Decoherence and programmable quantum computation

Jeff P. Barnes and Warren S. Warren
Chemistry Department, Princeton University, Princeton, New Jersey 08544-1009
(Received 22 February 1999; revised manuscript received 21 July 1999)

When coherent states of the electromagnetic field are used to drive the evolution of a quantum computer, a decoherence results due to the back reaction from the qubits onto the fields. We show how to calculate this effect. No assumptions about the environment are necessary, so this represents a useful model to test the fidelity of quantum error correcting codes. We examine two cases of interest. First, the decoherence from the Walsh-Hadamard transformations in Grover's search algorithm is found [Phys. Rev. Lett. **79**, 325 (1997)]. Interference effects, and decoherence-dependent phases, are present that could be useful in reducing the decoherence. Second, Shor's fault-tolerant controlled-NOT gate is examined, utilizing frequency-selective pulses [*Proceedings*, 35th Annual Symposium on Foundations of Computer Science (IEEE Press, New York, 1994), pp. 56–65]. This implementation is found not to be optimal in regards to fault-tolerant quantum computation. [S1050-2947(99)07212-1]

PACS number(s): 03.67.Lx, 32.80.Qk

I. INTRODUCTION

In the original concept of quantum computation, the isolated, coherent evolution of a quantum system corresponded to a series of logical operations which could be used to compute a solution to a problem [1]. Once a method of solving a given problem is decided upon, the logical steps in the method are translated into unitary transforms of a quantum system [2]. These transforms place constraints on the form for the system Hamiltonian H, which in turn constrains the architecture of the computer. In other words, the program determines the system propagator $U(t)=\exp(-iHt/\hbar)$, which constrains the form of H, whose parameters indicate the qubit-qubit interactions that must be present in order to carry out the program.

Such quantum computers suffer from a significant drawback: they are not programmable. Consider the case of NMR quantum computing. A given program to solve a given problem results in a set of J couplings between distinct spins, which in turn determines a geometry of the molecule to be used as the computer. Once the molecule is synthesized, it is useful only for the method of solving the problem originally decided upon. In contrast with the flexibility of classical, transistor-based computers, these quantum computers have their programs ''hard-wired'' into their architecture.

However, recent proposals for quantum computer architectures seek to overcome this limitation. They use external fields, generated by classical degrees of freedom, in order to drive the quantum system's evolution [3]. Since classical sources can easily be manipulated by the programmer, these methods offer a means by which the programmer can alter the evolution of the quantum system, and thus program the computer. Some of these proposals include the use of radio-frequency pulses acting upon nuclear spins in liquids [4–6], laser pulses acting upon ions trapped in resonators [7,8], and electrostatic fields generated from gated electrodes influencing the evolution of nuclear spins in semiconductors [9], or of electrons trapped in quantum dot structures [10].

A question that naturally arises when one contemplates such proposals is the following: How can the evolution of a quantum system remain coherent if it is interacting with classical degrees of freedom? Consider trying to produce an analog of the two-slit interference pattern with electrons, only using light beams to drive the electrons into two separate paths. The interaction of the field with the electron creates an entangled state of the electron and field, from which a measurement of the state of the light will reveal information about the position of the electron. To the extent to which the light carries information about which path the electron takes, interference is lost [11–13]. Such interference is central to the working of many quantum programs, e.g., Grover's search algorithm [14]. If we use classically generated fields to drive qubit evolution, will that interaction effectively measure the state of the qubits, and by doing so, destroy the coherent evolution of the system?

To answer this question, we derive quantitative decoherence rates for two cases. First, we examine the influence of driving the Walsh-Hadamard transform in Grover's quantum search algorithm [14] with an external field. Second, we give a more general method by which to calculate this decoherence mechanism, and then apply it to Shor's fault-tolerant controlled-NOT (CNOT) gate [15]. While these questions have been previously raised [16], to the authors knowledge no quantitative assessment of their importance has yet been given.

It is helpful to mention here that this decoherence mechanism will turn out to be smaller, by many orders of magnitude, than other decoherence mechanisms typically encountered. It certainly does not represent the most immediate difficulty with implementing NMR quantum computing [6,17]. Rather, the usefulness of this result is that the decoherence can be calculated without any assumptions about the nature of the environment. This is because the ''environment'' in this case is the well understood coherent state of the electromagnetic field. Thus it represents a useful toy model by which to test the fidelity of various quantum error correcting codes under arbitrarily harsh conditions [15,18–20]. Simulations utilizing different error models may be helpful in determining the accuracy threshold for fault-tolerant quantum computing [21].

II. GROVER'S ALGORITHM

A. Search algorithm

Before we consider how to drive a part of Grover's search algorithm, let us briefly review it here. Grover's quantum search algorithm is a method by which to retrieve elements in a subset of a larger set [14]. It acts upon K qubits, or two-level systems, whose levels are arbitrarily labeled as $|0\rangle$ and $|1\rangle$. A complete, orthonormal basis for the system is the product basis, e.g., for $K=3$, $\{|000\rangle,|001\rangle,|010\rangle,|011\rangle,|100\rangle,|101\rangle,|110\rangle,|111\rangle\}$. It is usual to refer to each element of the basis set by the integer whose binary expansion represents the string of 0's and 1's, so that $|3\rangle\equiv|011\rangle$. The elements of the set to be searched are labeled by integers from 0 to 2^K-1.

The subset whose elements we are searching for is specified according to a condition. For example, we could search for any integer-valued roots of a given polynomial within a fixed range. There are many problems for which, given an x of the set of possible solutions, it can be checked in a polynomial number of steps whether x is a solution to the problem, but no known method exists to find all solutions in polynomial steps [22]. These problems can be solved by a brute-force search over all possible solutions, which is what Grover's algorithm does. Since Grover's algorithm has been shown to be optimal [23–25], its performance is one important indicator of how quantum computation might outperform classical computation.

In what follows, we assume there is only a single solution y to the problem. It is not difficult to generalize this to multiple solutions [24]. The initial state of the quantum computer is $\Sigma_{x=0}^{2^K-1}|x\rangle/\sqrt{2^K}$. The goal is to transfer amplitude into the state $|y\rangle$ [14] so that a measurement of the system yields the solution. This is achieved by a series of transforms of the form $(WRWO)^N$. W's are products of operators acting on a single qubit, $\Pi_n W_n$. Each W_n is a Welsh-Hadamard transform, $W_n=\sqrt{2}(S_{n,x}-S_{n,z})$. We employ a notation which conforms to the common usage in magnetic resonance [26]. Each S indicates an operator that transforms only a single qubit, whose index is given by the first subscript. The second subscript indicates what the operator does. There are two projection operators, $S_{n,\alpha}=|1\rangle\langle 1|$ and $S_{n,\beta}=|0\rangle\langle 0|$, and the raising and lowering operators are $S_{n,+}=|1\rangle\langle 0|$ and $S_{n,-}=|0\rangle\langle 1|$. Also, the three Pauli operators are given by $S_{n,x}=(S_{n,+}+S_{n,-})/2$, $S_{n,y}=(S_{n,+}-S_{n,-})/2i$, and $S_{n,z}=(S_{n,\alpha}-S_{n,\beta})/2$.

The operators $R=-\mathbf{1}+2|0\rangle\langle 0|$ and $O=\mathbf{1}-2|y\rangle\langle y|$ are diagonal in the product basis. (The $\mathbf{1}$ is the unit operator.) The operator O is called the oracle. It is the only means by which the algorithm has knowledge of the solution. For example, if one were searching for the integer roots of $P(x)$, the O transform might flip the amplitude of only those states, $|x\rangle$, that satisfy $P(x)=0$. The combination WRW can also be written as $-\mathbf{1}+2(\Sigma_{x=0}^{2^K-1}|x\rangle)(\Sigma_{x=0}^{2^K-1}\langle x|)/2^K$, which is called the invert-about-average step.

The algorithm can be understood as a combination of two inversions, the first about $|y\rangle$ and the second about the state with an equal amplitude for all basis states. The two inversions result in a rotation, transferring amplitude into $|y\rangle$ [14,25]. For any normalized state of the computer, $\Sigma_{x=0}^{2^K-1}a_x|x\rangle$, the application of the transformation $WRWO$ alters the state as follows:

$$\begin{pmatrix} a_y \\ \dfrac{\sum_{x\neq y} a_x}{\sqrt{2^K-1}} \end{pmatrix} \overset{WRWO}{\rightarrow} \begin{pmatrix} 1-\dfrac{2}{2^K} & \dfrac{2}{2^K}\sqrt{2^K-1} \\ -\dfrac{2}{2^K}\sqrt{2^K-1} & 1-\dfrac{2}{2^K} \end{pmatrix} \times \begin{pmatrix} a_y \\ \dfrac{\sum_{x\neq y} a_x}{\sqrt{2^K-1}} \end{pmatrix}, \tag{1}$$

which is a rotation of the probability amplitude between $|y\rangle$ and all other states, with $\sin\varphi\approx 2^{1-K/2}$ for large K. When a_y and $\Sigma_{x\neq y}a_x$ have the same sign, the amplitude for the state $|y\rangle$ increases with every iteration, and decreases otherwise.

Note that R and O, unlike W, are not products of operators acting independently upon each qubit. To see this, write $R=-\mathbf{1}+2\Pi_n S_{n,\beta}=-\mathbf{1}+2\Pi_n(1/2-S_{n,z})$. When the product is expanded, terms such as $S_{n,z}S_{m,z}$ appear. Thus, they require qubit-qubit interactions to implement.

