Analytic solutions for quantum logic gates and modeling pulse errors in a quantum computer with a Heisenberg interaction

G.P. Berman\textsuperscript{1}, D.I. Kamenev\textsuperscript{1}, and V.I. Tsifrinovich\textsuperscript{2}

\textsuperscript{1}Theoretical Division and Center for Nonlinear Studies, Los Alamos National Laboratory, Los Alamos, New Mexico 87545 and
\textsuperscript{2}IDS Department, Polytechnic University, Six Metrotech Center, Brooklyn, New York 11201

We analyze analytically and numerically quantum logic gates in a one-dimensional spin chain with Heisenberg interaction. Analytic solutions for basic one-qubit gates and swap gate are obtained for a quantum computer based on logical qubits. We calculated the errors caused by imperfect pulses which implement the quantum logic gates. It is numerically demonstrated that the probability error is proportional to $\varepsilon^4$, while the phase error is proportional to $\varepsilon$, where $\varepsilon$ is the characteristic deviation from the perfect pulse duration.

PACS numbers: 03.67.Lx, 75.10.Jm

I. INTRODUCTION

It is known that the Heisenberg interaction alone can provide a universal set of gates for quantum computation \cite{1}. A computer based on the Heisenberg interaction does not require magnetic fields nor electromagnetic pulses. Implementations of a quantum computer using the Heisenberg interaction between the spins of the quantum dots or impurities in semiconductors promise clock-speeds in GHz region. The spins do not interact with each other unless one applies a voltage, which turns on the exchange interaction between a selected pair of spins.

In order to perform single-qubit rotations using the Heisenberg interaction, one should use coded, or logical, qubits. In this paper, we use the coding introduced in Ref. \cite{1} and derive optimal gate sequences to implement swap gate and basic one-qubit logic operations. The errors caused by imperfections of the pulses are investigated numerically. The random deviations in the areas of the pulses in our simulations are assumed to have a Gaussian
distribution with variance $\varepsilon$.

II. QUANTUM DYNAMICS

Consider the dynamics of a spin system with an isotropic Heisenberg interaction between neighboring spins. The Hamiltonian which describes the interaction $J(\bar{t})$ between $k$th and $(k+1)$th spins is

$$ H_k(\bar{t}) = J(\bar{t})S_k S_{k+1}, \quad (1) $$

where $\bar{t}$ is time, $S_k$ is the operator of the $k$th spin $1/2$. The solution of the Schrödinger equation with the Hamiltonian (1) can be written in the form

$$ \psi(\bar{t}) = \exp \left( -\frac{i}{\hbar} \int_0^{\bar{t}} J(\bar{t}') d\bar{t}' S_k S_{k+1} \right) \psi(0). \quad (2) $$

(We do not use the time-ordering operator because $[H_k(\bar{t}), H_k(\bar{t}')] = 0$.) Introducing a new effective dimensionless time,

$$ t = \frac{1}{2\pi \hbar} \int_0^{\bar{t}} J(\bar{t}') d\bar{t}', \quad (3) $$

one can write Eq. (2) as

$$ \psi(t) = \exp (-i2\pi t S_k S_{k+1}) \psi(0). \quad (4) $$

This is the solution of the following dimensionless Schrödinger equation:

$$ i \frac{\partial \psi(t)}{\partial t} = V_k \psi(t), \quad (5) $$

where

$$ V_k = 2\pi \left[ S_k^z S_{k+1}^z + \frac{1}{2} (S_k^+ S_{k+1}^- + S_k^- S_{k+1}^+) \right] \quad (6) $$

is the dimensionless Hamiltonian, $S_k^x$, $S_k^y$, and $S_k^z$ are the components of the operator $S_k$, $S_k^\pm = S_k^x \pm i S_k^y$. After decomposition of the wave function in the basis states $|n\rangle$,

$$ \psi(t) = \sum_n C_n(t) |n\rangle, \quad (7) $$

where the states $|n\rangle$ are defined below in Eqs. (11) and (46), one obtains a system of dimensionless differential equations for the expansion coefficients,

$$ i \dot{C}_n = \sum_m \langle n | V_k | m \rangle C_m, \quad (8) $$

where the dot indicates differentiation with respect to time $t$. 
The matrix elements in Eq. (8) can be calculated by action of the Hamiltonian $V_k$ in Eq. (6) on the physical qubits (spins) using the following relations:

$$
\begin{align*}
S_z^k |...0_k...\rangle &= \frac{1}{2} |...0_k...\rangle, \\
S_z^k |...1_k...\rangle &= -\frac{1}{2} |...1_k...\rangle, \\
S_k^+ |...0_k...\rangle &= 0, \\
S_k^+ |...1_k...\rangle &= |...0_k...\rangle, \\
S_k^- |...0_k...\rangle &= |...1_k...\rangle, \\
S_k^- |...1_k...\rangle &= 0.
\end{align*}
$$

