Dynamical Stabilization of Grover's Algorithm with Embedded Quantum Codes

Gernot Alber, Michael Mussinger and Aldo Delgado
Abteilung für Quantenphysik, Universität Ulm, D-89069 Ulm, Germany
(published in Proceedings of SPIE **4429**, 37 (2001))

ABSTRACT

Stabilizing quantum algorithms against external perturbations and preserving quantum coherence are main challenges in the area of quantum information processing. In this contribution main ideas underlying a new class of recently proposed embedded error-correcting quantum codes are discussed. These detected-jump correcting quantum codes are capable of stabilizing distinguishable qubits against spontaneous decay provided these decay processes originate from couplings to statistically independent reservoirs. Exploiting the classical information about which qubit has been affected by the environment these embedded quantum codes minimize the number of required control measurements and recovery operations as well as redundancy. Their stabilizing properties are exemplified by applying them to Grover's quantum search algorithm.

Keywords: Error correction, spontaneous decay, Grover's algorithm, quantum information, jump codes

1. INTRODUCTION

In order to exhibit characteristic quantum phenomena, such as quantum interference and entanglement, one has to protect physical systems against environmental influences which tend to destroy quantum coherence. A research area where this is particularly important is quantum information processing.[1–3] Research in this field is motivated to a large extent by the desire to push quantum phenomena into the macroscopic domain as far as possible in order to be capable of exploiting these phenomena for practical purposes. Quantum error correction is an important method for achieving this goal.

So far two main approaches have been developed for preserving coherence in quantum systems. Active quantum error-correcting codes (QECC) use basic ideas of classical error correction, generalized to the quantum domain. For this purpose quantum information is encoded in physical states in such a way that certain classes of errors can be detected without affecting coherence and entanglement. For the correction of these errors an appropriate sequence of unitary recovery operations has to be applied which is conditioned on previous control measurements. The basic strategy of passive error-correcting schemes is different. Thereby quantum information is encoded in those quantum states which are insensitive to a particular class of errors. Thus, perfect passive error correction does not require any control measurement or recovery operations.

In this contribution a recently introduced[4] new class of error correcting quantum codes is discussed which is capable of stabilizing distinguishable qubits against spontaneous decay. This quantum error correction method relies on embedding an active error correcting quantum code into a passive one and simultaneously exploiting classical information about which qubit has been affected by the environment. This embedding method leads to a significant reduction of the number of required control measurement in comparison with purely active error correction methods. Furthermore, by exploiting classical information about the 'position' of the error redundancy can be reduced significantly in comparison with other previously proposed embedding schemes. In addition, an interesting surprising connection between these new codes and combinatorial design theory can be established. This connection might turn out to be particularly useful for future generalizations of these error-correcting techniques. In order to exemplify basic stabilizing properties of this new class of error-correcting quantum codes numerical results are presented in which it is applied to stabilizing Grover's quantum search algorithm.[5] Due to their low redundancy, their simple structure and the small number of control measurements, these new error-correcting codes are particularly relevant for quantum computation which is based on trapped ions[6] or nuclear spins.[7]

This article is organized as follows: For the sake of completeness in Sec. 2 elementary facts about Grover's quantum search algorithm are recapitulated. In Sec. 3 basic ideas of quantum error correction are discussed and in Sec. 4 the recently proposed[4] new class of detected-jump correcting quantum codes is introduced. Codes which

are capable of correcting one error at a time are constructed for an arbitrary even number of physical qubits and basic properties of more general many error-correcting codes are outlined. Finally the connection between these detected-jump correcting quantum codes and elementary notions of combinatorial design theory is indicated.

2. GROVER'S QUANTUM SEARCH ALGORITHM

Recently, several quantum algorithms have been proposed which demonstrate that characteristic quantum phenomena, such as quantum interference and entanglement, may be exploited for performing computational tasks faster than by any other classical means. Most prominent examples are the quantum algorithms of Deutsch,[8] Simon,[9] Shor,[10] and Grover.[11] In this section elementary notions of quantum algorithms are introduced by recapitulating Grover's quantum search algorithm. In this latter algorithm a particular sequence of quantum gates enables one to find a specific item out of an unsorted database much faster than by any other known classical mean. This quantum algorithm was already realized experimentally for a small number of qubits.[12]

2.1. Quantum algorithms

A quantum algorithm consists of a sequence of unitary transformations *(gates)* applied on several distinguishable two-level quantum systems *(qubits)*. A qubit therefore is in a state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where $|0\rangle$ and $|1\rangle$ are the two base states of the two level system. The combination of n qubits *(quantum register)* can be in a highly entangled state

$$|\psi\rangle = \sum_{i_1,\ldots,i_n=0}^{1} \alpha_{i_1,\ldots,i_n} |i_1,\ldots,i_n\rangle. \tag{1}$$

To realize every possible quantum algorithm, one must be able to realize one qubit rotations and at least one two-qubit gate, i.e. an interaction between two different qubits. A simple example for a one-qubit gate is a *rotation* by π, i.e.

$$\alpha|0\rangle + \beta|1\rangle \xrightarrow{\pi} \beta|0\rangle + \alpha|1\rangle. \tag{2}$$

The *controlled not gate* is the most frequently used two-qubit gate (CNOT or XOR). We write C_{12}, where the first qubit is the control-qubit and the second one the target qubit. The target bit is flipped depending on whether the control bit is zero or one. Applied to the basis states of a combined two-qubit system, the CNOT has the following effect

$$|00\rangle \xrightarrow{C_{12}} |00\rangle \quad |01\rangle \xrightarrow{C_{12}} |01\rangle \quad |10\rangle \xrightarrow{C_{12}} |11\rangle \quad |11\rangle \xrightarrow{C_{12}} |10\rangle.$$

2.2. Grover's algorithm

Let us first of all consider a classical version of Grover's search algorithm. Consider an unsorted database with N items and a certain item x_0 you are searching for. As a particular example you can imagine a telephone directory with N entries and a particular telephone number x_0 you are looking for. Furthermore, assume that you are only given a black box for performing this data search. This black box, i.e. a so called oracle, can decide whether an item is x_0 or not. Thus, in mathematical terms you are given a Boolean function

$$f(x) = \delta_{x,x_0} = \begin{cases} 1 & x = x_0 \\ 0 & x \neq x_0 \end{cases} \tag{3}$$

with $\delta_{a,b}$ denoting the Kronecker delta function. The classical oracle allows you to evaluate this Boolean function for any element x of the database. Assuming that each application of this oracle requires one elementary step a classical random search process will require $N-1$ steps in the worst case and one step in the best possible case. Thus, for large values of N, on the average a classical algorithm will need $N/2$ steps to find the item x_0.

It has been shown by Grover[11] that with the help of his quantum search algorithm this task can be performed in $O(\sqrt{N})$ steps with a probability arbitrarily close to unity. Thereby one exploits the phenomenon of quantum interference. The basic idea of this quantum algorithm is to rotate an initial reference state of the qubit system representing the database in the direction of the searched state $|x_0\rangle$ with the help of a unitary quantum version of the oracle. It will become apparent from the subsequent discussion that apart from Hadamard transformations the dynamics of this rotation are analogous to a Rabi oscillation between this initially prepared reference state and the searched state $|x_0\rangle$. It has been shown that Grover's quantum search algorithm is optimal.[13,14]

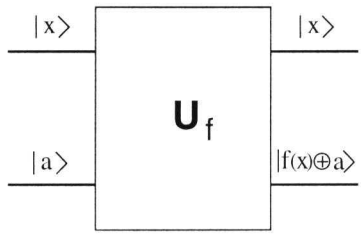

Figure 1. Schematic representation of the quantum oracle $\mathcal{U}_f$: For $f(x) \equiv x$ this quantum gate reduces to a CNOT gate; for $|a\rangle \equiv |a_0\rangle = 1/\sqrt{2}\,(|0\rangle - |1\rangle)$ it results in the conditional phase inversion I_{x_0} of Eq. (8) needed in Grover's quantum search algorithm.

