Vol. 93 (1998) ACTA PHYSICA POLONICA A No. 1

Proceedings of the International Conference "Quantum Optics IV", Jaszowiec, Poland, 1997

AGAINST QUANTUM NOISE

A. EKERT* AND CH. MACCHIAVELLO†

Clarendon Laboratory, University of Oxford, Oxford OX1 3PU, U.K.

This is a brief description of how to protect quantum states from dissipation and decoherence that arise due to uncontrolled interactions with the environment. We discuss recoherence and stabilization of quantum states based on two techniques known as "symmetrization" and "quantum error correction". We illustrate our considerations with the most popular quantum-optical model of the system–environment interaction, commonly used to describe spontaneous emission, and show the benefits of quantum error correction in this case.

PACS numbers: 89.70.+c, 03.65.Bz

1. Introduction

Suppose we want to transmit or store a block of l qubits (i.e. two-state quantum systems) in a noisy environment. Here "noisy" means that each qubit may become entangled with the environment. Thus due to spurious interactions with the environment the actual state of the l qubits, described by a density operator $\rho(t)$, will differ from the original state $|\Psi\rangle$. This deviation can be quantified by the fidelity

$$F(t) = \langle\Psi|\rho(t)|\Psi\rangle = 1 - \epsilon(t). \tag{1}$$

In order to maximize this fidelity we may try all sorts of tricks ranging from the most obvious one, i.e. isolating the qubits from the environment to more sophisticated methods such as "symmetrization" [1, 2], "purification" [3, 4], and "quantum error correction" [5]. The last method seems to be the most popular one at the moment and relies on encoding the state of l qubits into a set of n qubits and trying to disentangle a certain number of qubits from the environment after some period of time. In the following we describe, very briefly, how some of these techniques work.

We will assume that in the block of l qubits each qubit is coupled to a different environment. This is a perfectly reasonable assumption, which is valid if the coherence length of the environment/reservoir is less than the spatial separation between the qubits [6], and introduces a great deal of simplifications to the

*ekert@physics.ox.ac.uk.

†chiara@mildred.physics.ox.ac.uk. Also at: Dipartimento di Fisica Generale "A. Volta", Via Bassi 6, 27100 Pavia, Italy.

calculations. Basically it allows us to view any dissipation of l qubits as a set of independent dissipations of l single qubits (i.e. we ignore collective phenomena such as superradiance etc.).

The qubit–environment interaction leads to the qubit–environment entanglement, which in its most general form is given by

$$|0\rangle|R\rangle \longrightarrow |0\rangle|R_{00}(t)\rangle + |1\rangle|R_{01}(t)\rangle, \tag{2}$$

$$|1\rangle|R\rangle \longrightarrow |0\rangle|R_{10}(t)\rangle + |1\rangle|R_{11}(t)\rangle, \tag{3}$$

where states of the environment $|R\rangle$ and $|R_{ij}\rangle$ are neither normalised nor orthogonal to each other (thus we have to take additional care at the end of our calculations and normalise the final states). The r.h.s. of the formulae above can also be written in a matrix form as

$$\begin{pmatrix} |R_{00}\rangle & |R_{01}\rangle \\ |R_{10}\rangle & |R_{11}\rangle \end{pmatrix} \begin{pmatrix} |0\rangle \\ |1\rangle \end{pmatrix}, \tag{4}$$

and the 2×2 matrix can be subsequently decomposed into some basis matrices e.g. into the unity and the Pauli matrices

$$|R_0\rangle 1 + |R_1\rangle\sigma_x + \mathrm{i}|R_2\rangle\sigma_y + |R_3\rangle\sigma_z, \tag{5}$$

where $|R_0\rangle = (|R_{00}\rangle + |R_{11}\rangle)/2$, $|R_3\rangle = (|R_{00}\rangle - |R_{11}\rangle)/2$, $|R_1\rangle = (|R_{01}\rangle + |R_{10}\rangle)/2$, and $|R_2\rangle = (|R_{01}\rangle - |R_{10}\rangle)/2$. Thus the qubit initially in state $|\Psi\rangle$ will evolve as

$$|\Psi\rangle|R\rangle \longrightarrow \sum_{i=0}^{3} \sigma_i|\Psi\rangle|R_i\rangle \tag{6}$$

becoming entangled with the environment (we have relabelled the unity operator and the Pauli matrices $\{1, \sigma_x, \sigma_y, \sigma_z\}$ respectively as $\{\sigma_0, \sigma_1, \sigma_2, \sigma_3\}$). Its fidelity with respect to the initial state $|\Psi\rangle$ evolves as

$$F(t) = \sum_{i,j} \langle\Psi|\sigma_i|\Psi\rangle\langle\Psi|\sigma_j|\Psi\rangle\langle R_j(t)|R_i(t)\rangle. \tag{7}$$

The formula (6) describes how the environment affects any quantum state of a qubit and shows that a general qubit–environment interaction can be expressed as a superposition of unity and Pauli operators acting on the qubit. As we will see in the following, in the language of error correcting codes this means that the qubit state is evolved into a superposition of an error-free component and three erroneous components, with errors of the σ_x, σ_y and σ_z type.

