METHODS OF QUANTUM ERROR CORRECTION

Markus Grassl

Arbeitsgruppe *Quantum Computing*, Prof. Thomas Beth
Institut für Algorithmen und Kognitive Systeme, Universität Karlsruhe
Am Fasanengarten 5, 76 128 Karlsruhe, Germany
E-Mail: grassl@ira.uka.de

ABSTRACT

Owing to the high sensitivity of quantum mechanical systems to even small perturbations, means of error protection are essential for any computation or communication process based on quantum mechanics. After a short introduction to quantum registers and operations as well as quantum channels, different approaches to the problem of protecting quantum information are presented.

1. INTRODUCTION

The use of quantum mechanical systems opens new perspectives for both computation and communication purposes. On a quantum computer, large integers could be factored in polynomial time [1], threatening some public key cryptosystems like RSA. On the other hand, quantum mechanics allows secure key generation [2].

In all applications, the quantum mechanical systems must be protected against errors due to interactions with the environment. One approach to this task is based on encoding that either allows error detection and correction, or decouples the state of the system from the environment. Another class of techniques uses classical communication between the partners in order to establish the resources required for error-free quantum communication, or to allow a request for retransmission in case of failure.

2. QUANTUM BITS AND QUANTUM GATES

2.1. Quantum Registers

Classically, information is often represented by bits. A single bit takes either the value 0 or 1. In physical systems, 0 and 1 are represented by two different states of the system. These could be two different voltages, signals with two different frequencies, but also states on the quantum mechanical level, e. g., ground state and excited state of an electron of an atom or ion, the spin of a nucleus, or the polarization of photons. In Dirac notation, the two states are written as

$$\text{“0”} \mathrel{\hat{=}} |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \in \mathbb{C}^2 \quad \text{and} \quad \text{“1”} \mathrel{\hat{=}} |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \in \mathbb{C}^2.$$

In quantum mechanics, the principle of superposition allows a system to be simultaneously in different states. Mathematically, the state of the basic unit of quantum information, a *quantum bit* (or short *qubit*), is represented by the normalized linear combination

$$|q\rangle = \alpha|0\rangle + \beta|1\rangle \qquad \text{where } \alpha, \beta \in \mathbb{C},\ |\alpha|^2 + |\beta|^2 = 1.$$

The normalization condition stems from the fact that when extracting classical information from the quantum system by a measurement, the values 0 and 1 occur with probability $|\alpha|^2$ and $|\beta|^2$, resp.

Similar to classical registers, a quantum register is built by combining several qubits. Mathematically, this corresponds to the tensor product of two-dimensional vector spaces. Hence the state of a quantum register of length n could be any normalized complex linear combination of the 2^n mutually orthogonal basis states

$$|b_1\rangle \otimes \ldots \otimes |b_n\rangle =: |b_1 \ldots b_n\rangle = |\boldsymbol{b}\rangle \qquad \text{where } b_i \in \{0, 1\}.$$

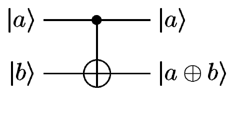
2.2. Quantum Gates

The laws of quantum mechanics say that any transformation on quantum systems is linear. Furthermore, in order to preserve the normalization any operation has to be unitary. Let us first consider operations involving only one qubit, i. e., one subsystem. Similar to the classical NOT gate, there is a quantum operation interchanging the states $|0\rangle$ and $|1\rangle$. But even on a single qubit, there is not only this “classical” operation. An important example for a non-classical operation on a single qubit is the Hadamard transformation given by

$$H := \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

Besides single qubit operations, the so-called controlled NOT gate ($CNOT$) plays an important rôle since any unitary operation on a 2^n-dimensional space can be implemented using only single qubit operations and $CNOT$ gates (see [3]). As a classical gate, the $CNOT$ gate corresponds to a gate with two inputs and two outputs. One of the inputs is copied to the first output, the second output is the XOR of the inputs. The transformation matrix of the $CNOT$ gate is given by:

$$CNOT := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$



On the right hand side, the notation for the $CNOT$ gate as a quantum circuit is given. Each of the horizontal lines (*wires*) corresponds to a qubit of the whole quantum register. The dot on the upper wire indicates that the transformation on the lower qubit (the target)—a NOT gate—is only applied when the state of the upper qubit (the control) is $|1\rangle$.