In Grover's quantum search algorithm the $N = 2^m$ elements of the database are represented by orthogonal states of a distinguishable m-qubit system. These orthogonal states constitute the computational basis of a quantum computer. The state $|0..0110..0\rangle$ of this computational basis, for example, corresponds to the element 0..0110..0 of the database in binary notation. The quantum oracle $\mathcal{U}_f$ is determined completely by the Boolean function of Eq. (3) and is represented by a quantum gate, i.e. by the unitary and hermitian transformation

$$\mathcal{U}_f : |x, a\rangle \rightarrow |x, f(x) \oplus a\rangle. \tag{4}$$

Thereby $|x\rangle$ is an arbitrary element of the computational basis and $|a\rangle$ is the state of an additional ancilla qubit which is discarded later. The symbol $\oplus$ denotes addition modulo 2. As far as complexity estimates are concerned it is assumed that this unitary transformation requires one elementary step. This assumption is analogous to the complexity estimate of the corresponding classical version of this search problem.

It is important to note that the elementary rotations in the direction of the searched quantum state $|x_0\rangle$ which are the key ingredient in Grover's algorithm can be performed with the help of this unitary oracle. Thus such a rotation can be performed without explicit knowledge of the state $|x_0\rangle$. Its implicit knowledge through the values of the Boolean function $f(x)$ is already sufficient. For large values of N it turns out that the number of elementary rotations needed to prepare state $|x_0\rangle$ is $O(\sqrt{N})$. To implement such an elementary rotation from the initial reference state $|s\rangle = |0...0\rangle$, for example, towards the final state $|x_0\rangle$ two different types of quantum gates are needed, namely *Hadamard* gates and *controlled phase inversions*. However, it has been shown by Grover[11] that this Hadamard transformation can also be replaced by any other unitary one-qubit operation.

A *Hadamard* gate $H^{(2)}$ is a unitary and hermitian one-qubit operation. It produces an equally weighted superposition of the two basis states according to the rule

$$|0\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \tag{5}$$

$$|1\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \tag{6}$$

A m-qubit Hadamard gate $H^{(2^m)}$ is defined by the m-fold tensor product, i.e. $H^{(2^m)} = H^{(2)} \otimes ... \otimes H^{(2)}$.

The remaining quantum gates needed for the implementation of the necessary rotation are *controlled phase inversions* with respect to the initial and searched states $|s\rangle = |0...0\rangle$ and $|x_0\rangle$. A controlled phase inversion with respect to a state $|x\rangle$ changes the phase of this particular state by an amount of π and leaves all other states unchanged. Thus the phase inversion I_s with respect to the initial state $|s\rangle$ is defined by

$$\begin{aligned} I_s|s\rangle &= -|s\rangle, \\ I_s|x\rangle &= |x\rangle \quad (x \neq s). \end{aligned} \tag{7}$$

The controlled phase inversion I_{x_0} with respect to the searched state $|x_0\rangle$ is defined in an analogous way. As state $|x_0\rangle$ is not known explicitly but only implicitly through the property $f(x_0) = 1$ this transformation has to be

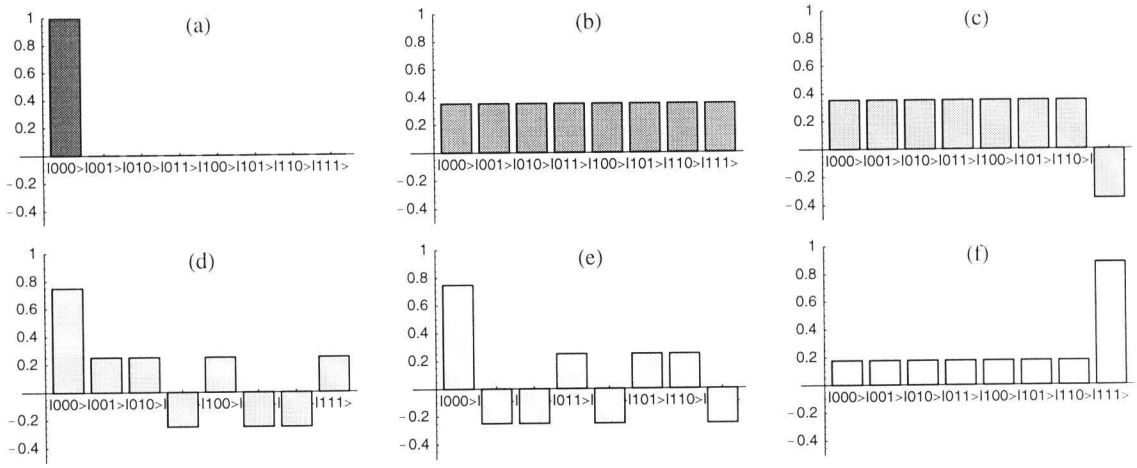

Figure 2. Amplitude distributions resulting from the various quantum gates involved in Grover's quantum search algorithm for the case of three qubits: The quantum states which are prepared by these gates are (a) $|s\rangle = |000\rangle$, (b) $H^{(2^m)}|s\rangle$, (c) $I_{x_0}H^{(2^m)}|s\rangle$, (d) $H^{(2^m)}I_{x_0}H^{(2^m)}|s\rangle$, (e) $-I_sH^{(2^m)}I_{x_0}H^{(2^m)}|s\rangle$, (f) $-H^{(2^m)}I_sH^{(2^m)}I_{x_0}H^{(2^m)}|s\rangle$. The searched state $|x_0\rangle$ entering the Boolean function of Eq. (3) is assumed to be state $|111\rangle$.

performed with the help of the quantum oracle. This task can be achieved by preparing the ancilla of the oracle of Eq. (4) in state $|a_0\rangle = 1/\sqrt{2}(|0\rangle - |1\rangle)$. As a consequence one obtains the required properties for the phase inversion I_{x_0}, namely

$$\begin{aligned} |x, f(x) \oplus a_0\rangle \equiv |x, 0 \oplus a_0\rangle = 1/\sqrt{2}(|x,0\rangle - |x,1\rangle) = |x, a_0\rangle \quad \text{for} \quad x \neq x_0, \\ |x, f(x) \oplus a_0\rangle \equiv |x, 1 \oplus a_0\rangle = 1/\sqrt{2}(|x,1\rangle - |x,0\rangle) = -|x, a_0\rangle \quad \text{for} \quad x = x_0. \end{aligned} \tag{8}$$

One should bear in mind that this controlled phase inversion can be performed with the help of the quantum oracle of Eq. (4) without explicit knowledge of state $|x_0\rangle$.

Grover's algorithm starts by preparing all m qubits of the quantum computer in the reference state $|s\rangle = |0...0\rangle$. An elementary rotation in the direction of the searched state $|x_0\rangle$ with the property $f(x_0) = 1$ is achieved by the gate sequence

$$Q = -I_s \cdot H^{(2^m)} \cdot I_{x_0} \cdot H^{(2^m)}. \tag{9}$$

In order to rotate the initial state $|s\rangle$ into state $|x_0\rangle$ one has to perform a sequence of n such rotations and a final Hadamard transformation at the end, i.e.

$$|f\rangle = HQ^n|s\rangle. \tag{10}$$

The effect of one elementary rotation Q is demonstrated in Fig. 2 for the case of three qubits, i.e. $m = 3$. The first Hadamard transformation $H^{(2^3)}$ prepares an equally weighted state. The subsequent quantum gate I_{x_0} inverts the amplitude of the searched state $|x_0\rangle = |111\rangle$. Together with the subsequent Hadamard transformation and the phase inversion I_s this gate sequence Q amplifies the probability amplitude of the searched state $|111\rangle$. In this particular case an additional Hadamard transformation finally prepares the quantum computer in the searched state $|111\rangle$ with a probability of 0.88.