We can carry on this description even if the qubit itself is not in a pure state $|\Psi\rangle$ but is entangled with some other qubits. For example, if in a three qubit register initially in state $\left|\widetilde{\Psi}\right\rangle = |0\rangle|0\rangle|0\rangle - |1\rangle|1\rangle|1\rangle$ the second qubit interacted with its environment then the state of the register at some time t is given by

$$\sum_{i=0}^{3} \sigma_i^{(2)} \left|\widetilde{\Psi}\right\rangle |R_i(t)\rangle = \sum_{i=0}^{3} [|0\rangle(\sigma_i|0\rangle)|0\rangle - (|1\rangle(\sigma_i|1\rangle)|1\rangle]|R_i(t)\rangle, \tag{8}$$

where the superscript (2) reminds us that the Pauli operators act only on the second qubit. We can then say that the second qubit was affected by quantum errors which are represented by the Pauli operators σ_i. Errors affecting classical

bits can only change their binary values ($0 \leftrightarrow 1$), in contrast quantum errors operators σ_i acting on qubits can change their binary values (σ_x), their phases (σ_z) or both (σ_y).

In general, a batch of n qubits initially in some state $\left|\widetilde{\Psi}\right\rangle$, each of them interacting with different environments, will evolve as

$$\prod_{k=1}^{n}\sum_{i=0}^{3}\sigma_i^{(k)}\left|\widetilde{\Psi}\right\rangle\left|R_i^{(k)}(t)\right\rangle, \tag{9}$$

namely multiple errors of the form $\sigma_i \otimes \sigma_j \cdots \otimes \sigma_k$ may occur, affecting several qubits at the same time.

So much about unwelcome dissipation, what about remedies?

2. Stabilization via symmetrization

The first proposed remedy was based on a symmetrization procedure [1]. The basic idea is as follows. Suppose you have a quantum system, you prepare it in some initial state $|\Psi_i\rangle$ and you want to implement a prescribed unitary evolution $|\Psi(t)\rangle$ or simply you want to preserve $|\Psi_i\rangle$ for some period of time t. Now, suppose that instead of a single system you can prepare R copies of $|\Psi_i\rangle$ and subsequently you can project the state of the combined system on the symmetric subspace, i.e. the subspace containing all states which are invariant under any permutation of the subsystems. The claim is that frequent projections on the symmetric subspace will reduce errors induced by the environment. The intuition behind this concept is based on the observation that a prescribed error-free storage or evolution of the R independent copies starts in the symmetric subspace and should remain in that subspace. Therefore, since the error-free component of any state always lies in the symmetric subspace, upon successful projection it will be unchanged and part of the error will have been removed. Note however that the projected state is generally not error-free since the symmetric subspace contains states which are not of the simple product form $|\psi\rangle|\psi\rangle\ldots|\psi\rangle$. Nevertheless it has been shown that the error probability will be suppressed by a factor of $1/R$ [2].

We illustrate here this effect in the simplest case of two qubits. The projection into the symmetric subspace is performed in this case by introducing the symmetrization operator

$$S = \frac{1}{2}(P_{12} + P_{21}), \tag{10}$$

where P_{12} represents the identity and P_{21} the permutation operator which exchanges the states of the two qubits. The symmetric-projection of a pure state $|\Psi\rangle$ of two qubits is just $S|\Psi\rangle$, which is then renormalised to unity. It follows that the induced map on mixed states of two qubits (including renormalization) is

$$\rho_1 \otimes \rho_2 \longrightarrow \frac{S(\rho_1 \otimes \rho_2)S^\dagger}{\mathrm{Tr}S(\rho_1 \otimes \rho_2)S^\dagger}. \tag{11}$$

The state of either qubit separately is then obtained by partial trace over the other qubit.

Consider for example the symmetric projection of $\rho \otimes \rho$ followed by renormalization and partial trace (over either qubit) to obtain the final state ρ_s of one

qubit, given that the symmetric-projection was successful. A direct calculation based on (11) yields

$$\rho \mapsto \rho_s = \frac{\rho + \rho^2}{\mathrm{Tr}(\rho + \rho^2)}. \tag{12}$$

For any mixed state ξ of a qubit the expression $\mathrm{Tr}\xi^2$ provides a measure of the purity of the state, ranging from $\frac{1}{4}$ for the completely mixed state $I/2$ (where I is the unit operator) to 1 for any pure state. From (12) we get

$$\mathrm{Tr}\rho_s^2 > \mathrm{Tr}\rho^2 \tag{13}$$

so that ρ_s is *purer* than ρ. This illustrates that successful projection of a mixed state into the symmetric subspace tends to enhance the purity of the individual systems.

To be more specific, let us assume now that the two copies are initially prepared in pure state $\rho_0 = |\Psi\rangle\langle\Psi|$ and that they interact with independent environments. After some short period of time δt the state of the two copies $\rho^{(2)}$ will have undergone an evolution

$$\rho^{(2)}(0) = \rho_0 \otimes \rho_0 \longrightarrow \rho^{(2)}(\delta t) = \rho_1 \otimes \rho_2, \tag{14}$$

where $\rho_i = \rho_0 + \varrho_i$ for some Hermitian traceless ϱ_i. We will retain only terms of first order in the perturbations ϱ_i so that the overall state at time δt is

$$\rho^{(2)} = \rho_0 \otimes \rho_0 + \varrho_1 \otimes \rho_0 + \rho_0 \otimes \varrho_2 + \mathrm{O}(\varrho_1 \varrho_2). \tag{15}$$

We can calculate the average purity of the two copies before symmetrization by calculating the average trace of the squared states

$$\frac{1}{2}\sum_{i=1}^{2} \mathrm{Tr}[(\rho_0 + \varrho_i)^2] = 1 + 2\mathrm{Tr}(\rho_0 \tilde{\varrho}), \tag{16}$$

where $\tilde{\varrho} = \frac{1}{2}(\varrho_1 + \varrho_2)$. Note that $\mathrm{Tr}(\rho_0\tilde{\varrho})$ is negative, so that the expression above does not exceed 1. After symmetrization each qubit is in state

$$\rho_s = [1 - \mathrm{Tr}(\rho_0\tilde{\varrho})]\rho_0 + \frac{1}{2}\tilde{\varrho} + \frac{1}{2}(\rho_0\tilde{\varrho} + \tilde{\varrho}\rho_0) \tag{17}$$

and has purity

$$\mathrm{Tr}(\rho_s^2) = 1 + \mathrm{Tr}(\rho_0\tilde{\varrho}). \tag{18}$$

Since $\mathrm{Tr}\rho_s^2$ is closer to 1 than (16), the resulting symmetrised system ρ_s is left in a purer state.

