Physical optimization of quantum error correction circuits

Guido Burkard* and Daniel Loss†
Department of Physics and Astronomy, University of Basel, Klingelbergstrasse 82, CH-4056 Basel, Switzerland

David P. DiVincenzo‡ and John A. Smolin§
IBM Research Division, T. J. Watson Research Center, P.O. Box 218, Yorktown Heights, New York 10598
(Received 18 May 1999)

Quantum error-correcting codes have been developed to protect a quantum computer from decoherence due to a noisy environment. In this paper, we present two methods for optimizing the physical implementation of such error correction schemes. First, we discuss an optimal quantum circuit implementation of the smallest error-correcting code (the three bit code). Quantum circuits are physically implemented by serial pulses, i.e., by switching on and off external parameters in the Hamiltonian one after another. In contrast to this, we introduce a parallel switching method which allows faster gate operation by switching all external parameters simultaneously, and which has potential applications for arbitrary quantum computer architectures. We apply both serial and parallel switching to electron spins in coupled quantum dots subject to a Heisenberg coupling $H = J(t)\mathbf{S}_1 \cdot \mathbf{S}_2$. We provide a list of steps that can be implemented experimentally and used as a test for the functionality of quantum error correction. [S0163-1829(99)03740-6]

I. INTRODUCTION

Quantum computers are capable of efficiently solving problems such as prime factoring[1] or simulating other quantum systems,[2] for which no efficient classical algorithm is known. A quantum computer is a device that stores and processes information which is physically represented in its quantum state.[3] Typically, such a device contains a collection of quantum two-state systems, e.g., spin-$\frac{1}{2}$ particles. The state of each two-state system then represents a quantum bit, or qubit, the smallest indivisible unit of information in a quantum computer. Computations are driven by interactions between the qubits, generating logic gates operating on them. A quantum gate operating on M qubits can be represented as a $2^M \times 2^M$ unitary matrix. Usually, a computation or algorithm is split up into a series of elementary gate operations involving only one or two qubits. In this representation, algorithms are also called quantum circuits. It has been demonstrated that there exist elementary two-qubit gates U which are universal when complemented with a sufficiently large set of single-qubit gates.[4] This means that any quantum algorithm can be split up into a quantum circuit which contains only U and single-qubit gates. Quantum circuits are in general not the most efficient way of implementing a quantum computation, as we will demonstrate in this paper.

First experimental realizations of quantum computation using trapped ions,[5] optical cavities,[6] and NMR,[7] involving two or three qubits, have been reported. Contrary to all of these systems, solid-state implementations have the potential for a large-scale quantum computer involving hundreds or thousands of qubits. In this paper, we will concentrate on a theoretical proposal to use coupled semiconductor quantum dots in which the spin of the excess electron on each dot represents a qubit.[8] Apart from electron spins in quantum dots, a number of other solid-state systems have been proposed for quantum computation: Nuclear spins of donor atoms in silicon,[9] Josephson junctions,[10] d-wave Josephson junctions,[11] and charge degrees of freedom in quantum dots.[12]

The physical implementation of quantum computation hinges upon the ability to find or design systems in which quantum phase coherence is maintained over long times compared to the duration of the typical controlled coherent operation. The discovery of quantum error-correcting codes has been a landmark in the effort to find methods to protect a quantum computer from the decohering effects of a noisy environment.[13] The smallest quantum error-correcting code for one qubit involving three code qubits has already been implemented in NMR.[14]

In this paper, we present theoretical methods for finding an optimal implementation of three-bit error correction. The optimization is understood here in terms of switching speed and switching complexity. The former is mainly motivated by the presence of decoherence which makes fast switching desirable, while the latter can be necessary if the physical implementation sets limits to the complexity of the switching. The two optimization goals usually are in conflict with each other, i.e., a fast implementation usually requires a complex switching mechanism while switching with a simple mechanism is slow. First, we will study the ''simple and slow'' switching provided by quantum circuits, and try to optimize it. Then, we will go on to ''complex and fast'' switching, for which we introduce parallel (as opposed to serial) pulses for the control parameters of the system, and show that the parallel pulses allow faster switching than serial pulses. We also introduce a numerical method for finding such parallel pulses for arbitrary gates and Hamiltonians. We note that in a similar approach, Sanders *et al.*[15] use a genetic algorithm to find optimized complex pulses to generate quantum gates using an Ising-type Hamiltonian for optically driven quantum dots coupled by dipole-dipole interactions. Our approach differs from this work in the underlying Hamiltonian (i.e., the mechanism proposed for quantum computation); in addition, the parallel pulses we suggest are

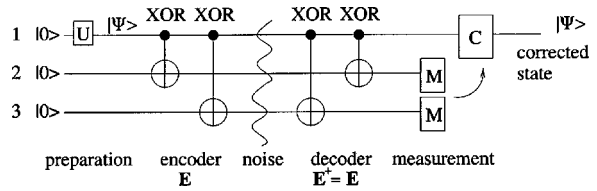

FIG. 1. The circuit representation for three-bit quantum error correction, where time is evolving from the left to the right. First, the three qubits (represented by the horizontal lines) are initialized. The following unitary transformation U on qubit 1 prepares the state $|\Psi\rangle$. The encoder E encodes the state $|\Psi\rangle$ in an entangled state of all three qubits. In the next step, (simulated) decoherence partly disrupts the state. After the decoding step (which is identical to the encoding), the qubits 2 and 3 are measured. If they are both one, qubit 1 has to be flipped ($C=\sigma_x$), otherwise qubit 1 is left unchanged ($C=\mathbb{1}$). If no more than one bit flip error occurred, the resulting state in register 1 is again $|\Psi\rangle$ despite the presence of the decoherence. The same circuit can also be used to protect the state $|\Psi\rangle$ against phase errors if, after the encoding step, each qubit is rotated by $\pi/2$ about the y axis and rotated back before the decoding.

general pulses that are discretized in time, whereas the pulses in Ref. 15 are chirped Gaussian pulses.

Three-qubit quantum error correction is able to correct either one bit flip or one phase flip error (correcting both types of errors requires a code with at least five code qubits[13]). The operation of the scheme is shown in the quantum circuit, Fig. 1. First, all three qubits (represented by horizontal lines) are initialized to the state $|0\rangle$, e.g., by polarizing the spins with a strong magnetic field. Then qubit one is rotated into an arbitrary state $|\Psi\rangle=U|0\rangle=\alpha|0\rangle+\beta|1\rangle$. The purpose of the quantum error correction scheme is to protect this state from external decoherence. In order to do this, the state $|\Psi\rangle$ is encoded in the highly entangled three-qubit state $|\Psi_L\rangle=E(|\Psi\rangle_1|0\rangle_2|0\rangle_3)=\alpha|0\rangle_1|0\rangle_2|0\rangle_3+\beta|1\rangle_1|1\rangle_2|1\rangle_3$.

