Entanglement in General Multipartite Quantum Systems and Its Role in Quantum Information Processing Tasks

Roman Gielerak

Institute of Control & Computation Engineering
University of Zielona Góra, ul. Podgórna 50, Zielona Góra 65-246, Poland
R.Gielerak@issi.uz.zgora.pl

Abstract. A major role playing by entanglement of quantum states in several, present day applications of genuine quantum technologies is briefly reviewed. Additionally, the notion and classification of multipartite entanglement has been presented. A new, monotone under (S)LOCC-operations measures of many-partite entanglement are defined and discussed briefly.

Keywords: quantum key distribution,teleportation protocols, multipartite entanglement,LOCC monotone functions.

1 Introduction

The opportunity of using genuine quantum behaviour of real matter at small scale has been considered for quite a long period as an interesting albeit purely academic challenge for developing a new computation model to perform effective computations of classically hardly computable functions [1]. The first real breakthrough in this area happened in the course of famous 1981 MIT 1st Conference on Physics and Computations [2] when Feynman has been suggested to use another quantum system to simulate a genuine quantum behaviour of a given quantum system as the only possibility to compute effectively the arising quantum effects. Soon, after this Conference the research activity in this narrow, academic area has been significantly increased. However the real eruption of activity and interest can be observed after discovery by P.Shor [3] of factorising big integers into prime factors algorithm working in polynomial time. As is widely known this is the only possibility to break the security of most popular cryptography protocols introduced in present day electronic communication industry. But, the point here is that in order to implement the Shor algorithm to factorise a big, 1024 bits integer in an acceptable time a quantum machine of a rather large scale (with quantum registers composing of thousands of quantum logical units) is necessary. Despite to unprecedented activity of all over the world scientific society (presumably, today it is hardly to find a developed country in the world where there are no several research groups that are working on this challenge) the present day existing and working machines looks to be

A. Kwiecień, P. Gaj, and P. Stera (Eds.): CN 2010, CCIS 79, pp. 15–28, 2010.

rather like small toys for kids. See [4,5,6] for a report on the present status of project of constructing Quantum Computer. A several, major breakthroughs in the fundamental Quantum Physics have to be achieved until the final, ultimate goal which is scalable Quantum Computing Machine working at our Macroscopic (and therefore classical) Reality will start to do an useful work.

The observed in last decades,exponential growth of computational power of all kinds of classical computers, PC including,sometimes summarised as Moor's Law is achieved mainly due to the technology miniaturisation process. Smaller and smaller chips like transistors consume less power, can be packed more densely and switch faster and faster. However. already today there are some technological processes that are to be controlled on atomic scales,dioxide insulating layers within each transistors produced is a good example of this. Providing the miniaturisation will progress with speed as observed in last decades a typical for genuine quantum effects domination scale (it is theoretically predicted that the border in between classical and quantum is of size of 10 nanometers) will be reached soon. Then the necessity, not only the opportunity (as today), of understanding deeper the quantum behaviour and the use of it to perform a useful calculations on this quantum scale should be stressed. Otherwise a serious slowing down of the progress in the computational power of computer technology do appear and the only today predictable possibility to breakthrough the forthcoming crisis is to build quantum computing machines. There are a number of quantum computing candidates, among those: superconductor-based quantum computers (including SQUID-based quantum computers), trapped ion quantum computer, optical lattices, topological quantum computer, quantum dot on surface (e.g. the Loss-DiVincenzo quantum computer), nuclear magnetic resonance on molecules in solution (liquid NMR), solid state NMR Kane quantum computers, electrons on helium quantum computers, cavity quantum electrodynamics (CQED), molecular magnet, fullerene-based ESR quantum computer, optic-based quantum computers, diamond-based quantum computer, BoseEinstein condensate-based quantum computer, transistor-based quantum computer – string quantum computers with entrainment of positive holes using an electrostatic trap, spin-based quantum computer, adiabatic quantum computation, rare-earth-metal-ion-doped inorganic crystal based quantum computers.

Such a large number of candidates shows explicitly that the topic, in spite of rapid progress, is still in its infancy. But at the same time there is also a vast amount of flexibility.

There is no doubts that quantum entanglement is this genuine quantum property that is the key resource of many fruitful applications of quantum information processing technology. For example, the realistic applications of entangled states include theirs major applications for quantum key distribution protocols (Quantum Cryptography, [7,8,6]). A still futuristic but fascinating visions of using quantum channels for communication purposes applies entanglement as the main tool for teleportation protocols implementations, see [9] and the so called dense coding protocols, see [10]. It is not excluded that the use of quantum channels will play more and more important role in future communication

technologies. The vision of global communications networks with an appropriate quantum communication channels present inside them seems to be a very realistic vision of a near future.