Let us now see how the fidelity changes by applying the symmetrization procedure. The average fidelity before symmetrization is

$$F_{bs} = \frac{1}{2}\sum_i \langle\Psi|\rho_0 + \varrho_i|\Psi\rangle = 1 + \langle\Psi|\tilde{\varrho}|\Psi\rangle, \tag{19}$$

while after successful symmetrization it takes the form

$$F_{as} = \langle\Psi|\rho_s|\Psi\rangle = 1 + \frac{1}{2}\langle\Psi|\tilde{\varrho}|\Psi\rangle. \tag{20}$$

The state after symmetrization is therefore closer to the initial state ρ_0.

For the generic case of R copies the purity of each qubit after symmetrization is given by [2]

$$\mathrm{Tr}(\rho_s^2) = 1 + 2\frac{1}{R}\mathrm{Tr}(\rho_0\tilde{\varrho}), \tag{21}$$

where now $\tilde{\varrho} = \frac{1}{R}\sum_{i=1}^{R}\varrho_i$, and the fidelity takes the form

$$\langle\Psi|\rho_s|\Psi\rangle = 1 + \frac{1}{R}\mathrm{Tr}(\rho_0\tilde{\varrho}). \tag{22}$$

Formulae (21) and (22) must be compared with the corresponding ones before symmetrization, i.e. (16) and (19). As we can see, ρ_s approaches the unperturbed state ρ_0 as R tends to infinity. Thus by choosing R sufficiently large and the rate of symmetric projection sufficiently high, the residual error at the end of a computation can, in principle, be controlled to lie within any desired small tolerance.

The efficiency of the symmetrization procedure depends critically on the probability that the state of the R qubits is successfully projected into the symmetric subspace. It has been shown that if the projections are done frequently enough, then the cumulative probability that they all succeed can be made as close as desired to unity. This is a consequence of the fact that the fidelity of the state of the R computers with respect to the corresponding error-free state for small times δt has a parabolic behaviour (see Sec. 5). Therefore the probability of successful projection, which is unity at the initial time, begins to change only to second order in time. If we project n times per unit time interval, i.e. we choose the time interval between two subsequent projections $\delta t = 1/n$, then the cumulative probability that all projections in one unit time interval succeed is given by

$$[1 - k(\delta t)^2]^n = \left(1 - \frac{k}{n^2}\right)^n \to 1 \quad \text{as} \quad n \to \infty. \tag{23}$$

Here k is a constant depending on the rate of rotation of the state out of the symmetric subspace. This effect is known as the "quantum watch-dog effect" or the "quantum Zeno effect".

3. Quantum encoding and decoding

The idea of protecting information via encoding and decoding lies at the foundations of the classical information theory. It is based on a clever use of redundancy during the data storage or transmission. For example, if the probability of error (bit flip) during a single bit transmission via a noisy channel is p and each time we want to send bit value 0 or 1 we can encode it by a triple repetition i.e. by sending 000 or 111. At the receiving end each triplet is decoded as either zero or one following the majority rule — more zeros means 0, more ones means 1. This is the simplest error correcting protocol which allows to correct up to one error.

In the triple repetition code the signalled bit value is recovered correctly both when there was no error during the transmission of the three bits, which happens with probability $(1-p)^3$, and when there was one error at any of the three locations, which happens with probability $3p(1-p)^2$. Thus the probability of the correct transmission (up to the second order in p) is $1-3p^2$ i.e. the probab-

ility of error is now $3p^2$, which is much smaller when compared with the probability of error without encoding and decoding p ($p \ll 1$). This way we can trade the probability of error in the signalled message for a number of transmissions via the channel. In our example the reduction of the error rate from p to $3p^2$ required to send three times more bits. If sending each bit via the channel costs us money we have to decide what we treasure more, our bank account or our infallibility. The triple repetition code encodes one bit into three bits and protects against one error, in general we can construct codes that encode l bits into n bits and protect against t errors. The best codes, of course, are those which for a fixed value l minimize n and maximize t.

Quantum error correction which protects quantum states is a little bit more sophisticated simply because the bit flip is not the only "quantum error" which may occur, as we have seen in the previous sections. Moreover, the decoding via the majority rule does not usually work because it may involve measurements which destroy quantum superpositions. Still, the triple repetition code is a good starting point to investigate quantum codes and even to construct the simplest ones.