The encoded state $|\Psi_L\rangle$ can then be subject to external noise causing a (partial) bit flip of one of the spins, $|\Psi_L\rangle\rightarrow\exp(i\epsilon\sigma_i^x)|\Psi_L\rangle=|\Psi_L'\rangle$, without the information contained in the encoded state $|\Psi_L\rangle$ being lost. The state $|\Psi_L\rangle$ is recovered (decoded) by applying the inverted encoding network $E^{-1}=E^\dagger=E$ which is identical to E since E is Hermitian. Then the qubits 2 and 3 are measured (for physical implementations of quantum measurements on spins in quantum dots, see Refs. 8 and 16–18). If both qubits are in state $|1\rangle$, then qubit 1 is flipped, otherwise it is left unchanged. This restores the state $|\Psi\rangle$ in qubit 1, which then can be measured in order to check the functionality of the scheme. It has to emphasized that the three-bit code is by far not the best code for protecting a quantum computer from decoherence, but since it is the most simple code it seems to be suited for the first experiments which test the functionality of quantum error correction.

If we choose to correct phase errors instead of bit errors, all three qubits have to be rotated about the y axis by $\pi/2$ after the action of the encoder gate E, and back again before the decoding step. These basis changes can be implemented by applying a homogeneous magnetic field $\pm B_y$ along the y axis for a duration $\pi\hbar/2g\mu_B B_y$. The encoded qubit has then the form $|\Psi_L\rangle=\alpha|-\rangle_1|-\rangle_2|-\rangle_3+\beta|+\rangle_1|+\rangle_2|+\rangle_3$, where $|\pm\rangle=(|0\rangle\pm|1\rangle)/\sqrt{2}$. We emphasize that the following considerations are applicable to both the bit and phase error-correcting codes.

For a first experiment one would probably want sufficiently low noise such that the state $|\Psi\rangle$ is not destroyed by ''natural'' noise. One would then introduce bit flips ''by hand'' by applying a random oscillatory magnetic field in the x direction and then check whether those artificial errors can be corrected for.

For the sake of concreteness, we will apply our methods to a system of coupled spins $\mathbf{S}_i$ with $s=\frac{1}{2}$ (each representing a qubit), subject to isotropic spin-spin interaction and local magnetic fields. With this model we capture the physics of electrons in coupled quantum dots.[8] We emphasize that a generalization to other systems with different Hamiltonians is straightforward and does not require a new method for optimizing the switching process.

Our paper is organized as follows. In Sec. II, we introduce the formalism that we use to describe the dynamics of electron spins in coupled quantum dots and other Heisenberg systems. The methods developed in Secs. III and IV, including the use of parallel pulses, are not special to the Heisenberg Hamiltonian Eq. (1). As an example, we give some results for transversely coupled spins (XY model) in Sec. V, because they are encountered when electronic spins are coupled using cavity QED.[19] The results of Secs. III–V are independent of the mechanisms that are involved in their physical implementation—they are derived under the assumption that the model Hamiltonian Eq. (1) [or Eq. (46)] is exact. In Sec. VI, we discuss some limitations and necessary conditions for the validity of this approach. Finally, in Sec. VII, we give a detailed list of instructions for both serial and parallel switching which must be followed in order to implement three-qubit quantum error correction in a system of spins subject to Heisenberg interactions in experiment.

II. MODEL

In the system we consider, the qubit is represented by the spin-$\frac{1}{2}$ state of the excess electron in a quantum dot, i.e., the ''spin up'' state $|\uparrow\rangle$ is identified with the logic state $|0\rangle\equiv|\uparrow\rangle$ and likewise $|1\rangle\equiv|\downarrow\rangle$, where the quantization axis is chosen along the z axis, $\sigma^z|\uparrow\rangle=+|\uparrow\rangle$ and $\sigma^z|\downarrow\rangle=-|\downarrow\rangle$.

The excess electron spins in a pair of quantum dots which are linked through a tunnel junction can be described by the Heisenberg Hamiltonian[8,16]

$$H(J,\mathbf{B}_i,\mathbf{B}_j)=J\mathbf{S}_i\cdot\mathbf{S}_j+\mathbf{B}_i\cdot\mathbf{S}_i+\mathbf{B}_j\cdot\mathbf{S}_j, \tag{1}$$

where $\mathbf{S}_i=\sigma_i/2$ describes the (excess) spin $\frac{1}{2}$ on dot i and J denotes the exchange energy, i.e., the energy gap between the spin singlet and triplet states.[8] This effective Hamiltonian can be derived from a microscopic model for electrons in coupled quantum dots,[16] see also Sec. VI. It is found that J can be changed using a variety of external parameters. Tuning the gate voltage between the coupled dots changes the height of the tunneling barrier and therefore directly alters J. Note that J is exponentially sensitive to barrier changes. Also, applying a magnetic field perpendicular to the 2DEG within which the quantum dots are defined greatly influences the exchange coupling J and can even result in a sign change of J for unscreened Coulomb interaction.[16] Some coupling of

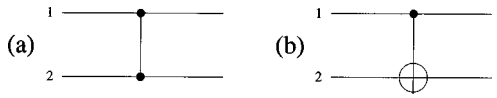

FIG. 2. Circuit notation of two universal gates: (a) The ''square-root-of-swap'' (S) gate, (b) the XOR gate.

the spin $\mathbf{S}_i$ to a local external magnetic field $\mathbf{B}_i$ is also necessary for quantum computation, and has been included in the Hamiltonian Eq. (1). Note that we have included the factor $g_i\mu_B$ in the definition of the magnetic field $\mathbf{B}_i$, where g_i is the g factor for dot i and μ_B is the Bohr magneton. The physical realization of the field gradients or inhomogeneous g factors required for the local magnetic fields is challenging, but there exist several possibilities for generating them.[16,18]

From the Hamiltonian Eq. (1) we can generate the following set of quantum gates:

$$U_i(\boldsymbol{\phi}) = \exp(i\boldsymbol{\phi}\cdot\mathbf{S}_i), \tag{2}$$

$$S \equiv S(i,j) \equiv U_{\text{swap}}^{1/2} = e^{-i\pi/8}\exp\left(i\frac{\pi}{2}\mathbf{S}_i\cdot\mathbf{S}_j\right). \tag{3}$$

The single-qubit operation $U_i(\boldsymbol{\phi})$ for the spin $\mathbf{S}_i$ is generated by applying a magnetic field pulse $\mathbf{B}(t)$ at the location of the spin $\mathbf{S}_i$ such that $\int_0^t d\tau\mathbf{B}(\tau)=\boldsymbol{\phi}$. Similarly, the ''square-root-of-swap'' gate[8] (which we denote by S in the following) is obtained by switching the interaction $J(t)$ between the spins $\mathbf{S}_i$ and $\mathbf{S}_j$ such that $\int_0^t d\tau J(\tau)=\pi/2$. We introduce the circuit notation for S in Fig. 2(a). Note that $U_i(\phi)$ is 4π-periodic in ϕ and 2π-periodic up to a global phase -1, which for our purposes is not important. Equations (2) and (3) are a universal set of gates. Other powers U_{swap}^{α} of the swap gate $U_{\text{swap}}=S^2=e^{-i\pi/4}\exp(i\pi\mathbf{S}_i\cdot\mathbf{S}_j)$: $(|ab\rangle=|a\rangle_i\otimes|b\rangle_j)$,

$$|00\rangle\mapsto|00\rangle,\ |01\rangle\mapsto|10\rangle,\ |10\rangle\mapsto|01\rangle,\ |11\rangle\mapsto|11\rangle, \tag{4}$$

can also be generated by the Hamiltonian Eq. (1), but are not necessary for universality, once $S=U_{\text{swap}}^{1/2}$ is included.

