

Error avoiding quantum codes and dynamical stabilization of Grover's algorithm

This article has been downloaded from IOPscience. Please scroll down to see the full text article.

2000 New J. Phys. 2 19

(<http://iopscience.iop.org/1367-2630/2/1/319>)

View [the table of contents for this issue](#), or go to the [journal homepage](#) for more

Download details:

IP Address: 38.107.179.210

The article was downloaded on 20/02/2012 at 07:50

Please note that [terms and conditions apply](#).

Error avoiding quantum codes and dynamical stabilization of Grover's algorithm

Michael Mussinger, Aldo Delgado and Gernot Alber

Abteilung für Quantenphysik, Universität Ulm, D-89069 Ulm, Germany

New Journal of Physics **2** (2000) 19.1–19.16 (<http://www.njp.org/>)

Received 31 March 2000; online 12 September 2000

Abstract. Dynamical stabilization properties of error avoiding quantum codes are investigated beyond the perturbative regime. As an example Grover's search algorithm and its behaviour under a particular class of coherent errors are studied. Numerical examples which demonstrate that error avoiding quantum codes may be capable of stabilizing quantum algorithms well beyond the regime for which they were designed originally are presented.

1. Introduction

According to a suggestion of Feynman [1] quantum systems not only are of interest for their own sake but also might serve for practical purposes. Thus they may be used for simulating other quantum systems which are less convenient to handle or they may be used for solving computational problems more efficiently than can be achieved by any other classical means. Two well known examples demonstrating the latter point are Shor's factorization algorithm [2] and Grover's search algorithm [3, 4].

Quantum systems which are capable of performing quantum algorithms are called quantum computers. So far several physical systems have been considered as potential candidates for quantum computers, such as trapped ions [5], nuclear spins of molecules [6] and, in the context of cavity quantum electrodynamics, atoms interacting with a single mode of the radiation field [7]. To describe the operation of a quantum computer theoretically it is advantageous to refrain from a detailed physical description of the particular quantum system involved. Thus, in analogy to the spirit of computer science, it is more useful to concentrate on those particular aspects which are essential for the performance of quantum computation. On this abstract level a generic quantum computer consists of m distinguishable smaller quantum systems which are frequently chosen as two-level systems with basis states $|1\rangle$ and $|0\rangle$, for example. The quantum information which can be stored in one of these two-level systems is called a qubit. Thus the state space of a generic quantum computer is spanned by the so-called computational basis

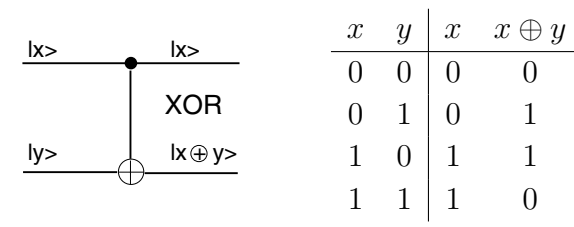


Figure 1. A quantum mechanical version of the classical XOR gate as an example of a quantum gate (a CNOT gate). The input state $|x, y\rangle$ is mapped onto the output state $|x, x \oplus y\rangle$.

which consists of the corresponding 2^m product states $|b_0\rangle = |0 \dots 00\rangle$, $|b_1\rangle = |0 \dots 01\rangle$, $\dots |b_{2^m-1}\rangle = |1 \dots 11\rangle$.

A typical quantum computation proceeds in several steps. Firstly, the quantum computer is prepared in an initial state. Secondly, a certain sequence of unitary transformations is performed. They are called quantum gates and usually entangle the m qubits. Thirdly, the final result is measured. Typically the solution of a particular computational problem is obtained with a certain probability only. A general quantum algorithm takes advantage of an essential feature of quantum theory, namely the interference between probability amplitudes and the fact that the dimensionality D of the state space of m distinguishable qubits increases exponentially with the number of qubits, i.e. $D = 2^m$. Among the best known quantum algorithms are the Shor algorithm [2] and Grover's search algorithm [3, 4, 8]. In the latter algorithm a particular sequence of quantum gates (see figure 1) allows one to find a specific item in an unsorted database much faster than can be done with any other known classical means. This quantum algorithm has already been realized experimentally for a small number of qubits [9].

Among the main practical problems one has to overcome in the implementation of quantum algorithms are non-ideal performances of the quantum gates [10] involved and random environmental influences, both of which tend to affect the relevant quantum coherence. To protect quantum computation against such errors, two major strategies have been proposed recently, namely active quantum error correction [11]–[19] and passive error avoiding quantum codes [20]–[24]. Active quantum error correction may be viewed as a generalization of classical error correction techniques to the quantum domain. Typically, active quantum error correction involves a properly chosen sequence of frequently repeated measurements. The approach of the error avoiding quantum codes is different. The main idea is to encode the logical information in one of those subspaces of the relevant Hilbert space which is not affected by the physical interactions responsible for the occurrence of errors [20]–[24]. Both theoretical approaches to error correction rely on the concept of redundancy, which is also fundamental for classical error correcting codes [25]. It is expected that error avoiding codes will offer more effective means for stabilizing quantum algorithms. This expectation is based on two facts. Firstly, there is no need for control measurements which are an essential ingredient of any active error correcting code. Secondly, in many cases a smaller number of *physical* qubits is needed for the representation of a given number of *logical* qubits.