The simplest interesting case of the most general qubit–environment evolution (3) is the case of decoherence [7] where the environment effectively acts as a measuring apparatus

$$|0\rangle|R\rangle \longrightarrow |0\rangle|R_{00}(t)\rangle, \tag{24}$$

$$|1\rangle|R\rangle \longrightarrow |1\rangle|R_{11}(t)\rangle. \tag{25}$$

Following our discussion in Sec. 1 we can see that this model leads only to dephasing errors of the σ_z type. It turns out that a phase flip can be handled almost in the same way as a classical bit flip. Again, consider the following scenario: we want to store, in a computer memory, one qubit in an *unknown* quantum state of the form $\alpha|0\rangle + \beta|1\rangle$ and we know that any single qubit which is stored in a register may, with a small probability p, undergo a decoherence type entanglement with an environment (Eq. (25)); in particular

$$(\alpha|0\rangle + \beta|1\rangle)|R\rangle \longrightarrow \alpha|0\rangle|R_{00}\rangle + \beta|1\rangle|R_{11}\rangle. \tag{26}$$

Let us now show how to reduce the probability of decoherence to be of the order p^2.

Before we place the qubit in the memory register we *encode* it: we can add two qubits, initially both in state $|0\rangle$, to the original qubit and then perform an encoding unitary transformation

$$|000\rangle \longrightarrow |C_0\rangle = (|0\rangle + |1\rangle)(|0\rangle + |1\rangle)(|0\rangle + |1\rangle), \tag{27}$$

$$|100\rangle \longrightarrow |C_1\rangle = (|0\rangle - |1\rangle)(|0\rangle - |1\rangle)(|0\rangle - |1\rangle), \tag{28}$$

generating state $\alpha|C_0\rangle + \beta|C_1\rangle$. Now, suppose that only the second stored qubit was affected by decoherence and became entangled with the environment

$$\alpha(|0\rangle + |1\rangle)(|0\rangle|R_{00}\rangle + |1\rangle|R_{11}\rangle)(|0\rangle + |1\rangle)$$

$$+\beta(|0\rangle - |1\rangle)(|0\rangle|R_{00}\rangle - |1\rangle|R_{11}\rangle)(|0\rangle - |1\rangle), \tag{29}$$

which, following Eq. (8), can be written as

$$(\alpha|C_0\rangle + \beta|C_1\rangle)|R_0\rangle + \sigma_z^{(2)}(\alpha|C_0\rangle + \beta|C_1\rangle)|R_3\rangle. \tag{30}$$

If vectors $|C_0\rangle$, $|C_1\rangle$, $\sigma_z^{(k)}|C_0\rangle$, and $\sigma_z^{(k)}|C_1\rangle$ are orthogonal to each other we can try to perform a measurement on the qubits and project their state either on the state $\alpha|C_0\rangle + \beta|C_1\rangle$ or on the orthogonal one $\sigma_z^{(2)}(\alpha|C_0\rangle + \beta|C_1\rangle)$. The first case yields the proper state right away, the second one requires one application of σ_z to compensate for the error. In this simple case one can even find a direct unitary operation which can fix all one qubit phase flips regardless their location. For example the transformation

$$\begin{aligned} |000\rangle &\to |000\rangle \qquad |100\rangle \to |011\rangle \\ |001\rangle &\to |001\rangle \qquad |101\rangle \to |110\rangle \\ |010\rangle &\to |010\rangle \qquad |110\rangle \to |101\rangle \\ |011\rangle &\to |111\rangle \qquad |111\rangle \to |100\rangle \end{aligned} \tag{31}$$

corrects any single bit flip $0 \leftrightarrow 1$ and when applied in the conjugate basis ($|0'\rangle = |0\rangle + |1\rangle$, $|1'\rangle = |0\rangle - |1\rangle$) it corrects any single phase flip (the bit flips become phase flips in the new basis). The snag is that using the scheme above we can correct up to one phase error σ_z or we can go to a conjugate basis and the same scheme will correct up to one amplitude error σ_x but it cannot correct up to one general error, be it amplitude or phase.

To fix this problem Peter Shor in 1995 combined the phase and the amplitude correction schemes into one constructing the following nine qubit code [5]:

$$|0\rangle \to \frac{1}{2\sqrt{2}}(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle) \tag{32}$$

$$|1\rangle \to \frac{1}{2\sqrt{2}}(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle). \tag{33}$$

This code involves double encoding, first in base $|0\rangle$ and $|1\rangle$ and then in base $|0'\rangle$ and $|1'\rangle$, and it allows to correct up to one either bit or phase flip. It turns out that the ability to correct both amplitude and phase errors suffices to correct any error due to entanglement with the environment. In other words the action of the environment on qubits can be viewed in terms of bit and phase flips.

4. Quantum error-correcting codes

The original nine qubit code of Shor can be further simplified. It has been shown that a five qubit code suffices to correct a single error of any type. Let us now specify the conditions for the existence of quantum error-correcting codes.

We say we can correct a single error $\sigma_i^{(k)}$ (where $i = 0 \ldots 3$ refers to the type of error) if we can find a transformation such that it maps all states with a single error $\sigma_i^{(k)} \left|\widetilde{\Psi}\right\rangle$ into the proper error-free state $\left|\widetilde{\Psi}\right\rangle$:

$$\sigma_i^{(k)} \left|\widetilde{\Psi}\right\rangle \longrightarrow \left|\widetilde{\Psi}\right\rangle. \tag{34}$$

To make it unitary we may need an ancilla

$$\sigma_i^{(k)} \left|\widetilde{\Psi}\right\rangle |0\rangle \longrightarrow \left|\widetilde{\Psi}\right\rangle |a_i^k\rangle. \tag{35}$$

