Quantum entanglement and its applications

Aditi Sen (De)*

Harish-Chandra Research Institute, Chhatnag Road, Jhunsi, Allahabad 211 019, India
Homi Bhabha National Institute, Training School Complex, Anushaktinagar, Mumbai 400 094, India

Quantum correlation, such as entanglement, is one of the important ingredients in most of the known quantum communication schemes. In this article, we first introduce the concept of entangled states and then discuss the communication protocols without security, both in a two-party and in a multiple-party domain.

Keywords: Entanglement, quantum correlations, quantum communication protocols, quantum dense coding, quantum teleportation.

Introduction

IN the last twenty years, path-breaking discoveries of communication and computational protocols, which promise better efficiencies by using quantum mechanics than their classical counterparts, have helped to rapidly develop the area of quantum information and computation science[1]. Pioneering inventions include the classical information transfer via quantum states with and without security[2–7] – quantum key distribution and quantum dense-coding protocols, quantum state transfer by using finite amount of classical communication[8,9], as achieved in quantum teleportation and factorization of large integers into their prime factors (prime factorization problem) in a polynomial time – Shor's algorithm[10]. These discoveries have a direct benefit for the society. For example, security of all classical cryptograhic schemes is based on the fact that some mathematical problems including prime factorization cannot be solved by currently available algorithms in a classical computer with a polynomial time. Hence, with the help of Shor's algorithm, quantum computer can break securities of all the existing classical cryptographic systems like passwords in internet banking, national security etc. Interestingly, it was shown that cryptography using quantum states can be secure even when quantum computer exists[4]. Success of quantum information science also lies in the fact that most of the proposals have already been realized in laboratories by using photons[11], ions[12,13], atoms in a cavity[14], atoms in optical lattices[15], etc.

The main ingredient in most of these schemes is the entanglement[16] shared between two or multiple parties. Bipartite entangled states shared between two distantly located parties are nowadays routinely achieved in laboratories. However, creation of entangled states, involving large number of parties, is still a challenging task. For example, maximum number of particles among which entanglement have been generated are: fourteen by using trapped ions[17], ten using photons[18] and five with superconducting qubits[19]. It is important to mention here that entangling multiple parties is important for better performance of quantum computer and quantum error correcting codes[1] than the classical ones[20–22].

In this article, we briefly discuss theoretical aspects of entanglement. In particular, we first give the definitions of entanglement and review briefly about entanglement measures. We then discuss two quantum communication protocols[23], namely quantum dense coding (DC) and quantum teleportation and their recent progress.

Entangled states

In this section, we first define entanglement[16] for states shared between two-parties and then extend it to a multipartite domain. Also, we briefly discuss the detection methods of entanglement and entanglement measures.

Definition of entanglement

Let us consider a situation where two parties, Alice and Bob, denoted by A and B respectively, are located in two distant locations. Suppose Alice prepares a quantum state, $|\psi_A\rangle$, belonging to the complex Hilbert space $\mathbb{C}_A$ and similarly, Bob prepares $|\psi_B\rangle$ in $\mathbb{C}_B$. The joint state shared between Alice and Bob in this case is given by

$$|\Phi_{AB}\rangle = |\psi_A\rangle \otimes |\psi_B\rangle, \tag{1}$$

in $\mathbb{C}_A \otimes \mathbb{C}_B$, which is called the product state. In other words, a pure state that can be prepared by Alice and Bob using local operations is said to be a product state.

A bipartite pure state which is not possible to prepare by local operations is called an entangled state[16], i.e. a state is said to be entangled if

$$|\Phi_{AB}\rangle \neq |\psi_A\rangle \otimes |\psi_B\rangle. \tag{2}$$

In $\mathbb{C}_A^2 \otimes \mathbb{C}_B^2$, a good example of an entangled state is the singlet state, given by $|\psi^-\rangle = 1/\sqrt{2}\,(|01\rangle - |10\rangle)$, where $|0\rangle$ and $|1\rangle$ represent eigenvectors of σ_z, with σ_α, $\alpha = x, y, z$ being the Pauli spin matrices. In fact, it can be shown that

*e-mail: aditi@hri.res.in

for singlet state $|0\rangle$ and $|1\rangle$ can be any two eigenvectors along any directions in a two-dimensional Hilbert space.

The above definitions can be generalized to mixed states. A bipartite state which can be prepared by Alice and Bob by using quantum mechanically allowed local operations and classical communication (LOCC) is known as a separable state, and can be written as

$$\rho_{AB} = \sum_{i=1}^{d} p_i \rho_A^i \otimes \rho_B^i, \tag{3}$$

where $p_i \geq 0$, $\forall i$, $\sum_i p_i = 1$, $\rho_A^i = |\psi_A^i\rangle\langle\psi_A^i|$ $(i = 1, \ldots, d)$ and similarly $\rho_B^i = |\psi_B^i\rangle\langle\psi_B^i|$ $(i = 1, \ldots, d)$. A state is said to be entangled if it cannot be written as convex combination of the product of local projectors, as given in eq. (3). An example of an entangled mixed state is the Werner state, introduced by Werner in 1989 (ref. 24). It is given by

$$\rho_W = p|\psi^-\rangle\langle\psi^-| + (1-p)\frac{I}{4}, \tag{4}$$

which can be shown to be entangled when $p > 1/3$, with I being the identity operator in the four-dimensional Hilbert space. The bipartite state space can then be divided into two classes – separable and entangled states (Figure 1). In this article, we will later show that entangled states are, in general, useful for several quantum communication protocols.