In order to determine the dependence of the ideal number of repetitions n on the number of qubits m it is convenient to analyze the repeated application of the gate sequence Q according to Eq. (10) in terms of the two states $|s\rangle$ and $|v\rangle = H^{(2^m)}|x_0\rangle$ whose overlap is given by $\epsilon = \langle s|v\rangle = \langle s|H^{(2^m)}|x_0\rangle = 2^{-m/2}$ for m qubits. It is straightforward to show that the unitary gate sequence Q preserves the subspace spanned by these two states,[11] i.e.

$$Q \begin{pmatrix} |s\rangle \\ |v\rangle \end{pmatrix} = \begin{pmatrix} 1 - 4\epsilon^2 & 2\epsilon \\ -2\epsilon & 1 \end{pmatrix} \begin{pmatrix} |s\rangle \\ |v\rangle \end{pmatrix}. \tag{11}$$

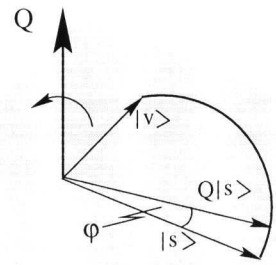

Figure 3. Q is a rotation in the subspace spanned by states $|s\rangle$ and $|v\rangle$.

Thus Q acts like a rotation in the plane spanned by states $|s\rangle$ and $|v\rangle$. The angle of rotation is given by $\varphi = \arcsin(2\epsilon\sqrt{1-\epsilon^2})$. After j iterations the amplitude of state $|v\rangle$ is given by[15]

$$\sin\left[(2j+1)\epsilon\right]. \tag{12}$$

Therefore, the optimal number n of repetitions of the gate sequence Q is approximately given by

$$n = \frac{\pi}{4\ \arcsin\left(2^{-m/2}\right)} - \frac{1}{2} \approx \frac{\pi}{4}\sqrt{2^m}\ \ (2^m \gg 1). \tag{13}$$

2.3. Hamiltonian description

If the database contains many elements, i.e. $N \equiv \epsilon^{-2} \gg 1$, the repeated application of the elementary rotation which is essential for Grover's search algorithm can be described by Hamiltonian quantum dynamics.[16] The elementary rotation Q can be approximated by the relation

$$Q = \mathbf{1} - \tau\ i/\hbar \mathbf{H}_G(\epsilon) + O(\epsilon^2) \tag{14}$$

which involves the Hamiltonian

$$\mathbf{H}_G = 2i\epsilon\frac{\hbar}{\tau}\ \left(|v\rangle\langle s| - |s\rangle\langle v|\right). \tag{15}$$

The elementary time τ might be interpreted as the physical time required for performing the elementary rotation Q. The Hamiltonian of Eq. (15) describes the dynamics of a quantum mechanical two level system whose degenerate energy levels $|s\rangle$ and $|v\rangle$ are coupled by a time-independent perturbation. In lowest order of ϵ these degenerate energy levels are orthogonal. The resulting oscillations between these coupled energy levels are characterized by the Rabi frequency $\Omega = 2\langle s|v\rangle/\tau$. Correspondingly, the repeated application of the elementary rotation Q can be determined with the help of Trotter's product formula,[17] namely

$$Q^n = (-I_s \cdot H^{(2^m)} \cdot I_{x_0} \cdot H^{(2^m)})^n = \exp\left(-\frac{i}{\hbar}\mathbf{H}_G\ \cdot \tau n\right) + O(\epsilon^2 n). \tag{16}$$

Thus, in the framework of this Hamiltonian description applying the elementary rotation Q n times is equivalent to a time evolution of the effective two-level quantum system over a time interval of magnitude $n\tau$. This Hamiltonian description demonstrates that the physics behind Grover's quantum search algorithm is the same as the physics governing the Rabi oscillations between degenerate or resonantly coupled energy eigenstates. As the errors entering Eq. (16) are of order $O(\epsilon^2 n)$ this Hamiltonian description is applicable only as long as $\epsilon^2 n \equiv n/2^m \ll 1$. Thus for a given size of the database it is valid only as long as the number of iterations is sufficiently small, i.e. $n \ll 2^m$. However, as Grover's search algorithm needs approximately $(\pi\sqrt{2^m}/4)$ steps to find the searched item the main condition which restricts the validity of this Hamiltonian description is a large size of the database, i.e. $\epsilon^2 \equiv 1/N \ll 1$.

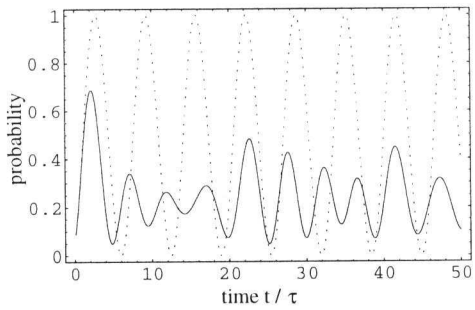

Figure 4. The probability of being in state $|x_0\rangle$ after $n = t/\tau$ iterations of Grover's quantum search algorithm for four qubits: the ideal dynamics according to the Hamiltonian time evolution characterized by Eqs.(15) and (16) (dotted line); the non-ideal case of coherent errors as characterized by Eqs. (15), (16) and (17) (solid line) with detunings $\omega_i\tau/\langle v|s\rangle = 1.35, 0.9, 1.1, 1.25$.

So far we have been concentrating on the ideal dynamics of Grover's quantum search algorithm. However, in practical applications it is very difficult to realize this search algorithm in an ideal way. Usually the ideal dynamics are affected by numerous perturbations. Physically one may distinguish two different kinds of errors, namely incoherent and coherent ones. Typically incoherent perturbations originate from a coupling of the physical qubits of a quantum computer to an uncontrollable environment. As a consequence the resulting errors are of a stochastic nature. Coherent errors may arise from non-ideal quantum gates which lead to a unitary but non-ideal time evolution of the quantum algorithm. A simple example of this latter type of errors are systematic detunings from resonance of the light pulses with which the required quantum gates are realized on the physical qubits. In the Hamiltonian formulation of Grover's algorithm such systematic detunings may be described by a perturbing Hamiltonian of the form

$$\mathbf{H}_d = \sum_{i=1}^{m} \hbar\omega_i \sigma_z^{(i)}. \tag{17}$$

In Eq. (17) it has been assumed that Grover's quantum algorithm is realized by m qubits and that the i-th qubit is detuned with respect to the ideal transition frequency by an amount ω_i. The Pauli spin-operator of the i-th qubit is denoted $\sigma_z^{(i)}$. In the presence of these systematic detunings and for a large number of qubits the dynamics of Grover's algorithm are described by the Hamiltonians of Eqs.(15) and (17).