2 Some Applications of Quantum Entanglement to the Future Quantum Communication Technologies

Some introductory material for reading this section, at least on the level for beginners, can be found in [11] and [12].

2.1 Quantum Cryptography Protocols Based on Quantum Key Distribution (QKD)

At present the security of the widely used RSA and connected, theory of numbers based encryption protocols relies on the computational complexity of finding period of an element in multiplicative group Z_N^*, for N a sufficiently big integer. In particular, the difficulty of factorization can be overcomed providing a suitable algorithm for computing periods of elements of Z_N^* is known. RSA is used to establish secure connections over Internet, enabling the transition of sensitive data such as passwords,credit cards details and online banking sessions. RSA also forms the heart of secure messaging protocol PGP (Pretty Good Privacy). As we have pointed out RSA is only conditionally secure and the construction of sufficiently large scale quantum computer will destroy this kind of security completely.

Quantum cryptography sometimes called quantum key distribution (QKD) offers absolute security of the corresponding encryption protocols as opposite to the only conditional security offered by all present day available classical technologies. Let us recall that already in 1917 Vernam [13] proposed one-time pad encryption scheme the absolute security of which was proven by Shannon in 1947 [14]. However the serious drawbacks of one-time pad among which the most serious is the question of session key distribution seems to be the most crucial ones for makings them insecure and impractical.

Quantum technology offers instead a very promising solution to all of the mentioned drawbacks of one-time pad protocol. There are mainly two types of QKD schemes. The first type of QKD schemes is based on quantum measurement process applied to earlier prepared and distributed states and includes several protocols among which the best known are BB84 protocol [15], B92 [16] protocol and others as well [17]. The other types of QKD schemes are entanglement based QKD schemes, the Ekert91 [18] and BBN92 [19] are the best known representatives of this family.

At the heart of any of entanglement based QKD protocol is the quantum entanglement of the used quantum states and Bell theorem known also as the violation of Bell inequalities in presence of entanglement [20]. In particular case of Ekert91 scheme the sender (traditionally called as Alice) and the receiver (Bob) are assumed to share a rather big reservoir of maximally entangled pairs

of photons. The photons are distributed in such a way that Alice and Bob each end up with one photon from each pair. We have to assume that Alice and Bob are space like separated (in accordance with the locality principle in 4D Minkowski space-time and the assumptions for applying Bell inequalities) and that they both measure polarisations of theirs photons. Although the particular results of their measurements are completely random certain correlations among theirs particular outcomes obtained are to be hold as predicted by Bell theorem. It follows that any attempt at eavesdropping (by Eve) will disturb these correlations in such a way that Alice and Bob immediately will be able to detect them. However, the disturbances of quantum correlations might have its origin not only in eavesdropping but also may be caused by imperfections in the transmission line and detectors. Therefore the presented scheme of QKD must be complemented with two additional steps. The first step should eliminate the erroneous bits caused by noise of channels used and this becomes to be possible by the so called information reconciliation step. Information reconciliation is a form of error correction carried out between Alice and Bob's keys, in order to ensure both keys are identical. It is conducted over the public channel and as such it is vital to minimise the information sent about each key, as this can be read by Eve. A common protocol used for information reconciliation is the cascade protocol, proposed in 1994 [21]. This operates in several rounds, with both keys divided into blocks in each round and the parity of those blocks compared. If a difference in parity is found then a binary search is performed to find and correct the error. If an error is found in a block from a previous round that had correct parity then another error must be contained in that block; this error is to be found and corrected as before. This process is repeated recursively, which is the origin of the cascade name for it. After all blocks have been checked, Alice and Bob both reorder their keys in the same random way, and a new round begins. At the end of multiple rounds Alice and Bob have identical keys with high probability, however Eve has gained some additional information about the key from the parity information exchanged. The second step necessary in the presence of eavesdropper is to reduce the amount of catched by him information about the session key below some minimal level (in fact reduction to any low level is possible) from which the reconstruction of the session key will be impossible at all. For this purpose the so called Privacy Amplification procedure has been formulated. Privacy Amplification is a method for reducing (and effectively eliminating) Eve's partial information about common Alice and Bob's key session. This partial information could have been gained both by eavesdropping on the quantum channel during key transmission (thus introducing detectable errors), and on the public channel during information reconciliation (where it is assumed Eve gains all possible parity information). Privacy amplification uses Alice and Bob's key to produce a new, shorter key, in such a way that Eve has only negligible information about the new key. This can be done using a universal hash function, chosen at random from a publicly known set of such functions, which takes as its input a binary string of length equal to the key and outputs a binary string of a chosen shorter length. The amount by which this new key is

shortened is calculated, based on how much information Eve could have gained about the old key (which is known due to the errors this would introduce), in order to reduce the probability of Eve having any knowledge of the new key to a very low value. See [6] for details concerning both additional steps.