If one goes beyond the bipartite regime, i.e. if one considers a state shared between N-parties, situated in distant laboratories, the characaterization of states, according to their entanglement, even for pure states, is not so easy. To illustrate this, let us consider a pure tripartite state[25], shared between Alice (A), Bob (B) and Claire (C) (for mixed states, see ref. 26). Suppose each of them prepares a quantum state, $|\psi_i\rangle$, $i = A, B, C$, in her/his laboratory. The joint state that they share is then given by

$$|\Psi_{ABC}\rangle = |\psi_A\rangle \otimes |\psi_B\rangle \otimes |\psi_C\rangle, \tag{5}$$

which is a fully separable state (FS). Suppose now that A and B share an entangled state, $|\phi_{AB}\rangle$, while they are unentangled with C. In this case, the state shared between A, B and C are called the biseparable states (BS), denoted by $(|\Psi_{A:BC}\rangle = |\phi_{AB}\rangle|\psi_C\rangle)$. Similarly, one can have biseparable states, $|\Psi_{B:AC}\rangle$ and $|\Psi_{C:AB}\rangle$, which are respectively, products in $B:AC$ and $C:AB$ bipartitions. On the other hand, a pure state is genuinely multipartite entangled if it is not a product across any bipartitions. For a schematic diagram of the set of tripartite states, see Figure 1. Two prominent examples of genuine multipartite entangled states are the Greenberger-Horne-Zeilinger (GHZ)[26] and the W (ref. 27) states, given respectively by

$$|\psi_{GHZ}\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle), \tag{6}$$

$$|\psi_W\rangle = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle). \tag{7}$$

In a similar fashion, N-party pure states can be divided into N classes, namely FS, k-separable ($k = 2, 3, \ldots, N-1$) and genuine multiparty entangled states[28].

It is interesting to note here that in case of pure two-qubit entangled states[29], it is always possible to transform an entangled state to another ones by LOCC with some non-zero probability, i.e. via stochastic local operations and classical communication (SLOCC). However, such equivalence does not exist in a tripartite or in a multipartite scenario. Specifically, there are two SLOCC inequivalent classes[25], the GHZ[30] and W class[31] for three-party pure states. For $N > 3$, infinite number of inequivalence classes exists[25,32].

After these definitions, a natural question that arises is how to detect these entangled states in the laboratory. With the development of quantum information science, several entanglement criteria, for both bipartite and multipartite states, have been proposed[16,33]. Some methods that distinguish entangled states from separable ones are based on mathematical tools, like complete positivity, majorization etc. Hence, they can only be applied when full information about the states, which can be obtained via state tomography[34,35], are available. Such methods include partial transposition[36,37], criterion based on von-Neumann entropy[38–41], majorization[42], covariance matrix crietria[43,44] to name a few. On the other hand, there are entanglement criteria like entanglement witness[45,46], violation of Bell inequality[47] which can be used to identify entangled states in the laboratory, even without performing tomography. See refs 16, 33 for details.

Entanglement measures

The next question is to measure the entanglement content of a prepared state. For a bipartite pure state, there exists a unique measure of entanglement which is the von-Neumann entropy of local density matrices of a given

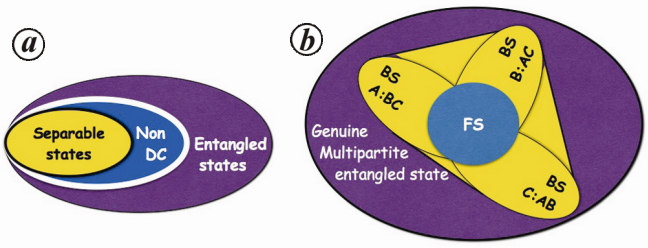

Figure 1. (Colour online) Classification of states according to entanglement. ***a***, Bipartite states – separable and entangaled states. We can also divide the set of states according to dense coding protocol – NonDC states represent the set of states which are not useful for dense coding protocol while the set of dense codeable states, which is a subset of entangled states, are good for dense coding (see section entangled states). ***b***, Tripartite states[86]; FS denotes the fully separable states; $A:BC$, $B:CA$ and $C:AB$ denote biseparable states which are products in the corresponding bipartitions. The rest of the states belongs to the set of genuine multipartite entangled states.

state. Hence, for an arbitrary bipartite pure state, $|\psi_{AB}\rangle$, entanglement can be quantified as

$$\mathcal{E}(|\psi_{AB}\rangle) = S(\rho_A), \tag{8}$$

where $S(.)$ denotes the von-Neumann entropy[38] and $\rho_A = \mathrm{tr}_B(|\phi_{AB}\rangle\langle\phi_{AB}|)$ is the reduced density matrix of $|\psi_{AB}\rangle$[48]. Important to note here that in case of pure states, other known quantum correlation measures[49,50], which are different than entanglement, also reduce to entropy of local density matrices, as given in eq. (8).

Quantification of entanglement for bipartite mixed states has also been carried out by using entanglement measure for pure states. Entanglement of an arbitrary state, ρ_{AB} can then be defined as

$$\mathcal{E}_F(\rho_{AB}) = \min \sum_i p_i \mathcal{E}(|\psi_i\rangle\langle\psi_i|), \tag{9}$$

where the minimization is performed over all possible pure state decomposition of $\rho_{AB} = \sum_i p_i |\psi_i\rangle\langle\psi_i|$. It is known as entanglement of formation (EoF)[51]. However, there are infinite number of such decompositions exist for ρ_{AB}, and hence it is, in general, not easy to compute.

In 1998, William K. Wootters[52] provided a compact form of this measure for two-qubit states, which has become extremely important for studying several physical systems like spin models, ultracold atoms in optical lattices[53,54]. In case of two-qubit states, eq. (9) reduces to

$$\mathcal{E}_F(\rho_{AB}) = h\left(\frac{1+\sqrt{1-C^2}}{2}\right), \tag{10}$$

$$\text{with } h(x) = -x\log_2 x - (1-x)\log_2(1-x). \tag{11}$$

Here $C = \max\{0, \lambda_1 - \lambda_2 - \lambda_3 - \lambda_4\}$ is known as the concurrence with λ_i^2, $i = 1, \ldots, 4$ being the eigenvalues of matrix $\rho_{AB}\tilde{\rho}_{AB}$ in decreasing order, and $\tilde{\rho}_{AB} = (\sigma_y \otimes \sigma_y)\rho_{AB}^*(\sigma_y \otimes \sigma_y)$ with a complex conjugation in ρ_{AB}^* being taken in computational basis. Such closed form of EoF is still missing for states in higher dimensions.