B. Adding classical fields

Consider how to drive the algorithm utilizing externally applied fields. The Walsh-Hadamard transforms W_n can be driven one qubit at a time. Some proposals include methods by which qubit-qubit couplings, and thus R and O, could also be driven [9,8]. We assume here that only the W_n are externally driven. Because of the nature of decoherence, it is reasonable to expect that when further transforms are driven, the decoherence rate will only increase.

The electromagnetic-field–qubit coupling is of the form $\kappa e(t)S_x$, where $e(t)$ is the classical electric-field amplitude, and κ is the coupling strength. [We are reserving capital $E(t)$ for the electric-field operator.] For magnetic transitions, substitute $b(t)$ for $e(t)$. The greatest possible control over the system occurs when any qubit can be separately driven by the field. This can be achieved by either spatial resolution or frequency resolution. In either case, the Fourier components of the pulses acting upon separate qubits do not overlap. To keep the derivations simple, we restrict the field modes to a single polarization and direction for each pulse. For example, our system could sit inside of a waveguide whose dispersion can be ignored. Since this artificially restricts the spontaneous emission process, we expect that a more complete derivation would result in an increased decoherence rate.

The entire qubit-field system is then described by a Hamiltonian of the form

$$H/\hbar=\sum_n \omega_n S_{n,z}+\sum_{n,m} J_{n,m}S_{n,z}S_{m,z} + \cdots + \kappa\sum_n e(\vec{r}_n,t)S_{n,x}. \tag{2}$$

The ω_n's are the level separation (in frequency units) for each qubit, and the $J_{n,m}$'s are qubit-qubit interactions that may be necessary to implement R and O. There might be higher-order coupling terms between qubits as well. The $e(\vec{r}_n,t)$ is the field that qubit n, at position $\vec{r}_n$, experiences at time t. We assume that the field pulses that drive the W_n are of constant amplitude, e_n, of one fixed polarization, and of fixed frequency, $\overline{\omega}_n$. Also, we assume that the field is strong enough so that we can ignore the qubit-qubit couplings during the pulse (but see Ref. [27]). To implement W_n, one needs to choose the parameters so that the propagator, given by

$$i\frac{\partial}{\partial t}W_n(t)=[\omega_n S_{n,z}+\kappa e_n\cos(\overline{\omega}_n t)S_{n,x}]W_n(t), \qquad (3)$$

gives the desired transform by some time T. Try a solution of the form $W_n(t)\equiv\exp(-i\overline{\omega}_n S_{n,z}t)\,Q_n(t)$, for some unknown transform Q, and drop the rapidly oscillating terms (make the rotating wave approximation). Then

$$\frac{\partial}{\partial t}Q_n=-i\left((\omega_n-\overline{\omega}_n)S_{n,z}+\frac{\kappa}{2}e_n S_{n,x}\right)Q_n. \qquad (4)$$

The propagator for a time-independent Hamiltonian of the form $\vec{a}\cdot\vec{S}$ is given by $\exp(-i\vec{a}\cdot\vec{S}t)=\cos(at/2)-2i\sin(at/2)\vec{a}\cdot\vec{S}/a$. In our case, $\vec{a}=(\kappa e_n/2,0,\omega_n-\overline{\omega}_n)$. We arrive at the correct result when the first and last components of this vector are equal in magnitude but opposite in sign. Thus, for some Ω, the field is detuned below the qubit by $\overline{\omega}_n=\omega_n-\Omega/\sqrt{2}$, and the field strength is $\kappa e_n/2=-\Omega/\sqrt{2}$, and the pulse duration is π/Ω. Thus

$$W_n=i\sqrt{2}\exp\left(-i\pi\frac{\overline{\omega}_n}{\Omega}S_{n,z}\right)(S_{n,x}-S_{n,z}). \qquad (5)$$

This is the form we seek, except for an extra phase factor. Since W_n is applied uniformly to each qubit in the system, if the spread of the $\overline{\omega}_n$ is not too large, it will be a constant factor for the entire quantum computer, and can be ignored. Otherwise, suitable time delays and phase shifts must be implemented to achieve this result.

C. Description of the quantum field

Before $t=0$, when the computation starts, the programmer creates pulses of the field that propagate toward and drive the qubits at separate times. This is accomplished in a classical manner by turning on and off a classical current source, $j(\vec{r},t)$, which interacts with the field through the vector potential $H_I(t)=-\int d\vec{r}\,A(\vec{r},t)j(\vec{r},t)$. (As before, we are assuming that j and the fields are polarized along one direction.) The current is classical in the sense that no quantum back reaction on the current source was included in the interaction Hamiltonian.

Grover's algorithm requires a series of pulses to drive each qubit n. Let the current distribution that drives qubit n be $j_n(\vec{r},t)$. It has significant Fourier components over a range of $\vec{k}\in\mathsf{K}(n)$. As discussed previously, $\mathsf{K}(n)$'s are mutually disjoint sets. To create pulse i in the series, turn j_n on for a short time Δt at time t_i. The field state is then transformed by $\exp(-iH_I(j_n(\vec{r},t_i))\Delta t/\hbar)=\Pi_{\vec{k}\in\mathsf{K}(n)}D_{\vec{k}}(z_{\vec{k}})$. $D_{\vec{k}}(z)=\exp(za_{\vec{k}}^{\dagger}+z^{\star}a_{\vec{k}})$ are called displacement operators, using $a_{\vec{k}}$ as the annihilation operator on the $\vec{k}$ field mode. They separately transform each mode of the field according to the complex-valued argument $z_{\vec{k}}\propto\Delta t\int j(\vec{r},t)\exp(i\vec{k}\cdot\vec{r})d\vec{r}$. Grover's algorithm is thus $(WRWO)^N\,\Sigma_{x=0}^{2^K-1}|x\rangle\Pi_n^{\text{qubits}}\Pi_{t_i}^{\text{pulses}}\Pi_{\vec{k}\in\mathsf{K}(n)}D_{\vec{k}}(z_{\vec{k}}(n,t_i))|\text{vac}\rangle$, where $|\text{vac}\rangle$ indicates the vacuum state of the field. The W_n's now act jointly over qubit n and the field state.

The displacement operators produce coherent field states that have many classical properties [28]. We require the following: $D_{\vec{k}}^{\dagger}(z)D_{\vec{k}}(z)=\mathbf{1}_{\vec{k}}$, and $D_{\vec{k}}^{\dagger}(z)a_{\vec{k}}D_{\vec{k}}(z)=a_{\vec{k}}+z$, and $D_{\vec{k}}^{\dagger}(z)a_{\vec{k}}^{\dagger}D_{\vec{k}}(z)=a_{\vec{k}}^{\dagger}+z^{\star}$. These lead to the following identity. Define the positive and negative frequency electric field operators as

$$E^{+}(\vec{r},t)=[E^{-}(\vec{r},t)]^{\dagger}=\sum_{\vec{k}}\ i\sqrt{\frac{\hbar\omega}{2\epsilon_0 L^3}}a_{\vec{k}}e^{i(\vec{k}\cdot\vec{r}-\omega t)}, \qquad (6)$$

where L is an arbitrary quantization volume. The total electric-field operator $E=E^{+}+E^{-}$ obeys Maxwell's operator equations for a source-free region. Given a function f that can be represented by a Taylor expansion, then the following operator equation holds:

$$f(E^{+}(\vec{r},t),E^{-}(\vec{r},t))\exp[-iH_I(j(\vec{r}',t'))\Delta t/\hbar]$$
$$=\exp[-iH_I(j(\vec{r}',t'))\Delta t/\hbar]f(E^{+}(\vec{r},t)+e^{+}(\vec{r},t;\vec{r}',t'),$$
$$E^{-}(\vec{r},t)+e^{-}(\vec{r},t;\vec{r}',t')), \qquad (7)$$

where $e^{\pm}$ is the *classical* amplitude of the positive or negative frequency components of the electric field that one expects at position $\vec{r}$ and time t, from the classical current distribution $j(\vec{r}',t')$, turned on for a short time Δt.

D. Walsh-Hadamard transform

The goal of this section is to find the form of the W_n when the field is quantized. We are going to use the idea that each pulse should only interact with one qubit, over one short-time interval, and then interact with no other qubit during any other time. We again assume square pulses, with constant frequency $\overline{\omega}_n$, and a detuning from a qubit resonance of $\Delta\omega=\omega_n-\overline{\omega}_n$. First, commute the displacement operators into Grover's algorithm until they are just to the right of the transform they will drive:

$$\prod_n \left\{ W_n(t_i) \prod_{\vec{k}\in \mathsf{K}(n)} D_{\vec{k}}(z_{\vec{k}}(n,t_i)) \right\} \times R \prod_n \left\{ W_n(t_{i-1}) \prod_{\vec{k}\in \mathsf{K}(n)} D_{\vec{k}}(z_{\vec{k}}(n,t_{i-1})) \right\} O \cdots,$$

$$\prod_n \left\{ W_n(t_2) \prod_{\vec{k}\in \mathsf{K}(n)} D_{\vec{k}}(z_{\vec{k}}(n,t_2)) \right\} \times R \prod_n \left\{ W_n(t_1) \prod_{\vec{k}\in \mathsf{K}(n)} D_{\vec{k}}(z_{\vec{k}}(n,t_1)) \right\} O \sum_{x=0}^{2^K-1} |x\rangle|\mathrm{vac}\rangle.$$

When D commutes past R, O, and W_m with $m\neq n$, the $z_{\vec{k}}$'s pick up a phase of $\exp(-i\omega t)$, due to the free propagation of the pulse while these calculations occur. However, D acting on qubit n at one time will not commute past W_n at any other time, even though classically the qubit is not within the pulse envelope. This reflects the interaction of the qubit with the vacuum field, i.e., spontaneous emission. Our interest is the decoherence that occurs as a result of the field-qubit interaction, so we ignore this commuter here (including it would increase the total decoherence rate). Thus, in trying to find the qubit propagator, we only need to consider W_n and those D, just to the right of W_n, that correspond to the pulse that classically drives the transition.