(9)

III. SINGLE QUBIT GATES

Let us consider only the first three spins, 0, 1, and 2, of the spin chain in Fig. 1. We suppose that initially there are two spins in the state $|0\rangle$ and one spin in the state $|1\rangle$. Since the Hamiltonians $V_k$ can not flip individual spins (but can only swap the neighboring spins) one can choose an invariant subspace spanned by only three states of the $2^3 = 8$ basis states:

$$
|020100\rangle, \quad |021100\rangle, \quad |120100\rangle,
$$

(10)

or by their normalized and orthogonal superpositions

$$
|0\rangle = |0_A\rangle = \frac{1}{\sqrt{2}}(|021100\rangle - |120100\rangle), \quad |1\rangle = |1_A\rangle = \sqrt{\frac{2}{3}} \left( |020100\rangle - \frac{1}{2} |021100\rangle - \frac{1}{2} |120100\rangle \right), \\
|2\rangle = |a_A\rangle = \frac{1}{\sqrt{3}} \left( |020110\rangle + |021100\rangle + |120100\rangle \right).
$$

(11)

We define the state $|0_A\rangle$ as the ground state of the logical qubit $A$; the state $|1_A\rangle$ as the excited state; and the state $|a_A\rangle$ as the auxiliary state. One can show that all matrix elements for transitions to the state $|a_A\rangle$ are equal to zero,

$$
\langle a_A | V_0 | 0_A \rangle = \langle a_A | V_0 | 1_A \rangle = \langle a_A | V_1 | 0_A \rangle = \langle a_A | V_1 | 1_A \rangle = 0.
$$

(12)
If the state $|a_A\rangle$ is initially not populated, it remains empty under the action of the Hamiltonians $V_0$ and $V_1$. For the single-qubit operations, analyzed in this Section we assume that initially $C_2(t = 0) = 0$ and we consider the dynamics including only the states $|0\rangle = |0_A\rangle$ and $|1\rangle = |1_A\rangle$.

The matrix elements of the two Hamiltonians have the form

$$V_0 : \begin{pmatrix} 0 & -\Omega/2 \\ -\Omega/2 & \Delta \end{pmatrix}, \quad V_1 : \begin{pmatrix} 3\Delta/2 & 0 \\ 0 & -\Delta/2 \end{pmatrix},$$

where

$$\Delta = -\pi, \quad \Omega = -\sqrt{3\pi}. \quad (14)$$

The solution of the Schrödinger equation generated by the diagonal matrix $V_1$ has the form

$$C_0(t) = e^{-i\Delta t/2}C_0(0), \quad C_1(t) = e^{i\Delta t/2}C_1(0). \quad (15)$$

The solution generated by the matrix $V_0$ is

$$C_0(t) = \left\{ C_0(0) \left[ \cos(\Lambda t/2) + i\frac{\Delta}{\Lambda} \sin(\Lambda t/2) \right] + iC_1(0) \frac{\Omega}{\Lambda} \sin(\Lambda t/2) \right\} e^{-i\Delta t/2},$$

$$C_1(t) = \left\{ C_1(0) \left[ \cos(\Lambda t/2) - i\frac{\Delta}{\Lambda} \sin(\Lambda t/2) \right] + iC_0(0) \frac{\Omega}{\Lambda} \sin(\Lambda t/2) \right\} e^{-i\Delta t/2}, \quad (16)$$

where

$$\Lambda = \sqrt{\Delta^2 + \Omega^2} = 2\pi. \quad (17)$$

For convenience, we present below all dependences expressed in terms of the frequencies $\Omega$, $\Delta$, and $\Lambda$, but not in terms of their numerical values.