In higher dimensions, one of the computationally simple bipartite entanglement measure is logarithmic negativity[55], which is the only available tool to study many-body Hamiltonians with higher spins. Other important entanglement measures include relative entropy of entanglement[56] based on geometry of state space, distillable entanglement[57], originated from a physical process under LOCC, known as distillation or purification of states.

With the development of entanglement theory, the basic properties that an entanglement measure, $\mathcal{E}$, should satisfy are also proposed[58]. They are as follows

(a) For a given state, ρ_{AB}, $\mathcal{E}(\rho_{AB}) \geq 0$ and vanishes if ρ_{AB} is separable.

(b) If ρ_{AB} transforms to an ensemble $\{p_i, \sigma_{AB}^i\}$ by LOCC, then

$$\mathcal{E}(\rho_{AB}) \geq \sum_i p_i \mathcal{E}(\sigma_{AB}^i), \tag{12}$$

ensuring non-increasing nature of entanglement using LOCC, known as monotonicity property of entanglement.

Most of the known entanglement measures, mentioned above as well as in the literature satisfy the above two properties. Apart from these two requirements, other properties are also recommended which an entanglement measure should follow in an asymptotic regime, i.e. when n copies of ρ_{AB} are considered.

Although there exists a considerable number of bipartite entanglement measures, only few multipartite entanglement measures are known, among which, only a fraction of them can be computed even for pure states. Based on geometry of quantum states, we introduce a genuine multipartite entanglement measure, known as generalized geometric measure[59,60]. For an N-party pure state, $|\psi_{A_1\ldots A_N}\rangle$, it is defined as

$$\mathcal{G}(|\psi_{A_1\ldots A_N}\rangle) = \max(1 - |\langle\phi_{A_1\ldots A_N}|\psi_{A_1\ldots A_N}\rangle|^2), \tag{13}$$

where maximization is taken over the set of non-genuinely multiparty entangled states. For example, in case of three-party, one has to maximize over the set of biseparable states.

By performing maximization over the set of FS states, one gets another multipartite entanglement measure, known as geometric measure of entanglement (GM)[61,62]. Interestingly, the former can be expressed in terms of Schmidt coefficients of different bipartitions of $|\psi_{A_1\ldots A_N}\rangle$, thereby enormously simplifying the computation for arbitrary pure states in any dimension[60]. It is then given by

$$\mathcal{G}(|\psi_{A_1\ldots A_N}\rangle) = 1 - \max\{\lambda_{A:B}^2 | A \cup B = A_1, A_2, \ldots, A_N, A \cap B = \Phi\}, \tag{14}$$

with $\lambda_{A:B}$ being the maximal Schmidt coefficient in each possible bipartition of $A:B$ of $|\psi_{A_1\ldots A_N}\rangle$. In contrast, the GM does not have a closed form, and hence it is not easy to compute for arbitrary multipartite states. Note here that changing the set in maximization of eq. (13) leads to different entanglement measures, characterizing different sets of multipartite states. It can be shown that these geometric measures are also entanglement monotones, i.e. cannot increase under LOCC. We have also recently extended GGM to multipartite mixed states and have obtained a closed form of GGM for several classes of mixed states[63].

Apart from these entanglement measures based on geometry of state spaces, a concept of monogamy for quantum correlations[64] has also been applied to obtain

multipartite computable measures. For multipartite entanglement measures, see refs 16, 32, 65.

Quantum communication protocols

In the last decade, several quantum communication protocols involving two or multiple parties were proposed. In this section, we mainly concentrate on communication schemes which do not involve any security issue. We also briefly discuss the recent theoretical progress of these protocols in a multipartite domain.

Quantum dense coding: transmission of classical information via quantum channel

In our daily life, classical information transfer plays an important role, ranging from television, internet, to national security. Here we consider a scenario where a sender, Alice, wants to send two classical bits[66] to a receiver, Bob. In this scenario, if Alice and Bob do not share any entangled states, Alice requires four dimensions or 4 distinguishable objects to send two bits. For example, suppose Alice wants to send to Bob whether it is raining in Allahabad or not, as well as whether P. V. Sindhu wins today's badminton match or not. Therefore, the information that she is going to send is as follows:

(a) In Allahabad, it is raining and P. V. Sindhu wins the match (00).
(b) It is not raining and P. V. Sindhu wins (01).
(c) It is raining and P. V. Sindhu does not win today's match (10).
(d) Lastly, neither it is raining nor P. V. Sindhu wins (11).

In the first parenthesis, we show the corresponding encoding of information in two bits. To encode two bits of classical information, one can use different distinguishable objects, e.g. four different colours of balls, four distingushable wave patterns, etc. Classically, the protocol goes as follows: After knowing the message, Alice sends, for e.g. one of the four balls to Bob. Bob decodes the information by looking at the colour of the ball.

In contrast, we now show that if Alice and Bob *a priori* share an entangled state, Alice requires only two dimensions to encode two bits of classical information. Before describing the protocol, one should emphasize that in this scenario, classical communication between the sender and receiver is forbidden, while use of quantum channel between them is allowed and hence quantum channels are free resources. We will come back to this point in the case of transfer of qubits which naturally has different free resource.

Initially, suppose that Alice and Bob share a singlet state $|\psi^-\rangle = 1/\sqrt{2}\ (|01\rangle - |10\rangle)$.

