m) copies of a maximally entangled state, and how large the ratio $\frac{m}{n}$ can be. (A variety of methods have been developed to do that – see [Gru02] for an overview.) Surprisingly, there is also a way to do entanglement concentration using only local quantum operations [HM01].

Entanglement purification – distillation: How to obtain, from n copies of a given mixed state ρ, as many as possible copies (say m) of a maximally entangled pure state, and how large the ratio $\frac{m}{n}$ can be – see [Gru02] for an overview.

Discovery, due to Horodeckis family, [HHH98b], that not all entangled mixed states are distillable, has been one of the big surprises at the development of QIPC science. Such states are called **bound entangled** and will be discussed in more details later. Moreover, it has been shown [VC01], that there are mixed states from which one can distill some entanglement, but less than it is needed to create those states.

Transformations of one state into another: Of large importance is to determine, when it is possible to transform one given state into another given one, exactly or asymptotically (having enough copies), deterministically (with probability one) or stochastically (with non-zero probability), and without or with a catalyst assistance, using operations of a certain type $\mathcal{O}$ (for example, LOCC). The related problem is to find out when are two states equivalent (mutually/reversibly transformable) using certain operations and modes of transformations. As expected, asymptotic and stochastic transformations yield usually simpler classifications. This problem is already quite well understood, see [Gru02] for overview, but still needs a lot of attention, especially for multipartite states, because it is so basic for classifications of entangled states.

MREGS (Minimal Reversible Entanglement Generating Sets): They are, for a given m, sets of states of minimal cardinality sufficient to generate all m-partite pure states by asymptotically reversible LOCC transformations. For bipartite states, the set containing one EPR state is a MREGS set. It is an open problem whether also for $m > 2$ there are finite MREGS (or whether there are infinitely many inequivalent types of entanglement), though some lower bounds for size of MREGS, depending on m, are known.

6.2. Quantification of entanglement

One of the key difficulties at the study of entanglement is that it is not clear how to quantify entanglement – especially of mixed and multipartite states.

In case of pure states of a bipartite system $A \otimes B$, a reasonable measure of entanglement of a state $|\phi\rangle$ is von Neumann entropy of the reduced density matrix, that is $E(|\phi\rangle) = -Tr\rho_A \lg \rho_A = -Tr\rho_B \lg \rho_B$, where $\rho = |\phi\rangle\langle\phi|$.

In the case of mixed bipartite states, the most natural – physically well motivated – measures of entanglement are entanglement of formation and distillation.

Entanglement of formation, $E_f(\rho)$, is defined as

$$E_f(\rho) = \inf \sum_j p_j E_f(\phi_j),$$

where infimum is taken over all pure-state decompositions of $\rho = \sum_j p_j |\phi_j\rangle\langle\phi_j|$. *Entanglement of distillation*, $E_d(\rho)$, is the average amount of maximally entangled states that can be distilled from several copies of ρ.

Another class of important measures of bipartite entanglement are that of *entanglement of relative entropies*, $E_r^S(\rho)$, that equal to the minimal "distance" of ρ to a set S of states (that are separable, or not-distillable, or have a similar property). These measures have interesting properties and serve as upper (lower) bounds for entanglement of distillation (asymptotic version of entanglement of formation).

For all basic measures of entanglement E, of importance is to consider their asymptotic (or regularized) versions $E^\infty(\rho) = \lim_{n\to\infty} \frac{E(\rho^{\otimes n})}{n}$. (Observe that entanglement of distillation is already the asymptotic measure.)

For any entanglement measure $\bar{E}$, it holds $\bar{E} = \bar{E}^\infty$ if $\bar{E}$ additive. It is a major open problem whether entanglement of formation is additive. A method has been developed, [MSW02], how to transfer additivity results for the Holevo capacity of quantum channels (another major open problem) to the additivity results for entanglement of formation of certain (sets of) states.

