Available online at www.sciencedirect.com
SCIENCE DIRECT®
Physica A 338 (2004) 68–75
PHYSICA A
www.elsevier.com/locate/physa

On the role of entanglement in quantum information

Chiara Macchiavello*

INFM & Dipartimento di Fisica 'A. Volta', Università degli Studi di Pavia, via Bassi 6, I-27100 Pavia, Italy

Abstract

We give a tutorial review on the role of entanglement of quantum systems in some tasks of quantum information theory and describe in particular how it can be exploited to achieve secure communication channels.

PACS: 03.67.−a; 42.50.Dv; 89.70.+c

Keywords: Quantum communication; Computation; Cryptography

1. Introduction

The last decades have witnessed a very rapid progress in the miniaturisation of the computer components and more generally of the physical systems that transmit and process information. If such a progress will continue at the same pace, in a short time the information carriers will reach the size of a single molecule or atom and therefore their quantum nature will become important. This does not have to be considered as a limitation, but on the contrary, as a unique opportunity that may allow the performance of new ways of computation and communications. Motivated mainly by the above considerations, the new field of quantum information, where the principles of quantum physics are merged with the ones of computer and information science, became very popular in the last few years (For recent reviews see, for example, Ref. [1]). Quantum information theory studies the transmission and processing of information when information itself is carried by quantum systems and is processed

* Fax: +39 0382 507563.
E-mail address: chiara@unipv.it (C. Macchiavello).

0378-4371/$ - see front matter
doi:10.1016/j.physa.2004.02.026

according to the laws of quantum mechanics. The recent achievements in this field include the discovery of new ways of information transmission, of secure communications and the performance of some kinds of computation faster than with classical means. A key ingredient and fundamental resource in the development of all these tasks is quantum entanglement.

The concept of quantum entanglement in the case of pure states, to which we will restrict in most of this paper, can be easily defined as follows. A system of two particles A and B is described by a quantum state $|\psi\rangle_{AB}$ that can be generally written as $|\psi\rangle_{AB} = \sum_{ij} c_{ij}|i\rangle_A \otimes |j\rangle_B$, where $\{|i\rangle_A\}$ and $\{|j\rangle_B\}$ are bases for particles A and B, respectively, and c_{ij} are normalised complex coefficients. Entangled pure states of two parties are defined as states that cannot be written in the factorised form

$$|\psi\rangle_{AB} = |\phi\rangle_A \otimes |\chi\rangle_B = \left(\sum_i c_i^{(A)}|i\rangle_A\right) \otimes \left(\sum_j c_j^{(B)}|j\rangle_A\right) \tag{1}$$

(for simplicity in the following we will omit the tensor product symbol $\otimes$). [1]

This paper is meant to be a brief, not exhaustive, introductory review of the role of entanglement in quantum information theory and will illustrate with some examples how precious entanglement is as a resource to achieve new communication protocols that have no classical analogue. We will first review the simple cases of quantum teleportation [2] and quantum dense coding [3]. We will then describe how entanglement can be exploited to achieve secure communication channels in the presence of noise [4].

2. Quantum teleportation

Let us consider two distant parties Alice and Bob. For simplicity in this paper, we will restrict our attention to two-dimensional quantum systems, called qubits. Suppose that Alice has a qubit in a state $|\psi\rangle$, which can be in principle unknown to her, and she wants to transfer the information of $|\psi\rangle$ to Bob. Alice can think of measuring the state and transmit the result to Bob who could then reconstruct it at his side, but a single measurement would not give her a complete knowledge of its wave function. If Alice knew the state she could also send a description of it by ordinary classical communication, but this would in principle require an infinite amount of information, which is needed to specify the complex coefficients that determine the state of the qubit. We will see in the following that a novel and efficient way to accomplish this task is possible if Alice and Bob share an entangled state. This protocol is known as quantum teleportation [2].

[1] Mixed entangled states are described by density operators that cannot be written as mixtures of product states (1).

Let us first define the set of states

$$|\psi^{\pm}\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_A|1\rangle_B \pm |1\rangle_A|0\rangle_B\right),$$

$$|\phi^{\pm}\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_A|0\rangle_B \pm |1\rangle_A|1\rangle_B\right), \tag{2}$$

where $\{|0\rangle, |1\rangle\}$ represents a basis for each qubit (we will consider the qubits as spin-$\frac{1}{2}$ particles, and therefore we choose the basis corresponding to the eigenstates of the Pauli operator σ_z). States (2) are maximally entangled and form a basis, called the Bell basis, for the states of two qubits.