Step 1 (encoding): Depending on the message, Alice performs unitary operations, $\{I, \sigma_z, \sigma_x, \sigma_y\}$ on her part. For example, if she wants to send the first message, she performs nothing while in case of sending 2nd option described above, she performs σ_z on her qubit. By performing single qubit operations by Alice, the joint state between Alice and Bob transforms as follows (table below shows the resulting state up to global phase with the corresponding unitary operators).

Unitary operators	States in AB
I	$\|\psi^-\rangle = 1/\sqrt{2}\ (\|01\rangle - \|10\rangle)$
σ_z	$\|\psi^+\rangle = 1/\sqrt{2}\ (\|01\rangle + \|10\rangle)$
σ_x	$\|\phi^-\rangle = 1/\sqrt{2}\ (\|00\rangle - \|11\rangle)$
σ_y	$\|\phi^+\rangle = 1/\sqrt{2}\ (\|00\rangle + \|11\rangle).$ (15)

Note here that all the above states, $\{|\psi^{\pm}\rangle, |\phi^{\pm}\rangle\}$, possess same amount of entanglement, by using eq. (8). They are known as the maximally entangled states or Bell states, and the corresponding basis is called the Bell basis. Moreover, we notice that these four states are local unitarily connected. It can be shown that if entanglement of two states are equal, they surely are connected by local unitary operations.

Step 2 (sending): After unitary operations, Alice sends her qubit to Bob via noiseless quantum channel.

Step 3 (decoding): At this point, Bob has both the qubits and since the states are orthonormal to each other, Bob can distinguish them by global operations and hence can decode the message. (see Figure 4 for a schematic representation of dense coding.)

This was the original protocol of quantum dense coding (DC), proposed by C. H. Bennett and S. J. Wiesner in 1992 and four years later, it was realized by using photons[7]. Since, it is not possible to prepare a pure state due to noisy environments, it is interesting to find the amount of information that can be sent, when Alice and

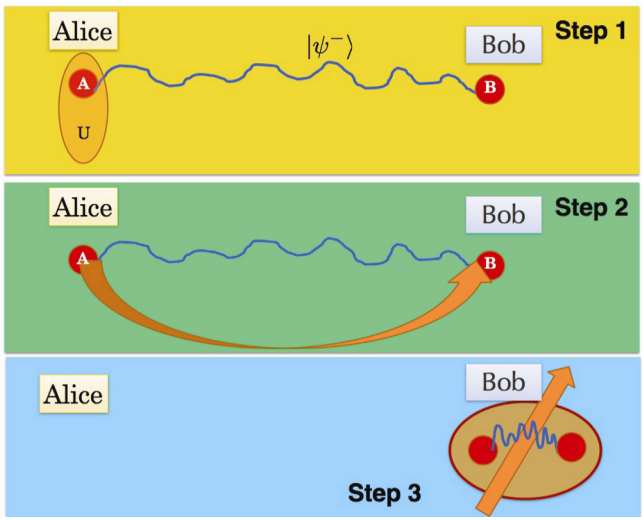

Figure 2. (Colour online) Schematic depiction of quantum dense coding protocol.

Bob share an arbitrary quantum state[67–70]. The capacity of DC, denoted by $\mathcal{C}$ of a shared state, ρ_{AB}, can be shown to be given by

$$\mathcal{C}(\rho_{AB}) = \log_2 d_A + S(\rho_B) - S(\rho_{AB}), \quad (16)$$

where d_A is the dimension of Alice's Hilbert space and ρ_B is the reduced density matrix of receiver's or Bob's side. The formula reveals that all bipartite pure entangled states are useful for DC, since $S(\rho_{AB}) = 0$ for pure states. According to DC capacity, one can classify the set of states as we have done in ref. 70 (Figure 1). A state, ρ_{AB}, is useful for dense coding (or is called dense-codeable) when $S(\rho_B) - S(\rho_{AB}) > 0$. Therefore, the quantum advantage of DC can be defined as $\mathcal{C}_{\text{adv}} = \max[0, S(\rho_B) - S(\rho_{AB})]$. In contrast to pure entangled states, there exist mixed states, e.g. Werner state which does not give quantum advantage in DC protocol even when it is entangled[69].

One of the main aims in any communication protocol is to establish a facility by which information can be transferred between several senders and several receivers. Similar to this spirit, one can consider a DC network, involving many parties. Towards this aim, we have proven that when the state shared between N senders and a single receiver is $\rho_{A_1A_2\cdots A_NB}$, the capacity of DC between N senders, $A_1, A_2, \ldots, A_N$, and a single receiver, B is given by

$$\mathcal{C}(\rho_{A_1A_2\cdots A_NB}) = \log_2 d_{A_1} d_{A_2} \ldots d_{A_N} + S(\rho_B) - S(\rho_{A_1A_2\cdots A_NB}), \quad (17)$$

where $d_{A_1} d_{A_2} \ldots d_{A_N}$ are the dimensions of N senders' Hilbert space.

The proof of the capacities requires maximization over encoding and decoding processes. The latter is simplified by using Holevo bound[71–75] on maximal mutual information[70]. Hence, optimizing Holevo bound over unitaries and probabilities lead to the capacities, given in eqs (16) and (17).

Let us now move to a scenario where there are N senders and two recievers which are far apart. The receivers cannot use global operations to decode the message sent by Alice and hence Holevo bound cannot be applied to obtain the capacity. However, when the operations are restricted to LOCC, we found a Holevo-like bound which we call the local Holevo bound[76,77]. In the two-receivers case, local Holevo bound comes as a remedy for studying the capacity. In 2004, we obtained an upper bound on the capacity of DC with two receivers[69] by using this local bound. This protocol is called distributed DC (see Figure 3 for such a network). It can be shown that the maximum capacity in this case by using multipartite entangled states can be achieved by the GHZ state, given in eq. (6). Such analysis also helps us to classify multipartite entangled mixed states according to their usefulness in DC protocols.