For encoded basis states of a single qubit $|C_0\rangle$ and $|C_1\rangle$ this implies [8]

$$A_k|C_0\rangle|0\rangle \longrightarrow |C_0\rangle|a_k\rangle \tag{36}$$

$$A_k|C_1\rangle|0\rangle \longrightarrow |C_1\rangle|a_k\rangle, \tag{37}$$

where A_k denotes all the possible types of independent errors affecting at most one of the qubits. The above requirement leads to the following unitarity conditions:

$$\langle C_0|A_k^\dagger A_l|C_0\rangle = \langle C_1|A_k^\dagger A_l|C_1\rangle = \langle a_k|a_l\rangle, \tag{38}$$

$$\langle C_0|A_k^\dagger A_l|C_1\rangle = 0. \tag{39}$$

The above conditions are straightforwardly generalised to an arbitrary t error correcting code, which corrects any kind of transformations affecting up to t qubits in the encoded state. In this case the operators A_k are all the possible independent errors affecting up to t qubits, namely operators of the form $\Pi_{i=1}^{t}\sigma_i$ acting on t different qubits. In the case of the so-called "nondegenerate codes" Eq. (38) takes the simple form [9]

$$\langle C_0|A_k^\dagger A_l|C_0\rangle = \langle C_1|A_k^\dagger A_l|C_1\rangle = 0. \tag{40}$$

This condition requires that all states which are obtained by affecting up to t qubits in the encoded states are all orthogonal to each other, and therefore distinguishable. This ensures that by performing suitable projections of the encoded state we are able to detect the kind of error which occurred and "undo" it to recover the desired error-free state. Condition (40), even if more restrictive than (38), is particularly useful because it allows to establish bounds on the resources needed in order to have efficient nondegenerate codes. Let us assume that the initial state of l qubits is encoded in a redundant Hilbert space of n qubits. If we want to encode 2^l input basis states and correct up to t errors we must choose the dimension of the encoding Hilbert space 2^n such that all the necessary orthogonal states can be accomodated. According to Eq. (40), the total number of orthogonal states that we need in order to be able to correct i errors of the three types σ_x, σ_y and σ_z in an n-qubit state is $3^i \begin{pmatrix} n \\ i \end{pmatrix}$ (this is the number of different ways in which the errors can occur). The argument based on counting orthogonal states then leads to the following condition:

$$2^l \sum_{i=0}^{t} 3^i \begin{pmatrix} n \\ i \end{pmatrix} \leq 2^n. \tag{41}$$

Equation (41) is the quantum version of the Hamming bound for classical error--correcting codes [10]; given l and t it provides a lower bound on the dimension of the encoding Hilbert space for nondegenerate codes. Let us mention that an explicit construction for quantum codes for some values (l, n, t) which saturate the quantum Hamming bound has been provided [11]. It is interesting that this bound has not been beaten so far by degenerate codes[‡].

[‡]In fact, during the "Workshop in Quantum Computation" in Torino in summer 1996 the authors offered a good bottle of Barolo wine to the first person who can construct quantum error correction codes which encode l qubits into n qubits, correct perfectly up to t errors, and which violate the quantum Hamming bound (41).

The quantum version of the classical Gilbert–Varshamov bound [10] can be also obtained, which gives an upper bound on the dimension of the encoding Hilbert space for optimal non degenerate codes

$$2^l \sum_{i=0}^{2t} 3^i \binom{n}{i} \geq 2^n. \tag{42}$$

This expression can be proved from the observation that in the 2^n dimensional Hilbert space with a maximum number of encoded basis vectors (or code-vectors) $|C^k\rangle$ any vector which is orthogonal to $|C^k\rangle$ (for any k) can be reached by applying up to $2t$ error operations of σ_x, σ_y, and σ_z type to any of the 2^l encoded basis vectors. Clearly all vectors which cannot be reached in the $2t$ operations can be added to the encoded basis states $|C^k\rangle$ as all the vectors into which they can be transformed by applying up to t amplitude and/or phase transformations are orthogonal to all the others. This situation cannot happen because we have assumed that the number of code-vectors is maximal. Thus the number of orthogonal vectors that can be obtained by performing up to $2t$ transformations on the code-vectors must be at least equal to the dimension of the encoding Hilbert space.

It follows from Eq. (41) that a one-bit quantum error correcting code to protect a single qubit ($l = 1$, $t = 1$) requires at least 5 encoding qubits and, according to Eq. (42), this can be achieved with less than 10 qubits. Indeed, Shor's nine qubit code can be simplified to the seven qubit code [12], and ultimately to the quantum Hamming bound [8, 13]. We will consider explicitly one form of the five qubit code in Sec. 6.

The asymptotic form of the quantum Hamming bound (41) in the limit of large n is given by

$$\frac{l}{n} \leq 1 - \frac{t}{n} \log_2 3 - H\left(\frac{t}{n}\right), \tag{43}$$

where H is the entropy function $H(x) = -x \log_2 x - (1-x)\log_2(1-x)$. The corresponding asymptotic form for the quantum Gilbert–Varshamov bound (42) is

$$\frac{l}{n} \geq 1 - \frac{2t}{n} \log_2 3 - H\left(\frac{2t}{n}\right). \tag{44}$$

As we can see from Eq. (43), in quantum error correction there is an upper bound on the error rate t/n which a code can tolerate. In fact, differently from the classical case, where any arbitrary error rate can be corrected by a suitable code, in the quantum world the ratio t/n cannot be larger than 0.18929 for nondegenerate codes.