In the subsequent discussion it is demonstrated that this is indeed the case. By considering Grover's quantum search algorithm it is shown that non-ideal perturbations may be corrected dynamically in an efficient way with the help of an appropriate error avoiding quantum code. By

generalizing recent perturbative results [26], it is demonstrated that error avoiding quantum codes may be applicable well beyond the type of errors for which they were originally designed. As a particular example, we discuss coherent errors which may arise from systematic detunings of the physical qubits of the quantum computer from the frequency of the light pulses which realize the required quantum gates. The corresponding error avoiding quantum code with the lowest degree of redundancy is more efficient at encoding quantum information than is any possible active error correcting code which saturates the quantum Hamming bound. The error avoiding quantum code [20] used consists solely of states which are factorizable in the computational basis. In this respect it differs significantly from the recently proposed error avoiding code of [21], for example, which also involves entangled states. Such factorizable codes may offer practical advantages insofar as the implementation of quantum gates in error avoiding subspaces is concerned.

The paper is organized as follows. In section 2 basic facts about Grover's quantum search algorithm are summarized. It is demonstrated that, for large databases, the dynamics of this quantum algorithm can be described by a two-level Hamiltonian which implies that there are Rabi oscillations between the initial state and the sought state. In section 3 general ideas underlying the construction of error avoiding quantum codes are discussed. An efficient error avoiding quantum code which is capable of stabilizing Grover's algorithm against a particular class of coherent errors is presented. The redundancy of this code is discussed and compared with that resulting from active error correcting codes which saturate the quantum Hamming bound. Numerical examples demonstrating the stabilizing capabilities of this error avoiding quantum code are presented in section 4.

2. Grover's quantum search algorithm

Consider an unsorted database with N items and a certain item x_0 for which you are searching. As a particular example you can imagine a telephone directory with N entries and a particular telephone number x_0 for which you are looking. Furthermore, assume that you are given a black box, i.e. a so-called oracle, which can decide whether an item is x_0 . Thus, in mathematical terms you are given a Boolean function

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

with $\delta_{a,b}$ denoting the Kronecker delta function. Usually the elements x of the database are assumed to be described by the N integers between zero and $N - 1$. Assuming that each application of the 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, on average a classical algorithm will need $N/2$ steps to find the sought item x_0 . It has been shown by Grover [3, 4] 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. The basic idea of this quantum algorithm is to rotate the initial state of the quantum computation in the direction of the sought state $|x_0\rangle$ by a sequence of unitary quantum versions of the oracle. It will become apparent from the subsequent discussion that, apart from Hadamard transformations, the dynamics of this rotation is analogous to a Rabi oscillation between the initially prepared state and the sought state $|x_0\rangle$. It has been shown by Zalka [27] that Grover's quantum search algorithm is optimal.

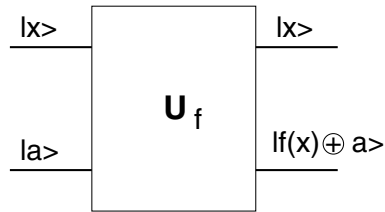


Figure 2. A schematic representation of the quantum oracle \mathcal{U}_f . For $f(x) \equiv x$ this quantum gate reduces to the CNOT gate of figure 1; for $|a\rangle \equiv |a_0\rangle = 1/\sqrt{2}(|0\rangle - |1\rangle)$ it results in the conditional phase inversion I_{x_0} of equation (9) that is needed in Grover's algorithm.

2.1. The characteristic gate sequence of Grover's search algorithm

In Grover's quantum search algorithm every element of the database is represented by a state of the computational basis of the quantum computer. Thus a database which is represented by m qubits has $N = 2^m$ distinguishable elements. The state $|0 \dots 0110 \dots 0\rangle$ of the computational basis, for example, corresponds to the element $0 \dots 0110 \dots 0$ of the database in binary notation. The quantum oracle \mathcal{U}_f (see figure 2) is determined completely by the Boolean function of equation (1) and is represented by a quantum gate, i.e. by the unitary and Hermitian transformation

$$\mathcal{U}_f : |x, a\rangle \rightarrow |x, f(x) \oplus a\rangle. \quad (2)$$

Thereby $|x\rangle$ is an arbitrary element of the computational basis and $|a\rangle$ is the state of an additional ancillary qubit which is discarded later. The symbol \oplus denotes addition modulo 2. This unitary form of the oracle depends on the Boolean function $f(x)$. Insofar 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.

For the subsequent discussion it is important to note that the elementary rotations in the direction of the sought 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 $|x_0\rangle$. Implicit knowledge of it through the values of the Boolean function $f(x)$ is sufficient. For large values of N it turns out that the number of elementary rotations needed to prepare the state $|x_0\rangle$ is $O(\sqrt{N})$. To implement such an elementary rotation from the initial state $|s\rangle = |0 \dots 0\rangle$, for example, towards the final state $|x_0\rangle$ two different types of quantum gates are needed, namely *Hadamard* gates and *controlled phase inversions*.