The problem with all above measures of entanglement is that they are difficult to compute because they require to solve an extremization problem. Only for 2×2 and 3×2 dimensional systems, we have an easily computable measure of entanglement, so called **concurrence** $C(\rho)$ [DW01], that can also be used to determine entanglement of formation because it holds $E_f(\rho) = H\left(\frac{1+\sqrt{1-(C(\rho))^2}}{2}\right)$, where $H(x)$ is the binary entropy function. The concurrence is defined as $C(\rho) = \max\{0, \lambda_1 - \lambda_2 - \lambda_3 - \lambda_4\}$, where λ_i are, in the descending order, eigenvalues of the matrix $\rho\hat{\rho}$, where σ_y is the Pauli matrix and $\hat{\rho} = (\sigma_y \otimes \sigma_y)\rho^*(\sigma_y \otimes \sigma_y)$. This strangly loooking measure has turned out to be surprisingly useful.

For bipartite states, both basic measures of entanglement can be seen as being defined in terms of such a "standard currency" as Bell states. They can be seen as the average amount of Bell states, needed to create a given state or to get distilled from it. This approach does not seem to be possible in the case of multipartite systems.

There have been various attempts to develop measures of entanglement for multipartite states. Most of them are attempts to generalize entanglement of relative entropy or concurrence – see [Gru02] for an overview.

Several of such generalizations are special cases of the hierarchy of measures of entanglement based on concurrence that was defined in [FMI02]. The k-th level of concurrence, for $k \leq d$, is defined for d-dimensional systems, by

$$C_k(|\phi\rangle) = \sum_{0 \leq i_0 < i_1 < \ldots < i_k \leq d-1} \lambda^{\downarrow}_{i_0} \lambda^{\downarrow}_{i_1} \ldots \lambda^{\downarrow}_{i_k},$$

where $\lambda^{\downarrow}_i$ is the ith largest eigenvalue of the reduced density matrix.

In general, it is already understood that a multicomponent entanglement measure is needed to quantify multipartite states, with each component representing a different type of entanglement.

7. Bound entanglement

In case of multipartite systems, bound entangled states (BE-states, for short), are such states that some initial entanglement is needed to create them, using LOCC, but no entanglement can be distilled from them by LOCC.

A simple example of bound entangled state is the state [Smo00]

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

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

The existence of bound entangled states was considered to be a puzzling phenomenon. Such states cannot be used at many important applications of entanglement, such as teleportation, where usually 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 bound entangled states. There are now several results showing that this is indeed the case.

First of all, in case of multipartite systems, a bound entangled 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.

However, quite surprisingly, bound entangled states are of some use. They can be *activated* [HHH98a], and *super-activated* [SST00]. In addition, a protocol has been described, so called *remote information concentration protocol* [MV00], that uses 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 therefore one can distill entanglement out of them. Hence, distillable entanglement is superadditive.

An intriguing problem is to find out which BE-states do not violate any Bell inequality. By [Dür01], there are multipartite BE-states that violate a Bell inequality, and by [KZG02], there is a bipartite BE-state that does not violate any Bell inequality.

8. ZOO of multipartite entanglement

As already mentioned, we still do not know whether for m-partite states, with $m > 2$, there are finite MREGS. This indicates that we can expect to have (very) many different types of entanglement.

Classification of multipartite states with respect to reversible transformations is, of course, not the only reasonable way to classify quantum states. Another important way is to consider two states as (stochastically) equivalent if each of them can be obtained from the other one by SLOCC – what actually means that two such states contain the same amount of entanglement.

For a special case of 3-partite and 4-partite qubit systems, quite a bit is already known about such different types of entanglement. For example, in 3-qubit systems [DVC00], we have four different types of pure states: (a) **Separable states** that are tensor products of three qubit states; (b) **Biseparable states**, that are not $A : B : C$ separable, but they are $AB : C$ or $AC : B$ or $A : BC$-separable; (c) So called **W-states**, with genuine entanglement of all three parties. They are the states that can be transformed, in a reversible way, by SLOCC, to the state $W = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle)$; (d) So called **GHZ-states**, again with genuine entanglement of all three parties together, but with no two of them entangled separatedly. They are states that can be transformed, in a reversible way, by SLOCC, to the GHZ state.