We can use ''square root of swap'' to generate the controlled phase flip gate U_{CPF}:

$$|00\rangle\mapsto|00\rangle, |01\rangle\mapsto|01\rangle, |10\rangle\mapsto|10\rangle, |11\rangle\mapsto-|11\rangle, \tag{5}$$

with the quantum circuit depicted in Fig. 3 (time evolving from the left to the right), or formally,[8]

$$U_{\text{CPF}} = e^{-i(\pi/2)}e^{i(\pi/2)S_1^z}e^{-i(\pi/2)S_2^z}Se^{i\pi S_1^z}S, \tag{6}$$

which in turn is related to the XOR gate U_{XOR} [Fig. 2(b)]:

$$|00\rangle\mapsto|00\rangle,\ |01\rangle\mapsto|01\rangle,\ |10\rangle\mapsto|11\rangle,\ |11\rangle\mapsto|10\rangle, \tag{7}$$

by the basis change

$$U_{\text{XOR}} = VU_{\text{CPF}}V^{\dagger},\qquad V=\exp(-i\pi S_2^y/2). \tag{8}$$

Since XOR with one-bit gates is a universal quantum gate,[4] this confirms that Eqs. (2) and (3) are a universal set of gates. In what follows, we will use the XOR gate to construct the gate E that performs the encoding for three-qubit quantum

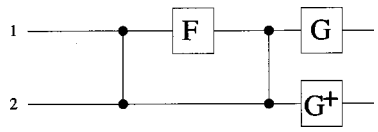

FIG. 3. A circuit representation for the conditional phase flip (CPF), Eq. (5), as given in Eq. (6). The single qubit rotations are $F=e^{i\pi S^z}$ and $G=e^{i(\pi/2)S^z}$. The CPF is related to the XOR gate Eq. (7) by the basis transformation Eq. (8).

error correction, as shown in Fig. 1, and can be obtained by two successive XOR gates [Fig. 4(a)],

$$E = U_{\text{XOR}}(1,3)U_{\text{XOR}}(1,2). \tag{9}$$

It has to be noted that the quantum gate which performs the encoding must only be equal to E in the subspace spanned by the states $|000\rangle$ and $|100\rangle$, because it is always guaranteed that the qubits 2 and 3 are initially in state $|0\rangle$. However, this is not true for the decoding gate which must be equal to E on the entire Hilbert space since it acts on an unknown state.

The very similar quantum gate [Fig. 4(b)]

$$E_T = U_{\text{XOR}}(2,3)U_{\text{XOR}}(1,2) \tag{10}$$

has the nice property that it can be used for implementing the quantum teleportation of one qubit as a quantum computation.[20] It is clear that our analysis of the XOR gate can also be used for implementing this gate.

III. SERIAL PULSE MODE

In the foregoing discussion we made clear why it is desirable to generate certain quantum gates or networks such as XOR, E, and E_T, and that it is indeed possible to produce them using a system of spins that are mutually coupled by the Heisenberg interaction Eq. (1). In fact, we know that we can generate every quantum gate using those interactions, since Eqs. (6) and (8) explicitly tell us how to produce XOR, which together with the set of single-qubit operations forms a universal set of gates for quantum logic.[4,21] We now go one step further and ask ourselves which is the *most efficient* way of implementing a certain quantum gate. More precisely, we are interested in minimizing the switching time τ_s for the desired quantum gate. This kind of optimization is crucial because the error probability per gate operation is proportional to the switching time, $\epsilon=\tau_s/\tau_\phi$, where τ_ϕ denotes the dephasing time of the system. Other criteria for optimization can be added, if, e.g., one kind of elementary task (say, spin-spin interactions) is much harder to perform than another (such as single-qubit rotations), or if the switching of parameters turns out to be difficult.

For the purpose of finding an optimal implementation of quantum gates, we first define which set of elementary op-

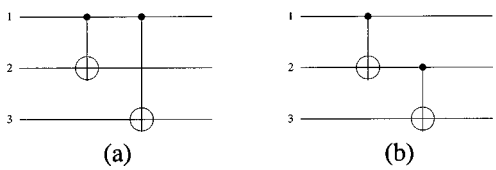

FIG. 4. The quantum circuits for (a) the three-bit encoder E, cf. Eq. (9), and (b) the teleportation encoder E_T, cf. Eq. (10).

erations we are going to use. We will call this set the serial pulse operations, since they can be achieved by ''switching on'' exactly one of the parameters $\vec{p}=(J,\mathbf{B}_1,\mathbf{B}_2)$ in the Hamiltonian Eq. (1) for some finite time. Clearly, XOR does not belong to this class of gate operations—it takes the whole sequence Eq. (6) to produce it. Note that the definition of serial (and later parallel) pulse operations depends on the Hamiltonian and on how we parametrize it. The distinction only makes sense if serial pulse operations correspond to physically switching on and off a part of the device, e.g., the magnetic field at the location of one of the spins. We will use the serial pulse operations defined in Eqs. (2) and (3).

A. XOR gate

As a first example for our efficiency analysis, we take the sequence Eq. (6) for XOR. We do not try to optimize the length of the single-qubit pulses. Instead we investigate whether it really takes two instances of S or if XOR can be performed with one S plus single-qubit operations. This is most reasonable if coupling two qubits is more costly (e.g., due to decoherence) than operating on a single qubit. Thus, our question is whether

$$S_1=[u_{21}\otimes u_{22}]S[u_{11}\otimes u_{12}] \tag{11}$$

is equal to U_{XOR} for some choice of single-qubit gates $u_{nm}=U_m(\phi_{nm})$ or not. We will shortly prove that the answer is negative and it indeed takes at least two S to produce XOR, but first we introduce the method we developed in order to prove this kind of ''no-go'' theorem. The idea is that very often quantum gates can be distinguished by their ability to produce entanglement. This property of quantum gates has the advantage that it is invariant under concatenation with arbitrary single-qubit gates.

We denote the product (pure) states in our two-qubit Hilbert space $\mathcal{H}=\mathcal{H}_2^{\otimes 2}$ by $\mathcal{P}=\{|\Psi\rangle\in\mathcal{H}|\,|\Psi\rangle=|\varphi\rangle\otimes|\chi\rangle;|\varphi\rangle,|\chi\rangle\in\mathcal{H}_2\}$.[22] Here, $\mathcal{H}_2$ denotes the single-qubit Hilbert space with basis $|0\rangle,|1\rangle$. A state $|\Psi\rangle\notin\mathcal{P}$ is called entangled. For every quantum gate (unitary matrix) U acting on $\mathcal{H}$, we define the subset $\mathcal{P}(U)=\{|\Psi\rangle\in\mathcal{P}|\,U|\Psi\rangle\in\mathcal{P}\}\subseteq\mathcal{P}$ of product states which are mapped onto a product state by U. The idea is now simply that two quantum gates U_1 and U_2 which have different $\mathcal{P}$ sets, $\mathcal{P}(U_1)\neq\mathcal{P}(U_2)$, obviously must be different: $U_1\neq U_2$ (note that this implication cannot be reversed). The $\mathcal{P}$ set of XOR is

$$\mathcal{P}(U_{\mathrm{XOR}})=\{|0\phi\rangle,|1\phi\rangle,|\phi\pm\rangle||\phi\rangle\in\mathcal{H}_2\}, \tag{12}$$

where we used the notation $|\pm\rangle=(|0\rangle\pm|1\rangle)/\sqrt{2}$.

