Entanglement Assisted Quantum Communication Schemes

Zoltán Kurucz

Theses of PhD Dissertation

Based on research carried out in Research Institute for Solid State Physics and Optics, Hungarian Academy of Sciences, Budapest, Hungary

Supervisor
József Janszky

University of Szeged
Szeged, 2007

The concept of information is of intrinsically physical origin. Information is stored, transmitted, manipulated, and processed by means of physical systems. When these systems obey the laws of quantum mechanics, quantum theory must be applied to information as well. In the Dissertation, quantum communication schemes are investigated in which quantum information is transmitted via a purely classical and a nonclassical (entangled) channel. Beyond quantum teleportation, the more general remote state preparation schemes and their properties are studied. The present summary condenses the main ideas and results.

Introduction

The simplest quantum systems have two well-defined and distinguishable levels that are conventionally denoted by orthogonal state vectors $|0\rangle$ and $|1\rangle$. From the quantum information point of view, such systems are all equivalent and referred to as quantum bits or *qubits*. In contrast to classical bits whose value is either "0" or "1", a qubit can have both the values $|0\rangle$ and $|1\rangle$ at the same time. This follows from the superposition principle of quantum mechanics: generic pure states of the qubit are given by complex superpositions of $|0\rangle$ and $|1\rangle$ described by two real angles as parameters, $|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle$. This property is the essence of many interesting phenomena in quantum information processing. For example, the main advantage of quantum computation over its classical counterpart is due to quantum parallelism: a function can be evaluated in multiple points in the same run, if the input is in a superposition state [1]. Famous example is Shor's prime factoring quantum algorithm [2] that is exponentially faster than all the presently known classical algorithms. However, quantum properties of physical systems are rather fragile. Even looking at them can destroy their quantum nature, and measurement transforms quantum information (the two real angles) into classical (a "0" or "1"). Quantum information cannot be entirely extracted, nor can it be exactly copied or cloned [3]. This fact provides the starting point of unbreakable quantum cryptographic ciphers [2].

The most interesting physics, however, starts when superposition principle is applied to multiple subsystems that are separated in space: the

existence of *entanglement* is one of the most peculiar characteristics of quantum mechanics. Consider for example two distinguishable spin-$\frac{1}{2}$ particles whose total angular momentum is zero. Regarding only the spin component of their wave function, they can be interpreted as quantum bits. Their spin state, the antisymmetric singlet is maximally entangled and has the following property. If the spin of the first particle is measured and found to point in a specific (but random) direction, then the spin of the other will point to the opposite direction with certainty, even though it has been indeterminate before. The importance of this phenomenon was first addressed by Einstein, Podolsky, and Rosen [4] mainly in philosophical context regarding non-locality and incompleteness of quantum theory. Later, Bell [5] and Clauser et al. [6] showed that entanglement leads to correlation between measurement outcomes that cannot be explained by any local classical theory and is of inherently quantum origin. Since then, entanglement has become a key *resource* in quantum information science. Entangled states, if disposable, can make it possible to perform many non-local operations that cannot be otherwise carried out by local operations and classical communication. Thus, entangled states serve as a resource to circumvent superselection rules posed by locality [7].

One of the most fundamental applications of entanglement is *quantum teleportation* [8]. It is a quantum communication protocol in which entanglement assists in exchanging quantum information when no direct transfer of any quantum system is possible and the communicating parties are restricted to local quantum operations and classical communication. Indeed, entanglement and classical communication together have the potential to be turned into quantum communication: a generic unknown qubit state can be perfectly transmitted while using up one pair of maximally entangled qubits (distributed between the parties in advance) and sending two bits of classical information in forward direction (from the sender to the receiver of the quantum information). The entanglement cost of teleportation is 1 ebit [9] per qubit transmitted. Less entangled resources like partially entangled or mixed states can also be used in teleportation [10]. However, the quantum communication capacity of such teleportation channels (the average quantum information they can convey) is decreased. Such imperfect teleportation schemes are either probabilistic or the transmitted state is distorted implying a decrease in transmission fidelity. For *reversible* channels [11], it is possible to undo distortions, but such schemes are always

probabilistic if the resource is not maximally entangled. Given a realistic, nonideally entangled resource, it is important to know whether the channel can be reversed and how to construct reversible protocols that are capable of exact, albeit probabilistic teleportation of generic quantum states [A, B]. This is one of the questions addressed in the Dissertation.