A *Hadamard* gate is a unitary one-qubit operation. It produces an equally weighted superposition of the two basis states according to the rule

$$|0\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad (3)$$

$$|1\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \quad (4)$$

or, in matrix notation,

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

An m -qubit Hadamard gate $H^{(2^m)}$ is defined by the m -fold tensor product, i.e. $H^{(2^m)} = H^{(2)} \otimes \dots \otimes H^{(2)}$. Thus, for two qubits, for example, $H^{(2^2)}$ is represented by the matrix

$$H^{(2^2)} = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}. \quad (5)$$

The Hadamard transformation is Hermitian and unitary. An arbitrary matrix element $H_{i,j}^{(2^m)}$ of a Hadamard transformation may be written in the general form

$$H_{i,j}^{(2^m)} = \frac{1}{\sqrt{2^m}} (-1)^{i \odot j}. \quad (6)$$

Here i and j denote binary numbers and the multiplication \odot is bitwise modulo 2, i.e. for $i = 1$, $j = 3$ and $m = 2$, one obtains $H_{1,3}^{(4)} = \frac{1}{2} (-1)^{(01 \odot 11)} = \frac{1}{2} (-1)^{(0 \times 1 + 1 \times 1)} = -\frac{1}{2}$. It has been shown by Grover [3, 4] that this Hadamard transformation can be replaced by any other unitary one-qubit operation.

The remaining quantum gates needed for the implementation of the necessary rotation are *controlled phase inversions* with respect to the initial and sought states $|s\rangle = |0 \dots 0\rangle$ 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 π and leaves all other states unchanged. Thus the phase inversion I_s with respect to the initial state $|s\rangle$ is defined by

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

For two qubits, for example, its matrix representation is given by

$$I_s = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \quad (8)$$

The controlled phase inversion I_{x_0} with respect to the sought state $|x_0\rangle$ is defined in an analogous way. Because the state $|x_0\rangle$ is not known explicitly but only implicitly through the property $f(x_0) = 1$, this transformation has to be performed with the help of the quantum oracle. This task can be achieved by preparing the ancillary of the oracle of equation (2) in the 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

$$\begin{aligned} |x, f(x) \oplus a_0\rangle &\equiv |x, 0 \oplus a_0\rangle = (1/\sqrt{2})(|x, 0\rangle - |x, 1\rangle) = |x, a_0\rangle & \text{for } x \neq x_0 \\ |x, f(x) \oplus a_0\rangle &\equiv |x, 1 \oplus a_0\rangle = (1/\sqrt{2})(|x, 1\rangle - |x, 0\rangle) = -|x, a_0\rangle & \text{for } x = x_0. \end{aligned} \quad (9)$$

One should bear in mind that this controlled phase inversion can be performed with the help of the quantum oracle of equation (2) only without explicit knowledge of the state $|x_0\rangle$.

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

$$Q = -I_s H^{(2^m)} I_{x_0} H^{(2^m)}. \quad (10)$$

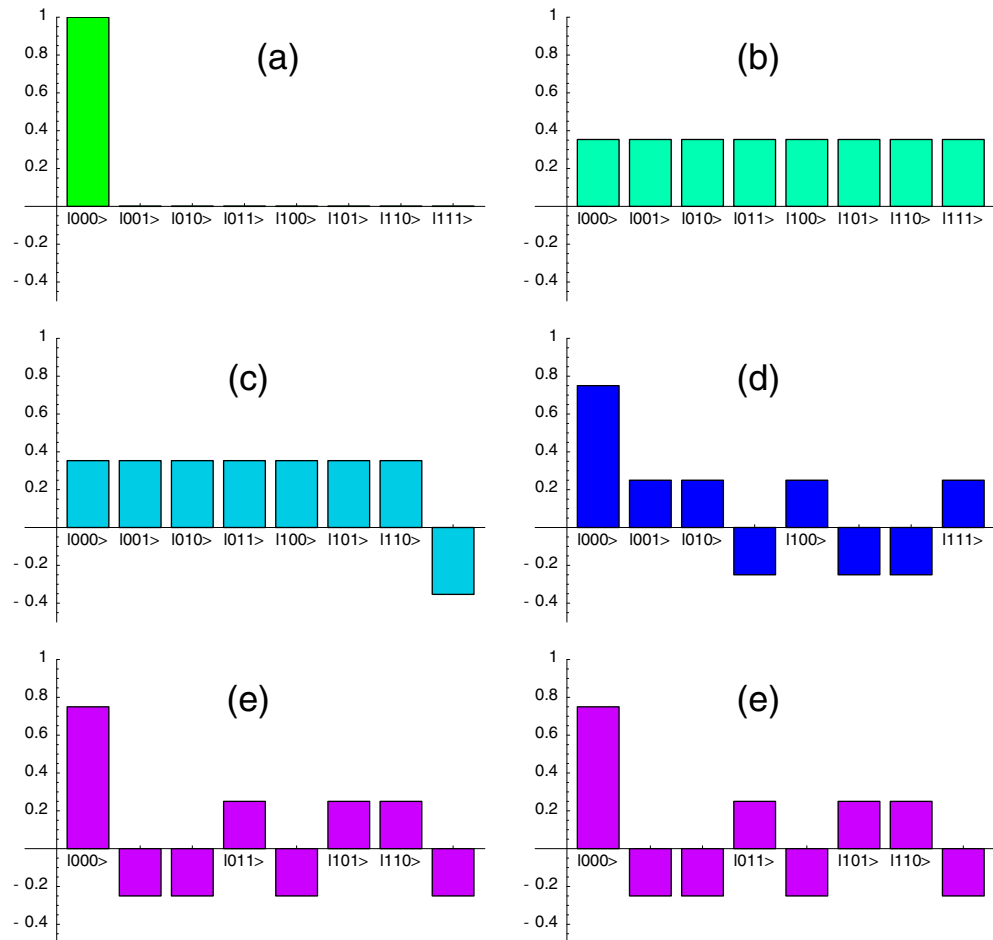


Figure 3. Amplitude distributions resulting from the various quantum gates involved in Grover's quantum search algorithm for the case of three qubits. The quantum states which are prepared by these gates are (a) $|s\rangle = |000\rangle$, (b) $H^{(2^m)}|s\rangle$, (c) $I_{x_0}H^{(2^m)}|s\rangle$, (d) $H^{(2^m)}I_{x_0}H^{(2^m)}|s\rangle$, (e) $-I_sH^{(2^m)}I_{x_0}H^{(2^m)}|s\rangle$ and (f) $-H^{(2^m)}I_sH^{(2^m)}I_{x_0}H^{(2^m)}|s\rangle$. The sought state $|x_0\rangle$ entering the Boolean function of equation (1) is assumed to be the state $|111\rangle$.