5. System–environment dynamics

In order to provide a tangible illustration of some abstract ideas discussed in the text we have picked up the most popular quantum-optical model of dissipation commonly used to describe spontaneous emission. A two-level atom, with two energy eigenstates $|0\rangle$ and $|1\rangle$ separated by $\hbar\omega_0$, interacting with an environment modelled as a set of quantised harmonic oscillators, e.g. a set of quantised modes of radiation with frequencies ω_m. The Hamiltonian of the combined system

$H = H_0 + V$ includes both the free evolution of the qubit and the environment. The free evolution Hamiltonian is given by

$$H_0 = \hbar\omega_0|1\rangle\langle 1| + \sum_m \hbar\omega_m a_m^\dagger a_m, \tag{45}$$

where a_m and $a_m^\dagger$ represent the annihilation and creation operators of the radiation mode of frequency ω_m. The interaction (in the rotating wave approximation) is described by

$$V = \sum_m \lambda_m|0\rangle\langle 1|a_m^\dagger + \lambda_m^*|1\rangle\langle 0|a_m, \tag{46}$$

where λ_m is the coupling constant between the qubit and the mode of frequency ω_m.

In order to find the time evolution of the relative states of the environment $|R_i(t)\rangle$ we need some knowledge about the qubit–environment interaction. Let us then have a closer look at a dissipative dynamics in our model of a qubit coupled to a continuum of field modes or harmonic oscillators. If all the oscillators in the environment are in their ground states and the qubit is initially prepared in state $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$ then the dynamics described by the Hamiltonian $H = H_0 + V$ does not affect state $|0\rangle$. It is state $|1\rangle$ which undergoes a decay. Let us then consider a case when the initial state of the combined system (qubit+environment) is

$$|\phi_i\rangle = |1\rangle(|0\rangle_1|0_2\rangle \ldots |0\rangle_f \ldots |0\rangle_{\max}), \tag{47}$$

meaning the qubit is in state $|1\rangle$ and all the harmonic oscillators in their ground states $|0\rangle$ (we will denote the state where all harmonic oscillators are in the ground state as the vacuum $|\mathbf{0}\rangle$). Possible final states of the combined system are

$$|\phi_f\rangle = |0\rangle(|0\rangle_1|0\rangle_2 \ldots |1\rangle_f \ldots |0\rangle_{\max}), \tag{48}$$

where the qubit decayed to state $|0\rangle$ and one of the harmonic oscillators got excited. Let us note that

$$H_0|\phi_i\rangle = \hbar\omega_0|\phi_i\rangle, \; H_0|\phi_f\rangle = \hbar\omega_f|\phi_f\rangle, \; \langle\phi_f|H_0|\phi_i\rangle = 0, \; \langle\phi_f|V|\phi_i\rangle = \lambda_f. \tag{49}$$

Let us write $|\phi(t)\rangle$ as

$$|\phi(t)\rangle = c_i(t)\mathrm{e}^{-\mathrm{i}\omega_0 t}|\phi_i\rangle + \sum_f c_f(t)\mathrm{e}^{-\mathrm{i}\omega_f t}|\phi_f\rangle \tag{50}$$

which, using our notation from the previous section, implies $|R_{00}\rangle = |0\rangle$, $|R_{01}\rangle = 0$, $|R_{10}(t)\rangle = \sum_f c_f(t)\mathrm{e}^{-\mathrm{i}\omega_f t}|1_f\rangle$ and $|R_{11}(t)\rangle = c_i(t)\mathrm{e}^{-\mathrm{i}\omega_0 t}|\mathbf{0}\rangle$.

In order to find the relevant time dependence we have to solve the Schrödinger equation

$$\mathrm{i}\hbar\dot{c}_i(t) = \sum_f \lambda_f^*\mathrm{e}^{-\mathrm{i}(\omega_f-\omega_0)t}c_f(t), \tag{51}$$

$$\mathrm{i}\hbar\dot{c}_f(t) = \lambda_f\mathrm{e}^{\mathrm{i}(\omega_f-\omega_0)t}c_i(t). \tag{52}$$

The second equation can be solved formally for $c_f(t)$

$$c_f(t) = -\frac{\mathrm{i}}{\hbar}\int_0^t \mathrm{d}t'\lambda_f\mathrm{e}^{\mathrm{i}(\omega_f-\omega_0)t'}c_i(t') \tag{53}$$

and after substituting this expression for $c_f(t)$ in Eq. (51) we obtain

$$\dot{c}_i(t) = -\int_0^t \mathrm{d}t' K(t-t') c_i(t'), \qquad K(\tau) = \frac{1}{\hbar^2}\sum_f |\lambda_f|^2 \mathrm{e}^{-\mathrm{i}(\omega_f-\omega_0)\tau}. \tag{54}$$

It is the function $\lambda_f = \lambda(\omega_f)$ which determines the character of the evolution.

• Parabolic decay

At short times, the exponential in $\mathrm{e}^{-\mathrm{i}(\omega_f-\omega_0)(t-t')}$ in $K(t-t')$ can be replaced by 1. This is justified when $t \ll 1/\Delta$, where Δ is a typical width of the $\lambda(\omega_f)$ curve. Usually, for a bell-shaped $\lambda(\omega_f)$ curve the order of Δ is pretty well approximated by ω_0. For example if we analyse spontaneous emission in the optical domain then $\omega_0 = \Delta = 10^{15}$ Hz thus the short time means here much less than 10^{-15} s. The integration in Eq. (53) together with the initial condition $c_i(t=0) = 1$ gives

$$|c_i(t)|^2 = |\langle\phi_i|\phi(t)\rangle|^2 = 1 - 2\frac{t^2}{\hbar^2}\sum_f \lambda_f^2. \tag{55}$$