The Hamiltonian of Eq. (3), except with the quantum field operators, describes W_n. Again, try a solution of the form $W_n \equiv \exp(-iH_0(n)t/\hbar)Q_n$ where $H_0(n)/\hbar = \Sigma_{k\in \mathsf{K}(n)} \omega a_{\vec{k}}^{\dagger} a_{\vec{k}} + \omega_n S_{n,z}$, and drop the rapidly rotating terms. Then

$$\frac{d}{dt}Q_n(t) = -i\frac{\kappa}{2}(S_{n,+}e^{i\omega_n t}E^+(\vec{r}_n,t) + S_{n,-}e^{-i\omega_n t}E^-(\vec{r}_n,t))Q_n(t). \tag{8}$$

The modes over $\mathsf{K}(n)$ in the operators $E^{\pm}$ slowly dephase during the interaction of the pulse with the qubit. This gives the effect of the pulse envelope on the qubit, but makes an exact solution difficult. However, our interest is to find only the lowest-order departures from classical behavior. The following trick is helpful: we are going to commute the D past Q_n. To do this, first insert a unit factor into the propagator, $\exp(-iH_0(n)t/\hbar)\Pi_{\mathsf{K}(n)} D_{\vec{k}} D_{\vec{k}}^{\dagger} Q_n(t) \Pi_{\mathsf{K}(n)} D_{\vec{k}}$. The leftmost D will commute to the front of the entire algorithm, and we solve for the new operator $P_n \equiv (\Pi D^{\dagger}) Q_n (\Pi D)$. From Eq. (7), this results in replacing $E^{\pm}$ with $E^{\pm}+e^{\pm}(t)$ in Eq. (8), where $e^{\pm}(t) = e_n e^{\mp i\omega_n t} e^{\mp i\phi_n}$ is the classical field, with pulse amplitude $2e_n$ and phase ϕ_n. The phase is added in to allow for an interesting observation later on.

Just as the Q_n's live in a rotating frame, the P_n's exist in a frame in which the coherent state of the field is mapped onto the vacuum state. The appearance of the classical field profiles in Eq. (8) implies that part of the qubit evolution is the same as if a ''classical'' field existed. Photons are still absorbed and emitted, but in such a way so that the coherent state of the field is not altered. However, the propagator also contains field operators, acting upon the transformed vacuum state of the field to create one-photon states which are orthogonal to the vacuum state. Because D is a unitary transform, the displaced one-photon states are orthogonal to the displaced vacuum states that describe the pulses. Thus W_n can entangle the qubit with a field state that is orthogonal to the original field state. This is precisely the description of a decoherence mechanism.

The idea that the classical field represents the lowest-order behavior of the system suggests that one should expand out P_n as a series in powers of the quantum field operators,

$$\frac{d}{dt}P_n^{(0)} = -i\frac{\kappa}{2}(e^+(t)S_{n,+}e^{i\omega_n t} + e^-(t)S_{n,-}e^{-i\omega_n t})P_n^{(0)},$$

for the classical behavior, and, for $j \geqslant 1$,

$$\frac{d}{dt}P_n^{(j)} = -i\frac{\kappa}{2}(e^+(t)S_{n,+}e^{i\omega_n t} + e^-(t)S_{n,-}e^{-i\omega_n t})P_n^{(j)} - i\frac{\kappa}{2}(E^+S_{n,+}e^{i\omega_n t} + E^-S_{n,-}e^{-i\omega_n t})P_n^{(j-1)}.$$

$P_n^{(0)}$ is the evolution under a completely classical field, while $P_n^{(1)}$ incorporates field operators once, so it represents the lowest order quantum effects. We expand $P_n^{(j)} \equiv S_{n,\alpha}P_{n,\alpha}^{(j)} + S_{n,\beta}P_{n,\beta}^{(j)} + S_{n,+}P_{n,+}^{(j)} + S_{n,-}P_{n,-}^{(j)}$, resulting in

$$\begin{aligned}
\frac{d}{dt}P_{n,\alpha}^{(0)} &= -i\frac{\kappa}{2}e^{i\omega_n t}e^+(t)P_{n,-}^{(0)}, \\
\frac{d}{dt}P_{n,\beta}^{(0)} &= -i\frac{\kappa}{2}e^{-i\omega_n t}e^-(t)P_{n,+}^{(0)}, \\
\frac{d}{dt}P_{n,+}^{(0)} &= -i\frac{\kappa}{2}e^{i\omega_n t}e^+(t)P_{n,\beta}^{(0)}, \\
\frac{d}{dt}P_{n,-}^{(0)} &= -i\frac{\kappa}{2}e^{-i\omega_n t}e^-(t)P_{n,\alpha}^{(0)},
\end{aligned} \tag{9}$$

and, for $j \geqslant 1$,

$$\begin{aligned}
\frac{d}{dt}P_{n,\alpha}^{(j)} &= -i\frac{\kappa}{2}e^{i\omega_n t}(e^+(t)P_{n,-}^{(j)} + E^+P_{n,-}^{(j-1)}), \\
\frac{d}{dt}P_{n,\beta}^{(j)} &= -i\frac{\kappa}{2}e^{-i\omega_n t}(e^-(t)P_{n,+}^{(j)} + E^-P_{n,+}^{(j-1)}), \\
\frac{d}{dt}P_{n,+}^{(j)} &= -i\frac{\kappa}{2}e^{i\omega_n t}(e^+(t)P_{n,\beta}^{(j)} + E^+P_{n,\beta}^{(j-1)}), \\
\frac{d}{dt}P_{n,-}^{(j)} &= -i\frac{\kappa}{2}e^{-i\omega_n t}(e^-(t)P_{n,\alpha}^{(j)} + E^-P_{n,\alpha}^{(j-1)}),
\end{aligned} \tag{10}$$

Call $\mathcal{L}_{\pm} = (d/dt)^2 \pm i\Delta\omega(d/dt) + (\kappa e/2)^2$ a pair of linear differential operators, recalling that $\Delta\omega = \omega_n - \overline{\omega_n}$ is the detuning, and the field amplitude is $2e_n$. We can then rearrange Eqs. (9) and (10) to read

$$\mathcal{L}_- P_{n,\alpha}^{(0)} = 0, \quad \mathcal{L}_+ P_{n,\beta}^{(0)} = 0, \quad \mathcal{L}_- P_{n,+}^{(0)} = 0, \quad \mathcal{L}_+ P_{n,-}^{(0)} = 0, \tag{11}$$

and, for $j \geqslant 1$,

$$\mathcal{L}_- P^{(j)}_{n,\alpha} = -i\frac{\kappa}{2}\left(\frac{d}{dt} - i\Delta\omega\right)(e^{i\omega_n t}E^+ P^{(j-1)}_{n,-}) - \left(\frac{\kappa}{2}\right)^2 e_n e^{-i\phi_n} e^{-i\bar{\omega}_n t}E^- P^{(j-1)}_{n,\alpha},$$

$$\mathcal{L}_+ P^{(j)}_{n,\beta} = -i\frac{\kappa}{2}\left(\frac{d}{dt} + i\Delta\omega\right)(e^{-i\omega_n t}E^- P^{(j-1)}_{n,+}) - \left(\frac{\kappa}{2}\right)^2 e_n e^{i\phi_n} e^{i\bar{\omega}_n t}E^+ P^{(j-1)}_{n,\beta},$$

$$\mathcal{L}_- P^{(j)}_{n,+} = -i\frac{\kappa}{2}\left(\frac{d}{dt} - i\Delta\omega\right)(e^{i\omega_n t}E^+ P^{(j-1)}_{n,\beta}) - \left(\frac{\kappa}{2}\right)^2 e_n e^{-i\phi_n} e^{-i\bar{\omega}_n t}E^- P^{(j-1)}_{n,+},$$

$$\mathcal{L}_+ P^{(j)}_{n,-} = -i\frac{\kappa}{2}\left(\frac{d}{dt} + i\Delta\omega\right)(e^{-i\omega_n t}E^- P^{(j-1)}_{n,\alpha}) - \left(\frac{\kappa}{2}\right)^2 e_n e^{i\phi_n} e^{i\bar{\omega}_n t}E^+ P^{(j-1)}_{n,-}. \quad (12)$$

The initial conditions are $P^{(0)}_{n,\alpha} = P^{(0)}_{n,\beta} = 1$ and $P^{(0)}_{n,\pm} = 0$, and all the $P^{(j)} = 0$ for $j \geq 1$; and for the first derivatives, $dP^{(0)}_{n,\alpha}/dt = dP^{(0)}_{n,\beta}/dt = 0$, and $dP^{(0)}_{n,\pm}/dt = -i(\kappa/2)e_n e^{\mp i\phi_n}$, and $dP^{(1)}_{n,\alpha}/dt = dP^{(1)}_{n,\beta}/dt = 0$, and $dP^{(1)}_{n,\pm}/dt = -i(\kappa/2)E^{\pm}(\vec{r}_n, 0)$, and all the $dP^{(j)}/dt = 0$ for all $j \geq 2$. We solve,

$$P^{(0)}_{n,\alpha} = e^{i\Delta\omega t/2}\left[\cos(\theta t) - i\frac{\sin(\theta t)}{\theta}\frac{\Delta\omega}{2}\right],$$

$$P^{(0)}_{n,\beta} = e^{-i\Delta\omega t/2}\left[\cos(\theta t) + i\frac{\sin(\theta t)}{\theta}\frac{\Delta\omega}{2}\right],$$

$$P^{(0)}_{n,+} = -ie^{i\Delta\omega t/2}\left[\frac{\sin(\theta t)}{\theta}\right]\frac{\kappa}{2}e_n e^{-i\phi_n},$$

$$P^{(0)}_{n,-} = -ie^{-i\Delta\omega t/2}\left[\frac{\sin(\theta t)}{\theta}\right]\frac{\kappa}{2}e_n e^{i\phi_n}, \quad (13)$$

where $\theta = \sqrt{\Delta\omega^2 + (\kappa e_n)^2}/2$. This is the usual expression for a Bloch vector influenced by a monochromatic field.