The complete mathematical proof of unconditional, absolute security of QKD protocols was appeared to be not an easy problem which was solved only in the last few years [17,19,22]. However, in real applications of QKD realistic devices used for that purpose contain many imperfections comparing with mathematically idealized QKD protocols to which the above mentioned proofs are referring. Summarising: the question of absolute security of realistic performance of QKD is still under active debate. Although there is still a big gap in between the theory and practise of QKD a lot of experimental work has been done successfully in the last years. In particular successful implementations of QKD protocols based on entanglement have been realised by free-space transfer of entangled pairs of photons over 144 km distance [23]. Concerning the present day realistic implementations of QKD schemes we note the longest distance over which QKD has been demonstrated using optic fibre is about 148.7 km (BB84 protocol) [24]. As it concerns free space the best result as it was already mentioned is 144 km ,the distance in between two of the Canarian Islands (Ekert91) [23] and (BB84 protocol) [25]. Attempts to extend QKD schemes to satellite communication level are also started with. At present there are at least four companies offering commercial quantum cryptography equipement: idQuantque (Geneva), MagiQ Technologies (New York), SmartQuantum (France) and QuintessenceLabs (Australia). It is interesting to recall that already in 2008 the first computer network protected exlusively by QKD protocols has been successfully tested during some scientific conference in Vienna. The name of this network is SECOQC (Secure Communication Based on Quantum Cryptography) and EU funded this project. The network used 200 km of standard fibre optic cable to interconnect six locations across Vienna and the town of St. Poelten located 69 km to the west [26].

Despite to powerfull progress in QKD implementations still, some crucial from the point of view of commercial applications problems, like the rather low bit rate and the problem of amplifications of quantum signals (the quantum repeater problem) making the transmission possible on a relatively small distances only has to be solved before QKD will start to dominate in computer security technology. The highest bit rate system currently demonstrated exchanges secure keys at 1 Mbit/s (over 20 km of optical fibre) and 10 kbit/s (over 100 km of fibre), achieved by a collaboration between the University of Cambridge and Toshiba and using the BB84 protocol with decoy pulses [27].

2.2 Quantum Teleportation Protocols and Dense Coding Protocols

It is not excluded, even more it is clear that the future communication technologies will use intensively quantum channels for transferring quantum and classical information purposes together with classical channels based technology. Especially interesting seems to be a vision of using quantum channels for performing the process of teleportation of classical and quantum as well information

and sending classical information through quantum channels using dense coding based protocols fot this purpose. Quantum teleportation, or entanglement-assisted teleportation, is a technique used to transfer quantum information from one quantum system to another. It does not transport the system itself as it is described by sciences-fiction writers, nor does it allow communication of information at superluminal (faster than light) speed as it seems to us today. Neither does it concern rearranging the particles of a macroscopic object to copy the form of another object. Its distinguishing feature is that it can transmit the information present in a quantum superposition, useful for quantum communication and computation. Again entanglement of quantum states used lies in the very origin of this way of communication. To start with let us explain in details a general teleportation protocol by which we can send both quantum and classical information encoded in quantum states. Reversing teleportation protocol we obtain the dense coding protocol by which we can send much more classical information then in any of previously known and used classical protocols.

The standard teleportation scheme involve three-partite quantum system $A \wedge B \wedge C$ with the corresponding Hilbert spaces of states $\mathcal{H}_A$, $\mathcal{H}_B$ and $\mathcal{H}_C$. It is assumed that a general mixed state ρ is given in the sector A and the problem is to "send it" to the spacely separated sector C. In the standard teleportation scenario it is assumed that an additional and sufficiently entangled (in most cases the maximally entangled state is used) bipartite state $\omega_{BC} \in E(\mathcal{H}_B \otimes \mathcal{H}_C)$ is at disposal of both AB and C. The teleportation based transfer of information contained in the state ρ allows to perform only local with respect to the decomposition $AB + C$ and physical operations (i.e. only completely positive and local operations are allowed) together with classical communication channel through which certain amount of supplementary (to conclude the teleportation process) classical information can be send. In most cases the above mentioned local operations are measurement operations which in general are realised through the Positive Operator Valued Maesure (POVM) $\mathbb{F}$ with a discrete spectrum $\sigma(F)$, see [28]. The first step of the protocol is to perform the measurement of $\mathbb{F}$ and if $x \in \sigma(\mathbb{F})$ is resulted then this information is sent through the adjusted classical channel to the receiver C. The receiver C must have a suitable library of keys $\{K(x), x \in \sigma(\mathbb{F})\}$ which are local (acting in C sector only) physical operations and such that if he applies the proper key $K(x)$ to its end of the state ω_{BC} i.e. $(\mathbb{I}_B \otimes K_x)(\omega_{BC})$ then the result of this operation should be exactly equal to ρ. All this can expressed by the following equality:

For any observable $A = A^\dagger \in \mathcal{H}_A$

$$\mathrm{Tr}_{\mathcal{H}_A}(\rho A) = \sum_{x \in \sigma(\mathbb{F})} \mathrm{Tr}\,(\rho \otimes \omega_{BC})\,(F_x \otimes K_x(A)) \tag{1}$$

where it is assumed (for simplicity only) that the space $\mathcal{H}_B$ is isomorphic to $\mathcal{H}_C$ i.e. $\dim(\mathcal{H}_B) = \dim(\mathcal{H}_C)$. A graphical exposition of the described teleportation process is presented in Fig. 1.