In order to obtain insight into the influence of this type of coherent errors the performance of Grover's algorithm under repeated applications of the elementary rotation Q is depicted in Fig. 4. The dynamics of the ideal Grover algorithm are depicted by the dashed line for the case of three qubits, i.e. $m = 3$. The Rabi oscillations with frequency $\Omega = 2\langle v|s\rangle/\tau$ are clearly visible. The solid line shows the probability of observing the quantum computer in state $|x_0\rangle$ in a case in which all the qubits are detuned from their ideal resonance frequency. One notices the deviations from the ideal behaviour. Due to the coherent nature of the errors the time evolution of the non-ideal algorithm exhibits revival phenomena.[18]

3. QUANTUM ERROR CORRECTION - BASIC CONCEPTS

One of the main practical problems one has to overcome in the implementation of quantum algorithms are non-ideal performances of quantum gates[19] or random environmental influences which both tend to affect quantum coherence. To protect quantum computation against such errors two major strategies have been pursued recently, namely *active quantum error correction*[20–24] and *passive error avoiding quantum codes*.[25–28] Both theoretical approaches to error correction rest on the concept of redundancy which is also fundamental for classical error-correcting codes.[29]

3.1. Active quantum error correction

Active quantum error correction schemes may be viewed as generalizations of classical error-correcting techniques to the quantum domain. Typically they involve a suitably chosen quantum error-correcting code (QECC) and

a sequence of quantum measurements. A non-degenerate code, which is the simplest example, has to map all possible states which may result from arbitrary environmental influences onto orthogonal states. According to basic postulates of quantum theory orthogonal quantum states can be distinguished and based on the results of suitable control measurements one may restore the original quantum state by a unitary recovery operation. These control measurements have to be designed in such a way that on the one hand it is possible to determine the characteristic properties of the error, the so called *syndrome*, but on the other hand it is impossible to gain information about the logical quantum state. Thus, consistent with this physical requirement, the orthogonal logic basis states (or code words) $|c_i\rangle$ $(i = 1, ..., N)$ of an active error-correcting code capable of correcting error operators $L_{\mathbf{a}}, L_{\mathbf{b}}, \ldots$ have to fulfill the conditions[24]

$$\langle c_i | L_{\mathbf{a}}^{\dagger} L_{\mathbf{b}} | c_j \rangle = \Lambda_{\mathbf{ab}} \delta_{ij}. \tag{18}$$

It has been shown[24] that these conditions are necessary and sufficient for the existence of conditioned unitary recovery operations which preserve quantum coherence. For $i \neq j$, for example, these conditions state that for given perturbations $L_{\mathbf{a}}$ and $L_{\mathbf{b}}$ orthogonal code words have to remain orthogonal. Otherwise it would not be possible to restore them again after these perturbations by a unitary recovery operation. For $i = j$ these conditions state that all code words have to be affected by two given perturbations $L_{\mathbf{a}}$ and $L_{\mathbf{b}}$ in the same way, i.e. the right hand side of Eq. (18) has to be independent of i. Otherwise the perturbations would destroy quantum coherence. In the special case of a non-degenerate quantum code the right hand side of Eq. (18) vanishes for $\mathbf{a} \neq \mathbf{b}$, i.e. $\Lambda_{\mathbf{ab}} = \lambda_{\mathbf{a}} \delta_{\mathbf{ab}}$. The code is called degenerate if $\Lambda_{\mathbf{ab}} \neq 0$ for $\mathbf{a} \neq \mathbf{b}$. An example of an optimal active QECC correcting arbitrary one-qubit errors was presented by Zurek et al..[22] This code needs five physical qubits for encoding one logical qubit.

If one wants to stabilize a quantum algorithm by an active QECC one has to determine the syndrome of each error periodically after sufficiently short time intervals. This is achieved by an appropriate sequence of unitary transformations and measurements. Conditioned on the results of these control measurements the corresponding unitary recovery operations have to be applied sufficiently fast. Typically decreasing the time between subsequent control measurements and recovery operations increases the success probability of the QECC. Thus, the typically large number of required control measurements and recovery operations are a main disadvantage of active QECCs.

3.2. Passive error-avoiding quantum codes

Here the approach is different: The main idea is to encode logical information in a subspace of the relevant Hilbert space which is not affected by the physical interactions responsible for the occurance of errors. Such a subspace is called a *decoherence free subspace* (DFS).[25–28] This aim is achieved by restricting oneself to degenerate eigenspaces of the relevant error operators. In the special case of a single error operator, say $\mathbf{E}$, for example, all the basis states $\{|\psi_i\rangle\}$ of such a DFS have to fulfill the relation

$$\mathbf{E}|\psi_i\rangle = c\,|\psi_i\rangle. \tag{19}$$

Comparison with Eq. (18) shows that error-avoiding quantum codes may be viewed as completely degenerate active QECCs. As the eigenvalue c of Eq. (19) does not depend on $|\psi_i\rangle$ all states of the DFS of the general form $\sum_i \alpha_i |\psi_i\rangle$ are affected by the error operator in the same way, i.e.

$$\mathbf{E}\,(\sum_i \alpha_i |\psi_i\rangle) = c\,(\sum_i \alpha_i |\psi_i\rangle). \tag{20}$$

As a DFS is preserved under the influence of errors this method of error correction is purely passive. There is no need for any control measurements and recovery operations.[30] For this reason, the performance of such a passive error-avoiding code does not depend on the probability of an error. If a code is tolerant to a given error, the error may occur arbitrary frequently. However, obviously a useful, ideal error avoiding quantum code can be constructed only in those rare case, in which a common, sufficiently highly degenerate eigenspace of the relevant error operators can be found.

3.3. An example of a passive error-correcting code

As an example of an error avoiding quantum code let us consider the case of coherent errors which may affect Grover's quantum algorithm and which can be characterized by the Hamiltonian $\mathbf{H}_d$ of Eq. (17). In the simple case of equal

detunings, i.e. $\omega_1 = ... = \omega_m \equiv \omega$, the error operator $\mathbf{E}$ reduces to the form

$$\mathbf{H}_e = \hbar\omega \sum_{i=1}^{m} \sigma_z^{(i)}. \tag{21}$$

It is easy to find highly degenerate DFSs of this error operator. All states with a fixed number of ones and zeros constitute a degenerate eigenspace of $\mathbf{H}_e$.[30,31] For an even number of qubits it is possible to find an error avoiding subspace with eigenvalue $c = 0$ so that

$$(\mathbf{H}_G + \mathbf{H}_e)\,|\psi\rangle = \mathbf{H}_G|\psi\rangle \tag{22}$$

for all elements $|\psi\rangle$ of this subspace. This subspace consists of all quantum states with zero total spin. For four qubits, for example, it is defined by the basis vectors $|0011\rangle, |0101\rangle, |0110\rangle, |1001\rangle, |1010\rangle, |1100\rangle$ and involves all states with the same number of zeros and ones. Four of these states may be used as a basis for the state space of two *logical* qubits. For these eigenstates the error Hamiltonian $\mathbf{H}_e$ maps onto zero, e.g.

$$\mathbf{H}_e|0011\rangle = \hbar\omega \sum_{i=1}^{m=4} \sigma_z^{(i)}|0011\rangle = \hbar\omega(1+1-1-1)|0011\rangle = 0.$$

To be able to use this code for quantum computation, also the quantum gates constituting an algorithm have to be "encoded". For the implementation of an algorithm on a DFS gates are required that act on the logical qubits as universal gates. For Grover's algorithm, for example, we have to realize a Hadamard gate and a controlled phase inversion on the logical states. The orthogonal complement of the DFS must not be mixed with the DFS. As an example, a Hadamard transformation $\tilde{H}$ defined on the simplest possible error avoiding code consisting of $|c_0\rangle = |01\rangle$ and $|c_1\rangle = |10\rangle$ could be represented by the transformation

$$|00\rangle \xrightarrow{\tilde{H}} |00\rangle; \quad |01\rangle \xrightarrow{\tilde{H}} \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle); \quad |10\rangle \xrightarrow{\tilde{H}} \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle); \quad |11\rangle \xrightarrow{\tilde{H}} |11\rangle. \tag{23}$$

This is a one qubit operation in the logical space which is physically implemented by a two-qubit gate. The physical implementation of gates acting on two logical qubits can be realized provided appropriate multi-particle interactions are available. Recently Bacon et al.[32] proposed a way of fault-tolerant computation on a DFS which is based on two-particle interactions.