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

$$|f\rangle = HQ^n|s\rangle. \quad (11)$$

The effect of the elementary rotation Q is demonstrated in figure 3 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 sought 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 sought state $|111\rangle$. In this particular case an additional Hadamard transformation finally prepares the quantum computer in the sought 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 analyse the repeated application of the gate sequence Q according

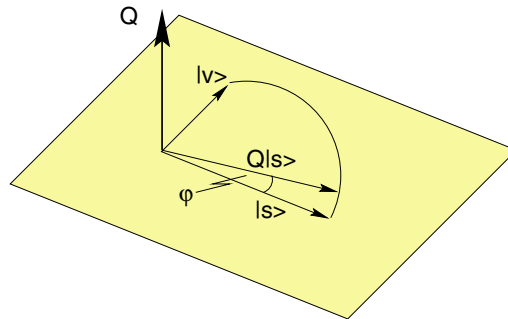


Figure 4. Q is a rotation in the subspace spanned by states $|s\rangle$ and $|v\rangle$.

to equation (11) 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 [3, 4], i.e.

$$Q \begin{pmatrix} |s\rangle \\ |v\rangle \end{pmatrix} = \begin{pmatrix} 1 - 4\epsilon^2 & 2\epsilon \\ -2\epsilon & 1 \end{pmatrix} \begin{pmatrix} |s\rangle \\ |v\rangle \end{pmatrix}. \quad (12)$$

Thus Q acts like a rotation in the plane spanned by states $|s\rangle$ and $|v\rangle$ (see figure 4). The angle of rotation is given by $\varphi = \arcsin[2\epsilon(1 - \epsilon^2)^{1/2}]$.

After j iterations the amplitude of state $|v\rangle$ is given by [8]

$$\sin[(2j + 1)\epsilon]. \quad (13)$$

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

$$n = \frac{\pi}{4 \arcsin(2^{-m/2})} - \frac{1}{2} \approx \frac{\pi}{4} \sqrt{2^m} \quad (2^m \gg 1). \quad (14)$$

Finally, it should be mentioned that several generalizations of Grover's original search algorithm which consider arbitrary initial states have also been presented [28, 29].

2.2. Hamiltonian representation of Grover's algorithm

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 (an alternative Hamiltonian description has been introduced by Fahri and Gutmann [30]). The elementary rotation Q can be approximated by the relation

$$Q = \mathbf{1} - \tau(i/\hbar)\mathbf{H}_G(\epsilon) + O(\epsilon^2) \quad (15)$$

which involves the Hamiltonian

$$\mathbf{H}_G = 2i\epsilon\frac{\hbar}{\tau}(|v\rangle\langle s| - |s\rangle\langle v|). \quad (16)$$

The elementary time τ might be interpreted as the physical time required for performing the elementary rotation Q . The Hamiltonian of equation (16) 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. To 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 [31], namely

$$Q^n = (-I_s H^{(2^m)} I_{x_0} H^{(2^m)})^n = \exp\left(-\frac{i}{\hbar} \mathbf{H}_G \tau n\right) + O(\epsilon^2 n). \quad (17)$$

Thus, in the framework of this Hamiltonian description, applying the elementary rotation Q n times is equivalent to a temporal 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. Since the errors entering equation (17) 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, because Grover's search algorithm needs approximately $(\pi\sqrt{2^m}/4)$ steps to find the sought item, the main condition which restricts the validity of this Hamiltonian description is a large size of the database, i.e. $\epsilon^2 \equiv 1/N \ll 1$.

2.3. An example of coherent errors

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 is 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 temporal evolution of the quantum algorithm. A simple example of this type of errors is systematic detuning 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

$$\mathbf{H}_d = \sum_{i=1}^m \hbar \omega_i \sigma_z^{(i)}. \quad (18)$$

In equation (18) 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 . A possible result is shown in figure 5. 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 is described by the Hamiltonians of equations (16) and (18).

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 figure 5. The dynamics of the ideal Grover algorithm for the case of three qubits, i.e. $m = 3$, is depicted by the broken line. The Rabi oscillations with frequency $\Omega = 2\langle v|s\rangle/\tau$ are clearly visible. The full line shows the probability of observing the quantum computer in the 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. Owing to the coherent nature of the errors, the temporal evolution of the non-ideal algorithm exhibits revival phenomena [32].