The solutions for $P^{(1)}$ are linear in the creation and annihilation operators. However, the field state they operate on is the vacuum state, so for the lowest order effect we will only require the solution for the creation operators. These are reasonably complex, so we simplify by setting $\Delta\omega = \Omega/\sqrt{2}$, $\kappa E = -\Omega/\sqrt{2}$, and the pulse length to π/Ω to reproduce the classical Walsh-Hadamard transform. Then, to lowest order, P is

$$\frac{i}{\sqrt{2}}\begin{pmatrix} e^{-i\pi/\sqrt{8}} & e^{-i\pi/\sqrt{8}}e^{i\phi_n} \\ e^{i\pi/\sqrt{8}}e^{-i\phi_n} & -e^{i\pi/\sqrt{8}} \end{pmatrix} + \frac{\kappa}{4\Omega}\sum_{\vec{k}\in K(n)}\sqrt{\frac{\hbar\omega}{2\epsilon_0 L^3}} \times \begin{pmatrix} e^{-i\pi/\sqrt{8}}e^{-i\phi_n}g_\beta & e^{-i\pi/\sqrt{8}}g_- \\ e^{i\pi/\sqrt{8}}e^{2i\phi_n}g_+ & e^{i\pi/\sqrt{8}}e^{-i\phi_n}g_\alpha \end{pmatrix} e^{-i\vec{k}\cdot\vec{r}_n}a^\dagger_{\vec{k}}. \quad (14)$$

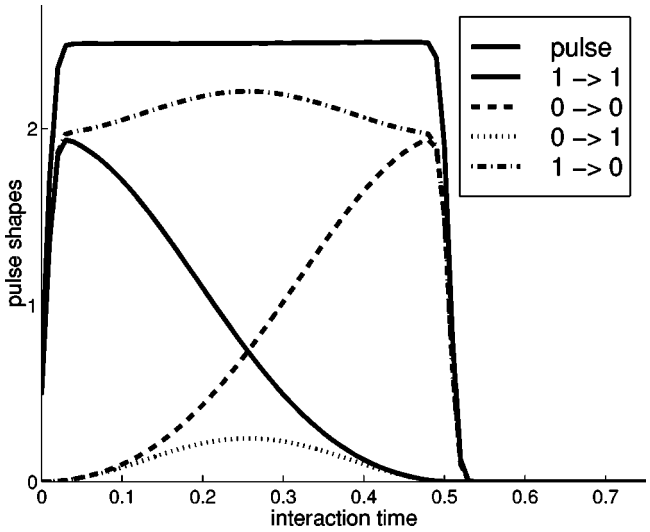

FIG. 1. A plot of the Fourier transform of the g functions of Eq. (15). Time is scaled to the parameter Ω^{-1}, which has arbitrary units, and the functions are unitless. They are the envelopes of one-photon states emitted by a qubit whose state changes are indicated. For comparison, the envelope of the classical pulse is also shown (not to scale).

The functions that give the Fourier components for the shape of the one-photon ''back reaction field'' are given by

$$g_\alpha = \frac{2x^2 + \frac{x}{\sqrt{2}} - 1 + \left(1 + \frac{x}{\sqrt{2}}\right)e^{i\pi x}}{2\sqrt{2}x(x^2-1)},$$

$$g_\beta = -\frac{1 + \frac{x}{\sqrt{2}} + \left(2x^2 + \frac{x}{\sqrt{2}} - 1\right)e^{i\pi x}}{2\sqrt{2}x(x^2-1)},$$

$$g_+ = -\frac{1 + e^{i\pi x}}{4(x^2-1)}, \quad g_- = \frac{(4x + 3\sqrt{2})(1 + e^{i\pi x})}{4\sqrt{2}(x^2-1)}, \quad (15)$$

for which $x \equiv (\omega - \bar{\omega}_n)/\Omega$. As in the classical field case, the extra phase factors of $\pm i\pi/\sqrt{8}$ in Eq. (14) can be compensated for. Now we can see a curious feature of the back reaction: g_+ picks up twice the phase $2\phi_n$ of any of the other terms. This is consistent with the property that the removal of a photon from a coherent state does not alter it, while the addition of a photon does, so to create an ''error'' by raising the qubit state, at least two absorptions need to occur. It also demonstrates that the phase of the field enters into the decoherence. Thus phase cycling [26] could be used to cancel signal from those computers that suffered a g_+ scattering event.

The Fourier transform of the g functions are given in Fig. 1. They are the time-domain envelopes of the one-photon states that accompany the change in the qubit state. At this point, Eq. (14) is exactly the kind of single-qubit decoherence that quantum error correction is typically designed to repair [18–20]. In the second part of this paper, we will examine an interesting case where this decoherence mechanism can flip multiple qubits at once.

Now setting the field phases to zero, we want to collect the sum of creation operators with the factors g into a single operator G that creates a normalized one-photon state, so that

$$P=\frac{i}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}+\epsilon\begin{pmatrix}\sqrt{I_\beta}G_\beta & \sqrt{I_-}G_-\\ \sqrt{I_+}G_+ & \sqrt{I_\alpha}G_\alpha\end{pmatrix}, \qquad (16)$$

where $G^\dagger G=\mathbf{1}$. To find the normalization for the one-photon states, first change Σ_ω into $(L/2\pi c)\int d\omega$. However, there is sufficient bandwidth to allow the square pulse, with Fourier components $(e^{i\pi x}-1)/x$. The one-photon states have their Fourier components concentrated in this range as well, so we can let the limits of integration extend to infinity. Finally, we assume the bandwidth is small compared to the center frequency of the pulse, so the $\sqrt{\omega}$ term can be removed from the integrand. This results in a prefactor of $\epsilon=(\kappa/4)\sqrt{\hbar\bar{\omega}_n/4\pi\epsilon_0 cL^2\Omega}$. By numerical integration, $I_\alpha=\int_{-\infty}^{\infty}|g_\alpha(x)|^2\,dx=4.297$, $I_\beta=4.297$, $I_+=0.617$, and $I_-=10.451$. Although the $G|\mathrm{vac}\rangle$ states are orthogonal to the initial coherent state, they are not mutually orthogonal. Later on, we will require their (non-normalized) overlap integrals $I_{\alpha,\beta}=\sqrt{I_\alpha I_\beta}\langle\mathrm{vac}|G_\alpha^\dagger G_\beta|\mathrm{vac}\rangle=\int_{-\infty}^{\infty}g_\alpha^\star(x)g_\beta(x)\,dx=0.614+i2.221$, $I_{\alpha,+}=-0.617+i1.110$, $I_{\alpha,-}=4.300-i3.331$, $I_{\beta,+}=0.617+i1.110$, $I_{\beta,-}=-4.300-i3.331$, and $I_{+,-}=-1.850$.

The important result of this section is the transformation, Eq. (16). Each qubit-field interaction has a probability amplitude, proportional to $\Omega^{-1/2}$, to entangle the qubit with a field state orthogonal to the original field state. Thus larger fields cause less decoherence. Actually, this may seem counterintuitive. Consider the interference pattern produced by a coherent beam of electrons incident upon a double slit. Now allow a laser to interact with one of the two paths the electron could travel from the slit to the detector. If photons are scattered out of the coherent modes into vacuum states, then the visibility of the interference pattern is degraded, as expected [11]. If, however, only stimulated emission is important, then the visibility of the interference pattern should increase as the laser intensity is increased. The Poisson statistics of a coherent state can more efficiently hide the information about which path the electron takes as the number of photons in the beam increases, when the incoherently emitted photon travels along with the original pulse. A similar situation has been noted with regard to *welcher Weg* experiments in atomic interferometry (see, e.g., Ref. [29]).