The above mentioned error avoiding code works ideal for equal detunings of all qubits from resonance. However, in realistic situations this case is scarcely realized. For the realistic assumption of unequal detunings in general the eigenstates of $\mathbf{H}_d$ are non-degenerate so that it is not possible to construct a perfect error avoiding quantum code. Therefore the practical question arises whether the presented error avoiding quantum code is still useful for stabilizing quantum algorithms against arbitrary systematic detunings.

The dynamics of Grover's algorithm in the presence of unequal detunings are depicted in Fig. 5. The dotted line represents the ideal dynamics in the absence of detunings for the case of 6 qubits as evaluated from the Hamiltonian of Eq. (15). The characteristic Rabi oscillations are clearly apparent. The corresponding dynamics for 8 qubits in the presence of arbitrarily chosen detunings are depicted by the solid line in Fig. 5. It is apparent that in this case a quantum search for state $|x_0\rangle$ is not successful at all. However, as apparent from the dashed line of Fig. 5 encoding the quantum information by the error avoiding code introduced above improves the performance considerably. Despite the fact that this error avoiding code has not been designed for these detunings it almost succeeds in finding the searched quantum state $|x_0\rangle$ after a number of iterations which is close to the ideal case (compare with Eq. (13)). Similar stability properties of error avoiding codes have been observed by Lidar et al.[33]

4. EMBEDDED QUANTUM CODES AND ONE ERROR DETECTED-JUMP CORRECTING QUANTUM CODES

Passive error avoiding quantum codes have the advantage that they do not require control measurements and recovery operations which are cumbersome to implement in practice. But this method can only be used in those rare cases in which one can find a sufficiently highly degenerate, common eigenspace of the relevant error operators. In many cases of practical interest such an error free subspace cannot be found. Thus, typically the best one can do is to combine active and passive error-correcting techniques to reduce the number of control measurements and recovery operations.

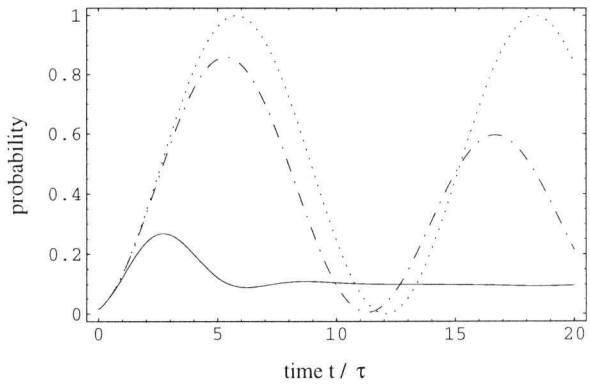

Figure 5. Probability of finding the quantum computer in the searched state $|x_0\rangle$ after $n = t/\tau$ iterations: ideal dynamics without detunings for 6 qubits (dotted line), with detunings and without error avoiding encoding for 6 qubits (solid line), with detunings and with error avoiding encoding using 8 physical qubits which can encode the quantum information of 6 logical qubits (dashed line). For the latter two cases the magnitudes of the detunings ω_i of the 8 qubits which determine the error operator of Eq. (17) are given by $\boldsymbol{\omega}_i$s with mean value $\overline{\omega} = \langle v|s\rangle/\tau$ and a variance of $\Delta\omega = 0.3\langle v|s\rangle$.

Furthermore, it is also desirable for such combined error-correcting quantum codes that their redundancies are as small as possible. In this section a recently proposed class of combined quantum codes[4] is discussed which is capable of stabilizing distinguishable qubits against spontaneous decay processes. This quantum error correction method relies on embedding an active error-correcting quantum code into a DFS and exploiting classical information about which qubit has been affected by the environment. This embedding method implies a significant reduction of the number of required control measurements in comparison with purely active error-correcting methods. Furthermore, exploiting the classically available information about the 'position' of the error also redundancy can be reduced significantly in comparison with other previously proposed embedded error-correcting schemes.

4.1. Description of spontaneous emission

In order to explain the main ideas let us consider n distinguishable qubits which are perturbed by statistically independent reservoirs inducing spontaneous decay processes. The assumption of statistical independence of the reservoirs is justified provided the characteristic wave lengths of the spontaneously emitted photons or phonons are small in comparison with distances between adjacent qubits. Within the Markov approximation the time evolution of the density operator ρ of these n qubits can be described by a master equation[34]

$$\dot{\rho(t)} = -\frac{i}{\hbar}[H, \rho(t)] + \frac{1}{2}\sum_{\alpha=1}^{n}\{[L_\alpha, \rho(t)L_\alpha^\dagger] + [L_\alpha\rho(t), L_\alpha^\dagger]\}. \tag{24}$$

Thereby the Lindblad operator $L_\alpha = \sqrt{\kappa_\alpha}\,|0\rangle\langle 1|_\alpha$ characterizes spontaneous decay of qubit α from its excited state $|1\rangle_\alpha$ into its stable state $|0\rangle_\alpha$ with rate κ_α. The coherent part of the n-qubit dynamics is described by the Hamiltonian H. Such a Hamiltonian description is also possible for some quantum algorithms as described in Sec. 2.3. In the case of radiative damping of quantum optical systems the derivation of Eq. (24) involves the Born- and the Markov approximations which are typically well fulfilled. These approximations rest on the assumption of weak couplings between resonantly excited two-level systems and the vacuum modes of the electromagnetic field and a sufficiently short correlation time of theses vacuum modes.[34,35] In solid state devices where spontaneous decay processes typically originate from couplings to phononic reservoirs this Markov approximation is usually only applicable for sufficiently high temperatures of the reservoirs.[36]

A formal solution of Eq. (24) is given by[34]

$$\rho(t) = \sum_{N=0}^{\infty}\sum_{\alpha_1,\ldots,\alpha_N}\int_0^t dt_N\int_0^{t_N} dt_{N-1}\ldots\int_0^{t_2} dt_1\;|\psi(t|t_N\alpha_N,..,t_1\alpha_1)\rangle\langle\psi(t|t_N\alpha_N,...,t_1\alpha_1)|. \tag{25}$$

Thus, if the initial state is pure, for example, the density operator $\rho(t)$ can be unravelled into a statistical ensemble of the pure states

$$|\psi(t|t_N\alpha_N,...,t_1\alpha_1)\rangle = e^{-i[\tilde{H}(t-t_N)]/\hbar}L_{\alpha_N}e^{-i[\tilde{H}(t_N-t_{N-1})]/\hbar}\ldots e^{-i[\tilde{H}(t_2-t_1)]/\hbar}L_{\alpha_1}e^{-i\tilde{H}t_1/\hbar}|\psi(t=0)\rangle. \quad (26)$$

Each of these unnormalized states characterizes the n-qubit system conditioned on the observation of N quantum jumps of qubits $\alpha_1,...,\alpha_N$ which take place at times $t_1 \leq ... \leq t_N$. The action of these quantum jumps is represented by the Lindblad operators $L_{\alpha_N},...L_{\alpha_1}$. The squared norm of the quantum state $|\psi(t|t_N\alpha_N,...,t_1\alpha_1)\rangle$ defines the probability with which the associated quantum trajectory $(t_1\alpha_1,...,t_N\alpha_N)$ contributes to $\rho(t)$. In this quantum jump representation the conditional time evolution between two successive quantum jumps is determined by the non-hermitian effective Hamiltonian $\tilde{H} = H - i(\hbar/2)\sum_{\alpha=1}^{n} L_\alpha^\dagger L_\alpha$.

4.2. One detected-jump correcting codes

The dynamics described by Eq. (24) can be stabilized against spontaneous decay in an effective way by an embedded quantum code. For this purpose one constructs first of all a DFS which stabilizes the conditional time evolution between two successive quantum jumps passively. In a second step one inverts the occuring quantum jumps with the help of an active QECC which is constructed within this DFS.[25,26,28,35,37] For this stabilization it is necessary to observe the n-qubit system continuously. Nevertheless, it is not necessary to apply additional gates to measure the error syndrome. What is required is a space resolved detection of the spontaneously emitted photons or phonons.