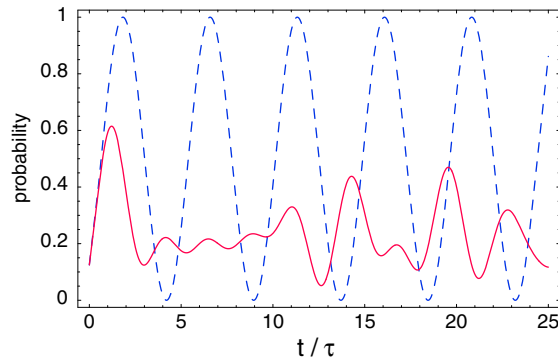


Figure 5. The probability of being in the state $|x_0\rangle$ after $n = t/\tau$ iterations of Grover's quantum search algorithm for three qubits: the ideal dynamics according to the Hamiltonian time evolution characterized by equations (16) and (17) (broken line); and the non-ideal case of coherent errors characterized by equations (16)–(18) (full line) with detunings $\omega_1 = 0.5\langle s|v\rangle/\tau$, $\omega_2 = 0.3\langle s|v\rangle/\tau$ and $\omega_3 = 0.2\langle s|v\rangle/\tau$.

3. Error avoiding quantum codes

In general there are two different strategies for correcting errors in quantum information processing. *Active quantum error correcting schemes* may be viewed as generalizations of classical error correction techniques to the quantum domain [11]–[14]. Typically they involve a suitably chosen quantum code 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 these orthogonal quantum states can be distinguished and, from the result of a control measurement, one may restore the original quantum state. So far these general techniques have been applied mainly to the stabilization of static quantum memories [33].

The second possible error correction strategy, which seems to be suitable also for stabilizing quantum algorithms, is based on *error avoiding quantum codes* [20]–[24]. These latter methods rely on knowledge of basic properties of the relevant error. The main idea is to encode the quantum information in those subspaces of the Hilbert space which are not affected by the errors. This aim is achieved by restricting oneself to degenerate eigenspaces of the relevant error operators. Thus, in the special case of a single error operator, say \mathbf{E} , the basis states $\{|\psi_i\rangle\}$ of such an error-free subspace have to satisfy the relation

$$\mathbf{E}|\psi_i\rangle = c|\psi_i\rangle. \quad (19)$$

Error avoiding quantum codes are completely degenerate error correcting codes in the sense that the code space is preserved under the influence of the errors and therefore no recovery operation is needed [34]. In the above-mentioned example of coherent errors which may affect Grover's algorithm this error operator is given by the Hamiltonian of equation (18), i.e. $\mathbf{E} = \mathbf{H}_d$. It is crucial for the success of an error avoiding code that the eigenvalue c of equation (19) does not depend on the states belonging to the error-free subspace. This implies that all possible elements of the error-free subspace of the general form $\sum_i \alpha_i |\psi_i\rangle$ are affected by the error operator in the

same way, i.e.

$$\mathbf{E}\left(\sum_i \alpha_i |\psi_i\rangle\right) = c\left(\sum_i \alpha_i |\psi_i\rangle\right). \quad (20)$$

It is apparent that a non-trivial error avoiding code is possible only if the eigenspace of the error operator \mathbf{E} is degenerate.

3.1. An error avoiding quantum code stabilizing coherent errors

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 equation (18). In the simple case of equal detunings, i.e. $\omega_1 = \dots = \omega_m \equiv \omega$, the error operator \mathbf{E} reduces to the form

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

It is easy to find highly degenerate error-free subspaces of this error operator. All states with a fixed number of ones and zeros constitute a degenerate eigenspace of \mathbf{H}_e [34, 35]. For an even number of qubits it is possible to find an error avoiding subspace with eigenvalue $c = 0$ so that

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

for all elements $|\psi\rangle$ of this subspace. For this purpose one is looking for quantum states with zero total spin. For four qubits, for example, this subspace is defined by the basis vectors $|0011\rangle$, $|0101\rangle$, $|0110\rangle$, $|1001\rangle$, $|1010\rangle$ and $|1100\rangle$ 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.

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

This particular error avoiding code works ideally for equal detunings of all qubits from resonance. It is formed by quantum states which factorize in the computational basis. So it is expected that the encoding of quantum information and the implementation of quantum gates in this error-free subspace will be considerably easier than will that in cases in which the error avoiding codes involve entangled quantum states.

3.2. Implementation of quantum gates in an error-free subspace

To realize a quantum algorithm in an error-free subspace one has to implement the necessary quantum gates in such a way that they do not mix the error-free subspace with its orthogonal complement [36, 37]. Consider two logical qubits, for example, which are encoded by four physical qubits. For this purpose one may choose the states $|0011\rangle$, $|0101\rangle$, $|0110\rangle$ and $|1001\rangle$ which have been mentioned in the previous subsection. This error avoiding code works ideally for stabilizing Grover's algorithm with respect to the error operator \mathbf{H}_e of equation (21) provided that it is possible to realize the required unitary transformations, namely Hadamard transformations and the controlled phase inversions.