For the case of four-qubit systems, there are 9 such different types of entangled pure states [VDMV01].

Four different types of three-qubit mixed states, that parallel the above classification of pure three-qubit states, have been shown in [ABLS01].

9. Entanglement sharing

Being a resource, it is intuitively clear that there have to be some restrictions on how entanglement can be shared. Some of the basic related questions are

- To which extend does entanglement between two objects restrict their entanglement with other objects?
- What are the general laws and limitations of entanglement sharing?
- Does the entanglement sharing potential grow with the dimension of particles?

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*).

In this context, a key question is how are related multipartite and bipartite entanglement. Namely, which pairs of parties are entangled in a given multipartite system, if other parties are traced out.

Of interest is also to study the function $E(d, n)$ that denotes, for the case of states of n-partite d-dimensional systems, the maximum of the minimal entanglement of formation in any two subsystems [DW01].

One way to characterize entanglement of multipartite states is to specify how entangled become different subparties if the rest of parties is traced out. Results in [KZM02] show that for a "typical" pure state of n qudits (states in d-diemensional systems) all subsystems of less than $\frac{n}{3}$ parties are either separable or bound entangled and that probability of finding an n-qudit entangled state having some $\frac{n}{3}$ qubits entangled falls exponentially with the dimension of the Hilbert space. This means that most of the states are highly entangled, but entanglement is quite spread out and not shared by small group of parties.

10. Entanglement in quantum cryptography

There are two ways entanglement plays an important role in quantum cryptography: a positive one and a negative one.

Positive is the fact that quantum entanglement allows perfectly secure transmission of information and unconditionaly secure generation of perfectly secret random binary 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 no physical systems are transmitted.

Moreover, by sharing n pairs of particles in the EPR state, both parties can implement quantum one-time pad cryptosystem without a need to share a classical key [Leu00]. This is again an absolutely secure way of transmission.

There are also several ways how entanglement can be used to generate shared and perfectly secret binary key. This is of importance for classical secret key cryptography which is so secure how secure is the key distribution.

For example, let Alice and Bob share n pairs of particles in the 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 again absolutely secure, because no information is transmitted.

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

11. Frequency and robustness of entanglement

There are many basic questions concerning frequency and robustness of entanglement. It is of large importance to answer them for getting a more clear picture concerning the role entanglement can play in theory and especially in practice of quantum information processing and in quantum physics in general. Some of these questions to be asked for any type $\mathcal{T}$ of entangled states are:

- Given any 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 type $\mathcal{T}$?

- Are there states of type $\mathcal{T}$ such that some ball of non-zero radius contains only states of the type $\mathcal{T}$?

For example, it has been shown [ZHSL98], that there are separable, entangled and also bound entangled states, such that a ball around them contains the same type of states.

Numerical results, reported in [ZHSL98], showed that the 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.

Results obtained so far also show that a pure state is more likely to be entangled, but a mixed state is more likely to be separable.

12. Challenges

Let us try to summarize some of the main challenges research in quantum entanglement is to deal with.

(a) To develop a comprehensive theory of all correlations – quantum and classical. (b) To explore entanglement capabilities of such physical processes as Hamiltonian interactions, unitary operations, ... Which physical interactions can create entanglement? How much? How to use them optimally? (c) To demonstrate experimentally entanglement for increasingly larger distances and to find out how much entanglement extend into the macroscopic world to systems of increasing complexity. (d) To search for entanglement in Nature and to explore how robust it is.[6] (e) To clear-up the role of mixed-states entanglement for quantum computations. (f) To qualify and quantify multipartite entanglement. (g) To discover laws and limitations of entanglement sharing.

Notes

1. In this context, it is interesting to ask: *Why von Neumann, who played such important role in the development of both quantum mechanics and computing, did not come up with the idea of quantum information processing*, or, even better, *whether somebody could come up at all, at his time, with such an idea*? (It seems safe to say that the main reason was the fact that at his time there was no computation complexity theory and therefore there was no way to see that the idea of quantum information processing, clearly extremely complex from the technology point of view, could pay off at all.)