E. Grover's algorithm with decoherence

Taking the result from the previous section, Grover's algorithm is now

$$\prod_j^{\text{steps}}\left[\prod_{n=1}^{K}\left(\mathbf{1}-\frac{i\epsilon}{\sqrt{2}}A_n(t_{j+1})\right)WRW \times\prod_{n=1}^{K}\left(\mathbf{1}-\frac{i\epsilon}{\sqrt{2}}B_n(t_j)\right)O\right]\left(\frac{1}{\sqrt{2^K}}\sum_x|x\rangle\right)|\mathrm{vac}\rangle. \qquad (17)$$

The displacement operators, now to the left of the algorithm, are not shown. A and B are from Eq. (16), from which a factor of W is first removed:

$$A_n=\begin{pmatrix}\sqrt{I_\beta}G_\beta+\sqrt{I_-}G_- & \sqrt{I_\beta}G_\beta-\sqrt{I_-}G_-\\ \sqrt{I_+}G_++\sqrt{I_\alpha}G_\alpha & \sqrt{I_+}G_+-\sqrt{I_\alpha}G_\alpha\end{pmatrix},$$

$$B_n=\begin{pmatrix}\sqrt{I_\beta}G_\beta+\sqrt{I_+}G_+ & \sqrt{I_-}G_-+\sqrt{I_\alpha}G_\alpha\\ \sqrt{I_\beta}G_\beta-\sqrt{I_+}G_+ & \sqrt{I_-}G_--\sqrt{I_\alpha}G_\alpha\end{pmatrix} \qquad (18)$$

We expand out Eq. (17), dropping terms of $O(\epsilon^2)$ and greater. As previously discussed, each A_n and B_n can entangle qubit n with field states that are mutually orthogonal, and orthogonal to the initial field state, since the spatial envelope of photons emitted during different Walsh-Hadamard transforms do not overlap. Thus the probability that the final qubit state is $|y\rangle$ is the sum of the squares of the separate terms in Eq. (17). This is what we wish to find.

After j successful steps of the algorithm, the computer state is given by

$$\left(\frac{\cos(j\varphi)}{\sqrt{2^K-1}}\sum_{x\neq y}|x\rangle+\sin(j\varphi)|y\rangle\right)|\mathrm{vac}\rangle,$$

where $\sin\varphi=2\sqrt{2^K-1}/2^K$ [25]. The general trend for the influence of the back reaction can be discerned from the specific example of $K=3$ qubits, with a solution $y=2$, or the state $|010\rangle$. Suppose the back reaction occurs for the first W of the two in the next step of the algorithm. If it is W for the least significant qubit, then the computer state becomes

$$\left\{\frac{\cos(j\varphi)}{\sqrt{2^K-1}}((B_\beta|0\rangle+B_+|1\rangle)+(B_\alpha|1\rangle+B_-|0\rangle) +(B_\alpha|3\rangle+B_-|2\rangle)+(B_\beta|4\rangle+B_+|5\rangle) +(B_\alpha|5\rangle+B_-|4\rangle) +(B_\beta|6\rangle+B_+|7\rangle)+(B_\alpha|7\rangle+B_-|6\rangle)) -\sin(j\varphi)(B_\beta|2\rangle+B_+|3\rangle)\right\}|\mathrm{vac}\rangle. \qquad (19)$$

The above subscripts indicate the matrix elements of B, so $B_\beta\equiv\langle 0|B|0\rangle$, $B_-\equiv\langle 0|B|1\rangle$, $B_\alpha\equiv\langle 1|B|1\rangle$, and $B_+\equiv\langle 1|B|0\rangle$. The decoherence, like the Walsh-Hadamard transform, is the same from qubit to qubit, so no qubit index is required. The amplitudes of pairs of states that differ at their least significant digit such as (0,1) and (2,3), and so on, are mixed. If the error occurs for the second least significant qubit, then

$$\left\{\frac{\cos(j\varphi)}{\sqrt{2^K-1}}((B_\beta|0\rangle+B_+|2\rangle)+(B_\alpha|1\rangle+B_-|3\rangle)+(B_\alpha|3\rangle+B_-|1\rangle)+(B_\beta|4\rangle+B_+|6\rangle)\right.$$
$$\left.+(B_\alpha|5\rangle+B_-|7\rangle)+(B_\beta|6\rangle+B_+|4\rangle)+(B_\alpha|7\rangle+B_-|5\rangle))-\sin(j\varphi)(B_\beta|2\rangle+B_+|0\rangle)\right\}|\text{vac}\rangle. \quad (20)$$

The difference is in which pairs of states are mixed, and whether the qubit involved in the back reaction was initially in state 0 or 1. This gives us the trend for the case of any number of K qubits. Summing the squares of these states over all the qubits, the total probability for a back reaction during the first of the two W's at step j, is

$$\frac{\epsilon^2}{2}\left[\frac{K}{2}\frac{2^K-2}{2^K-1}\cos^2(j\varphi)(|(B_\beta+B_-)|\text{vac}\rangle|^2+|(B_\alpha+B_+)|\text{vac}\rangle|^2)\right.$$
$$+(K-\|y\|)\left(\left|\frac{\cos(j\varphi)}{\sqrt{2^K-1}}B_-|\text{vac}\rangle-\sin(j\varphi)B_\beta|\text{vac}\rangle\right|^2+\left|\frac{\cos(j\varphi)}{\sqrt{2^K-1}}B_\alpha|\text{vac}\rangle-\sin(j\varphi)B_+|\text{vac}\rangle\right|^2\right)$$
$$\left.+\|y\|\left(\left|\frac{\cos(j\varphi)}{\sqrt{2^K-1}}B_\beta|\text{vac}\rangle-\sin(j\varphi)B_-|\text{vac}\rangle\right|^2+\left|\frac{\cos(j\varphi)}{\sqrt{2^K-1}}B_+|\text{vac}\rangle-\sin(j\varphi)B_\alpha|\text{vac}\rangle\right|^2\right)\right].$$

The factor $\|y\|$ appears since the back reaction depends upon whether a qubit was initially in state 0 or 1. When $2^K\gg 1$, we use the approximations $\Sigma_{j=1}^{\pi/2\varphi}\cos^2(j\varphi)\approx\int_0^{\pi/2}\cos^2 x\,dx/\varphi=\pi/4\varphi$, $\Sigma_{j=1}^{\pi/2\varphi}\sin^2(j\varphi)\approx\pi/4\varphi$, and $\Sigma_{j=1}^{\pi/2\varphi}\sin(j\varphi)\cos(j\varphi)\approx 1/2\varphi$. Keeping only the largest terms in K, the probability that a back reaction occurs for any qubit, and at any step, during the first of the two W transforms is given by

$$\frac{\epsilon^2}{2}\frac{\pi}{8}2^{K/2}\left[\frac{K}{2}(|(B_\beta+B_+)|\text{vac}\rangle|^2+|(B_\alpha+B_+)|\text{vac}\rangle|^2)\right.$$
$$+(K-\|y\|)(|B_\beta|\text{vac}\rangle|^2+|B_+|\text{vac}\rangle|^2)$$
$$\left.+\|y\|(|B_-|\text{vac}\rangle|^2+|B_\alpha|\text{vac}\rangle|^2)\right]. \quad (21)$$

If the back reaction occurs during the second W in an iteration, then j starts at 2 (the first invert-about-average step is always carried out), and the sign of the amplitude for $|y\rangle$ is positive. Taking the limit for large K, the cross-terms that depend upon the sign of a_y drop out, and the final expression is the same as above except with the B replaced with A, and the total probability for a back reaction is then the sum of these two. From Eq. (18), the matrix elements are expressed in terms of the normalization and overlap integrals, e.g., $|(B_\beta+B_-)|\text{vac}\rangle|^2+|(B_\alpha+B_+)|\text{vac}\rangle|^2=2(I_\alpha+I_\beta+I_++I_-)+4\,\text{Re}(I_{\beta,-}+I_{\alpha,+})$. Plugging in, the final probability to end up entangled with an orthogonal field state is

$$\epsilon^2\sqrt{2^K}(6.75K+7.71\|y\|). \quad (22)$$

If a computer is altered after emission of an incoherent photon, this does not necessarily imply that further iterations of Grover's algorithm cannot produce a useful result. How much do the orthogonal field states contribute to the correct final answer? First, note that the matrix elements of A and B all have similar magnitudes. Thus they equally mix the state $|y\rangle$ with the state connected to it by flipping the qubit that experiences the back reaction. Early in the algorithm when $\sin(j\varphi)\ll 1$, this does not increase the amplitude in a_y significantly, since the state that mixes with $|y\rangle$ has amplitude $\cos(j\varphi)/\sqrt{2^K}\ll 1$. At later times, however, the amplitude of $|y\rangle$ is near 1, so the back reaction decreases the probability to be in state $|y\rangle$ by roughly half.

Thus, a back reaction at step j sets the computer back to step $\approx j/2$. Recall from Eq. (1) that amplitude is rotated into $|y\rangle$ only when the signs of a_y and $\Sigma_{x\neq y}a_x$ are the same. For large K, the amplitude a_y is $\approx\sin(j\varphi)(\sqrt{I_\beta}G_\beta+\sqrt{I_-}G_-)|\text{vac}\rangle$. The other qubit states are entangled with field states that are partly orthogonal to this state, but the amplitude that lies along the same direction in the Hilbert space of the field is, for large K, $\cos(j\varphi)(I_\beta+I_{\beta,+}+I_{-,\beta}+I_{-,+})/\sqrt{I_\beta+I_-+2\,\text{Re}(I_{\beta,-})}=(-2.232+i0.448)\cos(j\varphi)$. The real part has switched sign, and so further iterations will actually remove amplitude from $|y\rangle$. In general, decoherence adds a random phase that will prevent the computer from recovering the correct result roughly half the time. The conclusion is that a continued operation of Grover's algorithm reduces the decoherence rate of Eq. (22) by roughly half, but cannot eliminate it.

III. CONTROLLED-NOT GATE

Nothing in Sec. II is necessarily troublesome to quantum computing, since quantum error correcting methods have been devised to correct these single-qubit errors [18–20]. Although codes to correct a greater range of errors than just the single-qubit errors can also be derived, they become more complex and difficult to implement. Thus an interesting question is the following: Are there cases for this decoherence where multiple qubit flips or phase flips occur? To find out, we first generalize the method to calculate the decoherence. We then examine a specific implementation of the fault-tolerant CNOT gate, as outlined by Shor [15]. The gate is fault tolerant when several assumptions can be made about

the nature of the decoherence [20]. A detailed calculation of the errors allows one to observe how well these assumptions are justified. It also represents an example of how the choice of a quantum computer architecture can influence the decoherence mechanism.