Let us now replace the noiseless quantum channel (step 2) for sending the qubit from Alice to Bob to a noisy one which will be more realistic from the experimental point of view. Therefore, it is important to modify the capacities for noisy quantum channels which are used after encodings (unitary operations) by the senders. In ref. 78, DC capacities of noisy channels are partially solved for several senders and a single receiver. Recently, we have established a connection between capacities of DC, for both noiseless and noisy channels, and shared multipartite entanglement[79]. We showed that one-to-one correspondence between entanglement and DC capacities which exists for pure bipartite states is no more valid in a multipartite setting.

The consequence of noise on upper bound of DC capacities of a network involving several senders and two receivers has also recently been found by us[80]. However, finding the capacities of DC between several senders and several receivers, i.e. in a network are still an open task, both in noiseless and noisy scenarios.

Another type of communication protocol which one can consider is as follows: suppose that a protocol involves many senders, say, reporters of a newspaper. They send their information individually to a single receiver, i.e. the editor of the newspaper. Suppose that all of them share an arbitrary multipartite mixed state. Let us concentrate on three parties, A (a receiver), and B and C as senders. If A wants to perform DC with B and C individually, we have shown that quantum advantage can only be obtained either between A and B or between A and C – exclusion principle of quantum DC[81,82]. Specifically, we have proven that for a given tripartite state, ρ_{ABC} in $\mathbb{C}^d \otimes \mathbb{C}^d \otimes \mathbb{C}^d$, we have

$$\mathcal{C}(\rho_{AB}) + \mathcal{C}(\rho_{AC}) \leq 2\log_2 d, \quad (18)$$

where ρ_{AB} and ρ_{AC} are reduced states of ρ_{ABC}. The proof can be done by using strong sub-additivity property of

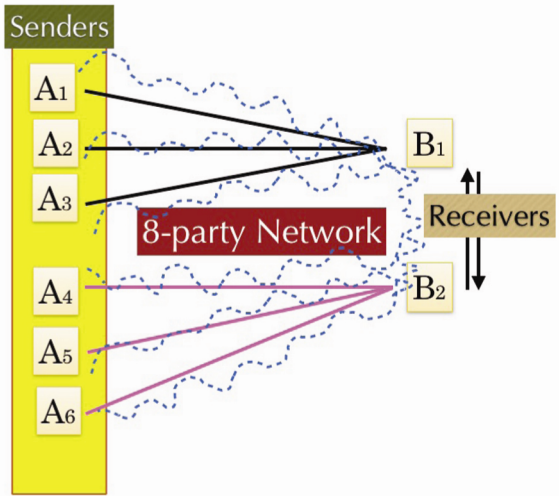

Figure 3. (Colour online) Quantum DC network, involving 8 parties, 6 senders and 2 receivers. Initially they share a 8-party entangled state which is shown by dashed lines. After encoding, i.e. unitary operations, A_1, A_2, A_3 and A_4 send their qubits to B_1, depicted as black solid line while the rest of the senders send their qubits to B_2 (pink solid lines). Finally, B_1 and B_2 perform LOCC to decode the message (solid arrows).

von Neumann entropy[1] and by eq. (16). The above relation can easily be generalized to an N-party system. In particular, for an N-party state, at most only a single reduced density matrix can have quantum advantage in DC.

Quantum teleportation: transfer of qubits

We now consider a protocol where Alice wants to send an unknown qubit, $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$ (with α and β being arbitrary complex numbers and $|\alpha|^2 + |\beta|^2 = 1$) to Bob[8]. Unlike DC protocol, Alice can send as much classical information as possible to Bob, although use of quantum channels is not allowed.

Before presenting the protocol, let us suppose that Alice and Bob share an unentangled state. In this case, one can show that to send an unknown qubit, Alice requires infinite amount of classical communication.

On the other hand, suppose that Alice and Bob share a singlet state, $|\psi^-\rangle$, and Alice wants to send $|\phi\rangle$ to Bob. Hence she posses two qubits – one part of a singlet and an unknown qubit. We describe the teleportation protocol in the following steps which is pictorially depicted in Figure 4.

Step 1 (measurement): Alice performs a measurement in the Bell basis, $\{|\psi^{\pm}\rangle, |\phi^{\pm}\rangle\}$, on both her qubits.

Step 2 (classical communication): Alice informs the measurement outcome to Bob. This means that Alice communicates two bits of classical information to Bob.

Step 3 (unitary operations/decoding): Depending on the measurement outcome, Bob performs an unitary operation on his qubit, shown in the table of Figure 4. He finally recovers the exact unknown state.

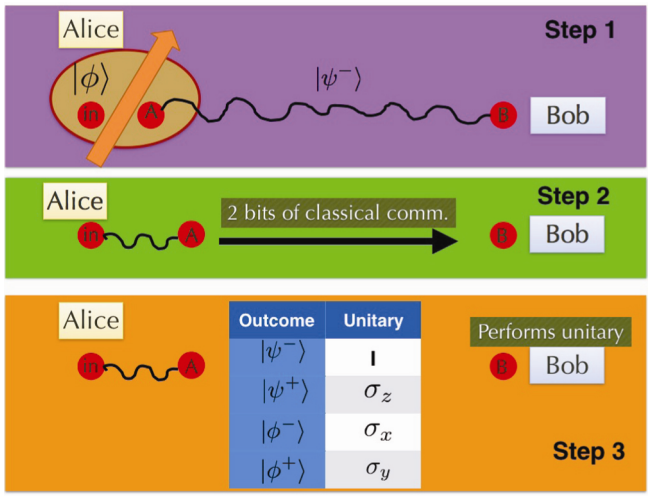

Figure 4. (Colour online) Quantum teleportation protocol.

Therefore, the above protocol shows that an unknown qubit can be transferred only by using two bits of classical communication if an entangled state is initially shared between two parties and an infinite amount of resource is reduced by using entanglement compared to the protocol with states having vanishing entanglement.