### A. One logical qubit flip

In order to flip the logical qubit $A$ using Eq. (16) we assume

$$C_0(0) = 1, \quad C_1(0) = 0, \quad (18)$$

and apply the Hamiltonian $V_0$ for time $t$. Then, one obtains

$$C_0(t) = \left[ \cos(\Lambda t/2) + i\frac{\Delta}{\Lambda} \sin(\Lambda t/2) \right] e^{-i\Delta t/2},$$

$$C_1(t) = i\frac{\Omega}{\Lambda} \sin(\Lambda t/2)e^{-i\Delta t/2}. \quad (19)$$
From this solution one can see that it is impossible to flip the logical qubit using only one pulse since the coefficient $C_0(t)$ in Eq. (19) does not become zero for any $t$. To solve this problem we use the pulse sequence

$$F_{A_{ph}}^h = V_0(t_3)V_1(t_2)V_0(t_1), \quad (20)$$

proposed in Ref. [1]. Here and below the superscript ‘ph’ indicates that the gate requires additional pulses to implement the phase correction. In Eq. (20) $V_i(t)$ indicates action of $i$th Hamiltonian during time $t$, and the sequence must be read from right to left. In this Section we obtain exact analytical expressions for $t_1$, $t_2$, and $t_3$.

A flip of the qubit A with the initial conditions (18) means making the transition $|0\rangle \rightarrow |1\rangle$. Using Eqs. (15), (16), and (18) and setting the amplitude $C_0(t) = 0$ after the action of the $F_{A_{ph}}^h$ gate, one obtains the equation

$$e^{-i\Delta t \left( t_1 - t_2 + t_3 \right)} \left\{ e^{-2i\Delta t_2} \left[ \cos(\Lambda t_1/2) + i \frac{\Lambda}{\Delta} \sin(\Lambda t_1/2) \right] \left[ \cos(\Lambda t_3/2) + i \frac{\Lambda}{\Delta} \sin(\Lambda t_3/2) \right] - \frac{\Omega^2}{\Lambda^2} \sin(\Lambda t_1/2) \sin(\Lambda t_3/2) \right\} = 0. \quad (21)$$

Equation (21) is satisfied when both the real and the imaginary parts of the expression in the curly brackets are equal to zero.

In order to solve Eq. (21) we first assume that $\cos(\Lambda t_1/2) \neq 0$, $\cos(2\Delta t_2) \neq 0$, and $\cos(\Lambda t_3/2) \neq 0$. Then, for

$$x = \tan(\Lambda t_1/2), \quad y = \tan(2\Delta t_2), \quad z = \tan(\Lambda t_3/2)$$

one obtains the following system of two coupled equations:

$$1 - xz + \frac{\Lambda}{\Delta} y(x + z) = 0,$$

$$y \left( 1 - \frac{\Delta^2}{\Lambda^2} xz \right) + \frac{\Lambda}{\Delta} (x + z) = 0. \quad (22)$$

Using Eqs. (14) and (17) and eliminating $y$, one has

$$(xz - 1)(4 - xz) = (x + z)^2. \quad (23)$$

Introducing the notations $x + z = 2b$ and $xz = c$ one can present $x$ and $z$ as the two solutions ($\xi_1 = x$ and $\xi_2 = z$) of the quadratic equation

$$\xi^2 - 2b\xi + c = 0. \quad (24)$$
Using definitions of $b$ and $c$ and Eq. (23) one can show that Eq. (24) has no real solution.

In a similar way one can show that there is no real solution when $\cos(\Lambda t_1/2) = 0$ or $\cos(\Lambda t_3/2) = 0$. For $\cos(2\Delta t_2) = 0$, the two solutions are

$$
t'_1 = \frac{\arctan(3 - \sqrt{5})}{\pi}, \quad t'_2 = \frac{1}{4}, \quad t'_3 = \frac{\arctan(3 + \sqrt{5})}{\pi}
$$

and

$$
t_1 = 1 - \frac{\arctan(3 - \sqrt{5})}{\pi}, \quad t_2 = \frac{3}{4}, \quad t_3 = 1 - \frac{\arctan(3 + \sqrt{5})}{\pi}.
$$

Below we use only the second solution (25).