The same result can be obtained directly by writing

$$|\phi(t)\rangle = \mathrm{e}^{-\mathrm{i}Ht/\hbar}|\phi_i\rangle = \left(1 - \frac{\mathrm{i}}{\hbar}Ht - \frac{1}{\hbar^2}H^2t^2 + \ldots\right)|\phi_i\rangle \tag{56}$$

which, together with Eq. (49) gives

$$|\langle\phi_i|\phi(t)\rangle|^2 = 1 - 2\frac{t^2}{\hbar^2}(\langle H^2\rangle - \langle H\rangle^2)\ldots = 1 - 2\frac{t^2}{\hbar^2}\sum_f \lambda_f^2 + \ldots \tag{57}$$

Thus for short times the decay is always parabolic. Let us mention in passing that from a purely mathematical point of view we have assumed here that expression $(\langle H^2\rangle - \langle H\rangle^2) = \sum_f \lambda_f^2$, i.e. the variance of the energy in the initial state $|\phi_i\rangle$ is finite. Needless to say in reality it is always finite but there are mathematical models in which, due to various approximations, this may not be the case (e.g. the Lorentzian distribution which has no finite moments).

• Exponential decay

Expression $|\lambda_f|^2\mathrm{e}^{-\mathrm{i}(\omega-\omega_0)\tau}$ viewed as a function of $\omega_f - \omega_0$ oscillates with frequency $1/\tau$ whereas $\lambda_f = \lambda(\omega_f)$ varies smoothly in the frequency domain. Again taking Δ as the typical width of the $\lambda(\omega_f)$ curve for $\tau \gg 1/\Delta$ the sum in $K(\tau)$ averages out to zero. This allows to substitute $c_i(t)$ for $c_i(t')$ in Eq. (51) which gives

$$\dot{c}_i(t) \approx -c_i(t)\int_0^t \mathrm{d}\tau K(\tau) \approx -c_i(t)\int_0^\infty \mathrm{d}\tau K(\tau). \tag{58}$$

Now we can calculate $\int_0^\infty \mathrm{d}\tau K(\tau)$ using the identity

$$\int_0^\infty \mathrm{d}\tau \mathrm{e}^{\mathrm{i}\omega\tau} = \lim_{\epsilon\to 0+}\int_0^\infty \mathrm{d}\tau \mathrm{e}^{\mathrm{i}(\omega+\mathrm{i}\epsilon)\tau} = \lim_{\epsilon\to 0+}\frac{\mathrm{i}}{\omega+\mathrm{i}\epsilon} = \mathrm{i}\mathrm{P}\frac{1}{\omega} + \pi\delta(\omega). \tag{59}$$

It gives

$$\int_0^\infty \mathrm{d}\tau K(\tau) = \frac{\gamma}{2} + \mathrm{i}\delta, \quad \frac{\gamma}{2} = \frac{\pi}{\hbar^2}|\lambda(\omega_f=\omega_0)|^2, \quad \delta = \mathrm{P}\sum_f \frac{|\lambda_f|^2}{\omega_0-\omega_f}. \tag{60}$$

Incorporating the energy shift $\hbar\delta$ into the modified energy separation $\hbar(\omega_0+\delta)$ we finally obtain

$$\dot{c}_i(t) = -\frac{\gamma}{2}c_i(t) \qquad \text{that is} \qquad c_i(t) = \mathrm{e}^{-\gamma t/2} \tag{61}$$

and consequently

$$c_f(t) = \frac{\lambda_f}{\hbar} \frac{1 - e^{i(\omega_f - \omega_0' + i\gamma/2)t}}{\omega_f - \omega_0' + i\gamma/2}. \tag{62}$$

Let us now go back to the language introduced in Sec. 1. The states of the environment $|R_0(t)\rangle$, $|R_1(t)\rangle$, $|R_2(t)\rangle$ and $|R_3(t)\rangle$ in the present context take the explicit form

$$|R_0(t)\rangle = \frac{1}{2}\left[1 + c_i(t)e^{-i\omega_0 t}\right]|\mathbf{0}\rangle, \tag{63}$$

$$|R_1(t)\rangle = \frac{1}{2}\sum_f c_f(t)e^{-i\omega_f t}|1\rangle_f, \tag{64}$$

$$|R_2(t)\rangle = -\frac{1}{2}\sum_f c_f(t)e^{-i\omega_f t}|1\rangle_f, \tag{65}$$

$$|R_3(t)\rangle = \frac{1}{2}\left[1 - c_i(t)e^{-i\omega_0 t}\right]|\mathbf{0}\rangle. \tag{66}$$

By formula (7), the fidelity of this process is given by

$$F(t) = \langle R_0(t)|R_0(t)\rangle + \langle R_3(t)|R_3(t)\rangle - 2\mathrm{Re}\langle R_0(t)|R_3(t)\rangle$$

$$= |c_i(t)|^2. \tag{67}$$

Therefore, the fidelity in the case of a parabolic decay takes the form

$$F_{\mathrm{par}}(t) = 1 - 2\frac{t^2}{\hbar^2}\sum_f \lambda_f^2, \tag{68}$$

while in the case of an exponential decay it has the exponential form

$$F_{\mathrm{exp}}(t) = e^{-\gamma t}. \tag{69}$$

6. Benefits of quantum error correction

In order to get an idea about the efficiency of quantum error correction, we will now discuss an explicit construction of the single error-correcting five qubit code. The initial state of the qubit $\alpha|0\rangle + \beta|1\rangle$ is encoded in state $\alpha|C_0\rangle + \beta|C_1\rangle$, where [13]

$$|C_0\rangle = |00010\rangle + |00101\rangle - |01011\rangle + |01100\rangle + |10001\rangle$$

$$-|10110\rangle - |11000\rangle - |11111\rangle, \tag{70}$$

$$|C_1\rangle = |00000\rangle - |00111\rangle + |01001\rangle + |01110\rangle + |10011\rangle$$

$$-|10100\rangle + |11010\rangle - |11101\rangle. \tag{71}$$

(To see the benefits of quantum error correction we do not need to use the explicit form of the code, we wrote it down here for those curious readers who may want to play with quantum error correcting codes.) These encoded states are chosen in such a way that conditions (40) are satisfied. Since this code can correct any type of error

affecting one qubit, it is suitable for protecting quantum states against spontaneous emission. We notice that the spontaneous emission process described in Sec. 5, unlike decoherence, involves both phase and amplitude errors and therefore it cannot be successfully defeated with less than five bit codes.

