Course 9

ENTANGLED PHOTONS AND QUANTUM COMMUNICATION

M. Aspelmeyer, C. Brukner, A. Zeilinger

Institut für Experimentalphysik, Universität Wien, Vienna, Austria
Institut für Quantenoptik und Quanteninformation, Österreichische Akademie der Wissenschaften
Vienna, Austria

D. Estève, J.-M. Raimond and J. Dalibard, eds.
Les Houches, Session LXXIX, 2003
Quantum Entanglement and Information Processing
Intricacion quantique et traitement de l’information
© 2004 Elsevier B.V. All rights reserved

337
Contents

1. Introduction ............................................. 341
2. Distributing quantum entanglement .................. 341
3. Quantum teleportation and entanglement swapping .. 344
4. Purification of entanglement ........................... 346
5. Quantum entanglement and information .............. 348
References .................................................. 353
1. Introduction

Quantum entanglement is at the heart of quantum physics [1]. It offers unique insights into the fundamental principles of our physical world and it provides at the same time the basis of novel communication protocols, which allow efficient communication and computation beyond the capabilities of their classical counterparts. Prominent examples are quantum cryptography [2–5], the simultaneous distribution of a cryptographic key that is ultimately secured by the laws of quantum physics, quantum dense coding [6, 7], a protocol to double the classically allowed capacity of a communication channel by encoding 2 bits of information per bit sent, or quantum teleportation [8, 9], the remote transfer of an arbitrary quantum state between distant locations. Further examples include entanglement-assisted classical communication [10, 11] to enhance the communication capacity in a noisy environment or methods to exploit the computational advantages provided by quantum entanglement for communication complexity problems [12–14]. These quantum communication protocols utilize entanglement as a resource and form the basis for a new emerging quantum information technology. To achieve quantum communication within a network it is a central task to be able to distribute and manipulate quantum entanglement, in principle up to a global scale. At present, the only suitable system for transmitting information in long-distance quantum communication are photons.

2. Distributing quantum entanglement

The generation of entangled photons is nowadays routine work in the laboratory. One of the methods to produce polarization-entangled photons is spontaneous parametric downconversion, in which pairs of single photons are emitted into separated spatial modes. The photons can then be distributed between different receivers, say Alice (A) and Bob (B). The overall two-photon state shared by the two can be any of the four maximally entangled Bell-states [15], for example

\[ |\Psi^-\rangle_{AB} = \frac{1}{\sqrt{2}} (|H\rangle_A |V\rangle_B - |V\rangle_A |H\rangle_B). \] (2.1)
The Bell states have the unique feature that all information on polarization properties is completely contained in the (polarization-)correlations between the separate photons, while the individual particle does not have any polarization prior to measurement. In other words, all of the information is distributed among two particles, and none of the individual systems carries any information. This is the essence of entanglement. At the same time, these (polarization-)correlations are stronger than classically allowed since they violate bounds imposed by local realistic theories via the Bell-inequality [16] or they lead to a maximal contradiction between such theories and quantum mechanics as signified by the Greenberger-Horne-Zeilinger theorem [17, 18]. Distributed entanglement thus allows to establish non-classical correlations between distant parties and can therefore be considered the quantum analogue to a classical communication channel, a quantum communication channel\textsuperscript{1}. This has, for example, immediate influence on the security of quantum key distribution protocols [19] and it is the basis for the quantum advantage of entanglement-based quantum communication and quantum computation schemes\textsuperscript{2}.

The possibility to establish such quantum communication channels over large distances offers the fascinating perspective to eventually take advantage of these novel communication capabilities in networks of increasing size. Naturally, non-trivial problems emerge in scenarios involving long distances or multiple parties. Experiments based on present fiber technology have demonstrated that entangled photon pairs can be separated by distances ranging from several hundreds of meters up to about 10 km [28–30], but no improvements by orders of magnitude are to be expected. Optical free-space links could provide a solution to this problem since they allow in principle for much larger propagation distances of photons because of the low absorption of the atmosphere in certain wavelength ranges. Single optical free-space links have been studied and successfully implemented already for several years for their application in quantum cryptography based on

\textsuperscript{1}Note, however, that in contrast to classical communication no information is physically transferred via a quantum channel. Instead, non-local correlations are established via local measurements and are subsequently utilized for communication or computation purposes.