In order to find $\mathcal{P}(S)$, it is useful to convince oneself that the ''square root of swap'' operates on a product state $|\phi\chi\rangle$ according to the very intuitive formula

$$S|\phi\chi\rangle=\frac{1}{1+i}(|\phi\chi\rangle+i|\chi\phi\rangle), \tag{13}$$

by first checking it for the basis of products of $|0\rangle$ and $|1\rangle$, and then using that the right-hand side of Eq. (13) is linear in $|\phi\rangle$ and $|\chi\rangle$. From this rule we conclude that all product states become entangled by S unless they are the product of two equal single-qubit states,

$$\mathcal{P}(S)=\{|\Psi\rangle\in\mathcal{P}|\exists\,|\phi\rangle\in\mathcal{H}_2:|\Psi\rangle=|\phi\phi\rangle\}. \tag{14}$$

For any choice of the u_{nm} in Eq. (11), we can construct the state $|0\rangle\otimes u_{12}^{\dagger}u_{11}|1\rangle$ which is in $\mathcal{P}(U_{\mathrm{XOR}})$ but not in $\mathcal{P}(S_1)$ since $S_1|\Psi\rangle$ is entangled. Therefore, $\mathcal{P}(S_1)\neq\mathcal{P}(U_{\mathrm{XOR}})$ and consequently $S_1\neq U_{\mathrm{XOR}}$ for any choice of u_{nm}. Thus, the sequence given in Eq. (6) is optimal in the sense that both ''square root of swap'' operations are really needed. Allowing arbitrary powers of U_{swap} does not reduce the number of two-qubit gates required for XOR either, since one $U_{\mathrm{swap}}^{\alpha}$, where α is not an even multiple of $\frac{1}{2}$, cannot act as a perfect entangler which is required for the XOR gate. For completeness, we give here the generalization of Eqs. (13) and (14) for arbitrary powers of swap,

$$U_{\mathrm{swap}}^{\alpha}|\phi\chi\rangle=e^{-i\pi\alpha/2}\left[\cos\left(\frac{\pi\alpha}{2}\right)|\phi\chi\rangle+i\sin\left(\frac{\pi\alpha}{2}\right)|\chi\phi\rangle\right], \tag{15}$$

$$\mathcal{P}(U_{\mathrm{swap}}^{\alpha})=\begin{cases}\mathcal{P}(S), & \alpha\neq\text{integer},\\ \mathcal{P}, & \alpha=\text{integer}.\end{cases}$$

It is interesting to check whether XOR could be performed with one S gate only if we know that the target qubit is initially in the state $|0\rangle$. If this were the case, one could save two S gates in the encoding step (this is not true for the decoding step). However, one finds that even in the subspace spanned by $|00\rangle$ and $|10\rangle$, the circuit Eq. (11) cannot reproduce an XOR gate, because for any choice of single-qubit rotations, $|00\rangle\in\mathcal{P}(U_{\mathrm{XOR}})$ and/or $|10\rangle\in\mathcal{P}(U_{\mathrm{XOR}})$ become entangled by S_1.

B. Three-bit encoder E

Regarding the three-bit encoder E, Eq. (9), our result tells us that the straightforward implementation of E requires ''square root of swap'' four times, i.e., twice for every XOR. This does not mean that there cannot be a more efficient implementation of E than given in Eq. (9). We can try to implement E using the serial pulse gate set instead of XOR's. It turns out that this is impossible with fewer than four S gates. The analysis still relies on the previously introduced $\mathcal{P}$ set but is slightly more complicated than the one for XOR since in the case of three qubits each gate S can be applied to one of three possible pairs of qubits.

It is clear that just one use of S (plus arbitrary single-qubit operations) cannot produce E,

$$U_1=[u_{21}\otimes u_{22}\otimes u_{23}]S(i,j)[u_{11}\otimes u_{12}\otimes u_{13}]\neq E, \tag{16}$$

for any choice of u_{nm} for the simple reason that E is able to entangle the qubit 1 with 2, and also 1 with 3, whereas $S(i,j)$ can only entangle the qubits i and j with each other (at most one pair).

It is less obvious that none of the sequences

$$U_2=U^{(3)}S(k,l)U^{(2)}S(i,j)U^{(1)} \tag{17}$$

with $U^{(n)}=u_{n1}\otimes u_{n2}\otimes u_{n3}$ can reproduce E. The idea of the following argument is the same as for the one for XOR: We are seeking a state $|\Psi\rangle$ that becomes entangled when acted on with the operator U_2 given in Eq. (17) but remains unentangled under the operation E, i.e., $|\Psi\rangle\in\mathcal{P}(E)\backslash\mathcal{P}(U_2)$. This

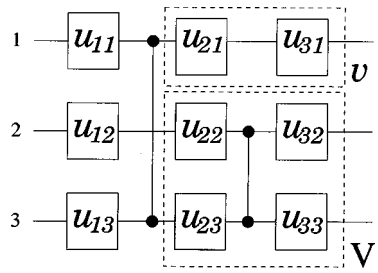

FIG. 5. Quantum circuits of the type described in Eq. (18). Dashed lines represent the grouping in Eq. (19).

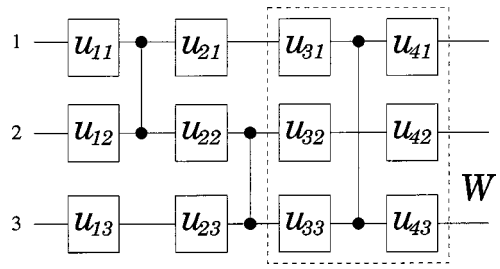

FIG. 6. Quantum circuits of the type described in Eq. (23). Dashed lines represent the grouping in Eq. (24).

is the case if $|\Psi\rangle$ is entangled by $S(i,j)$ and not disentangled by $S(k,l)$. We can exclude the case where $(k,l)=(i,j)$ or $(k,l)=(j,i)$, using the same argument as for U_1, defined in Eq. (16). In the remaining cases it is clear that if $|\Psi\rangle \in \mathcal{P}(E)$ is chosen such that it is entangled by $S(i,j)$, then it will not be disentangled again by $S(k,l)$, and we are done. Since Eq. (17) is invariant when i and j (or k and l) are interchanged, we can always arrange that i, j, and k are mutually different, and $l=i$. In the case where $j\neq 1$, the state $|\Psi\rangle=|0\rangle_i\otimes u_{1j}^{\dagger}u_{1i}|1\rangle_j\otimes|0\rangle_k\in\mathcal{P}(E)$ is not in $\mathcal{P}(U_2)$, because the entanglement between qubit j and the qubits i and k created by $S(i,j)$ cannot be undone by $S(i,k)$. For $j=1$ we choose the state $|\Psi\rangle=u_{1i}^{\dagger}u_{1j}|1\rangle_i\otimes|0\rangle_j\otimes|0\rangle_k\in\mathcal{P}(E)$ with the same property. This concludes our proof that there is no circuit U_2 of the form Eq. (17) which is equal to E. Note that this conclusion is independent of the choice of single-qubit operations in U_2, hence the inequality we proved concerns all circuits of the type U_2.