A. Calculation of the decoherence

Using the notation of Eqs. (2) and (6), we have a system of qubits and field modes whose evolution is described by

$$H/\hbar=\sum_n \omega_n S_{n,z}+\sum_{n>m} J_{n,m}S_{n,z}S_{m,z} + \cdots +\sum_{\vec{k}} \omega a_{\vec{k}}^{\dagger}a_{\vec{k}}+\kappa E\sum_n \mu_n S_{n,x}. \tag{23}$$

The $J_{n,m}$'s are needed to drive the CNOT gates. Let H_0 denote the terms in H that describe the evolution of the qubits alone. H_0 could include couplings besides the form give above, for example, the secular dipolar coupling $\Sigma_{n>m}(K_{n,m}/4)\times(S_{n,+}S_{m,-}+S_{n,-}S_{m,+})$. Call $|q\rangle$ the eigenstates of H_0, with eigenvalues $\hbar\omega_q$. Pairs of the $|q\rangle$ form two-level systems that are the qubits of the computer. The μ_n's describe the coupling of the field with each qubit. If qubits are chosen as the internal states of individual particles, and the field spatially overlaps with only a few of these particles, then mostly $\mu_n=0$. As previously, we ignore issues such as the divergence of the beam by restricting the modes of the field to a single polarization and direction.

To find the total qubit-field propagator during the action of a pulse, $U(t)$, first commute the displacement operators describing the coherent field state to the left. Spontaneous emission from qubits not under the influence of the field is ignored, so only the commuters of the displacement operators with those operators describing the field-qubit gate are calculated, as discussed previously. Thus $E^{\pm}\rightarrow E^{\pm}+e^{\pm}(t)$ in Eq. (23). Let $H(t)=H_C(t)+H_Q$, where H_Q contains the quantum-field–qubit coupling terms. Except for the photon number operators, $H_C(t)$ describes the behavior of the quantum computer under the influence of a completely classical driving field, $e(t)$. If the propagator for $H_C(t)$, call it $U_C(t)$, is known, then

$$U(t)=U_C(t)-\frac{i}{\hbar}\int_0^t dt' U_C(t-t')H_Q U_C(t') -\frac{1}{\hbar^2}\int_0^t dt'\int_0^{t'} dt'' U_C(t-t') \times H_Q U_C(t'-t'')H_Q U_C(t'')+\cdots \tag{24}$$

is a formal solution for $U(t)$.

There are multiple sources for errors here. First U_C might not be exactly the desired transform. This represents an imperfection in the coherent evolution of the computer. Then there is the first integral, call it U_E. It results from the quantum computer, accelerating under the influence of a driving field, emitting a photon in a state that is orthogonal to the coherent state of the field (in other words, incoherently), and thus altering the state of the computer. Finally, the higher-order terms represent multiple incoherent photon scattering processes.

Finding $U_C(t)$ can be a formidable task, especially for an arbitrary pulse shape. The simplest case is when $e(t)=e_0\cos(\bar{\omega}t)$, acting for a time T. In this case, we let $U_C(t)=\exp(-it\Sigma_{\vec{k}}\omega a_{\vec{k}}^{\dagger}a_{\vec{k}})\exp(-i\bar{\omega}t\Sigma_n S_{n,z})U_{C1}$, and make the rotating-wave approximation. The effective Hamiltonian for U_{C1} is then

$$\sum_n (\omega_n-\bar{\omega})S_{n,z}+\sum_{n>m} J_{n,m}S_{n,z}S_{m,z} + \cdots +(\kappa e_0/2)\sum_n \mu_n S_{n,x}, \tag{25}$$

which is time independent. Thus the eigenvalues λ_p and eigenvectors $|\psi_p\rangle$ can be numerically determined. Note that these states are not the same as $|q\rangle$. Since the lowest order decoherence comes only from emission of a photon, we can keep only the creation operators to find

$$\begin{aligned}
U_E&=-\frac{i}{\hbar}\int_0^T U_C(T-t')H_Q U_C(t')dt' \rightarrow -\frac{\kappa}{2}U_C(T)\sum_{\vec{k}} e^{i\vec{k}\cdot\vec{r}}\sqrt{\frac{\hbar\omega}{2\epsilon_0 L^3}}\\
&\times\int_0^T U_{C1}^{\dagger}(t')e^{it'(\Sigma_{\vec{k}}\omega a_{\vec{k}}^{\dagger}a_{\vec{k}}+\Sigma_n\bar{\omega}S_{n,z})}\left(a_{\vec{k}}^{\dagger}\sum_n \mu_n S_{n,-}\right)e^{-it'(\Sigma_{\vec{k}}\omega a_{\vec{k}}^{\dagger}a_{\vec{k}}+\Sigma_n\bar{\omega}S_{n,z})}U_{C1}(t')dt'\\
&=-\frac{\kappa}{2}U_C(t)\sum_{\vec{k}} e^{i\vec{k}\cdot\vec{r}}\sqrt{\frac{\hbar\omega}{2\epsilon_0 L^3}}a_{\vec{k}}^{\dagger}\int_0^T U_{C1}^{\dagger}(t')\left(\sum_n \mu_n S_{n,-}\right)U_{C1}(t')e^{i(\omega-\bar{\omega})t'}dt'\\
&=-\frac{\kappa}{2}\sum_{\vec{k}} e^{i\vec{k}\cdot\vec{r}}\sqrt{\frac{\hbar\omega}{2\epsilon_0 L^3}}e^{iT\Sigma_{\vec{k}}\omega a_{\vec{k}}^{\dagger}a_{\vec{k}}}a_{\vec{k}}^{\dagger}\sum_{p,q} e^{-i\bar{\omega}T\Sigma_n S_{n,z}}|\psi_p\rangle\langle\psi_p|\\
&\times\left(\sum_n \mu_n S_{n,-}\right)|\psi_q\rangle\langle\psi_q|e^{-i\lambda_p T}\frac{e^{i(\omega-\bar{\omega}+\lambda_p-\lambda_q)T}-1}{i(\omega-\bar{\omega}+\lambda_p-\lambda_q)}.
\end{aligned} \tag{26}$$

The difference between this derivation and the result in Sec. II is that, in general, an analytical determination of the frequency dependence of the one-photon states on the parameters in H_0 is not possible, unless an exact diagonalization of Eq. (25) is known. As previously, we can break U_E up according to its effect on the qubits, and collect the terms that create a normalized one-photon state. The normalization introduces a factor of $\sqrt{LT/c}$, along with unitless overlap integrals.

B. Implementing the CNOT gate

The CNOT gate is defined as the transform on two qubits that flips the second qubit only if the first qubit is 1. If a pair of qubits have distinct transition frequencies, and are coupled resulting in a spectrum as shown in Fig. 2, then a simple way to implement this gate is to use a frequency-selective pulse that drives only the transition $|11\rangle \leftrightarrow |10\rangle$. An illuminating account is found in Ref. [30]. Our interest is to use this technique to implement Shor's prescription for a fault-tolerant CNOT [15]. Two qubits are encoded into two separate seven-qubit spaces, which we label as $A1$–$A7$ and $B1$–$B7$. The codewords to be used are given in Ref. [31]. This particular code has the property that the application of CNOT gates from An to Bn for each n results in the application of a CNOT gate between the two encoded qubits. The encoding can correct one spin-flip error, but not in general two or more [31].

This gate is fault tolerant because each individual CNOT gate is a transversal operation: no more than one qubit in each codeword is acted upon during the entire process. Suppose one makes the natural assumption that errors occur only at those qubits that are ''acted upon'' by the gate, e.g., the CNOT gate from $A1$ to $B1$ does not influence the state of the $A2$ qubit. In that case, any error at $A1$ and $B1$ can not grow due to the action of subsequent CNOT gates. Further, to lowest order, any scrambling of the $A1$ and $B1$ qubits is still a single error per codeword, which can be corrected. The assumption that errors between separate qubits within a codeword are uncorrelated is one of several listed by Preskill [20].

We focus on the CNOT gate from $A1$ to $B1$, and suppose that the encoding, decoding, error correction, and the other CNOT gates, are all flawless. Further, we limit the calculation to $A1$, $B1$, $A2$, and $B2$, to avoid having to treat all 16 384 levels of the total system. We wish to selectively invert the fourth transition from the left in Fig. 2 with a square pulse. From Eq. (13) with $\Delta\omega = 0$, this can be achieved when the pulse length and field amplitude are related by $\kappa e_0 T = \pi$. To increase the accuracy of the gate, suppose all the transitions

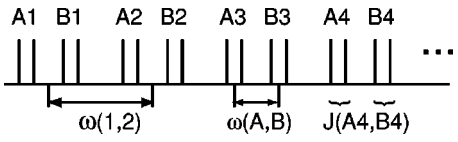

FIG. 2. The first 16 allowed transitions of 28 total, in a 14-qubit system used to implement a fault-tolerant CNOT gate. The two sets of seven qubits, labeled A and B, are used to encode a single qubit separately. Couplings from each A to B are necessary in order to drive the gate.

are equally spaced, with spacing $J = J(A1,B1) = J(A2,B2) = (\omega(A1) - \omega(A2))/2 = (\omega(A1) - \omega(B1))/4$. From Eq. (13), transitions detuned by $\Delta\omega = (2\pi/T)\sqrt{N^2 - 1/4}$, for positive integer N, suffer no change in their populations due to the pulse. Thus chosing the pulse length to be an integer multiple of $2\pi/J$ means that transitions further from the center frequency of the pulse are less likely to suffer spin-flip errors. In any case, as $T \to \infty$, U_C from Eq. (24) becomes a perfectly executed CNOT gate.