\textsuperscript{2}A further step is the utilization of higher-dimensional entanglement. Higher-dimensional quantum systems have several interesting properties, for example fundamental tests of quantum mechanics provide more striking divergence from classical theory with respect to tests of non-locality [20]. Further, the increased complexity provides fertile ground for the development of new and more efficient protocols not possible classically or even with qubits [14, 21, 22]. We have realized several experiments exploring quantum entanglement in higher-dimensional Hilbert spaces using orbital angular momentum of photons [23–25]. In a recent experiment we demonstrated quantum tomography of a qutrit, a three dimensional orbital angular momentum state of photons. This is the first experiment which provides full control over the quantum state of a triggered qutrit and is thus of importance for the implementation of more advanced quantum communication protocols [26, 27].
Entangled photons and quantum communication

Fig. 1. Free-space distribution of polarization-entangled photons (from [33]). The entangled-photon source was positioned on the bank of the Danube River. The two receivers, Alice and Bob, were located on rooftops and separated by approx. 600m, without a direct line of sight between each other. The inset shows the schematics of the telescopes consisting of a single-mode fibre coupler and a 5cm diameter lens. At the receiver telescopes, polarizers (Pol.) were attached to determine the polarization correlations and eventually violate a Bell-inequality. The lower figure shows a functional block diagram of the experiment. Detection signals from Alice were relayed to Bob using a long BNC cable. Singles and coincidence counting was performed locally at Bob and the results were shared between all three stations using LAN and Wave-LAN connections.

faint classical laser pulses [31, 32]. We have recently demonstrated a next crucial step, namely the distribution of quantum entanglement via two simultaneous optical free-space links in an outdoor environment [33]. Polarization-entangled photon pairs have been transmitted across the Danube River in the city of Vienna via optical free-space links to independent receivers separated by 600m and without a line of sight between them (see Figure 1). A Bell inequality between those receivers was violated by more than 4 standard deviations confirming the quality of the entanglement. In this experiment, the setup for the source generating the entangled photon pairs has been miniaturized to fit on a small optical breadboard and it could easily be operated completely independent from an ideal laboratory environment.

Obviously, terrestrial free-space links are limited to rather short distances because they suffer from possible obstruction of objects in the line of sight, from
atmospheric attenuation and, eventually, from the Earth’s curvature. To fully exploit the advantages of free-space links, it will eventually be necessary to use space and satellite technology. By transmitting and/or receiving either photons or entangled photon pairs to and/or from a satellite, entanglement can be distributed over truly large distances. This would allow quantum communication applications on a global scale. From a fundamental point of view, satellite-based distribution of quantum entanglement is also the first step towards exploiting quantum correlations on a scale larger by orders of magnitude than achievable in laboratory and even ground-based experimental environments. State of the art photon sources and detectors would already suffice to achieve a satellite-based quantum communication link over some thousands of kilometers [34–36]. The outdoor experiments described above represent a step towards satellite-based distributed quantum entanglement.

One principle limitation of photonic quantum communication schemes is the loss of photons in the quantum channel. This limits the bridgeable distance for single photons to the order of 100 km in present silica fibers [37, 38]. Recent experiments already achieve such distances [39, 40]. In principle, this drawback can eventually be overcome by subdividing the larger distance to be bridged into smaller sections over which entanglement can be teleported. The consequent application of so-called “entanglement swapping” [41] may result in transporting entanglement over larger distances. Additionally, to diminish decoherence effects possibly induced by the quantum channel, quantum purification might be applied to eventually implement a full quantum repeater [42]. In fact, the experimental building blocks for a full-scale quantum repeater based on linear optics have been successfully demonstrated over the last years by the realization of teleportation and entanglement swapping [9,43,44] and, only recently, by the implementation of quantum entanglement purification and distillation protocols [45–47].