Whenever a quantum jump occurs one has to apply the appropriate unitary recovery operation within a time interval short in comparison with the decay times and with the coherent evolution times of the system.[35] In contrast to other purely active ways of error correction this combination of a passive and an active quantum code guarantees perfect error correction even if the time between successive recovery operations does not tend to zero provided that each quantum jump is detected with a probability of unity and that the required recovery operation is applied instantaneously. However, similar assumptions are also required for other active QECC schemes in addition to a high frequency of recovery operations. For an embedded quantum code the mean number of required recovery operations equals the number of spontaneous decay events which is determined by the spontaneous decay rates κ_α of the qubits.

Recently, Plenio et al.[37] have presented such a one error-correcting embedded quantum code which applies to the important special case of equal decay rates of all the qubits. Their active QECC constructed within their DFS is capable of correcting spontaneous decay affecting a single logical qubit which is encoded by eight physical ones. Being consistent with the conditions of Eq. (18) this embedded error-correcting quantum code does not require any knowledge about which qubit is affected by the environment. However, its redundancy is rather large and it is not clear how to generalize their code to an arbitrary number of logical qubits.

The redundancy of embedded quantum codes can be reduced significantly by systematically taking into account the available information on which qubit has been affected by a quantum jump. If the qubits of a quantum computer couple to independent reservoirs both information about the jump time, say t, and about the jump 'position', say α, are available. Therefore, it is natural to exploit this additional information about the 'position' of a quantum jump for more efficient encoding. If one can determine not only the jump time t but also the jump position α by continuously monitoring the n-qubit quantum system, one has to correct the error operator L_α only for this particular value of α. As a consequence the corresponding active QECC has to fulfill Eqs.(18) for $\alpha = \beta$ only. The violation of conditions (18) for $\alpha \neq \beta$ offers the possibility to construct embedded quantum codes with a significantly smaller degree of redundancy.

As an example, let us consider the important special case of equal spontaneous decay rates of all the qubits, i.e. $\kappa_\alpha = \kappa_\beta \equiv \kappa$. If the number of physical qubits n is even, the DFS of maximal dimension with respect to the conditional time evolution between successive quantum jumps is formed by all possible n-particle quantum states with $(n/2)$ excited and $(n/2)$ unexcited qubits. This DFS is eigenspace of the operator $\sum_{\alpha=1}^{n} L_\alpha^\dagger L_\alpha$ with eigenvalue $\kappa(n/2)$ and with dimension $d = \binom{n}{n/2} \equiv n!/[(n/2)!]^2$. Thus, the conditional time evolution between successive quantum jumps is not perturbed by the reservoirs. Furthermore, for a given number of physical qubits n the dimension of this DFS is maximal so that the degree of redundancy is minimal. For the correction of quantum jumps we have to develop an active QECC within this DFS. Thereby we want to exploit the fact that we have to correct quantum jumps only which take place at a known 'position', say α. Let us start with the simplest possible case, namely the encoding of

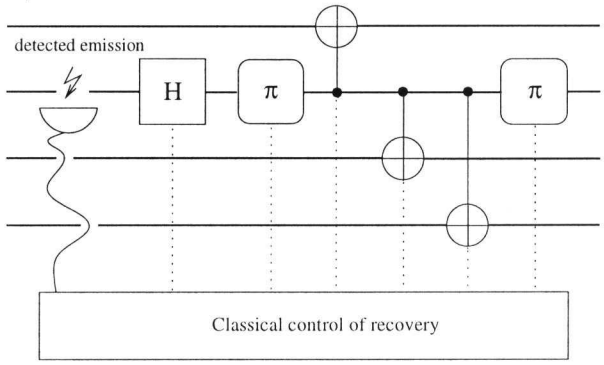

Figure 6. Network of quantum gates representing the sequence of unitary transformations recovering the state after a spontaneous emission. Here the second qubit of a four qubit register in a superposition of the codewords (27) is emitting a photon. After the detection of the emission, the sequence $\pi_2 C_{24} C_{23} C_{21} \pi_2 H_2$ is applied. The control of a $CNOT$ is depicted by $\bullet$, whereas $\oplus$ indicates that the value of the control qubit is added modulo 2 to the target qubit.

a single logical qubit with states $|0\rangle_L$ and $|1\rangle_L$. The following four-qubit encoding will do:

$$|0\rangle_L \rightarrow |c_0\rangle = \frac{|1100\rangle + |0011\rangle}{\sqrt{2}}, \quad |1\rangle_L \rightarrow |c_1\rangle = \frac{|0110\rangle + |1001\rangle}{\sqrt{2}}. \tag{27}$$

This encoding is formed by complementary pairs within this DFS. These complementary pairs involve an excited state at any 'position'. Provided the error 'position' α is known this encoding represents an active QECC with error distance $t = 1$ formed by basis states of the DFS with dimension $d = 6$. This encoding violates Eqs. (18) for $\alpha \neq \beta$ as $\langle c_0|L_4^\dagger L_2|c_1\rangle = 1/2\ \langle 0010|0010\rangle = 1/2$ and $\langle c_0|L_3^\dagger L_1|c_1\rangle = 1/2\ \langle 0001|0001\rangle = 1/2$, for example. Provided a quantum jump L_α has occured at 'position' α immediate application of the unitary recovery operator $R_\alpha = \pi_\alpha(\prod_{\beta\neq\alpha} C_{\alpha\beta})\pi_\alpha H_\alpha$ restores the unperturbed quantum state again. Thereby π_α, H_α, and $C_{\alpha\beta}$ represent a π-rotation, a Hadamard transformation of qubit α and a conditional $CNOT$ operation with control and target qubits α and β. Fig. 6 shows the recovery of a emission of the second qubit in a four qubit code. On the code space formed by all possible linear combinations of the logical qubits of Eq. (27) R_α is the left-inverse of the quantum jump operator L_α. For the construction of such a left-inverse unitary recovery operator R_α the orthogonal code words $|c_i\rangle$ have to fulfill the necessary and sufficient conditions

$$\langle c_i|L_\alpha^\dagger L_\alpha|c_j\rangle = \Lambda_\alpha \delta_{ij}. \tag{28}$$

These conditions reflect the fact the the invertibility conditions of Eq. (18) have to be fulfilled for $\alpha = \beta$ only. It should also be mentioned that it is also possible to encode a third logical quantum state, say $|2\rangle_L$, within the above mentioned DFS, i.e. $|2\rangle_L \rightarrow |c_2\rangle = \frac{1}{\sqrt{2}}(|1010\rangle + |0101\rangle)$. Thus, the three logical quantum states $|c_0\rangle, |c_1\rangle, |c_2\rangle$ involving 4 physical qubits with two of them being excited form a one-error detected-jump correcting quantum code which is denoted by 1-JC(4,2,3).

It is straightforward to generalize this construction to larger numbers of logical qubits. In analogy to Eq. (27) one starts from an even number n of physical qubits and from the corresponding DFS of dimension $d = \binom{n}{n/2}$. This DFS is formed by all possible n-qubit states with $(n/2)$ excited and $(n/2)$ unexcited qubits. Within this DFS one forms the logical states of the active QECC from all possible equally weighted complementary pairs of states. The resulting embedded quantum code can correct single-qubit errors up to an error distance $t = 1$. If one is able to detect the error position with a probability of unity and to apply the recovery operation instantaneously, the given code is perfect as long as the time between two successive jumps is nonzero. Under these conditions it works perfect provided all qubits decay with the same rate. For unequal decay rates stabilizing properties of a one error detected-jump correcting quantum code with six physical qubits are apparent from Fig. 7 where this code is used to stabilize Grover's algorithm. The one-error detected-jump correcting quantum code still succeeds almost perfectly in finding the final state $|x_0\rangle$.