The $F^{\text{ph}}_A$ gate generates different phases for two basis states,

$$
F^{\text{ph}}_A \begin{pmatrix} C_0 \\ C_1 \end{pmatrix} = \begin{pmatrix} e^{i\varphi_1} C_1 \\ e^{i\varphi_2} C_0 \end{pmatrix},
$$

where

$$
\varphi_1 = \frac{1}{2} \left[ \frac{3\pi}{4} + \arctan 2 - \arctan(\sqrt{5}/2) \right], \quad \varphi_2 = \frac{1}{2} \left[ \frac{3\pi}{4} + \arctan 2 + \arctan(\sqrt{5}/2) \right].
$$

In order to correct the phases, an additional pulse is required. The phase-corrected gate $F_A$ for flipping the qubit $A$ has the form

$$
F_A = V_1(t_4)F^{\text{ph}}_A = V_1(t_4)V_0(t_3)V_1(t_2)V_0(t_1).
$$

In order to find the time $t_4$ we use the solution (15). The additional phase-correcting pulse $V_1(t_4)$ modifies Eq. (26) to become

$$
F_A \begin{pmatrix} C_0 \\ C_1 \end{pmatrix} = \begin{pmatrix} e^{i(\varphi_1 + \Delta t_4/2)} C_0 \\ e^{i(\varphi_2 - 3\Delta t_4/2)} C_1 \end{pmatrix}.
$$

One can make the phases of the both states equal to each other by application of the $F_A$ gate if the condition

$$
\varphi_1 + \Delta t_4/2 = \varphi_2 - 3\Delta t_4/2
$$

is satisfied. This equation determines the last parameter,

$$
t_4 = 1 - \frac{\arctan(\sqrt{5}/2)}{2\pi},
$$

required to implement the phase-corrected flip of the qubit $A$. The flip gate for the qubit $A$ can be written as

$$
F_A \begin{pmatrix} C_0 \\ C_1 \end{pmatrix} = e^{i\Phi_F} \begin{pmatrix} C_1 \\ C_0 \end{pmatrix},
$$

where the overall phase for the single qubit flip gate is

$$
\Phi_F = -\frac{\pi}{8} + \frac{1}{2} \arctan 2 - \frac{1}{4} \arctan(\sqrt{5}/2).
$$
B. Hadamard transform

The Hadamard transform $H_A$ for the qubit $A$ can be performed using the pulse sequence

$$H_A = V_1(t_5)V_0(t_6)V_1(t_5).$$ (33)

Here the pulses $V_1(t_5)$ are used to provide the correct phases and the pulse $V_0(t_6)$ is needed to split each of the states $|0\rangle$ and $|1\rangle$ into a superposition of the states with equal probabilities. The time-intervals are

$$t_5 = \frac{3}{4} + \frac{\arctan(1/\sqrt{2})}{2\pi}, \quad t_6 = \frac{\arctan\sqrt{2}}{\pi}. \quad (34)$$

The Hadamard gate transforms the wave function as

$$H_A \begin{pmatrix} C_0 \\ C_1 \end{pmatrix} = \frac{e^{i\pi/2}}{\sqrt{2}} \begin{pmatrix} C_0 + C_1 \\ C_0 - C_1 \end{pmatrix}. \quad (35)$$

C. Phase gate

The phase gate $P_A(\theta)$ for the qubit $A$ can be performed using only one pulse

$$P_A(\theta) = V_1[t(\theta)], \quad (36)$$

where

$$t(\theta) = 1 - \frac{\theta}{2\pi}, \quad (37)$$

and the angle $\theta$ is defined in the interval $[0, 2\pi]$. The Phase gate transforms the wave function in the following way

$$P_A \begin{pmatrix} C_0 \\ C_1 \end{pmatrix} = e^{i\Phi_P(\theta)} \begin{pmatrix} C_0 \\ e^{i\theta}C_1 \end{pmatrix}. \quad (38)$$

The overall phase generated by the phase gate is

$$\Phi_P(\theta) = \frac{3\pi}{2} - \frac{3\theta}{4}. \quad (39)$$

The single qubit operations for the qubit $B$ in Fig. 1 can be performed using the same sequences like those for the qubit $A$ with the substitutions $V_0(t) \to V_3(t)$ and $V_1(t) \to V_4(t)$.
IV. SWAP GATE

It is convenient to analyze the spin states [from which the logical qubits are formed, see Eq. (11)]. Consider the four different spin states,

\[ |m\rangle = |\ldots 0_k 0_{k+1} \ldots \rangle, \quad |p\rangle = |\ldots 1_k 1_{k+1} \ldots \rangle, \]

\[ |i\rangle = |\ldots 1_k 0_{k+1} \ldots \rangle, \quad |j\rangle = |\ldots 0_k 1_{k+1} \ldots \rangle. \] (40)