There are two important points – if Alice does not communicate classically, Bob's state is in a maximally mixed state, having no information about the unknown qubit. It implies that signalling with a speed faster than light does not take place in this protocol. The second point is that there is no violation of *quantum no-cloning theorem* which states that unknown quantum states cannot be cloned[83]. Such violation is avoided, since the measurement performed by Alice destroys the original unknown qubit that she initially posses. Therefore, there is not a single time instance when two copies of the unknown qubit are with one of them.

Quantum teleportation clearly showed the advantage of entangled states. After its discovery, several experimental groups around the world have reported its implementation by using different physical systems. It was shown that when Alice and Bob share an arbitrary mixed two-qubit entangled state, quantum state transfer is possible with higher efficiencies than the scheme with a shared unentangled state[84,85]. Addressing the question of quantum teleportation-like schemes in a multipartite situation is not easy and only limited number of attempts have been made[23]. When the protocol involves four parties, we have found that genuine multipartite entanglement measure and multipartite quantum teleportation capacities do not have any simple relation[59].

Conclusion

This review contains the basic definitions of entanglement of shared bipartite as well as multipartite states. We then discuss two path-breaking discoveries in quamtum communication which essentially revolutinize communication protocols – quantum dense coding and quantum teleportation. We briefly report recent advancements of these two communication protocols, including some of our works in these directions.

1. Nielsen, M. A. and Chuang, I., *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge, 2000.
2. Bennett, C. H. and Brassard, G., Quantum cryptography: public key distribution and coin tossing. Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, 1984, p. 175.
3. Ekert, A. K., Quantum cryptography based on Bells theorem. *Phys. Rev. Lett.*, 1991, **67**, 661.
4. Gisin, N., Ribordy, G., Tittel, W. and Zbinden, H., Quantum cryptography. *Rev. Mod. Phys.*, 2002, **74**, 145.
5. Jennewein, T., Simon, C., Weihs, G., Weinfurter, H. and Zeilinger, A., Quantum cryptography with entangled photons. *Phys. Rev. Lett.*, 2000, **84**, 4729.