3. Quantum teleportation and entanglement swapping

Teleportation of quantum states [8] is an intriguing concept within quantum physics and a striking application of quantum entanglement. Besides its importance for quantum computation [48, 49], teleportation is at the heart of the quantum repeater [42], a concept eventually allowing the distribution of quantum entanglement over arbitrary distances and thus enabling quantum communication over large distances and even networking on a global scale.
The purpose of quantum teleportation is to transfer an arbitrary quantum state to a distant location, say from Alice to Bob, without transmitting the actual physical object carrying the state. Classically this is an impossible task, since Alice cannot obtain the full information of the state to be teleported without previous knowledge about its preparation. Quantum physics, however, provides a working strategy. Suppose, Alice and Bob share an ancilla entangled pair in advance. Alice then performs a Bell-state measurement between the teleporte particle and her shared ancilla, i.e. she projects the two particles into the basis of Bell-states. The four possible outcomes of this measurement provide her with two bits of classical information. Thus the quantum state to be teleported can be reconstructed at Bob’s side. After communicating the classical result to Bob, he can perform one out of four unitary operations to obtain the original state to be teleported. Note, that in one of the cases the original state is transferred instantaneously and no active transformation is required at Bob’s side. If Bob would have used his state beforehand as an input state for a quantum computational operation, the teleportation would define his input only after the actual computation has taken place. One thus achieves for these cases instantaneous quantum computation, which can provide additional computational advantage (although with exponentially small probability) for certain schemes [50].

An important feature of teleportation is that it provides no information whatsoever about the state being teleported. This means that an arbitrary unknown quantum state can be teleported. In fact, the quantum state of a teleporte particle does not have to be well defined and it could thus even be entangled with another photon. This means that a Bell-state measurement of two of the photons - one each from two pairs of entangled photons - results in the remaining two photons becoming entangled, even though they have never interacted in the past. Recently, we could demonstrate that by violating a Bell inequality between particles that never interacted with each other [44]. A repeated application of this so-called “entanglement-swapping” [41] can in principle be used to transfer quantum entanglement between distant sites (see Figure 2). In the context of Bell experiments to test for violations of local realism, entanglement-swapping can also be seen as a method to achieve event-ready detection of entangled particles, since a successful Bell-state measurement unambiguously indicates the completed preparation of an entangled pair [41].

Two recent results, both of relevance for long-distance quantum communication, are the demonstration of quantum state teleportation over a distance of several tens of meters [51] and the first realization of freely propagating teleported qubits [52], which eventually will allow the subsequent use of teleported states. In previous realizations of teleportation the teleported qubit had to be
detected (and thus destroyed) to verify the success of the procedure. This can be avoided by providing, in average, more entangled ancilla pairs than states to be teleported. In the new teleportation scheme, a successful Bell-state analysis results in freely propagating individual qubits, which can be used for further cascaded teleportation.

4. Purification of entanglement

Owing to unavoidable decoherence in the quantum communication channel, the quality of entangled states generally decreases with the channel length. Entanglement purification is a way to extract a subset of states of high entanglement and high purity from a larger set of less entangled states - and is thus needed to overcome the decoherence of noisy quantum channels. We were able for the first time to experimentally demonstrate a general quantum purification scheme for mixed polarization-entangled two-particle states [47]. The crucial operation for a successful purification step is a bilateral conditional NOT (CNOT) gate, which effectively detects single bit-flip errors in the channel by performing local CNOT operations at Alice’s and Bob’s side between particles of shared entangled states. The outcome of these measurements can be used to correct for such errors and eventually end up in a less noisy quantum channel [53]. For the case of polarization entanglement, such a “parity-check” on the correlations can be performed in a straightforward way by using polarizing beamsplitters (PBS) [54] that transmit horizontally polarized photons and reflect vertically polarized ones.
Consider the situation in which Alice and Bob have established a noisy quantum channel, i.e., they share a set of equally mixed, entangled states $\rho_{AB}$. At both sides the two particles of two shared pairs are directed into the input ports $a_1, a_2,$ and $b_1, b_2$ of a PBS (see Figure 3). Only if the entangled input states have the same correlations, i.e., they have the same parity with respect to their polarization correlations, the four photons will exit in four different outputs (four-mode case) and a projection of one of the photons at each side will result in a shared two-photon state with a higher degree of entanglement. All single bit-flip errors are effectively suppressed.