2. However, one should note that term *quantum non-locality* is quite confusing. Indeed, the best quantum theories we have – quantum field theories – satisfy the following locality condition: *operators with support in space-like separated regions commute.*

3. The term *hidden variable* is quite confusing. Such variables should not be hidden from us – they are hidden only with respect to the current formalism of quantum theory.

4. The term *Bell's inequalities* is nowadays used in a wide sense, to denote a whole set of inequalities, between average values of correlations of some quantum experiments, that can be used to demonstrate that no local hidden-variable model of the reality can derive all predictions of quantum mechanics.

5. An important open problem is whether this is true for all non-abelian groups. A positive answer would imply the existence of polynomial time quantum algorithm for graph isomorphism.

6. For example, every Bose-Einstein condensate is in a highly entangled state.

References

[ABLS01] A. Acin, D. Bruß, M. Lewenstein, and A. Sanpera. Classification of mixed three-qubit states. quant-ph/0103025, 2001.

[BBC+93] Ch. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Physical Review Letters*, 70:1895–1899, 1993.

[BCT99] G. Brassard, R. Cleve, and A. Tapp. Cost of exactly simulating quantum entanglement with classical communication. *Physical Review letters*, 83(9):1874–1787, 1999. quant-ph/9901035.

[BHU+02] B. Brezger, L. Hackermüler, S. Uttenhalter, J. Petachinka, and A. Zeilinger. Matter-wave interferometer for large molecules. quant-ph/0202158, 2002.

[BPM+97] D. Bouwmeester, J-W. Pan, K. Mattle, M.Eibl, H. Weinfurter, and A. Zeilinger. Experimental quantum teleportation. *Nature*, 390:575–579, 1997.

[BR01] S. Bandyopadhyay and V. Roychowdhury. Supercatalysis. quant-ph/0107103, 2001.

[Bru01] D. Bruß. Characterizing entanglement. quant-ph/0110078, 2001.

[BSST99] Ch. H. Bennett, P. W. Shor, J. A. Smolin, and A. V. Thapliyal. Entanglement-assisted classical capacity of noisy quantum channels. quant-ph/9904023, 1999.

[Dür01] W. Dür. Multipartite bound entangled states that do not violate Bell's inequality. quant-ph/0107050, 2001.

[DVC00] W. Dür, G. Vidal, and J. I. Cirac. Three qubits can be entangled in two inequivalent ways. quant-ph/0005115, 2000.

[DW01] K. Dennison and W. K. Wootters. Entanglement sharing among qudits. quant-ph/0106058, 2001.

[EPR35] A. Einstein, B. Podolsky, and N. Rosen. Can quantum mechanical description of physics reality be considered complete? *Physical Review*, 47:777–780, 1935.

[FMI02] H. Fan, K. Matsumoto, and H. Imai. Quantifying entanglement by concurrence hierarchy. quant-ph/0204041, 2002.

[Fuc02] Ch. A. Fuchs. Quantum mechanics as quantum information. q-p/0205039, 2002.

[GC99] D. Gottesman and I. L. Chuang. Quantum teleportation is a universal computational primitive. quant-ph/9908010, 1999.

[GI01] J. Gruska and H. Imai. Puzzles, mysteries and power of quantum entanglement. In *Proceedings of MCU'01, Cisenau, LNCS 2055*, pages 25–69, 2001.

[Gro97] L. K. Grover Quantum mechanics helps in searching for a needle in a haystack. *Physical Review Letters*, 78:325–328, 1997.

[Gru00] J. Gruska. *Mathematics unlimited, 2001 and beyond*, chapter Quantum computing challenges, pages 529–564. Springer-Verlag, 2000.

[Gru02] J. Gruska. *Quantum computing*. McGraw-Hill, 1999-2002. See also additions and updatings of the book on http://www.mcgraw-hill.co.uk/gruska.