In order to see this, we first need to determine what should be called an error. Starting from an initial codeword $|\Psi\rangle$, the state of the system just before error correction is

$$[U_{\mathrm{CNOT},A2-B2}(U_C + \epsilon U_E + \cdots)U_{\mathrm{CNOT},A2-B2}U_{\mathrm{CNOT},A1-B1}] \times \left[\prod_{n=1}^{7} U_{\mathrm{CNOT},An-Bn}|\Psi\rangle\right] \tag{27}$$

where U_{CNOT} is an error-free CNOT gate. The state of the right bracket of Eq. (27), $|\Psi_f\rangle$, is the correct final codeword. The operator in the left bracket of Eq. (27), $F + \epsilon G$, represents deviations from $|\Psi_f\rangle$ that the code must correct for.

The different errors are categorized as follows. The off-diagonal elements of F correspond to spin-flip errors due to an imperfect, but coherent, CNOT gate. Phase sign-flip errors, which we ignore here, are determined by the diagonal elements. There are 64 single spin flip elements, e.g., $|\langle 1110|F|1111\rangle|^2$ (states are listed as $|A1B1A2B2\rangle$). The code can also repair any of the 64 possible double spin flips on separate codewords, e.g., $|\langle 0011|F|1111\rangle|^2$. The remaining 112 off-diagonal elements are ''disallowed.'' The positions of the different errors in the unitary transform of Eq. (27) are shown in Fig. 3. A relative measure of the importance of these different processes is given by the sum of the absolute squares of their matrix elements, as shown in Fig. 4. Similarly, the off-diagonal elements of G are also spin-flip errors, but accompanied by an incoherently emitted photon. Assuming this photon is lost, we trace G over the field states before summing the squares of the matrix elements for the different kinds of errors. The elements of G also have the prefactor $\epsilon^2 = (\pi/16)(\kappa e_0)(\hbar\bar{\omega})/(\epsilon_0 e_0^2/2)(cL^2)$, which is proportional to the Rabi frequency per photon flux in the pulse.

The solid lines in Fig. 4 suggest the relative importance of the various errors in F as a function of pulse length. Since the pulse does influence $A2$ and $B2$, there is a possibility that double spin-flips within a codeword occurs. As the pulse duration lengthens, the excursions of the state vectors for $A2$ and $B2$ become smaller, and the gate more nearly fulfills the property that it acts only upon $A1$ and $B1$. Thus very short pulses must be avoided. Since the disallowed errors decrease as the square of the allowed errors, this fault tolerant CNOT represents a scalable implementation [15].

On the other hand, the dashed lines in Fig. 4 are sums of squares of elements in G, excluding the prefactor $\epsilon^2 \propto T$. The magnitude of ϵ depends greatly upon the method chosen to implement the gate (see Sec. IV), but for large enough T it will force the dashed lines of Fig. 4 to have a positive slope. As the pulse becomes longer, the field strength decreases, and eventually the probability for single and allowed double spin-flip errors to occur increases. Thus, very long pulses must also be avoided. The sum of the squared matrix ele-

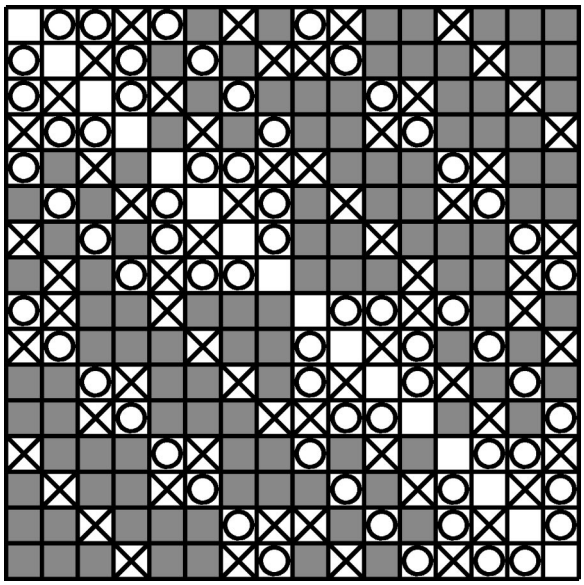

FIG. 3. A classification of the different errors found in the unitary transforms F and G from Eq. (27). Matrix elements are listed in the order $|0000\rangle$, $|0001\rangle$, $|0010\rangle$, and so on to $|1111\rangle$ (labeled as $|A1B1A2B2\rangle$). Circles are single spin-flips, crosses are double spin-flips where no more than one spin flip occurs in each codeword, and shaded elements are unrecoverable errors, with two or more spin-flips per codeword.

ments for the disallowed double spin flip errors asymptotically approaches $(JT/\pi)^{-2}$ for large T, the same as for the allowed errors in F. Thus, for large T, these errors scale as T^{-1}. This curious behavior can be explained as follows. For a weak field,

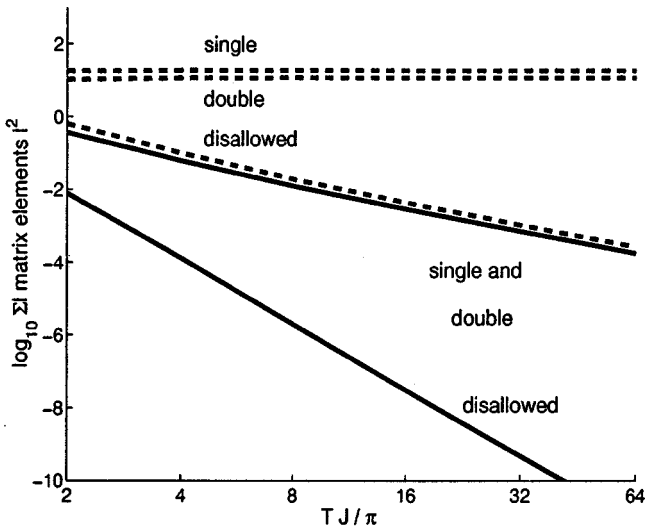

FIG. 4. The (unitless) sums of the squares of the matrix elements corresponding to different types of spin-flip errors in an implementation of a fault-tolerant CNOT gate, using frequency-selective pulses, as a function of the pulse length. Time is scaled to the separation of the different transitions (TJ is unitless). The solid lines are from F, where the single and allowed double spin-flip errors lie on the same line. Disallowed spin-flip errors (two or more spin-flips within a codeword) decrease as the square of the repairable errors. The dashed lines are from G, representing spin-flips accompanied by the incoherent emission of a photon. A prefactor $\epsilon^2 \propto T$ is not included in the plot.

$$|\psi_q\rangle \approx |q\rangle + \frac{\kappa e_0}{2} \sum_{q' \neq q} |q'\rangle \frac{\langle q'| \sum_n \mu_n S_{n,x} |q\rangle}{\omega_{q'} - \omega_q}. \quad (28)$$

The presence of the lowering operator in Eq. (26) means that at least one spin-flip occurs; because $|\psi_q\rangle$ mixes the different $|q\rangle$, a single coherent error can become a disallowed error. Thus, for frequency-selective pulses, the decoherence errors can scale in a worse way than the single spin-flip errors, although with a potentially small constant in front. This is consistent with the case of $\mu = 0$ for $A2$ and $B2$, where it can be shown that all the matrix elements in both F and G corresponding to the disallowed errors are zero, for any value of T.

IV. DISCUSSION

A. Grover's algorithm

When unitary transforms are driven by externally generated coherent fields in the manner discussed above, a decoherence mechanism exists that, with each applied pulse, tends to scramble the computer's memory. This decoherence mechanism is slightly different from the usual environmentally induced decoherence, in that it increases as the number of times the programmer attempts to manipulate the qubit system coherently. In the case of Grover's search algorithm where the Walsh-Hadamard transforms are externally driven, the degradation of the correct response scales as $\epsilon^2 K 2^{K/2}$.

A criticism of this analysis might be in the specific choice used to implement the W_n. Whatever method is chosen, the field-qubit propagators still hold, and some back reaction must exist (but see below). In general, the degradation should scale as the number of times a qubit transform is driven. For Grover's algorithm, if no error correction routines are implemented, then the amplitude of the field will have to increase exponentially with increasing number of qubits, K, in order to keep the error below a fixed bound. Clearly, this is not a scalable way to implement Grover's algorithm.

How important is this decoherence mechanism to the different proposed quantum computer schemes? Let us employ simple order of magnitude arguments, and ignore for the moment the implementation of error-correcting codes. As previously mentioned, the prefactor $\epsilon^2 = (1/64\pi)(\kappa E/\sqrt{2})(\hbar\overline{\omega})/(\epsilon_0 E^2/2)(cL^2)$ is proportional to the photon flux in the pulse per Rabi frequency of the qubit. The Walsh-Hadamard transforms are roughly a single Rabi cycle long, so ϵ^2 is also the inverse of the total number of photons in a pulse. The rest of the factors are of order unity, so that the probability for decoherence goes as $K2^{K/2}$ per number of photons per pulse.

Examine the case where lasers are used to drive single ions or atoms. A recent experimental demonstration of a logic gate using trapped $^9Be^+$ ions as qubits [32] used 1-mW pulses of $\approx 10^{-4}$-s duration at 300 nm. This corresponds to 10^{12} photons per pulse. The very small prefactor will not pose a problem for computations involving a polynomial number of steps with increasing K, but for Grover's algorithm this mechanism limits the number of qubits to ≈ 70.