Consider as an example a Hadamard transformation which acts in a two-dimensional error avoiding subspace of this kind. Hence it is assumed that the two basis states of this error avoiding

code are given by $|01\rangle$ and $|10\rangle$ and that they involve two physical qubits. Thus, we are looking for a transformation which performs the mappings

$$\begin{aligned} |01\rangle &\rightarrow (1/\sqrt{2})(|01\rangle + |10\rangle) \\ |10\rangle &\rightarrow (1/\sqrt{2})(|01\rangle - |10\rangle) \end{aligned} \quad (23)$$

and which does not mix the subspace spanned by $|01\rangle$ and $|10\rangle$ with the orthogonal space spanned by the basis states $|00\rangle$ and $|11\rangle$. In matrix notation we are looking for a unitary matrix of the form

$$\begin{pmatrix} * & 0 & 0 & * \\ 0 & 1 & 1 & 0 \\ 0 & 1 & -1 & 0 \\ * & 0 & 0 & * \end{pmatrix} \quad (24)$$

with $*$ denoting arbitrary entries which ensure unitarity. Such a transformation can be achieved by the gate sequence $CNOT_{21}(\mathbf{1} \otimes \tilde{H}^{(2)})CNOT_{21}$ with $\tilde{H}^{(2)} = -i\sigma_y H^{(2)}$. Here $CNOT_{21}$ is a controlled-not operation with the first qubit as the target and the second qubit as the control qubit and σ_y is the Pauli matrix. Thus in matrix notation this relation yields

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} -1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & -1 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & -1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}. \quad (25)$$

Obviously the final result does not mix the error avoiding subspace with its orthogonal complement. However, such a mixing might take place in the intermediate steps, depending on which set of universal quantum gates can be implemented. However, even in the worst possible case it suffices to ensure that the time spent by the quantum computer in the orthogonal complement of the error avoiding subspace is sufficiently small that the resulting errors can be neglected for all practical purposes. Under these circumstances it is expected that the implementation of quantum algorithms in error avoiding subspaces will be a powerful means for stabilizing quantum codes.

3.3. Code sizes of error avoiding quantum codes

In order to estimate the redundancy which has to be introduced for stabilizing a quantum algorithm by an error avoiding quantum code let us consider the particular example of section 3.1 in more detail. It has been argued that, in the case of coherent errors which can be characterized by the Hamiltonian of equation (21), an error avoiding quantum code can be constructed from basis states with equal numbers of ones and zeros. In order to minimize the redundancy it is desirable to maximize the dimension of the resulting error avoiding subspace. If one starts with m physical qubits, the dimension $D(m, q)$ of the corresponding error avoiding subspace with q qubits in state $|1\rangle$ and $m - q$ qubits in state $|0\rangle$, for example, is given by

$$D(m, q) = \binom{m}{q} \equiv \frac{m!}{q!(m-q)!}. \quad (26)$$

From elementary properties of binomial coefficients it is clear that $D(m, q)$ is maximum for $q = m/2$. Thus, for an even number of qubits m , the largest possible dimension of the resulting

error avoiding subspace is given by

$$D(m, m/2) = \frac{m!}{[(m/2)!]^2} \rightarrow 2^m \left(\frac{2}{m\pi} \right)^{1/2} \quad (m \gg 1). \quad (27)$$

Thus, in this case it is possible to encode

$$l = \log_2 D(m, m/2) \rightarrow m - \frac{\log_2 m}{2} + \log_2 [(2/\pi)^{1/2}] \quad (m \gg 1) \quad (28)$$

logical qubits with m physical ones. It is instructive to compare the redundancy of this error avoiding code described by equation (28) with the ones resulting from active error correcting quantum codes which saturate the quantum Hamming bound [13, 25]. If one wants to correct arbitrary errors of maximum length t with a non-degenerate error correcting quantum code, the number of physical and logical qubits m and l must satisfy the so-called quantum Hamming bound [13, 14, 25], i.e.

$$2^l \sum_{r=0}^t \nu^r \binom{m}{r} \leq 2^m. \quad (29)$$

Here the length t of an error is the number of one-qubit errors which can be detected by a single measurement and which can thus be corrected; ν is the number of different one-qubit errors the code is able to correct. This inequality reflects the fact that, in a non-degenerate error correcting quantum code, the actions of various error operators on any of the logical qubits must lead to orthogonal quantum states. The dimension of the resulting Hilbert space described by the left-hand side of the inequality (29) has to be smaller than the dimensions of the Hilbert spaces of all physical qubits. For the detuning given by (21), there is only one error, i.e. $\nu = 1$. Thus the number of logical qubits obtainable by a non-degenerate error correcting code of maximum length unity, i.e. $t = 1$, cannot be larger than

$$l_{>} = m - \log_2(m + 1). \quad (30)$$

On comparing equation (28) with equation (30), one realizes that the redundancy of this particular error avoiding quantum code is smaller than that of any non-degenerate error correcting code saturating the Hamming bound, i.e.

$$l - l_{>} \rightarrow \frac{1}{2} \log_2 m + \log_2 \left(\frac{\sqrt{2}}{\sqrt{\pi}} \right) > 0 \quad (m \gg 1). \quad (31)$$

For codes with maximum lengths larger than 1, we obtain $l_{>} \approx m - t \log_2 m$ (see figure 6). An error avoiding code may be considered as an error correcting code which is capable of correcting errors of infinite length, i.e. $t \rightarrow \infty$ [38]. In addition, its redundancy is smaller than that of a non-degenerate code which is able to correct only errors of distance $t = 1$.