Suppose that Alice and Bob share two qubits A and B prepared in the entangled state $|\psi^-\rangle$. Alice has also a qubit C in the (unknown) state $|\psi\rangle = a|0\rangle_C + b|1\rangle_C$, which she wants to teleport to Bob. The global state of the three qubits is then $|\Psi\rangle_{ABC} = |\psi\rangle_C|\psi^-\rangle_{AB}$, which can also be written as

$$|\Psi\rangle_{ABC} = \frac{1}{2}\left[|\psi^-\rangle_{CA}(-a|0\rangle_B - b|1\rangle_B) + |\psi^+\rangle_{CA}(-a|0\rangle_B + b|1\rangle_B)\right.$$
$$\left. + |\phi^-\rangle_{CA}(b|0\rangle_B + a|1\rangle_B) + |\phi^+\rangle_{CA}(-b|0\rangle_B + a|1\rangle_B)\right]. \tag{3}$$

Alice now performs a Bell measurement on her two qubits A and C, described by orthogonal projectors onto the four Bell states. The four outcomes are equally likely, and the corresponding states of Bob's qubit will be

$$-a|0\rangle_B - b|1\rangle_B = -|\psi\rangle_B, \tag{4}$$

$$-a|0\rangle_B + b|1\rangle_B = -\sigma_z|\psi\rangle_B, \tag{5}$$

$$b|0\rangle_B + a|1\rangle_B = \sigma_x|\psi\rangle_B, \tag{6}$$

$$-b|0\rangle_B + a|1\rangle_B = i\sigma_y|\psi\rangle_B, \tag{7}$$

where $\sigma_{x,y,z}$ are the Pauli operators. As we can see from the above expressions, the state of Bob's qubit is related to the original state to be transmitted $|\psi\rangle_C$ by a fixed unitary transformation (proportional either to the identity or to one of the Pauli operators), independently of the form of $|\psi\rangle_C$. Therefore, if Alice transmits to Bob the result of the Bell measurement, which consists in two bits of classical information, Bob will restore his qubit to the state $|\psi\rangle_B$ by applying either the identity or one of the Pauli operators to his qubit, depending on the results of Alice's measurement. Thus, the novelty of this protocol is that by sharing an entangled state Alice can communicate to Bob the full information contained in $|\psi\rangle$ by transmitting just two bits of classical information. We point out that this protocol has been successfully demonstrated experimentally in several laboratories (The first experiments were presented by Bouwmeester et al. [5]).

3. Quantum dense coding

Quantum dense coding exploits entanglement to enhance the transmission of classical information over a noiseless channel. The scenario is the following. Suppose that we

want to transmit classical information over a noiseless channel and we encode the information into the state of a qubit. Then the maximum amount of information that we can transmit is one bit: this can be attained by preparing the state of the qubit to be transmitted in one of two orthogonal states with equal prior probability $\frac{1}{2}$. If the sender, Alice, tries to encode more information in the qubit, by sending, for example, non-orthogonal states, then Bob will be unable to distinguish them sufficiently well to get more than one bit of information about the identity of the signal. However, if the qubit is entangled with another qubit then it is possible to transmit two bits of classical information through the channel, achieving a doubling of information capacity. We will now describe the protocol to realise this, known as quantum dense coding [3].

Suppose that Alice and Bob share a maximally entangled pair of two qubits, for example, the Bell state $|\psi^-\rangle$. It is well known that the sharing of entanglement cannot by itself lead to communication of information between Alice and Bob (see, for example, Ref. [6]). As we will see in this example, in order to transmit information by exploiting entanglement we need also transmission of classical information from Alice to Bob, which guarantees the impossibility of superluminal communications. The main point to notice here is that the state $|\psi^-\rangle$ can be transformed in any of the Bell states (2) by local operations performed only on Alice's side. Actually, Alice can transform the state $|\psi^-\rangle$ into the state $|\psi^+\rangle$ by applying the unitary operation σ_z to her particle, into the state $|\phi^-\rangle$ by applying the operation σ_x, and into the state $|\phi^+\rangle$ by applying the operation $i\sigma_y$.

In the quantum dense coding protocol Alice can decide to do nothing to her particle or apply one of the three Pauli operators σ_i. In this way, she is able to encode two bits of classical information into the entangled state $|\psi^-\rangle$. She then transmits her qubit over the communication channel to Bob. Bob will then have both particles at his side, whose state is one of the four Bell states. As mentioned above, since the Bell states are orthogonal they can be distinguished perfectly by performing a Bell measurement. The result of the measurement corresponds to the operation performed by Alice and thus to the two bits she wants to transmit. As we can see, by exploiting prior entanglement shared by Alice and Bob, two bits of classical information can be communicated by sending just a single qubit over the transmission channel. We want to conclude this section by mentioning that also the quantum dense coding protocol has been successfully demonstrated experimentally [7].