As an example, consider the circuit

$$U_2=U^{(3)}S(2,3)U^{(2)}S(1,3)U^{(1)}, \tag{18}$$

for which $i=3$, $j=1$, and $k=2$. By rewriting U_2 in the form shown in Fig. 5,

$$U_2=[v\otimes V(2,3)]S(1,3)U^{(1)}, \tag{19}$$

with $v=u_{31}u_{21}$ and $V(2,3)=(1\!\!1\otimes u_{32}\otimes u_{33})S(2,3)(1\!\!1\otimes u_{22}\otimes u_{23})$, and using Eq. (13), we observe that the product state $|\Psi\rangle=|0\rangle_1\otimes|0\rangle_2\otimes u_{13}^{\dagger}u_{11}|1\rangle_3\in\mathcal{P}(E)$ is mapped to

$$U_2|\Psi\rangle=\frac{1}{1+i}(v|\alpha\rangle_1\otimes V|\delta\rangle_{23}+iv|\beta\rangle_1\otimes V|\gamma\rangle_{23}). \tag{20}$$

The unitarity of u_{11} implies that $|\alpha\rangle=u_{11}|0\rangle$ is orthogonal to $|\beta\rangle=u_{11}|1\rangle$, and $|\gamma\rangle=u_{12}|0\rangle\otimes|\alpha\rangle$ is orthogonal to $|\delta\rangle=u_{12}|0\rangle\otimes|\beta\rangle$. The gates v and V are also unitary, thus $v|\alpha\rangle$ is orthogonal to $v|\beta\rangle$ and $V|\gamma\rangle$ is orthogonal to $V|\delta\rangle$, which implies that $U_2|\Psi\rangle$, Eq. (20), is an entangled state between qubuts 1 and the pair of quibits 2 and 3. From this we conclude that $|\Psi\rangle\in\mathcal{P}(E)$ is not in $\mathcal{P}(U_2)$, and therefore $E\neq U_2$.

Next, we develop a proof that even with the use of three S gates, E cannot be implemented. Since each S can couple one of three possible pairs $i_k,j_k=1,\ldots,3$, $i_k\neq j_k$, of qubits, there are $3^3=27$ sequences including three ''square-root-of-swap'' (S) gates, having the form

$$U_3=U^{(4)}S(i_3,j_3)U^{(3)}S(i_2,j_2)U^{(2)}S(i_1,j_1)U^{(1)}, \tag{21}$$

with arbitrary single-qubit gates $U^{(n)}=u_{n1}\otimes u_{n2}\otimes u_{n3}$. First we observe that if $(i_2,j_2)=(i_3,j_3)$ or $(i_2,j_2)=(j_3,i_3)$, then we can apply the same argument as for circuits of the type U_2 with $(i,j)=(i_1,j_1)$ and $(k,l)=(i_2,j_3)$. In the case where the first two S gates (but not the third one) act on the same pair of qubits, $(i_1,j_1)=(i_2,j_2)$ or $(i_1,j_1)=(j_2,i_2)$, we note that either $|0\rangle_{i_1}|0\rangle_{j_1}|0\rangle_k\in\mathcal{P}(E)$ or $|0\rangle_{i_1}|0\rangle_{j_1}|1\rangle_k\in\mathcal{P}(E)$, where $k\neq i_1,j_1$, becomes entangled by U_3. Therefore, $U_3\neq E$ if the first two or the last two S gates operate on the same pair of qubits. In all other cases, we can label the three qubits with three distinct numbers a, b, and c between 1 and 3 such that $S(i_1,j_1)=S(a,b)$, $S(i_2,j_2)=S(a,c)$, and $S(i_3,j_3)=S(b,x)$, with $x=a$ or $x=c$. The state $|\Psi\rangle$, defined as

$$\begin{aligned}&|0\rangle_a\otimes u_{1b}^{\dagger}u_{1a}|0\rangle_b\otimes u_{1c}^{\dagger}u_{2c}^{\dagger}u_{2a}u_{1a}|1\rangle_c \ \ (\text{if } a=1),\\ &u_{1a}^{\dagger}u_{1b}|0\rangle_a\otimes|0\rangle_b\otimes u_{1c}^{\dagger}u_{2c}^{\dagger}u_{2a}u_{1b}|1\rangle_c \ \ (\text{if } b=1),\\ &u_{1a}^{\dagger}u_{2a}^{\dagger}u_{2c}u_{1c}|0\rangle_a\otimes u_{1b}^{\dagger}u_{2a}^{\dagger}u_{2c}u_{1c}|0\rangle_b\otimes|1\rangle_c \ \ (\text{if } c=1),\end{aligned} \tag{22}$$

is chosen such that $|\Psi\rangle\in\mathcal{P}(E)$ and has the property that $S(a,b)U^{(1)}|\Psi\rangle$ is unentangled, but in $S(a,c)U^{(2)}S(a,b)U^{(1)}|\Psi\rangle$ there is entanglement between the qubits a and c. Finally, the $S(b,x)$ gate cannot remove the entanglement; in the final state $U_3|\Psi\rangle$, either the qubit a (if $x=c$) or the qubit c (if $x=a$) is entangled with the other two qubits, thus $|\Psi\rangle\notin\mathcal{P}(U_3)$. Since $|\Psi\rangle\in\mathcal{P}(E)$, this concludes our proof of the statement $U_3\neq E$. In order to illustrate our proof, we apply it to the specific example ($a=2$, $b=1$, $c=3$, $x=c=3$)

$$U_3=U^{(4)}S(1,3)U^{(3)}S(2,3)U^{(2)}S(1,2)U^{(1)}, \tag{23}$$

which can be written in the form (shown in Fig. 6)

$$WS(2,3)U^{(2)}S(1,2)U^{(1)}, \tag{24}$$

where W is a gate that does not couple qubit 2 with any other qubit. Applying this operator to the state $|\Psi\rangle=|0\rangle_1\otimes u_{12}^{\dagger}u_{11}|0\rangle_2\otimes u_{13}^{\dagger}u_{23}^{\dagger}u_{22}u_{11}|1\rangle_3$ proves that $U_3\neq E$ for any choice of the $U^{(n)}$, because $U_3|\Psi\rangle$ is entangled, $|\Psi\rangle\notin\mathcal{P}(U_3)$.

Strictly speaking, the gate which is used for encoding the qubit has to be equal to E only in the subspace spanned by $|000\rangle$ and $|100\rangle$, since it is guaranteed that the qubits 2 and 3 are prepared in the $|0\rangle$ state initially (note that this is not the case for the decoding step since the error syndrome is unknown when the state is decoded). This could in principle allow a more optimal implementation of the encoder circuit

than the one which we have described above. However, we find that $|000\rangle \in \mathcal{P}(E)$ and/or $|100\rangle \in \mathcal{P}(E)$ become entangled by any (nontrivial) circuit with three or fewer S gates. This statement is proven by exhausting all possible cases. It implies that even the encoding step requires at least four S gates.