Next let us examine the case for NMR quantum computing. First, let us address how to utilize the signal from a large number of independent quantum computers. Assume that a sample can be prepared in the ground state, and let us ignore the interaction of the computers with one another. The difficulties with these assumptions have been discussed elsewhere [33]. The application of Grover's algorithm results in a final state

$$|\Psi\rangle=\prod_{i=1}^{10^{23}}\left((1-\gamma^2/2)|y^{(i)}\rangle+\gamma\sum_x G(x)|x^{(i)}\rangle\right)|\mathrm{vac}\rangle,$$

where G creates orthogonal field states that contribute little amplitude to the correct solution. The total signal is the sum from all of the quantum computers in the sample, $\langle\Psi|\Sigma_i(|y^{(i)}\rangle\langle y^{(i)}|)|\Psi\rangle=N(1-\gamma^2/2)$. The point is that at low temperatures, the macroscopic decoherence rate is multiplied by the total number of independent quantum computers in the sample. Typically, NMR uses $\nu\approx10^8$ Hz, or a photon energy of 10^{-25} J. Pulses are 100 W for 10 μs, for a total energy of 10^{-3} J. Thus, there are 10^{22} photons per pulse. This limits Grover's algorithm for NMR to ≈140 qubits if we can do NMR on a single spin system, which is an improvement over other techniques. However, if we require the signal from a micromole of computers (10^{17}) in order to detect the final answer, then we are limited to ≈25 qubits. Electron spin resonance is not sufficiently better: $\nu\approx10^{10}$ Hz, pulses are 1 kW for 10 ns, and thus use 10^{18} photons.

If, as is usually the case, $\Omega\ll\omega_n$, then the number of photons required to generate W_n is proportional to $\Omega/(\kappa^2\omega_n)$. Thus physical systems with small values of ω_n or κ are the most resistant to the above decoherence mechanism. Unfortunately, such systems have other limitations: if ω_n is small, then the temperature of the system is required to scale with increasing K in an unfortunate manner [33]; while if κ is small, then the time required to drive a gate increases, which slows computation down.

Will driving qubits by externally applied, static electric fields [9] offer any significant advantages? A similar proposal could be envisioned for NMR by applying static magnetic fields along different directions to the individual spins to drive the gates. To describe such a process, note that these longitudinal fields are not independent degrees of freedom in the Coulomb gauge [34]. They arise from matrix elements between the qubits and the charged particles that give rise to the static field. Thus, for the case electrostatic fields from electrodes, decoherence might result from the field operators describing the motion of electrons at the Fermi level of the electrodes. Unfortunately, an explicit calculation of this decoherence is complicated by the band structure of the electrode, but it would be surprising if no decoherence was present.

B. Assumption of uncorrelated errors

The above observations suggest certain types of coherent manipulations of entire quantum computers should be avoided, even if they result in fewer coherently produced errors. If frequency-selective pulses are implemented, then it seems that an optimum pulse length must exist: longer pulses use weak fields whose quantum nature becomes more apparent to the qubit, while shorter pulses are less frequency selective, violating the idea that qubits not directly acted upon by the gate are immune to spin-flip errors. It should be noted that there do exist continuously amplitude- and phase-modulated pulses that can selectively invert transitions with high accuracy within a given bandwidth [35]. They do so partly by sending the states of qubits that are just outside of the bandwidth along complex orbits whose end points nearly match their starting points. It seems possible that pulses could be tailored to reduce these types of errors. A better solution might be to avoid these errors altogether by having the field spatially overlap with only those qubits to be driven.

Finally, we note a few other means by which to reduce this decoherence. First, the appearance of terms such as $|B_\beta+B_-|$ in Eq. (21) shows that destructive interference can lessen the probability of photon emission. It is known to be possible to quench spontaneous emission in multilevel systems [36]. It seems likely that certain systems could be designed to remove, through destructive interference, the lowest-order terms in Eq. (24). Second, for bulk quantum computation where there is an excess of signal, phase cycling can be used to cancel the signal from those computers that suffer certain kinds of errors.

V. CONCLUSIONS

Quantum computers that use external, classically generated electromagnetic fields to drive the evolution of the system undergo a decoherence induced by the quantum back reaction to those fields. The probability for the quantum system to be degraded increases as the total number of externally driven transforms, and inversely as the photon flux per pulse, per Rabi frequency of the transition. Algorithms that require an exponentially increasing number of pulses as the problem size increase, and thus require some form of error correction for a scalable implementation. It is also found that implementing fault-tolerant gates with externally applied fields that influence all qubits in the system at once, is not an optimal implementation, at least in regards to this decoherence mechanism.

ACKNOWLEDGMENT

We gratefully acknowledge support from the Air Force Office of Scientific Research.

[1] R. Feynman, Found. Phys. **16**, 507 (1986).
[2] D. Deutsch, Proc. R. Soc. London, Ser. A **425**, 73 (1989).
[3] S. Lloyd, Science **261**, 1569 (1993).
[4] J.A. Jones and M. Mosca, J. Chem. Phys. **109**, 1648 (1998).
[5] D.G. Cory, A.F. Fahmy, and T.F. Havel, in *Proceedings of the Fourth Workshop on Physics and Computation*, edited by T. Toffoli (New England Complex Systems Institute, Boston, 1996), pp. 87–91.

[6] N.A. Gershenfeld and I.L. Chaung, Science **275**, 350 (1997).
[7] J.I. Cirac and P. Zoller, Phys. Rev. Lett. **74**, 4091 (1995).
[8] S. Schneider, D.F.V. James, and G.J. Milburn, e-print quant-ph/9808012.
[9] B.E. Kane, Nature (London) **393**, 133 (1998).
[10] D.S. Chemla and D.A.B. Miller, in *Heterojunction Band Discontinuities, Physics, and Device Applications*, edited by F. Capasso and G. Margaritondo (North-Holland, New York, 1987).
[11] R. Feynman, R. Leighton, and M. Sands, *The Feynman Lectures on Physics* (Addison-Wesley, Reading, MA, 1965), Vol. III, Chap. 3.
[12] D. Giulini, E. Joos, C. Kiefer, J. Kupsch, I.-O. Stamatescu, and H. D. Zeh, *Decoherence and the Appearance of a Classical World in Quantum Theory* (Springer, Berlin, 1996).
[13] W. Zurek, Phys. Today **44**(10), 36 (1991).
[14] L. Grover, Phys. Rev. Lett. **79**, 325 (1997).
[15] P. Shor, in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, edited by S. Goldwasser (IEEE Press, New York, 1994), pp. 56–65.
[16] N. Imoto, Prog. Crystal Growth Charact. **33**, 295 (1996).
[17] D.G. Cory, A.F. Fahmy, and T.F. Havel, Proc. Natl. Acad. Sci. USA **94**, 1634 (1997).
[18] E. Knill and R. Laflamme, Phys. Rev. A **55**, 900 (1997).
[19] A. Steane, Proc. R. Soc. London, Ser. A **452**, 2551 (1996).
[20] J. Preskill, in *Introduction to Quantum Computation and Information*, edited by H.-K. Lo, S. Popescu, and T. Spiller (World Scientific, Singapore, 1998).
[21] C. Zalka, e-print quant-ph/9612028.
[22] M.R. Garey and D.S. Johnson, *Computers and Intractability. A Guide to the Theory of NP Completeness* (Freeman, New York, 1979).
[23] C.H. Bennet, E. Bernstein, G. Brassard, and U. Vazirani, e-print quant-ph/9701001.
[24] M. Boyer, G. Brassard, P. Hoeyer, and A. Tapp, e-print quant-ph/9605034.
[25] C. Zalka, e-print quant-ph/9711070.
[26] R.R. Ernst, G. Bodenhausen, and A. Wokaun, *Principals of Nuclear Magnetic Resonance in One and Two Dimensions* (Clarendon Press, Oxford, 1987).
[27] The assumption $\kappa E \gg J$ is useful to implement single qubit interactions only. In NMR terminology, it corresponds to the transformation of magnetization from a given spin, irregardless of J-J couplings (or hyperfine couplings for the case of ESR). Implementing transforms that *entangle* separate qubits, however, can involve the use of selective pulses that manipulate the magnetization within the J-J coupling (or hyperfine couplings) manifold, as shown for the CNOT gate.
[28] L. Mandel and E. Wolf, *Optical Coherence and Quantum Optics* (Cambridge University Press, Cambridge, England, 1995). Chap. 11.13.
[29] M.O. Scully, B.-G. Englert, and H. Walther, Nature (London) **351**, 111 (1991).
[30] D. G. Cory, M. D. Price, and T. F. Havel, Physica D **120**, 82 (1998).
[31] A.R. Calderbank and P. Shor, Phys. Rev. A **54**, 1098 (1996).
[32] C. Monroe, D. M. Meekhof, B. E. King, W. M. Itano, and D. J. Wineland, Phys. Rev. Lett. **75**, 4714 (1995).
[33] W.S. Warren, Science **277**, 1688 (1997).
[34] C. Cohen-Tannoudji, J. Dupont-Roc, and G. Grynberg, *Photons & Atoms: Introduction to Quantum Electrodynamics* (Wiley, New York, 1989).
[35] W.S. Warren and M.S. Silver, Adv. Magn. Reson. **12**, 247 (1988).
[36] H. Lee, P. Polynkin, M.O. Scully, and S.-Y. Zhu, Phys. Rev. A **55**, 4454 (1997).