6. Bennett, C. H. and Wiesner, S. J., Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. *Phys. Rev. Lett.*, 1992, **69**, 2881.
7. Mattle, K., Weinfurter, H., Kwiat, P. G. and Zeilinger, A., Dense coding in experimental quantum communication. *Phys. Rev. Lett.*, 1996, **76**, 4656.
8. Bennett, C. H., Brassard, G., Crépeau, C., Jozsa, R., Peres, A. and Wootters, W. K., Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.*, 1993, **70**, 1895.
9. Bouwmeester, D., Pan, J. W., Mattle, K., Eibl, M., Weinfurter, H., and Zeilinger, A., Experimental quantum teleportation. *Nature*, 1997, **390**, 575.
10. Shor, P. W., Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. Proceedings of the 35th Annual Symposium on Foundations of Computer Science (ed. Goldwasser, S.), IEEE Computer Society Press, 1994, 124134.
11. Pan, J. W., Chen, Z. B., Lu, C.-Y., Weinfurter, H., Zeilinger, A. and Zukowski, M., Multiphoton entanglement and interferometry. *Rev. Mod. Phys.*, 2012, **84**, 777.
12. Leibfried, D., Blatt, R., Monroe, C. and Wineland, D., Quantum dynamics of single trapped ions. *Rev. Mod. Phys.*, 2003, **75**, 281.
13. Hafner, H., Roose, C. F. and Blatt, R., Quantum computing with trapped ions. *Phys. Rep.*, 2008, **469**, 155.
14. Raimond, J. M., Brune, M. and Haroche, S., Manipulating quantum entanglement with atoms and photons in a cavity. *Rev. Mod. Phys.*, 2001, **73**, 565.
15. Mandel, O., Greiner, M., Widera, A., Rom, T., Hänsch, T. W. and Bloch, I., Controlled collisions for multi-particle entanglement of optically trapped atoms. *Nature*, 2003, **425**, 937.
16. Horodecki, R., Horodecki, P., Horodecki, M. and Horodecki, K., Quantum entanglement. *Rev. Mod. Phys.*, 2009, **81**, 865.
17. Monz, T. *et al.*, 14-qubit entanglement: creation and coherence. *Phys. Rev. Lett.*, 2011, **106**, 130506.
18. Wang, X.-L. *et al.*, Experimental ten-photon entanglement. *Phys. Rev. Lett.*, 2016, **117**, 210502.
19. Barends, R. *et al.*, Superconducting quantum circuits at the surface code threshold for fault tolerance. *Nature*, 2014, **508**, 500503.
20. Steane, A. M., Quantum computing. *Rept. Prog. Phys.*, 1998, **61**, 117.
21. Steane, A. M. and Lucas, D. M., Quantum computing with trapped ions, atoms and light, 2000, arXiv:quant-ph/0004053.
22. Cirac, J. I. and Zoller, P., A scalable quantum computer with ions in an array of microtraps. *Nature*, 2010, **404**, 579.
23. Sen (De), A. and Sen, U., Quantum advantage in communication networks. *Phys. News*, 2010, **40**, 17–32; arXiv:1105.2412 (quant-ph)).
24. Werner, R. F., Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model. *Phys. Rev. A*, 1989, **40**, 4277.
25. Dür, W., Vidal, G. and Cirac, J. I., Three qubits can be entangled in two inequivalent ways. *Phys. Rev. A*, 2000, **62**, 062314.
26. Greenberger, D. M., Horne, M. A. and Zeilinger, A., In *Bells Theorem, Quantum Theory, and Conceptions of the Universe* (ed. Kafatos, M.), Kluwer Academic, Dordrecht, The Netherlands, 1989.
27. Zeilinger, A., Horne, M. A. and Greenberger, D. M., In Proceedings of Squeezed States and Quantum Uncertainty (eds Han, D. *et al.*), NASA Conf. Publ., 1992, vol. 3135, p. 73.
28. Blasone, M., DellAnno, F., DeSiena, S. and Illuminati, F., Hierarchies of geometric entanglement. *Phys. Rev. A*, 2008, **77**, 062304.
29. An arbitrary two-dimensional quantum state is called a qubit (quantum bit).
30. An arbitrary normalized three-qubit states from the GHZ class, up to local unitary (LU), are given by[25] $|\Phi_{ghz}\rangle = \sqrt{K}(c_\delta|000\rangle + e^{i\mu}s_\delta \otimes_{i=1}^{3}|\eta_i\rangle)$ where $|\eta_i\rangle = c_{\gamma_i}|0\rangle + s_{\gamma_i}|1\rangle$, $c_k = \cos k$, $s_k = \sin k$, $k = \gamma_i$, δ and $K^{-1} = 1 + 2c_\delta s_\delta c_{\gamma_1} c_{\gamma_2} c_{\gamma_3} c_\mu$, K being the normalization factor, and $K \in (1/2, \infty)$, $\delta \in (0, \pi/4]$, $\gamma_i \in (0, \pi/2]$, $i = 1, 2, 3$, and $\mu \in [0, 2\pi)$.
31. Any states from the W-class, up to LU, can be written as[25] $|\Phi_w\rangle = \sqrt{a_1}|001\rangle + \sqrt{a_2}|010\rangle + \sqrt{a_3}|100\rangle + \sqrt{a_4}|000\rangle$ (19) with a_1, a_2, $a_3 > 0$, and $a_4 = 1 - (a_1 + a_2 + a_3) \geq 0$.
32. Walter, M., Gross, D. and Eisert, J., Multi-partite entanglement, arXiv: 1612:02437.
33. Gühne, O. and Toth, G., Entanglement detection. *Phys. Rep.*, 2009, **474**, 1.
34. DAriano, G. M., Vasilyev, M. and Kumar, P., Self-homodyne tomography of a twin-beam state. *Phys. Rev. A*, 1998, **58**, 636.
35. White, A. G., James, D. F. V., Eberhard, P. H. and Kwiat, P. G., Nonmaximally entangled states: production, characterization and utilization. *Phys. Rev. Lett.*, 1999, **83**, 3103.
36. Peres, A., Separability criterion for density matrices. *Phys. Rev. Lett.*, 1996, **77**, 1413.
37. Horodecki, M., Horodecki, P. and Horodecki, R., Separability of mixed states: necessary and sufficient conditions. *Phys. Lett. A*, 1996, **223**, 1.
38. The von Neumann entropy of an arbitrary state, σ is defined as $S(\sigma) = -\mathrm{tr}\sigma \log_2 \sigma$.
39. Cerf, N. and Adami, C., Negative entropy and information in quantum mechanics. *Phys. Rev. Lett.*, 1997, **79**, 5194.
40. Horodecki, R., Horodecki, P. and Horodecki, M., Separability of mixed states: necessary and sufficient conditions. *Phys. Lett. A*, 1996, **210**, 377.
41. Horodecki, R. and Horodecki, M., Information-theoretic aspects of inseparability of mixed states. *Phys. Rev. A*, 1996, **54**, 1838.
42. Nielsen, M. A. and Kempe, J., Separable states are more disordered globally than locally. *Phys. Rev. Lett.*, 2001, **86**, 5184.
43. Gühne, O., Hyllus, P., Gittsovich, O. and Eisert, J., Covariance matrices and the separability problem. *Phys. Rev. Lett.*, 2007, **99**, 130504.
44. Gittsovich, O., Gühne, O., Hyllus, P. and Eisert, J., Unifying several separability conditions using the covariance matrix criterion. *Phys. Rev. A*, 2008, **78**, 052319.
45. Lewenstein, M., Kraus, B., Cirac, J. I. and Horodecki, P., Optimization of entanglement witnesses. *Phys. Rev. A*, 2000, **62**, 052310.
46. Bruβ, D., Cirac, J. I., Horodecki, P., Hulpke, F., Kraus, B., Lewenstein, M. and Sanpera, A., Reflections upon separability and distillability. *J. Mod. Opt.*, 2002, **49**, 1399.
47. Terhal, B. M., Bell inequalities and the separability criterion. *Phys. Lett. A*, 2000, **271**, 319.
48. Bennett, C. H., Bernstein, H. J., Popescu, S. and Schumacher, B., Concentrating partial entanglement by local operations. *Phys. Rev. A*, 1996, **53**, 2046.
49. Modi, K., Brodutch, A., Cable, H., Paterek, T. and Vedral, V., The classical-quantum boundary for correlations: discord and related measures. *Rev. Mod. Phys.*, 2012, **84**, 1655.
50. Horodecki, M., Horodecki, P., Horodecki, R., Oppenheim, J., Sen (De), A., Sen, U. and Synak-Radtke, B., Local versus nonlocal information in quantum-information theory: formalism and phenomena. *Phys. Rev. A*, 2005, **71**, 062307.
51. Bennett, C. H., DiVincenzo, D. P., Smolin, J. and Wootters, W. K., Mixed-state entanglement and quantum error correction. *Phys. Rev. A*, 1996, **54**, 3824.
52. Wootters, W. K., Entanglement of formation of an arbitrary state of two qubits. *Phys. Rev. Lett.*, 1998, **80**, 2245.
53. Lewenstein, M., Sanpera, A., Ahufinger, V., Damski, B., Sen (De), A. and Sen, U., Ultracold atomic gases in optical lattices: mimicking condensed matter physics and beyond. *Adv. Phys.*, 2007, **56**, 243.