0-7803-5482-6/99/$10.00 ©2000 IEEE

3. QUANTUM CHANNELS

3.1. Open Quantum Systems

We assume that our quantum system interacts with an environment which is not or only partially accessible. Nevertheless, we can *model* the interaction by a unitary transformation $U_{\text{interaction}} = U_{\text{int}}$ on the Hilbert space formed by the system and its environment. Assuming that there is no prior entanglement of the system with the environment, the interaction operator reads as

$$|\psi\rangle_{\text{sys}} \otimes |\Psi\rangle_{\text{env}} \longmapsto U_{\text{interaction}} \left(|\psi\rangle_{\text{sys}} \otimes |\Psi\rangle_{\text{env}}\right).$$

After this interaction, the state need no longer be a tensor product. Since we cannot control the environment, we have to discard any information about the environment. This is mathematically reflected by *tracing out the environment*:

$$\begin{aligned}\rho_{\text{sys}} &= \operatorname{tr}_{\text{env}}\left(U_{\text{int}}\left(|\psi\rangle\langle\psi|_{\text{sys}} \otimes |\Psi\rangle\langle\Psi|_{\text{env}}\right) U_{\text{int}}^{\dagger}\right)\\ &= \sum_j A_j \left(|\psi\rangle\langle\psi|_{\text{sys}}\right) A_j^{\dagger}. \qquad (1)\end{aligned}$$

The state of our quantum system is now, in general, a mixed state given by the density operator ρ_{sys}. One interpretation of a mixed quantum state is that we have an ensemble of pure quantum states chosen according to a probability distribution. In our case, one can think of a measurement performed on the environment. Due to entanglement with the system, this may lead to different states of the system depending on the measurement outcome—but we do not know which state since the result of the measurement is discarded.

In order to model a quantum channel, we make use of equation (1). The disturbed quantum state ρ_{sys} can be expressed only in terms of the initial state $|\psi\rangle\langle\psi|_{\text{sys}}$ of the system and some interaction operators A_j which completely specify the channel.

3.2. Depolarizing and Erasure Channel

To illustrate the preceding, we consider two important quantum channels. Over a depolarizing channel [4], quantum information is transmitted undisturbed with probability $1-\varepsilon$, and it is replaced by a completely randomized quantum state with probability ε. A common assumption is that errors act independently on each qubit. In this case, for a single qubit equation (1) reads

$$\begin{aligned}\rho_{\text{sys}} &= (1-\varepsilon)\cdot|\psi\rangle\langle\psi|_{\text{sys}} + \varepsilon \cdot \mathbb{1}\\ &= (1-3/4\cdot\varepsilon)\, id\left(|\psi\rangle\langle\psi|_{\text{sys}}\right) id\\ &\quad +\varepsilon/4 \sum_{j=x,y,z} \sigma_j \left(|\psi\rangle\langle\psi|_{\text{sys}}\right)\sigma_j\end{aligned}$$

(where σ_x, σ_y, and σ_z are the *Pauli matrices*). For a small error probability ε, errors affecting a small number of qubits are more likely than errors involving a large number of qubits.

A related quantum channel is the quantum erasure channel [5]. Again, the quantum state is transmitted undisturbed with probability $1-\varepsilon$. In case of an error, the quantum state is replaced by a quantum state $|e\rangle$ that is orthogonal to all other quantum states. Equation (1) now reads

$$\rho_{\text{sys}} = (1-\varepsilon)\cdot|\psi\rangle\langle\psi|_{\text{sys}} + \varepsilon\cdot|e\rangle\langle e|.$$

Similar to classical erasures, the state $|e\rangle$ indicates that an error occurred, i. e., side-information about positions of errors is available for the decoding process. Note that by adding the state $|e\rangle$ we have increased the dimension of the Hilbert space of the system by one. Alternatively, we may use any state of the original space instead of $|e\rangle$ and describe the positions of errors by other means.

4. ENCODING TECHNIQUES

When quantum information has to be stored, there is no feed-back channel from the receiver to the sender. Then, information must be encoded in such a manner that possible errors can be corrected, or that no errors occur.