4. Numerical examples

In the previous section we have developed an error avoiding quantum code which is capable of correcting coherent errors. These errors were assumed to be caused by systematic detunings of the physical qubits of the quantum computer from the frequency of the laser pulses implementing the action of the quantum gates. This error avoiding quantum code works perfectly provided that all physical qubits are detuned from the frequency of these laser pulses by the same amount. However, in realistic situations this case is hardly ever realized. For the realistic assumption of



Figure 6. The maximum number of logical qubits l versus the number of physical qubits m for the error avoiding quantum codes which are capable of stabilizing the error operator of equation (21) (diamonds) (compare with equation (28)). The corresponding relation $l_{>}(m)$ obtained from equation (29) characterizing the quantum Hamming bound is indicated by stars ($t = 1$), triangles ($t = 2$) and boxes ($t = 3$).

unequal detunings in general the eigenstates of H_d are non-degenerate so that it is not possible to construct a perfect error avoiding quantum code. Therefore the practical question of whether the presented error avoiding quantum code of section 3 is still useful for stabilizing quantum algorithms against arbitrary systematic detunings arises. A first general result in this direction was derived by Lidar *et al* [26]. They have shown in a perturbative analysis that any error avoiding quantum code is stable against weak perturbations. However, so far questions concerning the maximal range of validity of an error avoiding quantum code have not been addressed.

The dynamics of Grover's algorithm in the presence of arbitrary detunings is depicted in figure 7. The broken line represents the ideal dynamics in the absence of detunings for the case of six qubits evaluated from the Hamiltonian of equation (16). The characteristic Rabi oscillations are clearly apparent. The corresponding dynamics for eight qubits in the presence of arbitrarily chosen detunings is depicted by the dotted line in figure 7. It is apparent that, in this case, a quantum search for the state $|x_0\rangle$ is not at all successful. However, as is apparent from the full line in figure 7, encoding the quantum information by the error avoiding code of section 3 improves the performance considerably. Despite the fact that this error avoiding code has not been designed for these detunings, it almost succeeds at finding the sought quantum state $|x_0\rangle$ after a number of iterations which is close to that of the ideal case (compare with equation (14)). Similar stability properties of error avoiding codes have been observed by Lidar *et al* [26].

In order to obtain more insight into the stabilizing properties of this error avoiding code, let us investigate the probability of success in the presence of arbitrary detunings in more detail. For this purpose we consider eight physical qubits whose detunings ω_i are distributed randomly according to a normal distribution. According to figure 6 these eight physical qubits are capable of encoding six logical qubits. In figure 8 the average value of the maximum probability of finding the quantum computer in the sought state $|x_0\rangle$ for various values of the variance of the randomly chosen detunings is depicted. The lower sequence of dots (stars) refers to Grover's algorithms without error avoiding encoding and the upper sequence of points (diamonds) refers to error avoiding encoding according to section 3. It is apparent that error avoiding encoding is

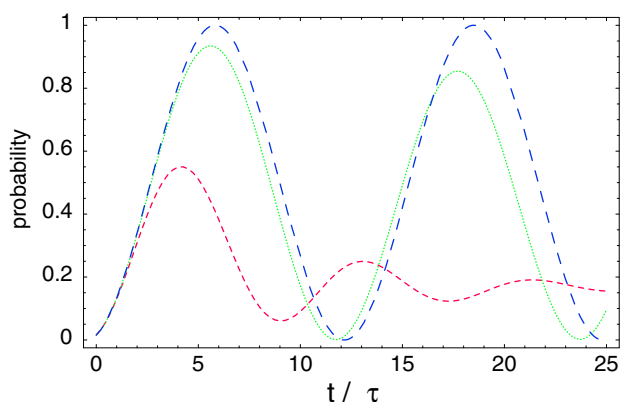


Figure 7. The probability of finding the quantum computer in the sought state $|x_0\rangle$ after $n = t/\tau$ iterations: ideal dynamics without detunings for six qubits (broken line); with detunings and without error avoiding encoding for eight qubits (dotted line); and with detunings and with error avoiding encoding using eight physical qubits which can encode the quantum information of six logical qubits (full line). For the latter two cases the magnitudes of the detunings ω_i of the eight qubits which determine the error operator of equation (18) are given by $\omega_i\tau/\langle v|s\rangle = 0.92065, 1.1436, 0.71449, 1.39566, 1.29707, 0.70149, 1.19195$ and 1.00343 .

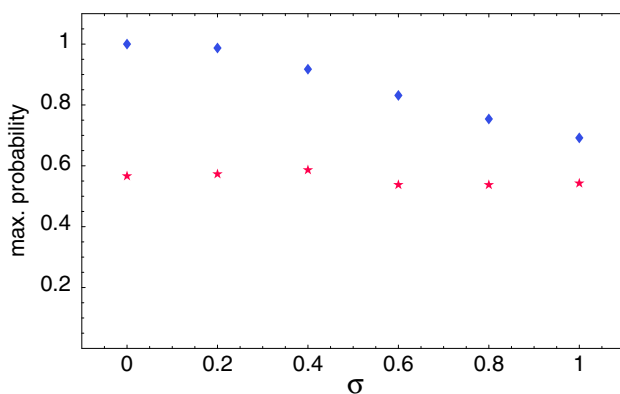


Figure 8. The average maximum probability of success for Grover's algorithm with eight qubits in the presence of randomly chosen detunings: with error avoiding encoding according to section 3 (diamonds); and without error avoiding encoding (stars). The detunings ω_i of the eight physical qubits were chosen randomly according to a normal distribution with mean value $\bar{\omega} = 0.5\langle v|s\rangle/\tau$. The corresponding variance σ of these detunings is plotted on the x -axis in units of the mean value $\bar{\omega}$.

very successful as long as the difference between the detunings of the qubits is sufficiently small. Only in extreme cases in which these differences become comparable to the typical magnitudes of the detunings is this type of error avoiding code no longer capable of stabilizing Grover's algorithm in a satisfactory way.