The probability that the state undergoes exponential decay in the presence of spontaneous emission is approximately given by

$$P_{\rm dec}(t) = 1 - F_{\rm exp}(t) = 1 - {\rm e}^{-\gamma t}. \tag{72}$$

If we assume that the five qubits decay independently from each other, the probability that none of them decays is given by

$$P_{\rm no\ dec}(t) = {\rm e}^{-5\gamma t}, \tag{73}$$

while the probability that only one of them decays is

$$P_{1\ \rm dec}(t) = {\rm e}^{-4\gamma t}(1 - {\rm e}^{-\gamma t}). \tag{74}$$

Since by construction the above error correction scheme corrects perfectly the encoded state when only one of the qubits is affected, the fidelity of reconstruction of the state after the error correction is at least as high as the probability of having at most one qubit decay during the process, that is

$$F_{\rm ec}(t) \geq P_{\rm no\ dec}(t) + 5P_{1\ \rm dec}(t) == {\rm e}^{-4\gamma t}(5 - 4{\rm e}^{-\gamma t}). \tag{75}$$

In order to have a successful error correction the such fidelity must be greater than the fidelity $F_{\rm exp}(t)$ corresponding to a single qubit in the absence of error correction. This is true when the decay probability $P_{\rm dec}(t)$ is much smaller than one, namely when the correction procedure is applied at times $t \ll 1/\gamma$. Actually, for $t \ll 1/\gamma$ the fidelity of reconstruction after error correction is bounded by

$$F_{\rm ec}(t) \geq 1 - 10\gamma^2 t^2 + {\rm O}(t^3), \tag{76}$$

namely it has parabolic form, while the single qubit decay probability is

$$P_{\rm dec}(t) \approx 1 - \gamma t. \tag{77}$$

7. Concluding remarks

Research in quantum error correction in its all possible variations has become vigorously active and any comprehensive review of the field must be obsolete as soon as it is written. Here we have decided to provide only some very basic knowledge, hoping that this will serve as a good starting point to enter the field. The reader should be warned that we have barely scratched the surface of the current activities in quantum error correction neglecting topics such as group theoretical ways of constructing good quantum codes [14], concatenated codes [15], quantum fault tolerant computation [16] and many others. Many interesting papers in these and many related areas can be found at the Los Alamos National Laboratory e-print archive (http:/xxx.lanl.gov/archive/quant-ph).

This work was supported in part by the European TMR Research Network ERP-4061PL95-1412, the TMR Marie Curie Fellowship Programme, Hewlett–Packard, The Royal Society London and Elsag-Bailey, a Finmeccanica Company.

References

[1] D. Deutsch, talk presented at the Rank Prize Funds Mini-Symposium on Quantum Communication and Cryptography, Broadway, England 1993; A. Berthiaume, D. Deutsch, R. Jozsa, in: *Proc. Workshop on Physics and Computation — PhysComp94*, IEEE Computer Society Press, Dallas, Texas, 1994.

[2] A. Barenco, A. Berthiaume, D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, *SIAM J. Comput.* **26**, in press.

[3] C.H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J.A. Smolin, W.K. Wootters, *Phys. Rev. Lett.* **76**, 722 (1996).

[4] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, A. Sanpera, *Phys. Rev. Lett.* **77**, 2818 (1996).

[5] P. Shor, *Phys. Rev. A* **52**, R2493 (1995).

[6] G.M. Palma, K.-A. Suominen, A. Ekert, *Proc. R. Soc. Lond. A* **452**, 567 (1996).

[7] W.H. Zurek, *Phys. Today*, Vol. 44, October, p. 36 (1991).

[8] C.H. Bennett, D.P. DiVincenzo, J.A. Smolin, W.K. Wootters, *Phys. Rev. A* **54**, 3824 (1996).

[9] A. Ekert, C. Macchiavello, *Phys. Rev. Lett.* **77**, 2585 (1996).

[10] F.J. MacWilliams, N.J.A. Sloane, *The Theory of Error Correcting Codes*, North-Holland, Amsterdam 1977.

[11] D. Gottesman, *Phys. Rev. A* **54**, 1862 (1996).

[12] A. Steane, *Phys. Rev. Lett.* **77**, 793 (1996); A. Steane, *Proc. R. Soc. Lond. A* **452**, 2551 (1996).

[13] R. Laflamme, C. Miquel, J.P. Paz, W.H. Zurek, *Phys. Rev. Lett.* **77**, 198 (1996).

[14] A.R. Calderbank, E.M. Rains, P.W. Shor, N.J.A. Sloane, *Phys. Rev. Lett.* **78**, 405 (1997).

[15] E. Knill, R. Laflamme, e-print quant-ph/9608012.

[16] P.W. Shor, e-print quant-ph/9605011; D.P. DiVincenzo, P.W. Shor, *Phys. Rev. Lett.* **77**, 3260 (1996).