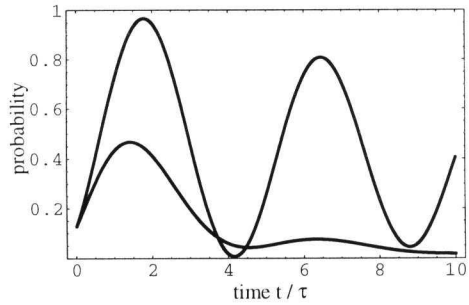

Figure 7. Time evolution of Grovers algorithm as described by Eq. (24) for decay rates randomly selected from a Gaussian ensemble with mean decay rate $\overline{\kappa} = \langle \nu \, | s \rangle / \tau$ and a variance $\Delta\kappa = (2/5)\ \overline{\kappa}$: with an embedded code using 6 qubits to encode 3 logical qubits (upper curve); 3 qubits without encoding (lower curve).

The constructed one-error correcting quantum codes are optimal in the sense that for a given number n of physical qubits the number of logical qubit states l is maximal and of magnitude $l = \binom{n-1}{n/2-1} \equiv \frac{1}{2}\binom{n}{n/2}$. This can be shown by the following dimension estimate. For a given number n of physical qubits, k of which are excited, and a given number t of errors at known 'positions' $\alpha_1, ..., \alpha_t$ the number of logical states l is bounded by the inequality $l \leq \binom{n-t}{k-t}$. This upper bound originates from the fact that after t quantum jumps t qubits are in state $|0\rangle$ at known 'positions'. As the logical states have to be recovered from these latter states by a unitary transformation the dimension of the corresponding Hilbert space, namely $\binom{n-t}{k-t}$, also determines the maximum possible number of orthogonal logical states. Using the basic symmetry property of binomial coefficients the maximum number of logical qubits is achieved for $k = [n/2]$. Thereby $[x]$ denotes the largest integer smaller or equal to x. So we arrive at the final result that for $t = 1$ the maximum number of logical quantum states is given by $l = \binom{n-1}{n/2-1} \equiv (1/2)\binom{n}{n/2}$.

Due to their simplicity these one-error detected-jump correcting quantum codes are suited well for stabilizing quantum algorithms. There is no need for control measurements determining the error syndrome. The required error position and jump time are obtained by monitoring qubits continuously. In the case of radiative decay, for example, the spontaneously emitted photons may be detected by photodetection or one may measure the resulting recoil acting on the physical qubit. In particular, this latter method may also be applicable to phononic decay processes. These aspects and the minimal redundancy of these quantum codes make them particularly attractive for stabilizing quantum computers which are based on arrays of trapped ions[6] or nuclear spins.[7]

4.3. Multiple-jump codes and error-designs

The constructed one-error detected-jump correcting quantum codes can be generalized to an arbitrary number t of errors and an arbitrary number of qubits.[4] The resulting quantum codes are capable of correcting up to t errors simultaneously. Correspondingly, we define a t-detected-jump correcting quantum code $t - JC(n, k, l)$ by a set of l orthogonal code words $\{|c_i\rangle, i = 1, ..., l\}$ formed by linear superpositions of n-qubit states each of which involves k excited and $n - k$ unexcited states. Analogous to Eqs.(28) these code words have to fulfill the conditions

$$\langle c_i | L_{\mathbf{e}}^{\dagger} L_{\mathbf{e}} | c_j \rangle = \Lambda_{\mathbf{e}} \delta_{ij} \tag{29}$$

which are sufficient and necessary for the existence of unitary recovery operations. Thereby the error operator $L_{\mathbf{e}}$ denotes an arbitrary product of Lindblad operators, say $L_{\alpha_m} ... L_{\alpha_1}$, corresponding to a jump pattern $\mathbf{e} \equiv (\alpha_1, \ldots, \alpha_m)$ of length m. Eqs. (29) have to be fulfilled for all possible jump patters $\mathbf{e}$ of length m not greater than t. According to this terminology our previously constructed optimal one-error correcting codes are of the type $1 - JC(n, n/2, (1/2)\binom{n}{n/2})$ with n being even. Furthermore, our previous dimensional estimate implies that t-detected-jump correcting quantum codes of the type $t - JC(n, n/2, \binom{n-t}{n/2-t})$ would be optimal.

A general method for constructing $t - JC(n, k, l)$ codes with $t \geq 2$ is not known at present. However, for codewords consisting of linear superpositions of quantum states with equal amplitudes one can establish an illuminating connection with combinatorial design theory.[38,39] This link to this well developed area of discrete mathematics is expected to be particularly fruitful for the further exploration of general $t - JC(n, k, l)$-codes. In order to exhibit

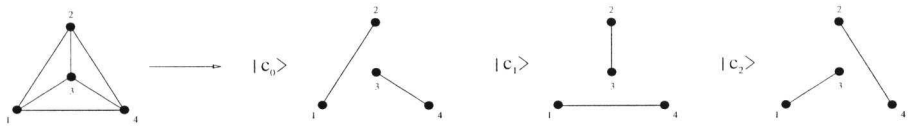

Figure 8. Schematic representation of the finite affine plane associated with the $1 - JC(4, 2, 3)$-code. Also indicated is the partition of blocks defining the $1 - JC(4, 2, 3)$-code which is associated with the three code words $|c_0\rangle, |c_1\rangle, |c_2\rangle$.

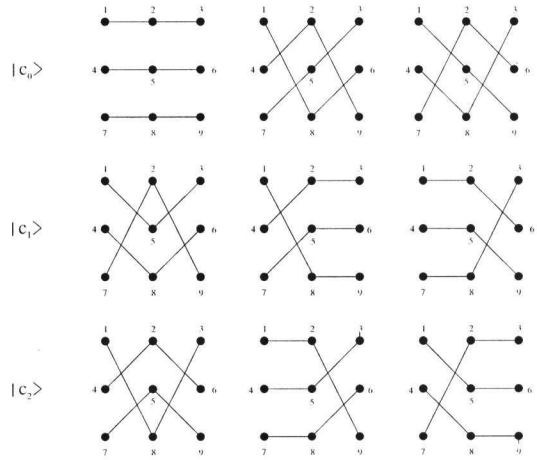

Figure 9. Partition of blocks defining the $2 - JC(9, 3, 3)$-code.

basic ideas of this connection let us reconsider the previously introduced optimal $1 - JC(4, 2, 3)$-code as a simple example. The set of the three code words $|c_0\rangle, |c_1\rangle, |c_2\rangle$ can be represented graphically by the connected diagram depicted in Fig. 8. Each point of this diagram is associated with a qubit and two connected points, i.e. a block, indicates that these two qubits are in the excited state $|1\rangle$. Within the framework of finite geometry this connected diagram forms an affine finite plane over a binary field. In this context the six blocks of Fig. 8 represent lines, i.e. one dimensional subspaces of this geometry. The three code words $|c_0\rangle, |c_1\rangle, |c_2\rangle$ correspond to the three possible disjoint pairs of blocks, i.e. to the three possible parallel pairs of lines. An example of a $2 - JC(9, 3, 3)$-code which is constructed with the help of this analogy by using known results of design theory[38] is depicted in Fig. 9.