C. Teleportation encoder E_T

Now we consider the teleportation encoder gate E_T, Eq. (10), which is shown in Fig. 4(b). The gate E_T consists of two XOR gates, but in contrast to E these two XORs are arranged in a less symmetric way. As a consequence, $\mathcal{P}(E_T)$ is only a subset of (and not equal to) $\mathcal{P}(E)$, since, e.g., $|0+0\rangle$ is in $\mathcal{P}(E)$ but not in $\mathcal{P}(E_T)$. Again, we can ask whether it is feasible to assemble E_T using fewer than the four S gates that are used when we simply combine Eqs. (6), (8), and (10). The answer is again negative. The proof of this statement is similar to the one given for E. It is again clear that a circuit involving one S cannot entangle any pair of the three qubits, as it should in order to reproduce E_T.

A circuit of the form U_2, Eq. (17), involving two S gates cannot be equal to E_T either. We first note that if $S(i,j)=S(k,l)$, then U_2 cannot produce entanglement between the third qubit $m \neq i,j$ and i or j, and thus $U_2 \neq E_T$, because E_T can entangle any pair of qubits. If $S(i,j) \neq S(k,l)$, we find that either $|\Psi\rangle = |0\rangle_i|0\rangle_j|0\rangle_k \in \mathcal{P}(E_T)$ or $|\Psi\rangle = |1\rangle_i|0\rangle_j|0\rangle_k \in \mathcal{P}(E_T)$, where $k \neq i,j$, is entangled by the gate $S(i,j)$. Since this entanglement cannot be undone by $S(k,l) \neq S(i,j)$, the state $U_2|\Psi\rangle$ is entangled. Thus, we have found a state which is in $\mathcal{P}(E_T)$ and not in $\mathcal{P}(U_2)$ and therefore $U_2 \neq E_T$.

We finally explore whether a circuit U_3 containing three S gates as in Eq. (21) can reproduce E_T. For $S(i_2,j_2)=S(i_3,j_3)$ we can see that this is not the case by applying the same argument as above for a circuit with two S. In the opposite case, $S(i_2,j_2) \neq S(i_3,j_3)$, either the state $|0\rangle_{i_1}|0\rangle_{j_1}|0\rangle_k \in \mathcal{P}(E_T)$ or the state $|0\rangle_{i_1}|0\rangle_{j_1}|1\rangle_k \in \mathcal{P}(E_T)$, with $k \neq i_1, j_1$, is entangled by $S(i_2,j_2)$ or $S(i_3,j_3)$. Because $S(i_3,j_3) \neq S(i_2,j_2)$, entanglement produced by $S(i_2,j_2)$ is not undone by $S(i_3,j_3)$ and therefore we have found a state in $\mathcal{P}(E_T)$ which is not in $\mathcal{P}(U_3)$, completing the proof for $U_3 \neq E_T$ for the case of three S gates. This finally implies that, like E, the teleportation encoder E_T cannot be constructed using fewer than four S gates.

D. Numerical search

The method that was presented for proving inequalities between two gates U_1 and U_2 involving the sets $\mathcal{P}(U_1)$ and $\mathcal{P}(U_2)$ has the advantage that it yields rigorous results although we do not know the details about the involved single-qubit operations. Sometimes, however, proofs become lengthy and rather unsystematic, so we would like to have a better tool for the complex cases. Unfortunately, we do not have such a tool which is capable of giving rigorous proofs for inequalities, like the $\mathcal{P}$-set method. However, we have developed a computer algorithm that searches for the M qubit gate U_g in the set

$$U\{U^{(n)}\} = U^{(N+1)} X_N U^{(N)} \cdots X_2 U^{(2)} X_1 U^{(1)}, \qquad (25)$$

where the X_n are arbitrary but fixed 2,3, . . . ,M qubit gates and $U^{(n)} = u_{n1} \otimes \cdots \otimes u_{nM}$ are arbitrary and variable products of single-qubit gates (several u_{nk} can be unity). A result of a numerical search is a list $\{u_{nk}\}$ of single-qubit gates, which satisfy the equation $U\{U^{(n)}\} = U_g$. The computer algorithm can therefore (in the case of a successful run) ''prove'' equalities, but one or several unsuccessful runs do not constitute a proof that the gate U_g cannot be constructed with a given sequence X_n, $n=1,\ldots,N$. Note that the situation is thus exactly opposite to the $\mathcal{P}$-set method. The operation of the computer algorithm consists of minimizing the function

$$f(\{u_{nk}\},\alpha) = \| e^{i\alpha} U\{u_{nk}\} - U_g \|^2 \qquad (26)$$

numerically in the space of all possible combinations of single-qubit gates u_{nk}, where the matrix norm is given by $\|A\|^2 = \mathrm{Tr}(A^\dagger A)$. The single-qubit gates u_{nk} are parametrized by the three angles φ_{nk}, θ_{nk}, and ψ_{nk} according to the prescription

$$u_{nk} = \begin{pmatrix} \cos(\theta_{nk}) & -e^{i(\varphi_{nk}+\psi_{nk})} \sin(\theta_{nk}) \\ e^{i\varphi_{nk}} \sin(\theta_{nk}) & e^{i\psi_{nk}} \cos(\theta_{nk}) \end{pmatrix}. \qquad (27)$$

Including the global phase α, we count $3M(N+1)+1$ real parameters. If the numerical search yields a minimum

$$f(\{u_{nk}\},\alpha) = 0, \qquad (28)$$

then the corresponding sequence Eq. (25) is identical to U_g.

The numerical results for $U_g = U_{\mathrm{XOR}}$ and $X_n = S$ support the analytical result, i.e., there is no circuit for $N=1$. For $N=2$, we find a vast number of circuits other than Eq. (6) combined with Eq. (8). For $U_g = E, E_T$, we do not find a solution for $N<4$, as guaranteed by the result of our previous analysis. As previously remarked, the gate for the encoding must be equal to E only in the subspace spanned by $|000\rangle$ and $|100\rangle$ (the gate for decoding has to be equal to E on the entire three-qubit Hilbert space). A numerical search with this relaxed constraint was performed by minimizing the function $\tilde{f}(\{u_{nk},\alpha\}) = ||(e^{i\alpha}U\{u_{nk}\} - E)P||^2$, where $P = |000\rangle\langle 000| + |100\rangle\langle 100|$ denotes the projector onto the relevant subspace. The numerical analysis confirmed our earlier formal result that $UP \neq EP$ if U involves fewer than four S gates.