4. Entanglement-based quantum cryptography

Secure communications between two parties can be achieved if the sender and the receiver share a secret key that consists in a sequence of random numbers as long as the message to be transmitted and is never reused. This is a fundamental result in classical cryptography and leads to a cryptographic protocol known as one-time pad. However, classical cryptographic protocols suffer from the problem of secure quantum key distribution, since in principle an eavesdropper could have monitored the key while it was transmitted from Alice to Bob without Alice and Bob being aware of the eavesdropping attack. This problem is solved in quantum cryptography, where the key

is encoded in quantum states in such a way that Alice and Bob can be aware of any attempt to gain some knowledge about it. Actually, a measurement performed on the quantum system in which the key is encoded in general perturbs it and the perturbation can be detected by the legitimate users. The security of the key distribution process is then guaranteed by the laws of quantum mechanics.

The first quantum cryptographic scheme was proposed in 1984 by Bennett and Brassard [8], and it was based on the transmission of four states of a single qubit. In 1991 a novel scheme based on the use of entangled states was presented by Ekert [9]. The main ingredient of this scheme is the distribution of singlet states $|\psi^-\rangle$, such that for each pair a particle is sent to Alice and the other one to Bob. The key is then established by performing local measurements at Alice's and Bob's sides. We can see from the form of the state $|\psi^-\rangle$ that if Alice performs a measurement of her qubit in the $\{|0\rangle, |1\rangle\}$ basis she gets a random outcome. Moreover, if Bob then performs a measurement on his qubit in the same basis he will always obtain the opposite result as Alice. Due to the invariance of the singlet state under bilateral SU(2) rotations, the same holds also for a different choice of measurement bases, provided that the same choice is performed by Alice and Bob. The entanglement-based scheme then works as follows: Alice and Bob share a certain number of singlet states. For each pair Alice and Bob choose to perform a measurement according to one of the three fixed bases. Alice chooses among the basis $\{|0\rangle_A, |1\rangle_A\}$, the basis rotated by $\pi/4$ and the basis rotated by $\pi/2$ in the x–z plane (corresponding to the eigenstates of the σ_x operator), while Bob has at disposal the basis $\{|0\rangle_B, |1\rangle_B\}$, the basis rotated by $\pi/4$ and the one rotated by $-\pi/4$. After performing the measurements Alice and Bob reveal publicly for each distributed pair which type of measurement basis they chose. When the choice of Alice and Bob correspond to the same basis the outcomes of their measurements are perfectly anticorrelated and they give the secret key. The outcomes corresponding to different measurement directions can be used to test Bell inequalities and therefore find out whether an eavesdropper has interacted with the two-qubit system.

As proposed originally, the entanglement-based scheme was secure only for transmission over noiseless channels, because the transmission of the message has to be suspended as soon as an eavesdropper, or some noise, is detected. The scheme was later proved to be secure even in the presence of noise along the key distribution channel, by supplementing it with a quantum privacy amplification procedure [4]. The idea that motivates this procedure is that any two particles that are jointly in a pure state cannot be entangled with a third particle. Therefore, any procedure that delivers qubit pairs in pure states must have eliminated the entanglement between any of those pairs and any other external system that can have previously interacted with the pairs. The measurements to establish the key are then performed after the quantum privacy amplification (QPA) technique has been applied, and therefore the security of the protocol is guaranteed by the fact that the final pairs are actually in the singlet state. The QPA procedure is based on an iterative quantum algorithm that starts with a set of qubit pairs in a mixed state (namely the state after the interaction of the pairs with an eavesdropper and/or with the environment) and, after performing local operations at Alice's and Bob's sides and communication of classical information, would discard

some of them and leave the remaining ones in states converging to the pure singlet state. In this way, the degree of entanglement between the pairs and any eavesdropper will continue to decrease and can be brought to an arbitrary low value.

The QPA procedure proposed in Ref. [4], proved to converge in Refs. [10,20], consists in simple operations. A single step of the iterative procedure involves two pairs. Alice performs the unitary operation

$$U_A = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -i \\ -i & 1 \end{pmatrix} \tag{8}$$

on each of her two qubits; Bob performs the inverse operation

$$U_B = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix} \tag{9}$$

on his. Note that the two operations correspond, respectively, to rotations by $\pi/2$ and $-\pi/2$ about the x-axis.

Then Alice and Bob each perform a quantum Controlled-Not operation on their particles, defined as

$$\overset{\text{control}}{|x\rangle}\ \overset{\text{target}}{|y\rangle} \rightarrow \overset{\text{control}}{|x\rangle}\ \overset{\text{target}}{|x \oplus y\rangle} \quad (x, y) \in \{0, 1\}\,, \tag{10}$$

where one pair comprises the two control qubits and the other one the two target qubits, and $\oplus$ denotes addition modulo two. Alice and Bob then measure the target qubits in the $\{|0\rangle, |1\rangle\}$ basis. If the outcomes coincide (e.g. both spins up or both spins down) they keep the control pair for the next round, and discard the target pair. If the outcomes do not coincide, both pairs are discarded.