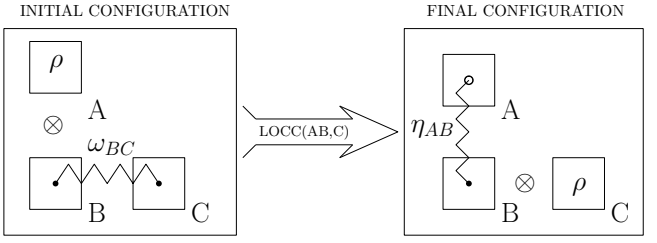

Fig. 1. The general scheme of teleportation

The fundamental question is of course whether teleportation processes as described are possible at all and both on theoretical level and experimental as well.

Example 1. Teleportation of pure states of qubit protocol [29].

This was historically the first teleportation protocol discovered for teleporting pure states of qubit. In this case the corresponding Hilbert spaces are given by 2d complex Euclidean spaces C^2 and the corresponding entangled state (which is maximally entangled state in fact) is given by:

$$|\Psi_{BC}\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) \quad . \tag{2}$$

Let $|\Psi_A\rangle$ be any pure state of qubit that will be teleported. The measurement arrangement here reduces to the orthodox von Neumann measurement in the of Bell vectors composed orthonormal basis of $C^2 \otimes C^2 = C^4$ which are defined as:

$$\begin{array}{l} |\phi_{\pm}\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle \pm |11\rangle\right) \\ |\psi_{\pm}\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle \pm |10\rangle\right) \end{array} \quad . \tag{3}$$

The only possible outcomes of such an experiment are given as pairs of numbers (00), (01), (10) and (11) and all can arise with the same probability equal to 0.25. The resulted pair of bits is then send to receiver C through classical channel and the corresponding library of keys used by him in order to obtain a state $|\Psi_A\rangle$ in his register is given by $\{\mathbb{I}, \sigma_Z, \sigma_X, i\sigma_Y\}$. This is depicted graphically in Fig. 2.

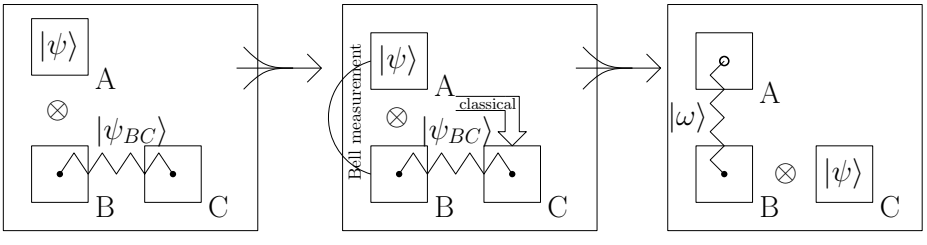

Fig. 2. Teleporting of qubit state using maximally entangled state $|\psi_{BC}\rangle$ and orthogonal measurement in Bell basis together with classical channel

It is interesting to observe that from mathematical point of view the teleportation process just described is nothing more then the following algebraic identity:

$$|\Psi\rangle|\Psi_{BC}\rangle = \frac{1}{2}|\phi_+\rangle(\mathbb{I}|\Psi_A\rangle) + \frac{1}{2}|\phi_-\rangle(\sigma_Z|\Psi_A\rangle) + \\ + \frac{1}{2}|\psi_+\rangle(\sigma_X|\Psi_A\rangle) + \frac{1}{2}|\psi_-\rangle(-i\sigma_Y|\Psi_A\rangle) \ . \tag{4}$$

It follows from the anylysis of Werner [30] that the following general result can be proven:

Theorem 1. *Let us assume that* $\dim(\mathcal{H}_A) = \dim(\mathcal{H}_B) = \dim(\mathcal{H}_C) < \infty$. *Then there exist infinitely many unitarly unequivalent scenarios of teleportation protocols as desribed in Fig. 1.*

Concerning experimental demonstrations of teleportation we referr to [31] (photonic states) and [32] (atomic states).