Exact and deterministic teleportation of a generic qubit state requires one pair of maximally entangled qubits (1 ebit) and classical communication of two bits, and these resources are necessary in the sense that neither of them can be cut down [12]. However, resources can be traded off if the qubit state (the two real angles) is known to the sender. This case is called *remote state preparation*, since quantum communication is combined with quantum state engineering. For a trivial example, suppose that the sender directly tells the two real angles to the receiver who then prepares a physical instance of the quantum information locally at his place. This method uses no prior entanglement but needs classical communication of infinitely many bits to convey the two real numbers. Less than 1 ebit of entanglement is needed if the sender provides finite amount of classical information about the target state [13]. On the other hand, the classical communication cost can be arbitrarily close to 1 bit per qubit, but at the cost of using up entangled resources [14].

Resources can also be cut down if the input is restricted to an ensemble of special qubit states. For example, if the contributing parties agree in advance that they are going to prepare only states lying on the equator of the Bloch sphere (that is, the spin of a spin-$\frac{1}{2}$ particle is aligned perpendicular to the z axis), then 1 ebit of entanglement and 1 bit of classical communication suffice [15]. The method is based on the special property of the singlet state that if the first particle's spin component in spatial direction $\vec{n}$ is measured, then the spin of the second one gets aligned in the same direction as well: it is parallel or antiparallel to $\vec{n}$ depending on the measurement outcome. So if the sender wants to remotely prepare the state $|\vec{n}\rangle_B$ (the state in which the spin is aligned with the unit direction vector $\vec{n}$), the only thing she needs to do is to measure the spin component of her part of the entangled pair in direction $\vec{n}$. If the outcome is $-\frac{1}{2}$ (and this happens with probability $\frac{1}{2}$), then the receiver's state becomes $|\vec{n}\rangle_B$ correctly, while a result of $+\frac{1}{2}$ shows that his state is just the antipodal state $|-\vec{n}\rangle_B$. Then the sender sends to the receiver 1 bit of classical information: the measurement result. There is nothing to do for the receiver in

the first case, but in the second case, he has to flip his spin in order to obtain the right output. This spin flip operation—that maps any pure state to its orthogonal complement, $\alpha|0\rangle + \beta|1\rangle \mapsto \beta^*|0\rangle - \alpha^*|1\rangle$—is the antiunitary time reversal operation and, thus, it cannot be carried out physically. However, restricted to states on the equator of the Bloch sphere, namely, to states of the form $|\phi\rangle = (|0\rangle + e^{i\varphi}|1\rangle)/\sqrt{2}$, the unitary π-rotation along the z axis can substitute the required antiunitary recovery transformation, and it can be realized physically. This *equatorial method* can also be generalized from qubits to higher dimensional quantum systems [16]. Then equally weighted superpositions of all the computational basis states can be prepared. These states form a $D-1$ dimensional real submanifold in the D dimensional complex Hilbert space, and their remote preparation requires $\log_2 D$ ebits of entanglement and the same number of bits of classical communication as resources [C]. The method can be extended to systems with infinite dimensional state spaces as well [E].

An important question regarding quantum communication is whether any additional information about the transmitted state can be gained from the classical message or from the output quantum systems, compared to what can be learned from the single instance of the transmitted state that arrives at the receiver. If, for example, the probability distribution of the classical message depends on the target state in case of a nonideal teleportation or remote state preparation scheme, then the message does contain accessible information about the input. Since the input state can be unknown in teleportation and unknown states cannot be cloned, such a leakage of information would inevitably introduce losses and noise in the transmission process [11]. Therefore, it is necessary for noiseless teleportation that the classical message does not correlate with the transmitted quantum information [A]. On the other hand, if the quantum communication protocol does not leak information, it can be securely incorporated into cryptographic protocols and distributed quantum computation tasks [17]. Such quantum communication schemes are called *oblivious*. It can be shown [18] that oblivious remote state preparation of generic pure states requires at least 1 ebit of entanglement and 2 bits of classical communication per qubit. Oblivious schemes, thus, play an important role in quantum information theory. The question then naturally arises: what makes an entanglement assisted quantum communication scheme oblivious, and how to construct

remote state preparation schemes that are such. One of the main results of the Dissertation answers this question [F].