We want to mention that the QPA method presented above is also known as a technique for entanglement purification. The aim of entanglement purification techniques is actually to distill from a set of mixed entangled states a smaller number of pairs with an increased purity and a higher fidelity with respect to a maximally entangled pair, such as for instance a Bell state, by performing local operations and classical communication. The first entanglement purification technique was proposed in Ref. [11] to achieve faithful quantum teleportation over noisy channels. Entanglement purification can also be successfully applied to solve other tasks in quantum information, such as, for example, long distance communication via quantum repeaters [12]. We also want to stress that entanglement purification techniques have been successfully achieved experimentally [13].

5. Summary and outlook

In this paper, we have briefly reviewed the concept of entanglement and its role in some tasks of quantum information theory. For reasons of space we had to restrict to few simple examples and we chose the protocols of quantum teleportation,

quantum dense coding and entanglement-based quantum cryptography with entanglement purification. However, entanglement has proved to be a precious resource also in many other tasks, such as for example to increase the precision of frequency standards [14], to improve the sensitivity of quantum measurements [15] and to enhance the transmission of classical information over noisy channels with correlated noise [16]. We also want to mention that a great deal of effort is now devoted to understanding the meaning of entanglement for mixed states and to studying ways to classify and quantify it, also in the cases of more than two particles (for a tutorial review of this kind of topics see Ref. [17]).

We finally want to point out that, aside from the above-mentioned theoretical activity, there has been also a recent and rapid progress in many laboratories all over the world in the experimental generation and manipulation of entangled states (For a recent review see Ref. [18]). As already mentioned before, this new technology has allowed to achieve the protocols discussed in this paper. Moreover, recent demonstration of long distance entanglement distribution [19] and of efficient entanglement detection schemes [20] have been experimentally achieved, opening the way to future novel applications.

Acknowledgements

This work has been supported in part by the EC program QUPRODIS (Contract No. IST-2002-38877).

References

[1] A. Steane, Rep. Prog. Phys. 61 (1998) 117 (the issue of Phys. World, 11 (1998));
M. Nielsen, I. Chuang, Quantum Computation and Quantum Information, Cambridge University Press, Cambridge, 2000;
C. Macchiavello, G.M. Palma, A. Zeilinger (Eds.), Quantum Computation and Quantum Information Theory, World Scientific, Singapore, 2001.
[2] C.H. Bennett, et al., Phys. Rev. Lett. 70 (1993) 1895.
[3] C.H. Bennett, S.J. Wiesner, Phys. Rev. Lett. 69 (1992) 2881.
[4] D. Deutsch, et al., Phys. Rev. Lett. 77 (1996) 2818.
[5] D. Bouwmeester, et al., Nature 390 (1997) 575;
D. Boschi, et al., Phys. Rev. Lett. 80 (1998) 1121.
[6] D. Bruß, et al., Phys. Rev. A 62 (2000) 62302.
[7] K. Mattle, et al., Phys. Rev. Lett. 76 (1996) 4656.
[8] C.H. Bennett, G. Brassard, in: Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, IEEE, New York, 1984, p. 175.
[9] A.K. Ekert, Phys. Rev. Lett. 68 (1991) 661.
[10] C. Macchiavello, Phys. Lett. A 246 (1998) 385.
[11] C.H. Bennett, et al., Phys. Rev. Lett. 76 (1996) 722.
[12] H.-J. Briegel, et al., Phys. Rev. Lett. 81 (1998) 5932.
[13] J.W. Pan, et al., Nature 423 (2003) 6938.
[14] J.J. Bollinger, et al., Phys. Rev. A 54 (1996) R4649;
S.F. Huelga, et al., Phys. Rev. Lett. 79 (1997) 3865.
[15] G.M. D'Ariano, et al., Phys. Rev. Lett. 87 (2001) 270404.

[16] C. Macchiavello, G.M. Palma, Phys. Rev. A 65 (2002) 050301.
[17] D. Bruß, J. Math. Phys. 42 (2002) 4237.
[18] F. De Martini, C. Monroe (Eds.), Experimental quantum computation and information, Proceedings of the International School of Physics, "Enrico Fermi", IOP Press, Amsterdam, 2002.
[19] M. Aspelmeyer, et al., Science 301 (2003) 621.
[20] M. Barbieri, et al., Phys. Rev. Lett. 91 (2003) 227901;
M. Bourennane, et al., quant-ph/0309043.