For example, they might start off with the mixed state $\rho_{AB} = F \cdot |\Phi^+\rangle\langle\Phi^+|_{AB} + (1 - F) \cdot |\Psi^-\rangle\langle\Psi^-|_{AB}$, where $|\Phi^+\rangle = (|HH\rangle + |VV\rangle)$ is another Bell state. Then, only the combinations $|\Phi^+\rangle_{a_1,a_2} \otimes |\Phi^+\rangle_{b_1,b_2} \otimes |\Psi^-\rangle_{a_1,a_2} \otimes |\Psi^-\rangle_{b_1,b_2}$ will lead to a four-mode case, while $|\Phi^+\rangle_{a_1,a_2} \otimes |\Psi^-\rangle_{b_1,b_2}$ and $|\Psi^-\rangle_{a_1,a_2} \otimes |\Phi^+\rangle_{b_1,b_2}$ will be rejected. Finally, a projection of the output modes $a_4, b_4$ into the basis $|\pm\rangle = \frac{1}{\sqrt{2}}(|H\rangle \pm |V\rangle)$ is needed to create the pure states $|\Phi^+\rangle_{a_3,b_3}$ with probability $F' = F^2 / (F^2 + (1 - F)^2)$ and $|\Psi^+\rangle_{a_3,b_3}$ with probability $1 - F'$, respectively. The fraction $F'$ of the desired state $|\Phi^+\rangle$ becomes larger for $F > \frac{1}{2}$. In other words, the new state $\rho'_{AB}$ shared by Alice and Bob after the bilateral parity
operation demonstrates an increased fidelity with respect to a pure, maximally entangled state. This is the purification of entanglement.

Typically, in the experiment, one photon pair of fidelity 92% could be obtained from two pairs, each of fidelity 75%. Also, although only bit-flip errors in the channel have been discussed, the scheme works for any general mixed state, since any phase-flip error can be transformed to a bit-flip by a rotation in a complementary basis. In our experiments, decoherence is overcome to the extent that the technique would achieve tolerable error rates for quantum repeaters in long-distance quantum communication based only on linear optics and polarization entanglement.

5. Quantum entanglement and information

Quantum communication utilizes the information content of entangled systems as an additional resource. We suggest that the relation between quantum entanglement and information is a much more fundamental one and even inherent to quantum physics.

The various debates about the conceptual significance of quantum mechanics can to a large part be seen as a debate of what quantum physics refers to. Does it refer to reality directly or does it refer to (our) knowledge, and therefore to information? If quantum physics refers to reality, which reality is it? Is it the reality which appears to us, or is it a more complicated reality, like the one alluded to in the Many-Worlds interpretation?

Significant inspiration can be obtained from Niels Bohr, who, for example, according to Aage Petersen liked to say [55]: "There is no quantum world. There is only an abstract quantum physical description. It is wrong to think that the task of physics is to find out how Nature is. Physics concerns what we can say about Nature."

To us, it is thus suggestive that knowledge is the central concept of quantum physics. In modern language, knowledge can be equated with information. Therefore, one firstly needs a proper measure of information. One might be tempted to use Shannon’s measure

\[ I = - \sum_i p_i \log p_i, \] (5.1)

where, \( p_i \) is the probability of sign \( i \) to occur in a sequence.