4.1. Quantum Error-Correcting Codes

Unlike classical information, unknown quantum information cannot be copied [6]. Therefore, the simple idea of a—say triple—repetition code does not work. Nevertheless, it is possible to encode quantum information in a subspace of a higher dimensional space such that error correction is possible. Following the first example of a quantum error-correcting code (QECC) of Shor [7], a theory of QECC has been developed [8].

The main idea of QECC is to find an orthogonal decomposition of a large Hilbert space into a smaller subspace where the information is stored—the code space—and so-called error spaces which are orthogonal images of the code space. Information about the error is obtained by means of a measurement projecting on one of these spaces. The measurement, however, does not yield information about the quantum information itself.

Surprisingly, there is a close connection to error correcting codes over finite fields [9, 10, 11]. Moreover, a lot of code families have their quantum counterpart, such as Reed-Muller codes [12], BCH codes [13], and Reed-Solomon codes [14]. For cyclic QECC, a great variety of encoding and decoding techniques exist, e. g., based on spectral techniques or on the quantum version of linear shift registers [15].

4.2. Error Free Subspaces

When more information about the interaction between the system and the environment is available, alternate techniques for protecting quantum information may be applicable. While QECC require an active recovery process after an error occurred, the idea of error free subspaces is to avoid errors. More precise, information is encoded in a subspace of the system on which the system/environment interaction acts trivially (or as a common phase factor). Obviously, a precise model of this interaction has to be known. For general errors, there need not be such an error free subspace, but there are subspaces that are unaffected by, e. g., strongly correlated errors [16, 17].

5. COMMUNICATION PROTOCOLS

Although it is not possible to transmit quantum information by classical information only—since this would allow to copy quantum states—, an additional communication channel for classical information is helpful as we will show below.

5.1. Teleportation

Astonishingly, quantum information can be transmitted by classical information when the two parties—say Alice and Bob—initially share an additional resource, a so-called EPR pair (see [18, 19] for the theory and [20] for experiments). The process of teleportation is reflected by the quantum circuits shown in Fig. 1.

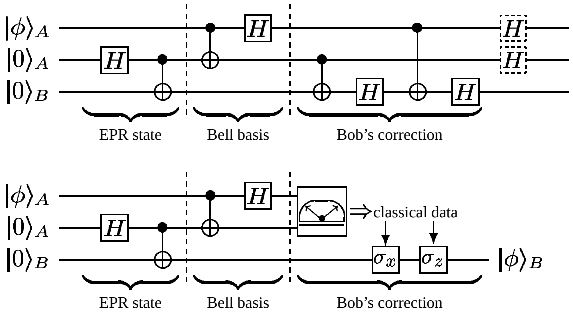


Figure 1: Quantum circuit for teleportation.

The upper circuit transforms the quantum state $|\phi\rangle|00\rangle$ into $|00\rangle|\phi\rangle$. The first part produces an EPR state $(|00\rangle + |11\rangle)/\sqrt{2}$ in the last two qubits. This may be done at any time before the communication. Then the first two qubits (of Alice) are transformed into the so-called Bell basis. The next operations are conditioned on the first two qubits and act on the last qubit (of Bob). The final Hadamard transforms on Alice's qubits reset them to the state $|0\rangle$. After the preparation of the EPR state, the only interactions between Alice's qubits and Bob's qubit are transformations that are conditioned on the first two qubits. It is now possible to measure Alice's qubits and transmit the—classical—outcome to Bob who performs the final operations according to the data received. This procedure is depicted in the lower circuit.

In summary, the transmission of one qubit has been replaced by the transmission of two classical bits, at the prize of initially sharing an EPR pair. Hence a quantum state must be sent anyhow, and this state is also subject to errors. However, this particular quantum state can be sent at any time before the actual communication.

5.2. Entanglement Purification and Quantum Repeaters

In order to send quantum information by teleportation, the parties need EPR pairs. If these EPR pairs are distributed over noisy quantum channels, the teleportation process is also noisy. It has been shown that it is possible to distill a small number of better EPR pairs starting from a supply of many EPR pairs [21]. This process of entanglement purification is sketched as follows. Both parties operate locally on their half of each EPR pair. Some of the qubits are measured, and the results of the measurement are communicated. Hence, in addition to the quantum channel for the distribution of the EPR pairs, a bi-directional classical channel is required. Based on the measurement results, some of the particles are discarded. This decreases the number of remaining noisy EPR pairs, but increases their quality. The final EPR pairs are used for teleporting the quantum state.