The protocol of quantum teleportation can be extended to states of dynamical variables with continuous spectra [19]. Such systems are, for example, modes of the electromagnetic field or spinless massive particles moving in one dimension. In the latter case, the dynamical variables can be the standard position and momentum, but they can be the canonical action-angle coordinates as well. Since the spectra of these variables are not the same, there are essentially different continuous variable teleportation protocols. Good examples are the quantum optical protocol based on quadrature variables of the electromagnetic field [20] and another one based on photon number and phase [21]. Quantum information processing on continuous variables provides an interesting alternative to the "traditional" qubit-based approach [22, 23]. There are also probabilistic quantum state engineering schemes based on conditional measurements performed on one of two entangled light beams. However, they are different from remote state preparation, as an essential feature of the latter is that it is deterministic. A comprehensive study of continuous variable remote state preparation has been missing so far. The other main result of the Dissertation intends to fill this gap.

Aims and objectives

One of the main objectives of the research was to investigate whether partially entangled states can be directly utilized in exact quantum communication protocols with no need of entanglement distillation in advance, and how to construct teleportation protocols to a given partially entangled state. Since quantum information is transmitted via a purely classical and a nonclassical (entangled) channel, the question naturally arises what are the roles of these two kinds of channels in the information transfer, whether it is possible to draw a balance between the amounts of transferred and leaked information. Oblivious remote state preparation schemes play an important role in this aspect. One of the tasks was, therefore, to give a condition for schemes to be oblivious.

Remote state preparation of equatorial states is exact and deterministic, but the set of preparable states is restricted. It was also the object of

the research to determine what other kinds of ensembles can be prepared, and to design various schemes for them. An interesting question was whether the set of preparable states can be extended if the receiver is allowed to apply not only realizable unitary but nonphysical antiunitary transformations as well. Finally, how to generalize the equatorial method to continuous variable quantum systems.

Research methods

Bipartite quantum communication schemes studied in the Dissertation exploit nonclassical correlation present in entangled states in order to transmit quantum information as follows. First, assume that an entangled pair of quantum systems is distributed between the sender and the receiver in advance. In the first step of a quantum communication protocol, the sender performs a measurement on her half of the entangled pair (system A). In the case of quantum teleportation, this is a Bell-type measurement that projects the unknown state of the input system and the state of system A onto an entangled state. In the case of the equatorial method, there is no input system, the target state is completely known to the sender. The measurement is a projective von-Neumann measurement performed on system A alone, and the eigenstates of the measurement depends explicitly on the state to be remotely prepared. After the measurement, systems A and B are no longer entangled, but there is still a significant classical correlation between the measurement result and the state of system B. In the second step, the sender sends a classical message to the receiver. The message depends on the measurement result, but it can be an explicit function of the target state as well. In the third step of the protocol, the receiver performs a local quantum operation on his system that he chose from a prearranged set of operations according to the message he received. In the above two examples, this is a unitary operation. At the end of the process, the state of system B no longer depends on the random measurement outcome, it contains the original quantum information only. It is important that this information stays hidden as long as the classical message is obscure to the receiver. Therefore, quantum communication cannot be faster than its classical counterpart, and it does not violate causality.

Many of the results of the Dissertation is based on *antilinear* operator representation of bipartite entangled states. Although antilinear (also known as conjugate linear) operators in quantum mechanics usually appear in the context of time reversal symmetries, quantum information theory also provides some interesting application. Suppose that systems A and B are in the pure entangled state $|\Psi\rangle_{AB}$. If a complete measurement performed on system A yields the eigenstate $|\phi\rangle_A$, then the state of system B becomes determinate: $|\psi\rangle_B = \lambda\, {}_A\langle\phi|\Psi\rangle_{AB}$. Since this partial inner product is conjugate linear in its first argument, the map