3 The Mathematical Notion of Entanglement

Let $\mathcal{G}$ be a quantum system composed from n smaller parties $\mathcal{G}_i$ which we assume are separated spatially, however, a classical communication in between them is still allowed. From quantum physics we know that to subsystems $\mathcal{G}_i$ there are associated in an unique (up to unitary isomorphisms) Hilbert spaces $\mathcal{H}_i$ of states and the states of composite system $\mathcal{G}$ are associated with the space $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \ldots \otimes \mathcal{H}_n$, where $\otimes$ means the (completed if dimensions of $\mathcal{H}_i$ are infinite) tensor product operation. The pure states of $\mathcal{G}$ are then given by (rays) normalised vectors $|\psi\rangle \in \mathcal{H}$ and the corresponding space of pure states will be denoted as $\partial E(\mathcal{H})$. The corresponding mixed states are given by linear, of trace class semi-positive maps of $\mathcal{H}$ and form a compact and convex subset $E(\mathcal{H})$ the topological boundary of which is exactly the set $\partial E(\mathcal{H})$. The source of all of problems connected with entanglement is that $E(\mathcal{H})$ is not a Choquet simplex and therefore there do exist infinitely many different decompositions of a given state $\rho \in E(\mathcal{H})$ into pure states from $\partial E(\mathcal{H})$.

Let $Par(n)$ be a set of all partitions of a given n-element set $X = \{x_1, \ldots, x_n\}$, the number of elements of $Par(n)$ is given by the corresponding Bell number $B(n)$. For a given partition $\pi \in Par(n)$ of the form $\pi = (X_1, \ldots, X_k)$ the number k stands for the length $|\pi|$ of π. The following partial order $\prec_f$ will be used in the following: we say that a partition $\pi = (X_1, \ldots, X_k)$ is finer that a partition $\pi' = (Y_1, \ldots, Y_l)$ iff for each $i \in \{1, \ldots, k\}$ there exists $l \in \{1, \ldots, l\}$ such that $X_i \subseteq Y_l$. This will be denoted as $\pi \prec_f \pi'$. Then, in the poset $(Par(X), \prec_f)$, there exists a maximal element $\pi_{\max} = (X)$ and minimal $\pi_{\min} = (\{x_1\}, \ldots, \{x_n\})$ as well.

Let $|\psi\rangle \in \partial E(\mathcal{H})$. We will say that the vector state $|\psi\rangle$ is π-separable state, where $\pi = (X_1, \ldots, X_k)$, iff $|\psi\rangle$ can be written as

$$|\psi\rangle = \bigotimes_{i=1}^{k} |\psi_{X_i}\rangle, \text{ where } |\psi_{X_i}\rangle \in \partial E(\bigotimes_{\alpha \in X_i} \mathcal{H}_\alpha) \tag{5}$$

and π is the finest partition for which (5) hold.

In particular a state $|\psi\rangle \in \partial E(\mathcal{H})$ is called completely separable iff $|\psi\rangle$ is $\pi_{\min}$-separable. The dual notion is that of partial entanglement. A state $|\psi\rangle \in \partial E(\mathcal{H})$ is called completely entangled iff $|\psi\rangle$ is $\pi_{\max}$-separable and is π-entangled iff it is π-separable and $\pi \notin \{\pi_{\max}, \pi_{\min}\}$. If $|\psi\rangle$ is π-separable state, $\pi = (X_1, \ldots, X_k)$, then for any $i : |X_i| \geq 2$ the state $|\psi_{X_i}\rangle$ is completely entangled on X_i.

A similar definition can be introduced to treat the case of general quantum states $\rho \in E(\mathcal{H})$. A state $\rho \in E(\mathcal{H})$ is called π-separable state iff there exists $\pi \in Par(\{1, \ldots, n\})$ for which the following representation exists:

$$\rho = \sum_{\alpha} P_\alpha \otimes_{i \in \{1,\ldots,|\pi|\}} \rho^\alpha_{X_i}, P_\alpha \geq 0, \sum_{\alpha} P_\alpha = 1, \rho^\alpha_{X_i} \in E(\bigotimes_{j \in X_i} \mathcal{H}_j). \tag{6}$$

Having a particular state $|\rho\rangle \in E(\mathcal{H})$ we want to answer the question whether this state is entangled or not. In the two-partite case certain useful criterions have been developed in the past twenty years due to activity of many peoples. For an extensive and up to date well written reviews see [33,34].

In the case of two-partite systems and for pure states the complete answer to the question of entanglement and the amount of it is provided by the Schmidt decomposition theorem [28]. In the case of general two-partite systems (however the finite dimensional situations are mainly explored till now) several techniques checking whether a given mixed state ρ is entangled or not have been worked out and certain methods for definite answering this question (based on Linear Programming Algorithms) are at our disposal at present. Although the definite answer to the question of entanglement can be obtained the important point is that this problem is known to be NP-HARD problem [35]. However, a plenty of polynomially complex methods can be used for this purpose also. However, the price for a use of a reasonable calculationaly complex method is that all of them are not giving definite answer to the question of entanglement. The so called PPT-criterion of Peres [28,36,33] the cross norm criterion [33,34] and several witness constructions are known examples [34,33].