Yet it turns out that Shannon’s measure is not adequate in order to describe the knowledge gained in an individual quantum experiment [56]. This feature can be understood in various ways. One most central one is that the logarithmic dependence of the Shannon measure of information is related to the postulate that
the information gained in a series of observations of different properties must be independent from the specific sequence in which the properties are read out. Clearly, such a requirement is not valid in quantum mechanics any more, unless the properties are commuting, which is in general an exception. So, what is desired is a measure of information which accounts for complementarity and describes the total information obtainable in a complete set of quantum experiments. We have suggested elsewhere [57] that the most appropriate measure of information is

$$I = \sum_i p_i p_i$$

(5.2)

which may be viewed as the sum of the individual probabilities weighed by these probabilities themselves. The total information content $I_{total}$ of a quantum system is then obtained as a sum of individual measures of information $I_j$ (of the type given in (5.2)) over a complete set of maximally mutually complementary observables (indexed by $j$)

$$I_{total} = \sum_j I_j = \sum_j \sum_i p_{ij} p_{ij}.$$  

(5.3)

Here $p_{ij}$ denotes the probability to observe the $i$-th outcome of the $j$-th observable.

Maybe the notion of mutually complementary observables might need to be explained further. A famous example is given by the three components of a spin-$1/2$ particle taken along three directions orthogonal in space (not to be confused with orthogonal quantum states). From an operational point of view, two variables $A$ and $B$ are maximal mutually complementary if the knowledge of one completely precludes any knowledge of the other. In the case of spin, if $A$ represents the spin along the $z$-direction, then $B$ might represent the spin along any direction orthogonal to $z$ in space. It is a well known feature that if the spin along $z$ is well defined, the spin along these other directions is maximally undefined. To come back to our example, the sum $\sum_j$ in (5.3) in the case of spin has to be taken along any three spatially orthogonal directions, i.e., $j = x, y, z$.

It has not escaped our attention that equation (5.3) can be put onto a nicely visualizable foundation if one defines an information space spanned by mutually complementary states [58]. Then $I_{total}$ just represents the square of the length of a vector in that information space when the square of the length of individual components is just given by $I_j$.

If, as we have suggested above, quantum physics is about information then we have to ask ourselves what we mean by a quantum system. It is then imperative to avoid assigning any variant of naive classical objectivity to quantum states [59].
Rather it is then natural to assume that the quantum system is just that to which the probabilities in equations (5.2) and (5.3) refer, and no more. So, the notion of an independently existing reality becomes void.

We might therefore ask how much information a quantum system might carry stressing again that by "carry" we just refer to the total amount of information and not to the objective existence of any subject actually carrying the information.

It is obvious that a large system, being our mental representative of the information characterizing it, carries a lot of information, very many bits. Then, how does that amount of information scale with the size of the object? It is very suggestive to assume that the smaller a system, the less information it carries. One may even consider the amount of information carried by a system as defining its "size". So, basically we postulate (1) that the amount of information carried by any system is finite and (2) that the amount of information is lesser the smaller the system. These assumptions may be supported by referring to Feynman [60]: "It always bothers me that, according to the laws as we understand them today, it takes a computing machine an infinite number of logical operations to figure out what goes on in no matter how tiny a region of space, and no matter how tiny a region of time. How can all that be going on in that tiny space? Why should it take an infinite amount of logic to figure out what one tiny piece of space/time is going to do?" Evidently, Feynman's problem is solved if the "tiny piece of space-time" only contains a finite amount of information, and the less, the smaller the piece is.

We arrive at a natural limit when a system only represents one bit of information. Once that is achieved, the system can only represent the yes/no answer to one question. If the system is asked another question, the answer by necessity has to be random. Thus, randomness is a fundamental feature of our world [61, 62]. This, we suggest, also provides a natural foundation for complementarity. Consider, for example, a simple two-path interferometer as shown in Figure 4.