$$\hat{A}_\Psi \colon \mathscr{H}_A \to \mathscr{H}_B, |\phi\rangle_A \mapsto {}_A\langle\phi|\Psi\rangle_{AB}$$

defines an antilinear operator. This operator completely and uniquely describes the bipartite pure state. In more general, taking mixed states into account, bipartite states can be characterized by *completely $*$-copositive* superoperators. Kraus decomposition of such superoperators comprises antilinear operators $\hat{A}_i$: $\hat{M} \mapsto \sum_i \hat{A}_i \hat{M} \hat{A}_i^\dagger$. This antilinear operator representation is found to be of utmost convenience in describing quantum information processing schemes, because state transformations can be easily obtained by combining the corresponding antilinear operators.

Thesis points

1. The antilinear (relative state) operator representation of entangled states is applied in the description of nonideal teleportation on finite dimensional Hilbert spaces. The two antilinear operators corresponding to the shared entangled resource and to the joint measurement can be simply combined to obtain the state transformation that describes the teleportation channel. The probabilistic teleportation channel is linearly reversible if and only if the probability of the successful measurement outcome(s) does not depend on the input state, i.e., the process is oblivious. In this case, the channel is unitarily reversible as well, and it can be used in exact probabilistic teleportation. Given a pure but partially entangled state, an entanglement matching condition is derived which the joint measurement has to fulfil in order for the channel to be reversible. [A, B]

2. The problem of oblivious quantum communication is analyzed. A general criterion for exact remote state preparation schemes to be oblivious is given: it is sufficient and necessary that the positive operator elements of the sender's generalized measurement (POVM), which depend on the state to be prepared, are completely $*$-copositive. For schemes based on pure states, this condition is equivalent to that the measurement eigenstates depend antilinearly on the target state. [F]

3. The antilinear operator formalism is applied to exact deterministic remote state preparation schemes that utilize unitary recovery transformations [C]. Alternative easy-to-use conditions for such schemes to exist and to be oblivious are presented in terms of commutation relations [F]. A method is shown how to construct schemes in higher dimensional state spaces by combining lower dimensional protocols.

4. It is shown that a onepartite, positive operator valued measurement (POVM), whose positive operator elements depend on an unknown generic (unrestricted) quantum state and are completely $*$-copositive, can always be traced back to a bipartite joint measurement that is performed on the system under consideration and on an ancilla prepared in the unknown state. It cannot be traced back, however, if the unknown state is restricted; for example, it is a qubit state chosen from the equator of the Bloch sphere. As a consequence, equatorial remote state preparation does require from the sender to have complete classical knowledge about the target state, and a single instance of it at the sender's hand (as in teleportation) is not enough.

5. It is pointed out that the equatorial method cannot be extended to deterministic and exact remote preparation of an unrestricted state using 1 ebit of entanglement and 1 bit of classical communication per qubit. In three or more dimensional Hilbert space, the set of remotely preparable states cannot be extended to the entire Hilbert space, not even in the case when the receiver applies the recovering transformations on his future operations, that are known to him, instead of recovering the target state, that is unknown to him. In this latter case, all the measurement statistics could be correctly reproduced. [D]

6. Remote state preparation of equatorial ensembles is generalized to continuous variable quantum systems. Based on the spectra of the dynamical variables, three cases are presented in momentum, particle number, and canonical phase representations. It is shown that the ensemble of preparable states is parameterized by infinitely (either continuous or countable) many real angles, while the classical communication cost is only one real number or an unbounded integer [E, G]. Possibility of quantum optical realizations and effects of finite entanglement and detector inefficiencies are also considered.