So, we can assume that a suitable procedure enabling us to check whether a given state of 2-partite system $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$ is separable or entangled is given.

2p-Oracle: Is entangled?

input : $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$, $\rho \in E(H)$, the 2p decomposition
output: YES, if ρ is entangled, NO if ρ is separable

For further use let us recall what the Schmidt decomposition theorem tells us. For any $|\psi\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2$ there exists a sequence of strictly positive numbers

$(\lambda^1_{|\psi\rangle}, \ldots, \lambda^k_{|\psi\rangle}) \equiv \lambda_{|\psi\rangle}$ called a Schmidt coefficients of $|\psi\rangle$ and where $k = \min(\dim(\mathcal{H}_1), \dim(\mathcal{H}_2))$ is the so called Schmidt rank of a vector $|\psi\rangle$ and a pair of ON bases $\{\Theta^1_i\}, \{\Theta^2_i\}$ in $\mathcal{H}_1$ and respectively in $\mathcal{H}_2$ and such that the following eguality holds:

$$|\psi\rangle = \sum_{i=1}^{k} \lambda^i_{|\psi\rangle} |\Theta^1_i\rangle |\Theta^2_i\rangle \ . \tag{7}$$

SD-Function

input : $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$, $|\psi\rangle \in \partial E(H)$
output: $[r_{|\psi\rangle}, \lambda_{|\psi\rangle}, \{\Theta^1_i\}, \{\Theta^2_i\}]$

where $r_{|\psi\rangle}$ is the Schmidt rank of $|\psi\rangle$, $\lambda_{|\psi\rangle} = (\lambda^1_{|\psi\rangle}, \ldots, \lambda^k_{|\psi\rangle})$, $k = r_{|\psi\rangle} \leq \min(\dim \mathcal{H}_1, \dim \mathcal{H}_2)$, $\{\Theta^i_\alpha\}, i = 1, 2$ are the corresponding ON-bases in $\mathcal{H}_i$

In the paper [37] certain algorithms for answering the question of partial separability (and thus of entanglement) in the case of n-partite systems have been presented. We summarise the results of [37].

n-partite-Oracle: Is entangled?

input : $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \ldots \otimes \mathcal{H}_n$, the decomposition of the system, $\rho \in E(H)$
output: $X = (X_1, \ldots, X_k) \in Par(I_n)$ such that ρ is X-separable

However, the serious drawback of methods introduced in [37] is that they are all of nonpolynomial (in n) calculational complexity.

One of the important corollaries of [37] is that in the case of n-partite systems several incomparable (here we mean the comparison by the use of (S)LOCC class of operations and appropriately adopted to the case discussed, see below) kinds of partial entanglement do appear.

Let $\rho \in E(\mathcal{H})$ and let $X = (X_1, \ldots, X_k)$ be the corresponding partition given by the use of previous n-partite Oracle. Any reasonable measure $\mathcal{M}_n$ of amount of entanglement included in ρ should obey the following requirements:

($\mathcal{E}_n(1)$) $\mathcal{M}_n$ is separating the subset of complete separable states from the remaining (open) part of $E(\mathcal{H})$,

($\mathcal{E}_n(2)$) $\mathcal{M}_n$ must be invariant under $LU(X)$-operations, when $LU(X) = U(X_1) \otimes \ldots \otimes U(X_k)$ for $X = (X_1, \ldots, X_k) \in Par(I_n)$ and $U(X)$ is the group of unitaries acting on $\mathcal{H}_X$,

($\mathcal{E}_n(3)$) $\mathcal{M}_n$ must be monotone under $(S)LOCC(X)$ class of operations, which means that for any $\rho \in E(\mathcal{H})$ and with $X = (X_1, \ldots, X_k)$ as above, for

any $X^{'} \prec_{finer} X$ and the action of local physical operations Θ, local with respect to the partition $X^{'} = (Y_1, \ldots, Y_i)$:

$$\mathcal{M}_n(\Theta(\rho)) \leq \mathcal{M}_n(\rho) \ ,$$

$(\mathcal{E}_n(4))$ $\mathcal{M}_n$ should obey natural continuity requirements.

Even in the case of 2-partite systems it is not an easy task to construct the corresponding function, although some definition and proceduras are given the real drawback of all of them is that they are hardly to be effectively calculable [38]. A mathematical proof of the generic NP-hardness of computing such functions is known [35].

Any function $\mathcal{M}_n$ obeying $\mathcal{E}_n(2)$ – $\mathcal{E}_n(3)$ (and $\mathcal{E}_n(4)$) will be called n-partite entanglement monotone (resp. continuous n-partite entanglement monotone) function.