[HHH98a] M. Horodecki, P. Horodecki, and R. Horodecki. Bound entanglement can be activated. quant-ph/9806058, 1998.

[HHH98b] M. Horodecki, P. Horodecki, and R. Horodecki. Mixed-state entanglement and distillation: is there a "bound" entanglement in nature? quant-ph/9801069, 1998.

[HM01] M. Hayashi and K. Matsumoto. Variable length universal entanglement concentration by local operations and its application to teleportation and dense coding. quant-ph/0109028, 2001.

[JKP01] B. Julsgaard, A. Kozhekin, and E. S. Polzik. Experimental long-lived entanglement of two macroscopic objects. quant-ph/0106057, 2001.

[JL02] R. Jozsa and N. Linden. On the role of entanglement in quantum computational speed-up. quant-ph/0201143, 2002.

[JP99] I. D. Jonathan and M. B. Plenio. Entanglement-assisted local manipulation of pure quantum states. quant-ph/9905071, 1999.

[Ken02] A. Kent. Causal quantum theory and the collapse locality loophole. quant-ph/0204104, 2002.

[KZG02] D. Kaszilowski, M. Zukowski, and P. Gnacinski. Bound entanglement and local realism. *Physical Review A*, 65:032107, 2002.

[KZM02] V. M. Kendom, K. Zyckowski, and W. J. Munro. Bounds on entanglement in qudit systems. quant-ph/0203037, 2002.

[Leu00] D. W. Leung. Quantum Vernam cipher. quant-ph/0012077, 2000.

[Mar02] T. W. Marshall. Nonlocality – the party may be over. quant-ph/0203042, 2002.

[MSW02] K. Matsumoto, T. Shimono, and A. Winter. Additivity of the Holevo channel capacity and of the entanglement of formation. In preparation, 2002.

[MV00] M. Murao and V. Vedral. Remote information concentration using a bound entangled state. quant-ph/0008078, 2000.

[Raz99] R. Raz. Exponential separation of quantum and classical communication complexity. In *Proceedings of* 31*st ACM STOC*, pages 358–367, 1999.

[Raz02] A. A. Razborov. Quantum communication complexity of symmetric predicates. quant-ph/0204025, 2002.

[RB00] R. Raussendorf and H. J. Briegel. Quantum computing with measurement only. quant-ph/0010033, 2000.

[Sch35] E. Schrödinger. Die gegenwartige Situation in der Quanenmechanik. *Natürwissenschaften*, 23:807–812, 823–828, 844–849, 1935.

[Sho96] P. W. Shor. Fault-tolerant quantum computation. In *Proceedings of* 37*th IEEE FOCS*, pages 56–65, 1996.

[Sho97] P. W. Shor Polynomial time algorithms for prime factorization and discrete logarithms on quantum computer. *SIAM J. on Computing*, 26(5):1484–1509, 1997.

[Smo00] J. A. Smolin. A four-party unlockable bound-entangled state. quant-ph/0001001, 2000.

[SST00] P. W. Shor, J. Smolin, and A. Thapliyal. Superactivation of bound entanglement. quant-ph/0005117, 2000.

[VC01] Guifré Vidal and J. I. Cirac. When only two thirds of the entanglement can be distilled. quant-ph/0107051, 2001.

[VDMV01] F. Verstraete, J. Dehaene, B. De Moor, and H. Verschede. Four qubits can be entangled in nine different ways. quant-ph/0109033, 2001.

[VW01] F. Verstraete and M. M. Wolf. Entanglement versus Bell violations under local filtering operations. quant-ph/0112012, 2001.

[Wer89] R. F. Werner. Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model. *Phys. Review A*, 40:4277–4281, 1989.

[Wer00] R. F. Werner. All teleportation and dense coding schemes. quant-ph/0003070, 2000.

[ZHSL98] K. Zyczkowski, P. Horodecki, A. Sampera, and M. Lewenstein. On the volume of mixed entangled states. quant-ph/9804024, 1998.