For quantum communication over larger distances, a scheme using quantum repeaters has been proposed and analyzed [22]. Again, the first phase of the protocol aims at improving the quality of EPR pairs to be used for teleportation in the second phase. Initially, EPR pairs are generated and purified between neighboring communication partners. Then, entanglement swapping is performed at the repeaters to establish EPR pairs between both neighbors. The idea of entanglement swapping is illustrated in Fig. 2. Initially, particles 1 and 2 resp. 3 and 4 are in EPR states. Performing a Bell measurement on particles 2 and 3 results in an EPR state between particles 1 and 4, without any direct interaction between these particles.

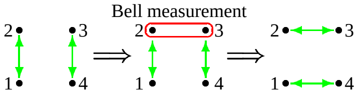


Figure 2: Entanglement swapping.

The whole process is repeated several rounds, where in each round the distance between the communication partners increases. The total number of rounds is logarithmic in the number of repeaters since they are organized as a binary tree (see Fig. 3).

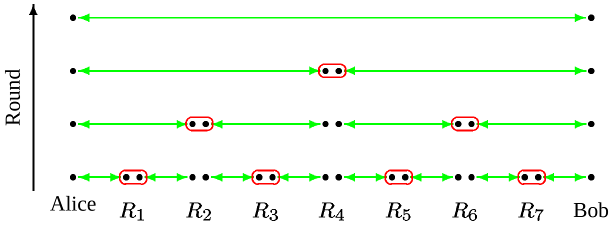


Figure 3: Scheme for generating EPR pairs between Alice and Bob using repeaters R_i. Entanglement purification is used to increase the quality of the EPR pairs (along the arrows). Entanglement swapping (indicated by ovals) is used to increase the distance between the EPR pairs.

5.3. Other Protocols

A common feature of all error control techniques described so far is that there is a non-zero probability of failure. Furthermore, it cannot be detected whether the correction step was successful. For particular systems, it is possible to use a quantum communication protocol that achieves perfect transmission [23]. Before sending the quantum states, the sender prepares an auxiliary state that has the function of a backup. After the quantum state was sent, it is possible to detect whether the transmission was successful. If not, the backup system can be used to restore the original state, followed by another attempt to transmit the quantum state. For this scheme, it is guaranteed that the transmission is perfect, at the cost that the number of attempts until success is not fixed.

6. FINAL REMARKS

This list of error control techniques for quantum systems is, of course, not complete. We have rather aimed at presenting several approaches which differ in their prerequisites, e. g., whether an additional channel for communication of classical information is available or not.

Most of the literature on quantum computation and communication can be found at the Los Alamos National Laboratory archive `http://xxx.lanl.gov/archive/quant-ph`.

7. REFERENCES

[1] Peter W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms", in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*. Nov. 1994, pp. 124–134, IEEE Computer Society Press, see also LANL preprint quant-ph/9508027.

[2] Charles H. Bennett and Gilles Brassard, "An Update on Quantum Cryptography", in *Advances in Cryptology: Proceedings of CRYPTO 84*, G. R. Blakley and David Chaum, Eds., New York, 19.–22.Aug. 1984, vol. 196 of *Lecture Notes in Computer Science*, pp. 475–480, Springer.

[3] Adriano Barenco, Charles H. Bennett, Richard Cleve, David P. DiVincenzo, Norman Margolus, Peter Shor, Tycho Sleator, John A. Smolin, and Harald Weinfurter, "Elementary gates for quantum computation", *Physical Review A*, vol. 52, no. 5, pp. 3457–3467, Nov. 1995, see also LANL preprint quant-ph/9503016.

[4] Charles H. Bennett, David P. DiVincenzo, John A. Smolin, and William K. Wootters, "Mixed State Entanglement and Quantum Error Correction", *Physical Review A*, vol. 54, no. 5, pp. 3824–3851, Nov. 1996.

[5] Markus Grassl, Thomas Beth, and Thomas Pellizzari, "Codes for the Quantum Erasure Channel", *Physical Review A*, vol. 56, no. 1, pp. 33–38, July 1997, see also LANL preprint quant-ph/9610042.

[6] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned", *Nature*, vol. 299, no. 5886, pp. 802–803, 28. Oct. 1982.