54. Amico, L., Fazio, R., Osterloh, A. and Vedral, V., Entanglement in many-body systems. *Rev. Mod. Phys.*, 2008, **80**, 517.
55. Vidal, G. and Werner, R. F., Computable measure of entanglement. *Phys. Rev. A*, 2002, **65**, 032314.
56. Vedral, V., Plenio, M. B., Rippin, M. A. and Knight, P. L., Quantifying entanglement. *Phys. Rev. Lett.*, 1997, **78**, 2275.
57. Bennett, C. H., Brassard, G., Popescu, S., Schumacher, B., Smolin, J. A. and Wootters, W. K., Purification of noisy entanglement and faithful teleportation via noisy channels. *Phys. Rev. Lett.*, 1996, **76**, 722.
58. Horodecki, M., Horodecki, P. and Horodecki, R., Limits for entanglement measures. *Phys. Rev. Lett.*, 2000, **84**, 2014.
59. Sen (De), A. and Sen, U., Channel capacities versus entanglement measures in multiparty quantum states. *Phys. Rev. A*, 2010, **81**, 012308.
60. Biswas, A., Prabhu, R., Sen (De), A. and Sen, U., Genuine multipartite entanglement trends in gapless-gapped transitions of quantum spin systems. *Phys. Rev. A*, 2014, **90**, 032301.
61. Barnum, H. and Linden, N., Monotones and invariants for multiparticle quantum states. *J. Phys. A*, 2001, **34**, 6787.
62. Wei, T.-C. and Goldbart, P. M., Geometric measure of entanglement and applications to bipartite and multipartite quantum states. *Phys. Rev. A*, 2003, **68**, 042307.
63. Das, T., Roy, S. S., Bagchi, S., Misra, A., Sen (De), A. and Sen, U., Generalized geometric measure of entanglement for multiparty mixed states. *Phys. Rev. A*, 2016, **94**, 022336.
64. Coffman, V., Kundu, J. and Wootters, W. K., Distributed entanglement. *Phys. Rev. A*, 2000, **61**, 052306.
65. Dhar, H. S., Pal, A. K., Rakshit, D., Sen (De), A. and Sen, U., Monogamy of quantum correlations – a review. arXiv: 1610.01069.
66. The smallest unit in a classical computer which can take a binary value {0, 1}, is called a bit (binary digit). Computation in a classical computer has been performed by using bits.
67. Bose, S., Plenio, M. B. and Vedral, V., Mixed state dense coding and its relation to entanglement measures. *J. Mod. Opt.*, 2000, **47**, 291.
68. Hiroshima, T., Optimal dense coding with mixed state entanglement. *J. Phys. A: Math. Gen.*, 2001, **34**, 6907.
69. Bruß, D., D'Ariano, G. M., Lewenstein, M., Macchiavello, C., Sen (De), A. and Sen, U., Distributed quantum dense coding. *Phys. Rev. Lett.*, 2004, **93**, 210501.
70. Bruß, D., Lewenstein, M., Sen (De), A., Sen, U., DAriano, G. M. and Macchiavello, C., Dense coding with multipartite quantum states. *Int. J. Quantum Inf.*, 2006, **4**, 415.
71. Gordon, J. P., In Proceedings of the International School Phys. Enrico Fermi, Course XXXI (ed. Miles, P. A.), Academic Press, NY 1964, p. 156.
72. Levitin, L. B., In Proceedings of the VI National Conference Inf. Theory, Tashkent, 1969, p. 111.
73. Holevo, A. S., *Probl. Pereda. Inf.*, 1973, **9**, 3; *Probl. Inf. Transm.* 1973, **9**, 110.
74. Yuen, H. P. and Ozawa, M., Ultimate information carrying limit of quantum systems. *Phys. Rev. Lett.*, 1993, **70**, 363.
75. Yuen, H. P., In *Quantum Communication, Computing, and Measurement* (eds Hirota, O. *et al.*), Plenum, NY, 1997.
76. Badziag, P., Horodecki, M., Sen (De), A. and Sen, U., Locally accessible information: how much can the parties gain by cooperating? *Phys. Rev. Lett.*, 2003, **91**, 117901.
77. Horodecki, M., Oppenheim, J., Sen (De), A. and Sen, U., Distillation protocols: output entanglement and local mutual information. *Phys. Rev. Lett.*, 2004, **93**, 170503.
78. Shadman, Z., Kampermann, H., Macchiavello, C. and Bruß, D., Optimal super dense coding over noisy quantum channels. *New J. Phys.*, 2010, **12**, 073042.
79. Das, T., Prabhu, R., Sen (De), A. and Sen, U., Multipartite dense coding versus quantum correlation: noise inverts relative capability of information transfer. *Phys. Rev. A*, 2014, **90**, 022319.
80. Das, T., Prabhu, R., Sen (De), A. and Sen, U., Distributed quantum dense coding with two receivers in noisy environments. *Phys. Rev. A*, 2015, **92**, 052330.
81. Prabhu, R., Pati, A. K., Sen (De), A. and Sen, U., Exclusion principle for quantum dense coding. *Phys. Rev. A*, 2013, **87**, 052319.
82. Nepal, R., Prabhu, R., Sen (De), A. and Sen, U., Maximally-densecoding-capable quantum states. *Phys. Rev. A*, 2013, **87**, 032336.
83. Wootters, W. K. and Zurek, W. H., A single quantum cannot be cloned. *Nature*, 1982, **299**, 802.
84. Horodecki, P., Horodecki, M. and Horodecki, R., General teleportation channel, singlet fraction and quasi-distillation. *Phys. Rev. A*, 1999, **60**, 1888.
85. Verstraete, F. and Verschelde, H., Fidelity of mixed states of two qubits. *Phys. Rev. A*, 2002, **66**, 022307.
86. Acin, A., Bruβ, D., Lewenstein, M. and Sanpera, A., Classification of mixed three-qubit states. *Phys. Rev. Lett.*, 2000, **87**, 040401.

doi: 10.18520/cs/v112/i07/1361-1368