As is well known, in such an interferometer, we can either define the path $|a\rangle$ or $|b\rangle$ taken by a particle. In that case, the trajectory after the semi-reflecting beam-splitter is completely random, or, in other words, detectors I or II each will register particles with the same probability of 50%. On the other hand, we can prepare the state in a coherent superposition of $|a\rangle$ and $|b\rangle$ in such a way that, by adjusting the relative phase, all particles end up in detector I and no particles in detector II. In other words, in the outgoing beam leading to detector I, constructive interference happens, and destructive interference happens in the outgoing beam II. The observations of the path the particle takes inside the interferometer and of the interference are an example of two mutually maximally complementary observations.

This behaviour can be understood very simply on the basis of our most elementary quantum system carrying just one bit of information. It is then up to the
Fig. 4. Two-Path Interferometer. The source emits coherent waves of which two beams are selected and incident on the beam-splitter. Each of the two beams has the same amplitude for being transmitted or reflected at the beam-splitter, and thus the outgoing beams are coherent superpositions of the incoming ones.

experimentalist to decide whether she wants to prepare the system such that the one bit of information is used to completely determine the path, a binary variable, in which case no information is left to determine the fate of the particle after the beam splitter. Then the outcome, which detector, I or II, fires, must be completely random. Alternatively, the experimentalist prepares the system such that the one bit of information defines which detector fires, i.e. the interference, in which case the path is completely undefined. Evidently, intermediate cases are possible, where both, path information and interference, each are partly defined.

We note that we are thus led to a natural explanation of quantum complementarity. Our measure of information defined in equation (5.3) provides a perfect measure also for the intermediate cases, where path is partially defined and also interference is obtained with partial visibility only such that their information contents totally sum up to one bit [63].

Concluding this chapter, we note that using our approach, we were able to explain some other important features of quantum mechanics, most notably, Malus' law [58] which describes the cosine dependence of the probability upon the angle between the measurement direction and the direction along which the spin is well defined. We were also able to obtain a natural understanding of entanglement [64]. For example, if one considers entanglement of two spin-1/2 particles, one has two elementary systems in our sense, and thus two bits of information
available. These two bits can be used in principle to encode properties of the individual particles themselves, which is basically classical coding. On the other hand, the two bits can be completely used up to fully define joint information only, that is, information about how possible measurement results on the particles relate to each other. If done in that way, one automatically obtains the four Bell states. That way one obtains a natural basis for Schrödinger’s definition of entanglement [1]. Finally, we note that using our approach we were able to derive the Liouville equation describing the quantum evolution in time of a two-state system [58].

Clearly, a number of important questions remain open. Of these, we mention here two. The first one refers to continuous variables. The problem there is that with continuous variables, one in principle has an infinite number of complementary observables. One might attack this question by generalizing the definition of equation (5.2) to infinite sets. This, while mathematically possible, leads to conceptually difficult situations. The conceptual problem in our eyes is related to the fact that we wish to define all notions on operationally verifiable bases or foundations, that is, on foundations which can be verified directly in experiment. It is obvious that an infinite number of complementary observables can never be realized in experiment. In our opinion, it is therefore suggestive that the concept of an infinite number of complementary observables and therefore, indirectly, the assumption of continuous variables, are just mathematical constructions which might not have a place in a final formulation of quantum mechanics.

This leads to the second question, namely, how to derive the Schrödinger equation. If our assumption just expressed is correct, namely that continuous variables are devoid of operational and therefore physical meaning in quantum mechanics, there is no need to express the Schrödinger equation based on continuous variables in our new language. Indeed, one then should refer to situations where one always has a finite number of complementary observables only. In our opinion such a point of view is experimentally well founded, as any experiment will always lead only to a finite number of bits and a finite number of the experimental results on the basis on which only a finite number of observables can be operationally defined.

It has not escaped our attention that our way of reasoning also leads to new possibilities of understanding why we have quantum physics, i.e. Wheeler’s famous question “Why the quantum?”. Identifying systems with the information they carry, we note that information necessarily is quantized. One can have one proposition, two propositions, three propositions etc., but obviously the concept of, say, $\sqrt{2}$ propositions is devoid of any meaning. Therefore, since information is quantized that way, our description of information, which is quantum mechanics, also has to be quantized.
References


Entangled photons and quantum communication