The impossibility of reducing the number of S gates required for E led us to the idea that it might be useful to replace S by a three-qubit gate which is directly generated by the three-qubit Hamiltonian $H_3 = J(\mathbf{S}_1 \cdot \mathbf{S}_2 + \mathbf{S}_2 \cdot \mathbf{S}_3 + \mathbf{S}_3 \cdot \mathbf{S}_1)$, describing three simultaneously interacting spins with equal coupling constant J. We find that the analog of S for three spins is the gate

$$S_3 = e^{-i\pi/3} \exp\left(i \frac{4\pi}{9} \frac{H_3}{J} \right), \qquad (29)$$

which is obtained when the interaction J is switched on for time $\tau = 4\hbar\pi/9J$. In analogy to Eq. (13), we can express the action of S_3 on product states as

$$S_3|\alpha_1\alpha_2\alpha_3\rangle = -e^{i\pi/3}|\alpha_1\alpha_2\alpha_3\rangle + \frac{e^{i\pi/6}}{2\sqrt{3}}\sum_{\sigma\in\mathcal{S}_3}|\alpha_{\sigma 1}\alpha_{\sigma 2}\alpha_{\sigma 3}\rangle, \tag{30}$$

where the second term is the symmetrization of the input state ($\mathcal{S}_3$ denotes the permutation group of three objects). Whereas $S^4=1$, we find that $S_3^3=-1$. In exact analogy to the ''square-root-of-swap'' gate, $\mathcal{P}(S_3)$ consists of states that have the form $|\alpha\rangle\otimes|\alpha\rangle\otimes|\alpha\rangle$, $|\alpha\rangle\in\mathcal{H}_2$. We can show that E is not equal to any gate involving only one or two S_3. The case of three S_3 was studied numerically, but no circuit representation for E was found.

IV. PARALLEL PULSE MODE

Operating a system described by the Hamiltonian $H(\vec{p})$ with parameters $\vec{p}=(J,\mathbf{B}_1,\mathbf{B}_2)$ given in Eq. (1) as a quantum gate in the serial pulse mode is not optimal in the following sense: If several or all parameters $\vec{p}$ can be changed simultaneously, we expect that a given quantum gate, say XOR, can be performed faster than by changing only one parameter at a time as in the serial pulse mode. Generally, all parameters $\vec{p}$ are arbitrary functions of time such that the time evolution operator after time t is a functional in $\vec{p}$ given by the time-ordered exponential

$$U_t[\vec{p}(\tau)]=T\exp\left(\frac{i}{\hbar}\int_0^t H(\vec{p}(\tau))\,d\tau\right). \tag{31}$$

Given some quantum gate U_g, we would now like to solve the integral equation $U_t[\vec{p}(\tau)]=U_g$ for the functions $\vec{p}(\tau)$. For unrestricted time t and unbounded functions $\vec{p}(\tau)$ we immediately know how to construct such a solution by using the known universal set of gates Eqs. (2) and (3) in the serial pulse mode. In general, this is not the optimal solution of $U_t[\vec{p}(\tau)]=U_g$. An optimal solution is given by a set of bounded functions $|p_i(\tau)|<M_i$ requiring minimal time t for a fixed set of bounds M_i. Since it is not feasible to find an optimal solution among all such bounded functions, we will restrict ourselves to piecewise-constant functions. Splitting up the time interval t into $N\geqslant 1$ parts, we write

$$\begin{aligned} U_N(\vec{p}^{\,(1)},\ldots,\vec{p}^{\,(N)};\phi) &= e^{i\phi}U_N(\vec{p}^{\,(N)})\cdots U_2(\vec{p}^{\,(2)})U_1(\vec{p}^{\,(1)}), \\ U_k(\vec{p}^{\,(k)}) &= \exp\{2\pi i H(\vec{p}^{\,(k)})\}. \end{aligned} \tag{32}$$

For every time ''slice,'' we have the freedom to choose a new set of parameters $\vec{p}^{\,(k)}=(\mathbf{J}^{(k)},\mathbf{B}_1{}^{(k)},\mathbf{B}_2{}^{(k)})$. Note that we allow for an arbitrary total phase ϕ. By discretizing the problem in this way we have reduced the free parameters in the problem from the P functions $p_i(t)$ to PN real parameters $p_i^{(k)}$, $i=1,\ldots,P$, $k=1,\ldots,N$, where P denotes the number of parameters $\vec{p}$ [in the case of the Heisenberg Hamiltonian Eq. (1), $P=7$]. The functions $p_i(t)$ are related to the discrete parameters $p_i^{(k)}$ through the relation

$$p_i(t)=\frac{2\pi\hbar}{\tau_k}p_i^{(k)},\quad t_{k-1}\leqslant t<t_k, \tag{33}$$

where $\tau_k=t_k-t_{k-1}$ and $t_0=0$, $t_N=t$; the time step τ_k has been absorbed into the dimensionless parameters $p_i^{(k)}$. Once the problem is discretized, it becomes suitable for numerical treatment using the minimizer algorithm presented in Sec. III, minimizing the function $\|U_g-U_N\{p_i^{(k)};\phi\}\|^2$ with respect to the $PN+1$ parameters $p_i^{(k)}$ and ϕ. We try to find a solution to $U_N\{p_i^{(k)};\phi\}=U_g$ starting from $N=1$ and then increasing N in unit steps. In practice, N is limited by the available computational resources.

One approach to the problem would then be to fix N and t_i (e.g., use time steps of equal size, $\tau_k=\tau=t/N$). Then, the constraint $|p_i(\tau)|<M_i$ implies $|p_i^{(k)}|<\tau_k M_i/2\pi\hbar$. In the following, however, we solve $U_N\{p_i^{(k)};\phi\}=U_g$ with fixed N (chosen as small as possible) without any constraint for $p_i^{(k)}$ and then calculate t for given bounds M_i using the formula [cf. Eq. (33)]

$$t=\sum_{k=1}^{N}\tau_k=\sum_{k=1}^{N}\max_i\left(\frac{2\pi\hbar}{M_i}|p_i^{(k)}|\right). \tag{34}$$

The parameter $p_i^{(k)}$ with the largest $p_i^{(k)}/M_i$ ratio determines the switching time for the kth step.

A. XOR gate

We now want to use this method for finding a pulse sequence $\vec{p}^{\,(k)}$ that generates the quantum XOR gate, Eq. (7). Since XOR is the same as the conditional phase flip (CPF) up to the basis change Eq. (8), we will first try to generate CPF. In the S_z basis, the Heisenberg Hamiltonian $H(J,\mathbf{B}_1,\mathbf{B}_2)$, Eq. (1), can be written in the following matrix form:

$$\frac{1}{2}\begin{pmatrix} B_1^z+B_2^z & B_2^x-iB_2^y & B_1^x-iB_1^y & 0 \\ B_2^x+iB_2^y & B_1^z-B_2^z-J & J & B_1^x-iB_1^y \\ B_1^x+iB_1^y & J & B_2^z-B_1^z-J & B_2^x-iB_2^y \\ 0 & B_1^x+iB_1^y & B_2^x+iB_2^y & -B_1^z-B_2^z \end{pmatrix}, \tag{35}$$

where an irrelevant constant energy contribution is omitted. We find analytically that CPF can be obtained in one time step ($N=1$), i.e. for constant parameters $\vec{p}$,

$$\begin{aligned} U_{\mathrm{CPF}} &= \exp[2\pi i H(J,\mathbf{B}_1,\mathbf{B}_2)], \\ J &= k-n-2m-\tfrac{1}{2}, \\ \mathbf{B}_1 &= \tfrac{1}{2}(0,0,n+\tfrac{1}{2}+\sqrt{k^2-J^2}), \\ \mathbf{B}_2 &= \tfrac{1}{2}(0,0,n+\tfrac{1}{2}-\sqrt{k^2-J^2}), \\ \phi &= -\pi(n+\tfrac{1}{2}), \end{aligned} \tag{36}$$

where n and m are arbitrary integers and k is an integer satisfying $2|k|\geqslant|n+2m+\frac{1}{2}|$. This solution is obtained by setting $B_i^x=B_i^z=0$ and diagonalizing the resulting Hamiltonian matrix