These states form two one-dimensional and one two-dimensional invariant subspaces. The states \( |m\rangle \) and \( |p\rangle \) are eigenstates of the Hamiltonian \( V_k \),

\[ V_k(t)|m\rangle = e^{-i\frac{\pi}{4}t}|m\rangle, \quad V_k(t)|p\rangle = e^{-i\frac{\pi}{4}t}|p\rangle. \] (41)

The states \( |i\rangle \) and \( |j\rangle \) are transformed as

\[ V_k(t)|i\rangle = e^{i\frac{\pi}{4}t} [\cos(\pi t)|i\rangle - i\sin(\pi t)|j\rangle], \]

\[ V_k(t)|j\rangle = e^{i\frac{\pi}{4}t} [\cos(\pi t)|j\rangle - i\sin(\pi t)|i\rangle]. \] (42)

From Eqs. (41) and (42) one can see that the pulse \( V_k(1/2) \) can be used as a swap gate between the \( k \)th and \( (k + 1) \)th spins. After the pulse \( V_k(1/2) \) all states acquire the phase \(-i\pi/4\).

The swap gate between the spins can be used for implementation of the swap gate between the logical qubits. The two logical qubits, A and B, in Fig. 1 are formed by the superpositions of the spin states involving six spins. Consider one state of the superposition, for example, the state \( |0_5 0_4 1_3 0_2 1_1 0_0\rangle \). The spins 0, 1, and 2 are related to the logical qubit A and the spins 3, 4, and 5 are related to the logical qubit B. Using five swaps between the neighboring spins one can move the state of the 5th spin to the zeroth spin,

\[ C_{5,0}|0_5 0_4 1_3 0_2 1_1 0_0\rangle = e^{-i\frac{\pi}{4}} |0_5 1_4 0_3 1_2 0_1 0_0\rangle, \] (43)

where \( C_{5,0} \) is the operator or the cyclic permutation,

\[ C_{5,0} = V_0 \left( \frac{1}{2} \right) V_1 \left( \frac{1}{2} \right) V_2 \left( \frac{1}{2} \right) V_3 \left( \frac{1}{2} \right) V_4 \left( \frac{1}{2} \right). \] (44)

Three successive applications of the operator \( C_{5,0} \) result in the swap gate \( S_{AB} \) between the logical qubits (below called swap gate),

\[ S_{AB} = C_{5,0} C_{5,0} C_{5,0}. \] (45)
The swap gate $S_{AB}$ produces an overall phase $\pi/4$ for the wave function. The total number of pulses required to execute the swap gate is 15. Note that the result of the swap gate is independent of a kind of coding of the logical qubits through the spin states.

V. MODELING ERRORS IN THE SWAP GATE

In spite of the rather simple form of the swap gate $S_{AB}$, it does implement a complex logic operation on logical qubits. Indeed, if initially one has a basis logical state, e.g. $|1_B0_A\rangle$, in the process of applying the swap gate one has a superposition of many states, while, finally, only one state ($|0_B1_A\rangle$) survives, and all other states disappear.

Numerical simulations of the swap gate between the qubits A and B were performed in the invariant Hilbert subspace spanned by the following 15 [$15 = C_6^2 = 6!/2!4!$] states:

$$
|0\rangle = |0_B0_A\rangle, \quad |1\rangle = |0_B1_A\rangle, \quad |2\rangle = |1_B0_A\rangle, \quad |3\rangle = |1_B1_A\rangle,
$$

$$
|4\rangle = |0_Ba_A\rangle, \quad |5\rangle = |1_Ba_A\rangle, \quad |6\rangle = |a_B0_A\rangle, \quad |7\rangle = |a_B1_A\rangle,
$$

$$
|8\rangle = |a_Ba_A\rangle, \quad |9\rangle = |000\ 011\rangle, \quad |10\rangle = |000\ 101\rangle, \quad |11\rangle = |000\ 110\rangle,
$$

$$
|12\rangle = |011\ 000\rangle, \quad |13\rangle = |101\ 000\rangle, \quad |14\rangle = |110\ 000\rangle.
$$