5. Summary and conclusions

It has been demonstrated that error avoiding quantum codes may offer efficient methods for stabilizing quantum codes dynamically against errors. As a particular example we discussed the stabilization of Grover's quantum search algorithm against coherent errors which may arise from systematic detunings of the physical qubits from the frequency of the light pulses implementing the quantum gates. Even though originally the error avoiding quantum code had been constructed for the special case of equal detunings of all the qubits, it has been shown that it is also capable of stabilizing this quantum algorithm to a satisfactory degree in other non-ideal cases well beyond the perturbative regime. The error avoiding quantum code considered consists solely of quantum states which are factorizable in the computational basis. This may offer advantages insofar as the implementation of the necessary quantum gates in this error-free subspace is concerned. Although the stabilizing ability of error avoiding quantum codes has been demonstrated for one particular quantum code and one particular class of coherent errors only, it is expected that similar capabilities will also be found in more general cases which may also involve incoherent errors.

After the submission of this paper we became aware of a preprint by Kempe *et al* [39] concerning quantum computation on decoherence-free subspaces. In this preprint some of the issues addressed in section 3.2 are also considered.

Acknowledgments

This work was supported by the DFG within the SPP 'Quanteninformationsverarbeitung'. Stimulating discussions with Thomas Beth, Markus Grassl and Dominik Janzing are acknowledged. AD acknowledges support by the DAAD.

References

- [1] Feynman R P 1982 *Int. J. Theor. Phys.* **21** 467–88
- [2] Shor W 1994 *Proc. 35th Ann. Symp. on Foundations of Computer Science* ed S Goldwasser (Los Alamitos, CA: IEEE Computer Society) p 124
- [3] Grover L K 1997 *Phys. Rev. Lett.* **79** 325
- [4] Grover L K 1998 *Phys. Rev. Lett.* **80** 4329
- [5] Cirac J I and Zoller P 1995 *Phys. Rev. Lett.* **74** 4091
- [6] Gershenfeld N and Chuang I 1997 *Science* **275** 350
- [7] Pellizzari T, Gardiner S A, Cirac J I and Zoller P 1995 *Phys. Rev. Lett.* **75** 3788
- [8] Boyer M, Brassard G, Hoyer P and Tapp A 1998 *Fortschr. Phys.* **46** 493
- [9] Chuang I L, Gershenfeld N and Kubinec M 1998 *Phys. Rev. Lett.* **80** 3408
- [10] Miquel C, Paz J P and Zurek W H 1997 *Phys. Rev. Lett.* **78** 3971
- [11] Shor P W 1995 *Phys. Rev. A* **52** R2493
- [12] Calderbank A R and Shor P W 1996 *Phys. Rev. A* **54** 1098
- [13] Gottesman D 1996 *Phys. Rev. A* **54** 1862
- [14] Laflamme R, Miquel C, Paz J P and Zurek W H 1996 *Phys. Rev. Lett.* **77** 198
- [15] Steane A M 1996 *Phys. Rev. Lett.* **77** 793
- [16] Bennett C H, Di Vincenzo D P, Smolin J A and Wootters W K 1996 *Phys. Rev. A* **54** 3824
- [17] Kitaev A Yu 1996 *Russ. Math. Surveys* **53** 1191
- [18] Knill E and Laflamme R 1997 *Phys. Rev. A* **55** 900
- [19] Steane A 1998 *Rep. Prog. Phys.* **61** 117–73

- [20] Duan L M and Guo G C 1997 *Phys. Rev. Lett.* **79** 1953
- [21] Zanardi P and Rasetti M 1997 *Phys. Rev. Lett.* **79** 3306
- [22] Zanardi P 1998 *Phys. Rev. A* **57** 3276
- [23] Zanardi P 1999 *Phys. Rev. A* **60** R729
- [24] Lidar D A, Chuang I L and Whaley K B 1998 *Phys. Rev. Lett.* **81** 2594
- [25] Welsh D 1988 *Codes and Cryptography* (Oxford: Clarendon)
- [26] Lidar D A, Bacon D and Whaley K B 1999 *Phys. Rev. A* **60** 1944
- [27] Zalka C 1999 *Phys. Rev. A* **60** 2746
- [28] Biham E, Biham O, Biron D, Grassl M and Lidar D A 1999 *Phys. Rev. A* **60** 2742
- [29] Gingrich R M, Williams C P and Cerf N J 2000 *Phys. Rev. A* **61** 052313
- [30] Fahri E and Gutmann S 1998 *Phys. Rev. A* **57** 2403
- [31] Schulman L 1981 *Techniques and Applications of Path Integration* (New York: Wiley)
- [32] Averbukh I Sh and Perelman N F 1989 *Phys. Lett. A* **139** 449
- [33] Pellizzari T, Beth Th, Grassl M and Müller-Quade J 1996 *Phys. Rev. A* **54** 2698
- [34] Lidar D A, Bacon D and Whaley K B 1999 *Phys. Rev. Lett.* **82** 4556
- [35] Duan L M and Guo G C 1998 *Phys. Rev. A* **57** 737
- [36] Bacon D, Kempe J, Lidar D A and Whaley K B 1999 *Preprint lanl e-print quant-ph/9909058*
- [37] Beige A, Braun D and Knight P 1999 *Preprint lanl e-print quant-ph/9912004*
- [38] Knill E, Laflamme R and Viola C 2000 *Phys. Rev. Lett.* **84** 2525
- [39] Kempe J, Bacon D, Lidar D A and Whaley K B 2000 *Preprint lanl e-print quant-ph/0004064*