Now, we present an example of such n-partite monotone that will be called weakest k-clique entangled. For this we assume that $\rho \in E(\mathcal{H})$ is completely entangled state.

For any $k \in \{1, \ldots, \frac{n}{2}\}$ let $C_k(n) \equiv \{$the set of all k-elements subsets of $I_n = \{1, 2, \ldots, n\}\}$. The elements of $C_k(n)$ will be called k-cliques in the following. Any $X \in C_k(n)$ definies 2-partition $(X, I_n \setminus X)$ of I_n. Let $\mathcal{M}_2$ stands for any 2-partite monotone. With the use of $\mathcal{M}_2$ we define the strength of entanglement in between X and $I_n \setminus X$ that is contained in the state ρ:

$$\widetilde{es}_k(X, X^c)(\rho) = \mathcal{M}_2(\rho, \mathcal{H}_X, \mathcal{H}_{X^c}) \tag{8}$$

Then the weakest k-clique entangled is defined as

$$wes_k(\rho) = \inf\{\widetilde{es}_k(X, X^c)(\rho)\}, X \in C_k(n) \ . \tag{9}$$

Our main result of this contribution is formulated now:

Theorem 2. *Let $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \ldots \otimes \mathcal{H}_n$ be a n-partite system and let $\rho \in E(\mathcal{H})$ be completely entangled state. Then for any 2-partite continous monotone $\mathcal{M}_2$ and any $k \in \{1, \ldots, \frac{n}{2}\}$ the function wes_k as defined in (9) is (continous) n-partite entanglement monotone.*

A detailed discussion of the introduced n-partite entanglement monotone measures shall be presented in a separate, forthcoming publications where also certain numerical examples obtained by the use of Zielona Gora Quantum Computing System [39] will be presented as well.

4 Summary

The quantum entanglement is this genuine quantum property by use of which, otherwise impossible tasks may be achieved. Among the best known applications of entanglement are: quantum key disribution offering an absulute secure

exchange of information, superdense coding, quantum state teleportation, information exchanges through time and many ohers as well, most of them is even hardly to predict today. Quantum entanglement already now has found many interesting applications in present day state of art in the emerging technologies of quantum computing and quantum cryptography, for example it has been used to realize practically quantum teleportation tasks. At the same time, it prompts some of the more philosophically oriented discussions concerning quantum theory. The correlations predicted by quantum mechanics, and observed in experiment, reject the principle of local realism, which is that information about the state of a system can only be mediated by interactions in its immediate surroundings and that the state of a system exists and is well-defined before any measurement [40]. Efforts to quantify the amount of entanglement included in a typically entangled quantum states are therefore very important to understand better a very nature of quantum world.The present paper contains both the very condensed review of the actual applications of quantum entanglement in the existing technology and also presents the main ideas of our very recent attempts to understand qualitatively the phenomenon of multipartite entanglement [37].

References

1. Deutsch, D.: Quantum Theory the Church-Turing principle and the universal quantum computer. Proceed. R. Soc. 400, 97–117 (1985)
2. Feynman, R.P.: Keynote talk by R.P. Feynman, 1st Conference on Physics and Computations. MIT, Cambridge (1981); International Journal of Theoretical Physics 21, 467–488 (1982)
3. Shor, P.: Algorithms for quantum computations: discrete log and factoring. In: Goldwasser, S. (ed.) Proceedings of the 35th Annual Symposium on the Foundations of Computer Sciencem, pp. 124–134. IEEE Computer Society Press, Los Alamitos (1994)
4. Petit, C.: Quantum Computer Simulates Hydrogen Molecule Just Right. Science News (January 2010)
5. DiCarlo, L.: Demonstration of two-qubit algorithms with a superconducting quantum processor. Nature 460, 240–244 (2009)
6. Bennett, C.H., Bessette, F., Brassard, G., Salvail, L., Smolin, J.: Experimental Quantum Cryptology 5(1), 3–28 (1992)
7. Gisin, N., Ribordy, G., Tittel, W., Zbinden, H.: Quantum cryptography. Rev. Mod. Phys. 74, 145–194 (2002)
8. Lo, H.-K., Lutkenhaus, L.: Quantum Cryptography: from theory to practise. Physics in Canada 63, 191 (2007)
9. Vaidman, L.: Teleportation of Quantum States. Phys. Rev. A 49, 1473–1476 (1994)
10. Peres, A.: What is actually teleported? IBM Journal of Research and Development 48(1)
11. Bugajski, S., Klamka, J., Wegrzyn, S.: Foundation of quantum computing. Part 1. Archiwum Informatyki Teoretycznej i Stosowanej 13(2), 97–142 (2001)
12. Bugajski, S., Klamka, J., Wegrzyn, S.: Foundation of quantum computing. Part 2. Archiwum Informatyki Teoretycznej i Stosowanej 14(2), 93–106 (2002)
13. Vernam, G.S.: Cipher printing telegraph systems for secrets wire and racho telegram communications. J.AIEE, 109 (1926)