The dynamics was simulated using the evolution operators built using the eigenstates of the Hamiltonians $V_k$, $k = 0, 1, \ldots, 5$, in the 15-dimensional space. When the time-intervals $t$ for the pulses were exactly equal to $t = t_0 = 1/2$, the errors in implementation of the swap gate were of the order of $10^{-15}$, i.e. accuracy was limited only by the round-off errors. Since $t$ is proportional to the area of the pulse, the form of the pulse is not important. However, in an experiment there is always some deviation in $t$ from its optimal value $t_0$. To understand the error caused by this deviation, we modeled the swap gate with imperfect pulses. The duration of each imperfect pulse is taken as

$$
t = t_0 + \delta t,
$$

where the random deviation $\delta t$ is assumed to have the Gaussian distribution $\exp[-(\delta t)^2/(2\varepsilon^2)]$.

We define the probability error as

$$
P_S = ||C_j(T)||^2 - |C_i(0)||^2, \quad C_i(0) = 1,
$$

where $C_i(0)$ is the initial state of logical qubits.
FIG. 2: (a) The average probability error $P_S$ and (b) the average phase error $Q_S$ of the swap gate as a function of $\varepsilon$ (filled circles). The least square fits (solid lines), show that: (a) the probability error increases as $P_S = 3.183 \times 10^3 \times \varepsilon^{3.998}, \chi^2 = 43.5$; (b) the phase error is given by $Q_S = 10.2033 \times \varepsilon^{1.0031}, \chi^2 = 1.0$.

where $T$ is the duration of the swap gate and the final state $|j\rangle$ is related to the initial state $|i\rangle$ as

$$|j\rangle = S^i_{AB}|i\rangle. \quad (49)$$

Here $S^i_{AB}$ is the ideal swap gate. The probability error $P_S$, shown in Fig. 2(a), increases as a function of $\varepsilon$ approximately as $3.2 \times 10^3 \times \varepsilon^4$.

Next, we study the phase errors [see Fig. 2(b)], caused by the random fluctuation of the pulse duration $t$. Under the action of the sequence (45) of the perfect pulses the four logical basis states $|00\rangle$, $|01\rangle$, $|10\rangle$, and $|11\rangle$ transform correspondingly to $|00\rangle$, $|10\rangle$, $|01\rangle$, and $|11\rangle$ with the same phase shift. Under the action of the imperfect pulses we obtain four different phase shifts for the basis states. We define the phase error $Q_S$ as the maximum difference between these phase shifts. From Fig. 2(b) one can see that the phase error is approximately equal to $10.2\varepsilon$.

The data in Figs. 2(a,b) are averaged over 1000 runs with different randomly chosen initial states $|i\rangle$ and different random deviations $\delta t$ from the ideal pulse duration $t_0$. In Figs. 2(a,b) $\chi^2$ was calculated as

$$\chi^2 = \sum_{k=1}^{K} \frac{(y_k - \bar{y}_k)^2}{(\delta y_k)^2},$$

where the index $k$ labels the points on the graphs, $K$ is the number of points, $y_k = P^k_S$ in
Fig. 2(a) and $y_k = Q_k^{3}$ in Fig. 2(b) are the coordinates of the circles, $\bar{y}_k$ are the corresponding coordinates of the points on the straight lines for the same values of $\varepsilon$; $\delta y_k$ are the corresponding standard deviations.

VI. CONCLUSION

In this paper, analytic solutions for quantum logic gates are obtained for a quantum computer with an isotropic Heisenberg interaction between neighboring identical spins arranged in a one-dimensional spin chain. Single qubit flip, Hadamard and phase transforms are implemented by using, respectively, 4, 3, and 1 pulse(s). The swap gate is realized using 15 pulses. The probability and phase errors caused by imperfect pulses for the swap gate are calculated numerically. The probability error is proportional to $\varepsilon^4$, while the phase error is proportional to $\varepsilon$, where $\varepsilon$ is the characteristic deviation from the perfect pulse duration.

Acknowledgments

We thank G. D. Doolen for useful discussions. This work was supported by the Department of Energy (DOE) under Contract No. W-7405-ENG-36, by the National Security Agency (NSA), and by the Advanced Research and Development Activity (ARDA).

[1] D. P. DiVincenzo, D. Bacon, J. Kempe, G. Burkard, and K. B. Whaley, Nature (London) 408, 339 (2000); quant-ph/0005116 (v2) (2002).

[2] S.L. Meyer, Data Analysis for Scientists and Engineers (Peer Management Consultants, Ltd., Evanston, 1992).