[7] Peter W. Shor, "Scheme for reducing decoherence in quantum computer memory", *Physical Review A*, vol. 52, no. 4, pp. R2493–R2496, 1995.

[8] Emanuel Knill and Raymond Laflamme, "Theory of quantum error-correcting codes", *Physical Review A*, vol. 55, no. 2, pp. 900–911, Feb. 1997, see also LANL preprint quant-ph/9604034.

[9] A. Robert Calderbank, Eric. M. Rains, P. W. Shor, and Neil J. A. Sloane, "Quantum Error Correction Via Codes over GF(4)", *IEEE Transactions on Information Theory*, vol. IT-44, no. 4, pp. 1369–1387, July 1998, see also LANL preprint quant-ph/9608006.

[10] Thomas Beth and Markus Grassl, "The Quantum Hamming and Hexacodes", *Fortschritte der Physik*, vol. 46, no. 4–5, pp. 459–491, 1998.

[11] Markus Grassl and Thomas Beth, "Relations between Classical and Quantum Error-Correcting Codes", in *Workshop "Physik und Informatik"*, Werner Kluge, Ed., DPG-Frühjahrstagung, Heidelberg, 1999, pp. 45–58.

[12] Andrew Steane, "Quantum Reed-Muller Codes", *IEEE Transactions on Information Theory*, vol. IT-45, no. 5, pp. 1701–1703, July 1999, see also LANL preprint quant-ph/9608026.

[13] Markus Grassl and Thomas Beth, "Quantum BCH Codes", in *Proceedings X. International Symposium on Theoretical Electrical Engineering*, W. Mathis and T. Schindler, Eds., Magdeburg, Sept. 6–9, 1999, Universität Magdeburg, pp. 207–212.

[14] Markus Grassl, Willi Geiselmann, and Thomas Beth, "Quantum Reed-Solomon Codes", in *Proceedings Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (AAECC-13)*, Marc Fossorier, Hideki Imai, Shu Lin, and Alain Poli, Eds., Honolulu, Hawaii, November 15-19 1999, vol. 1719 of *Lecture Notes in Computer Science*, pp. 231–244, Springer, see also LANL preprint quant-ph/9910059.

[15] Markus Grassl and Thomas Beth, "Cyclic Quantum Error-Correcting Codes and Quantum Shift Registers", LANL preprint quant-ph/9910061, 1999.

[16] P. Zanardi and M. Rasetti, "Noiseless Quantum Codes", *Physical Review Letters*, vol. 79, no. 17, pp. 3306–3309, Oct. 27 1997, see also LANL preprint quant-ph/9705044.

[17] D. A. Lidar, I. L. Chuang, and K. B. Whaley, "Decoherence-Free Subspaces for Quantum Computation", *Physical Review Letters*, vol. 81, no. 12, pp. 2594–2597, 21. Sept. 1998.

[18] Charles H. Bennett and Stephen J. Wiesner, "Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states", *Physical Review Letters*, vol. 69, no. 20, pp. 2881, 16. Nov. 1992.

[19] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richards Jozsa, Asher Peres, and William K. Wootters, "Teleporting an Unknown Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels", *Physical Review Letters*, vol. 70, no. 13, pp. 1895–1899, 29. Mar. 1993.

[20] Harald Weinfurter, Dik Bouwmeester, Thomas Jennewein, Jian-Wei Pan, Gregor Weihs, and Anton Zeilinger, "Quantum Communication and Entanglement", in *Proceedings ISCAS 2000*, 2000.

[21] Charles H. Bennett, Gilles Brassard, Sandu Popescu, Benjamin Schumacher, John A. Smolin, and William K. Wootters, "Purification of Noisy Entanglement and Faithful Teleportation via Noisy Channels", *Physical Review Letters*, vol. 76, no. 5, pp. 722–725, 28. Jan. 1996.

[22] W. Dür, H.-J. Briegel, J. I. Cirac, and P. Zoller, "Quantum repeaters based on entanglement purification", *Physical Review A*, vol. 59, no. 1, pp. 169–181, Jan. 1999, see also LANL preprint quant-ph/9803056.

[23] S. J. van Enk, J. I. Cirac, and P. Zoller, "Ideal Quantum Communication over Noisy Channels: A Quantum Optical Implementation", *Physical Review Letters*, vol. 78, no. 22, pp. 4293–4296, 2. June 1997.