14. Shannon, C.: Communication theory of secrecy systems. Bell System technical Journal 28(4), 656 (1949)
15. Bennett, C.H., Brassard, G.: Quantum Cryptography: Public key distribution and coin tessing. In: Proc. IEEE Computer Systemsand Signal Processing, pp. 175–179. IEEE, Bangalore (1984)
16. Bennett, C.H.: Quantum cryptography using any two nonorthogonal states. Phys. Rev. Lett. 68, 3121 (1992)
17. Lo, H.-K., Chau, H.-F.: Unconditional security of quantum key distribution over arbitrary long distances. Science 283, 2050
18. Ekert, A.K.: Quantum cryptography based on Bell theorem. Phys. Rev. Lett. 67, 661 (1991)
19. Acin, A., Gisin, N., Masanes, L.: From Bell theorem to secure QKD. Phys. Rev. Lett. 97, 120405 (2006)
20. Bell, J.S.: Speakable and unspeakable in quantum mechanics. Cambridge University Press, Cambridge (1987)
21. Brassard, G., Salvail, L.: Secret key reconcilation by public discussion. In: Helleseth, T. (ed.) EUROCRYPT 1993. LNCS, vol. 765, pp. 410–423. Springer, Heidelberg (1994)
22. Mesanes, L., Winter, A.: Unconditional security of key distribution from causality constrains. `http://arxiv.quant/ph/06066048` (2006)
23. Ursin, R.: + 17 coauthors: Entanglement based quantum communication over 144 km. Nature 3, 481 (2007)
24. New Jornal of Physics 8, 193 (2006)
25. Schmitt-Manderbach et al.: Experimental demonstration of the free space decoy-state quantum key distribution over 144 km. Phys. rev. lett. 98, 1010504 (2007)
26. `http://news.bbc.co.uk/1/hi/sci/tech/7661311.stm`
27. Dixon, A.R., Yuan, Z.L., Dynes, J.F., Sharpe, A.E., Shields, A.J.: Optics Express 16(23), 18790–18979
28. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information. Cambridge University Press, Cambridge (2000)
29. Bennett, C.H., et al.: Teleporting an Unknown Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels. Phys. Rev. Lett. 70, 1895–1899 (1993)
30. Werner, R.F.: All teleportation and Dense coding schemes, `http://arXiv.quant/ph/003070v1`
31. Barrett, M.D., et al.: Deterministic Quantum Teleportation of Atomic Qubits. Nature 429, 737 (2004)
32. Riebe, M., et al.: Deterministic Quantum Teleportation with Atoms. Nature 429, 734–737 (2004)
33. Bengtsson, I., Życzkowski, K.: Geometry of Quantum States: An Introduction to Quantum Entanglement. Cambridge University Press, Cambridge (2006)
34. Horodecki, R., Horodecki, P., Horodecki, M., Horodecki, K.: Quantum entanglement. Rev. Mod. Phys (2007), `http://arxiv.org/abs/quant-ph/0702225`
35. Gurvits, L.: Classical deterministic complexity of Edmonds' Problem and quantum entanglement. In: Proceedings of the thirty-fifth annual ACM symposium on Theory of computing (October 2003)
36. Gruska, J.: Quantum Computing. McGraw-Hill, New York (1999)
37. Gielerak, R., Sawerwain, M.: Twopartite, combinatorial approach to partial k-separability problem for general multipartite states, `http://arXiv.quant/ph/1003.0103v1`
38. Plenio, M.B., Virmani, S.: An introduction to entanglement measures. Quant. Inf. Comp. 7, 1 (2007)

39. Sawerwain, M., Gielerak, R.: Natural quantum operational semantics with predicates. Int. J. Appl. Math. Comput. Sci. 18(3), 341–359 (2008)
40. Jaeger, G.: Entanglement, Information and the Interpretation of Quantum Mechanics. Springer, Heidelberg (2009)
41. Bouwmeester, D., Pan, J.W., Mattle, K., Eibl, M., Weinfurter, H., Zeilinger, A.: Experimental Quantum Teleportation. Nature 390(6660), 575–579 (1997)
42. Boschi, D., et al.: Experimental Realization of Teleporting an Unknown Pure Quantum State via Dual classical and Einstein-Podolsky-Rosen channels. Phys. Rev. Lett. 80(6), 1121–1125 (1998)
43. Marcikic, I., et al.: Long-Distance Teleportation of Qubits at Telecommunication Wavelengths. Nature 421, 509 (2003)