References

[1] D. Deutsch, *Proc. R. Soc. Lond. A* **400**, 97–117 (1985).
[2] M. A. Nielsen and I. L. Chuang, *Quantum computation and quantum information* (Cambridge University Press, Cambridge, 2000).
[3] W. K. Wootters and W. H. Zurek, *Nature* **299**, 802–803 (1982).
[4] A. Einstein, B. Podolsky, and N. Rosen, *Phys. Rev.* **47**, 777–780 (1935).
[5] J. S. Bell, *Physics* **1**, 195 (1964).
[6] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, *Phys. Rev. Lett.* **23**, 880–844 (1969).
[7] S. D. Bartlett, T. Rudolph, and R. W. Spekkens, (2006). quant-ph/0610030.
[8] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, *Phys. Rev. Lett.* **70**, 1895–1999 (1993).
[9] H. K. Lo and S. Popescu, *Phys. Rev. Lett.* **83**, 1459–1462 (1999). quant-ph/9902045.
[10] S. Popescu, *Phys. Rev. Lett.* **72**, 797–799 (1994).
[11] M. A. Nielsen and C. M. Caves, *Phys. Rev. A* **55**, 2547–2556 (1997). quant-ph/9608001.
[12] H. K. Lo, *Phys. Rev. A* **62**, 012313 (2000). quant-ph/9912009.
[13] I. Devetak and T. Berger, *Phys. Rev. Lett.* **87**, 197901 (2001). quant-ph/0102123.
[14] C. H. Bennett, P. Hayden, D. W. Leung, P. W. Shor, and A. Winter, *IEEE Trans. Inform. Theory* **51**, 56–74 (2005). quant-ph/0307100.
[15] A. K. Pati, *Phys. Rev. A* **63**, 014302 (2000). quant-ph/9907022.
[16] M.-Y. Ye, Y.-S. Zhang, and G.-C. Guo, *Phys. Rev. A* **69**, 022310 (2004). quant-ph/0307027.
[17] D. Gottesman and I. L. Chuang, *Nature* **402**, 390–393 (1999).
[18] D. W. Leung and P. W. Shor, *Phys. Rev. Lett.* **90**, 127905 (2003). quant-ph/0201008.
[19] L. Vaidman, *Phys. Rev. A* **49**, 1473–1476 (1994).
[20] S. L. Braunstein and H. J. Kimble, *Phys. Rev. Lett.* **80**, 869–872 (1998).
[21] G. J. Milburn and S. L. Braunstein, *Phys. Rev. A* **60**, 937–942 (1999). quant-ph/9812018.
[22] S. Lloyd and S. L. Braunstein, *Phys. Rev. Lett.* **82**, 1784–1787 (1999). quant-ph/9810082.
[23] D. Gottesman, A. Kitaev, and J. Preskill, *Phys. Rev. A* **64**, 012310 (2001). quant-ph/0008040.

Related publications

[A] Z. Kurucz, M. Koniorczyk, and J. Janszky: Quantum teleportation with partially entangled states. *Fortschr. Phys.* **49**, 1019–1025 (2001). quant-ph/0308020.

[B] Z. Kurucz, M. Koniorczyk, P. Adam, and J. Janszky: An operator description of entanglement matching in quantum teleportation. *J. Opt. B: Quantum Semiclass. Opt.* **5**, S627–S632 (2003).

[C] Z. Kurucz and P. Adam: Preparable ensembles for remote state preparation. *J. Opt. B: Quantum Semiclass. Opt.* **7**, 135–138 (2005).

[D] Z. Kurucz, P. Adam, and J. Janszky: Simulating measurement statistics in remote state preparation. *Acta Phys. Hung. B: Quant. El.* **23**, 49–54 (2005).

[E] Z. Kurucz, P. Adam, Z. Kis, and J. Janszky: Continuous variable remote state preparation. *Phys. Rev. A* **72**, 052315 (2005). quant-ph/0510074.

[F] Z. Kurucz, P. Adam, and J. Janszky: General criterion for oblivious remote state preparation. *Phys. Rev. A* **73**, 062301 (2006). quant-ph/0605057.

[G] Z. Kurucz, P. Adam, and J. Janszky: Remote state preparation in quadrature basis. *Acta Phys. Hung. B: Quant. El.* **26**, 319–326 (2006).

Further publications

[H] M. Koniorczyk, Z. Kurucz, A. Gábris, and J. Janszky: General optical state truncation and its teleportation. *Phys. Rev. A* **62**, 013802 (2000).

[I] S. Farkas, Z. Kurucz, and M. Weiner: Poincaré covariance of relativistic quantum position. *Int. J. Theor. Phys.* **41**, 79–88 (2002). quant-ph/0009102.