Summary

A new kind of embedded quantum codes[4] has been discussed which is capable of stabilizing distinguishable qubits against spontaneous decay. Being an embedded code it combines advantages of active QECCs and of passive quantum error correction. In particular, the mean number of required recovery operations equals the mean number of spontaneous decay events and the dynamics between successive quantum jumps are stabilized passively. Furthermore, by exploiting information about the error position the redundancy of these quantum codes is significantly smaller than the one of previously proposed embedded quantum codes. Numerical simulations demonstrate that these quantum codes work well also in cases where the distinguishable qubits decay spontaneously with unequal rates. Due to their minimal redundancy the constructed optimal one-error detected-jump correcting quantum codes are particularly relevant for stabilizing quantum computers which are based on arrays of trapped ions[6] or nuclear spins.[7] The discussed connection with combinatorial design theory may turn out to be particularly useful for the further exploration of many-error detected-jump correcting quantum codes.

ACKNOWLEDGMENTS

This work was supported by the DFG within the SPP 'Quanteninformationsverarbeitung'. A.D.'s work was supported by the DAAD. We are grateful to Thomas Beth, Markus Grassl and Chris Charnes for introducing us into the

fascinating area of design theory. Helpful discussions with Dominik Janzing, Dietmar Fischer and Holger Mack are acknowledged.

REFERENCES

1. J. Gruska, *Quantum Computing*, McGraw-Hill, 1999.
2. D. Bouwmeester, A. Ekert, and A. Zeilinger (Eds.), *The Physics of Quantum Information*, Springer, Berlin, 2000.
3. G. Alber, Th. Beth, M. Horodecki, P. Horodecki, R. Horodecki, M. Rötteler, H. Weinfurter, R. Werner, and A. Zeilinger, *Quantum Information*, Springer, Berlin, 2001.
4. G. Alber, Th. Beth, Ch. Charnes, A. Delgado, M. Grassl, and M. Mussinger, "Stabilizing distinguishable qubits against spontaneous decay by detected-jump correcting quantum codes", submitted to *Phys. Rev. Lett.*
5. M. Mussinger, A. Delgado, and G. Alber, "Error avoiding quantum codes and dynamical stabilization of Grover's algorithm", *New Journal of Physics* **2**, 19.1 -19.16, 2000.
6. J. I. Cirac and P. Zoller, " A scalable quantum computer with ions in an array of microtraps", *Nature*, London, **404**, 579, 2000.
7. B. E. Kane, "A silicon-based nuclear spin quantum computer", *Nature*, London **393**, 133, 1998.
8. D. Deutsch,"Quantum theory, the Church-Turing principle and the universal quantum computer", *Proc. Roy. Soc. London A*, 400.97-117, (1985).
9. D. R. Simon, "On the power of quantum computation", in *Proceedings of 35th Annual Symposium on the Foundation of Computer Science, 1994, Los Alamitos, California*, pp.116, IEEE Computer Society Press, New York, 1994.
10. W. Shor, in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, edited by S. Goldwasser, p. 124, IEEE Computer Society, Los Alamitos, CA, 1994.
11. L. K. Grover, "Quantum Mechanics Helps in Searching for a Needle in a Haystack", *Phys. Rev. Lett.* **79**, 325 (1997); " Quantum Computers Can Search Rapidly by Using Almost Any Transformation", *Phys. Rev. Lett.***80**, 4329 (1998).
12. I. L. Chuang, N. Gershenfeld, and M. Kubinec, "Experimental Implementation of Fast Quantum Searching", *Phys. Rev. Lett.* **80**, 3408 (1998).
13. E. Bernstein, U. Vazirani, "Quantum complexity theory", *SIAM Journal on Computing* **26**, 1411 (1997).
14. C. Zalka, "Grover's quantum searching algorithm is optimal", *Phys. Rev. A* **60**, 2746 (1999).
15. M. Boyer, G. Brassard, P. Hoyer, and A. Tapp, "Tight Bounds on Quantum Searching", *Fortschr. Phys.* **46**, 493 (1998).
16. An alternative Hamiltonian description has been introduced by E. Fahri and S. Gutmann, "Analog analogue of a digital quantum computation", *Phys. Rev. A* **57**, 2403 (1998).
17. L. Schulman, *Techniques and Applications of Path Integration*,Wiley, New York, 1981.
18. I. Sh. Averbukh and N. F. Perelman, "Fractional revivals: universality in the long-term evolution of quantum wave packets beyond the correspondence principle dynamics", *Phys. Lett. A* **139**, 449 (1989).
19. C. Miquel, J. P. Paz, and W. H. Zurek, "Quantum Computation with Phase Drift Errors", *Phys. Rev. Lett.* **78**, 3971 (1997).
20. P. W. Shor, " Scheme for reducing decoherence in quantum computer memory", *Phys. Rev. A* **52**, R2493 (1995).
21. D. Gottesman, "Class of quantum error-correcting codes saturating the quantum Hamming bound", *Phys. Rev. A* **54**, 1862 (1996).
22. R. Laflamme, C. Miquel, J. P. Paz, and W. H. Zurek, " Perfect Quantum Error Correcting Code" *Phys. Rev. Lett.* **77**, 198 (1996).
23. A. M. Steane, "Error Correcting Codes in Quantum Theory", *Phys. Rev. Lett.* **77**, 793 (1996).
24. E. Knill and R. Laflamme, "Theory of quantum error-correcting codes", *Phys. Rev. A* **55**, 900 (1997).
25. L. M. Duan and G. C. Guo, "Preserving Coherence in Quantum Computation by Pairing Quantum Bits", *Phys. Rev. Lett.* **79**, 1953 (1997).
26. P. Zanardi and M. Rasetti, "Noiseless Quantum Codes", *Phys. Rev. Lett.* **79**, 3306 (1997).
27. P. Zanardi, "Dissipation and decoherence in a quantum register", *Phys. Rev. A* **57**, 3276 (1998); "Computation on an error-avoiding quantum code and symmetrization", *Phys.Rev. A* **60**, R729 (1999).

28. D. A. Lidar, I. L. Chuang, and K. B. Whaley, "Decoherence-Free Subspaces for Quantum Computation", *Phys. Rev. Lett.* **81**, 2594 (1998).
29. D. Welsh, *Codes and Cryptography*, Clarendon Press, Oxford,1988.
30. D. A. Lidar, D. Bacon, and K. B. Whaley, "Concatenating Decoherence-Free Subspaces with Quantum Error Correcting Codes", *Phys. Rev. Lett.* **82**, 4556 (1999).
31. L. M. Duan and G. C. Guo, "Reducing decoherence in quantum-computer memory with all quantum bits coupling to the same environment", *Phys. Rev. A* **57** 737 (1998).
32. D. Bacon, J. Kempe, D. A. Lidar, and K. B. Whaley, "Universal Fault-Tolerant Quantum Computation on Decoherence-Free Subspaces", *Phys. Rev. Lett.* **85** 1758 (2000).
33. D. A. Lidar, D. Bacon, and K. B. Whaley, "Robustness of decoherence-free subspaces for quantum computation", *Phys. Rev. A* **60**, 1944 (1999).
34. H. J. Carmichael, in *An Open Systems Approach to Quantum Optics*, Springer Verlag, Berlin, 1993.
35. H. Mabuchi and P. Zoller, "Inversion of Quantum Jumps in Quantum Optical Systems under Continuous Observation", *Phys. Rev. Lett.* **76**, 3108 (1996).
36. U. Weiss, *Quantum Dissipative Systems*, Series in Modern Condensed Matter Physics, Vol. 2, World Scientific, Singapore, 1993.
37. M. B. Plenio, V. Vedral, and P. L. Knight, "Quantum error correction in the presence of spontaneous emission", Phys. Rev. A **55**, 67 (1997).
38. Th. Beth, D. Jungnickel, and H. Lenz, *Design Theory*, Vol. I, 2nd edition, Cambridge University Press, Cambridge, 1999.
39. Th. Beth, D. Jungnickel, and H. Lenz, *Design Theory*, Vol. II, 2nd edition, Cambridge University Press, Cambridge, 1999.