$$H=\frac{1}{2}\begin{pmatrix} A & 0 & 0 & 0 \\ 0 & -J+B & J & 0 \\ 0 & J & -J-B & 0 \\ 0 & 0 & 0 & -A \end{pmatrix}, \tag{37}$$

where $A=B_1^z+B_2^z$ and $B=B_1^z-B_2^z$. The conditional phase flip CPF is invariant under the basis change that diagonalizes Eq. (37), and we can then solve the equation $\exp(i\phi)\exp(2\pi iH)=U_{\mathrm{CPF}}$ in the basis where both H and U_{CPF} are diagonal. This yields the four equations $e^{\pi iA}=e^{2\pi i\lambda_+}=e^{2\pi i\lambda_-}=-e^{-\pi iA}=e^{-i\phi}$, where $\lambda_\pm=(-J\pm\sqrt{J^2+B^2})/2$ and $\pm A/2$ are the eigenvalues of H. From these four equations we obtain the result Eq. (36) for ϕ, $A=B_1^z+B_2^z$, $B=B_1^z-B_2^z$, and J. Applying the basis change V from Eq. (8) to these solutions, we can build XOR with a total of $N=3$ steps. The integers k, m, and n can be chosen such that the switching time Eq. (34) is minimal for a given set of constraints M_J, M_{B_1}, M_{B_2}. In the specific case where all constraints are equal to M, we find that the solution for $k=1$, $m=n=0$,

$$J=\tfrac{1}{2},\quad B_1^z=\tfrac{1}{4}(1+\sqrt{3}),\quad B_2^z=\tfrac{1}{4}(1-\sqrt{3}), \tag{38}$$

has the shortest switching time,

$$t_{\mathrm{CPF},p}=\frac{2\pi\hbar}{4M}(1+\sqrt{3})=0.683\frac{2\pi\hbar}{M}, \tag{39}$$

less than half the time which is used for the serial pulse quantum circuit Eq. (6), $t_{\mathrm{CPF},s}=1.5\times 2\pi\hbar/M$. Note that since the coupling is isotropic, the same gate (in a rotated basis) can be achieved with a magnetic field along any desired direction. In order to obtain the XOR gate, we must spend in addition twice the time $0.25\times 2\pi\hbar/M$ for the basis change V, Eq. (8). The total switching time is then

$$t_{\mathrm{XOR},p}=\frac{2\pi\hbar}{4M}(3+\sqrt{3})=1.183\frac{2\pi\hbar}{M}, \tag{40}$$

about 59% of the time required for the serial pulse quantum circuit, Eq. (6), including the change of basis Eq. (8), $t_{\mathrm{XOR},s}=2\times 2\pi\hbar/M$. Of course, the basis change applied here is again a ''serial pulse'' action and therefore not optimal. We therefore study Eq. (32) directly for the XOR gate, without using the CPF gate. It turns out that no solution exists for $N=1$. For $N=2$ our optimizer algorithm finds the numerical solution

$$U_{\mathrm{XOR}}=e^{i\phi}\exp[2\pi iH(\vec{p}^{\,(2)})]\exp[2\pi iH(\vec{p}^{\,(1)})], \tag{41}$$

with the parameter values[23]

k	$J^{(k)}$	$B_{1x}^{(k)}$	$B_{2x}^{(k)}$	$B_{1y}^{(k)}$	$B_{2y}^{(k)}$	$B_{1z}^{(k)}$	$B_{2z}^{(k)}$
1	0.187	−0.025	**0.464**	0.205	0.195	−0.420	0.395
2	**0.617**	−0.220	0.345	−0.384	0.244	0.353	0.108

(42)

and the global phase $\phi=-0.8481\pi$. The total switching time for equal bounds is in this case $t_{\mathrm{XOR},p}=(0.4643+0.6170)2\pi\hbar/M=1.0813\times 2\pi\hbar/M$, compared to $t_{\mathrm{XOR},s}=2\times 2\pi\hbar/M$ for the serial switching. The numbers in boldface in Eq. (42) indicate which parameter limits the switching time in each step. The solution Eq. (42) appears to be a unique optimum for the case $N=2$.

B. Three-bit encoder E

We can further parallelize the three-bit encoder E, Eq. (9). Instead of concatenating two XOR gates (which may or may not be produced using parallel pulses), we now try to find a more efficient parallel pulse sequence for E, given a system of three qubits which exhibit pairwise couplings among each other that can all be switched on simultaneously. The Hamiltonian for this three-spin system can be written as

$$H=\sum_{1\leq i<j\leq 3}J_{ij}\mathbf{S}_i\cdot\mathbf{S}_j+\sum_{i=1}^{3}\mathbf{B}_i\cdot\mathbf{S}_i. \tag{43}$$

We find that there is a representation of the three-bit error correction encoder E which consists of three parallel pulses only, instead of the four which it takes to perform two sequential XOR gates. The following parallel pulse sequence produces E up to a global phase $\phi=\pi/2$:

k	$J_{12}^{(k)}$	$J_{23}^{(k)}$	$J_{13}^{(k)}$	$B_{1x}^{(k)}$	$B_{2x}^{(k)}$	$B_{3x}^{(k)}$
1	0.0000	**8.2500**	0.0000	1.1153	6.1737	6.1739
2	−0.9256	−5.3608	0.7863	**5.7603**	5.2422	1.7475
3	0.0000	−1.7500	0.0000	0.4345	**3.5255**	**3.5255**
k	$B_{1y}^{(k)}$	$B_{2y}^{(k)}$	$B_{3y}^{(k)}$	$B_{1z}^{(k)}$	$B_{2z}^{(k)}$	$B_{3z}^{(k)}$
1	−1.6737	−0.2263	0.2262	1.1153	1.4649	−1.4649
2	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
3	2.1709	1.4118	1.4118	0.4345	1.2560	1.2560

(44)

For equal bounds the total switching time of $t_{E,p}=17.54\times 2\pi\hbar/M$ is much larger than the four-pulse time $2t_{\mathrm{XOR},p}=2.163\times 2\pi\hbar/M$. Note that a better three-pulse solution was not found, but cannot be excluded.

V. ANISOTROPIC SYSTEMS

Systems where the spin-spin coupling is anisotropic are not described by the Heisenberg Hamiltonian Eq. (1) that we studied as a generator for quantum gates in the previous sections. In the two most notable cases, the Ising and the XY systems, it is known that universal quantum computation is possible. In the case of a system described by the Ising Hamiltonian $H_I=JS_1^zS_2^z$ and a homogeneous magnetic field in the z direction, there is a particularly simple realization of the CPF gate with constant parameters, namely $U_{\mathrm{CPF}}=\exp[i\pi(1-2S_1^z-2S_2^z+4S_1^zS_2^z)/4]$.[8] One might be tempted by this to ''transform'' the Heisenberg interaction Eq. (1) into an Ising interaction by adding time-dependent fields $H_0(t)=\mathbf{B}_1(t)\cdot\mathbf{S}_1+\mathbf{B}_2(t)\cdot\mathbf{S}_2$ to the coupling Hamiltonian $V(t)=J(t)\mathbf{S}_1\cdot\mathbf{S}_2$ such that the coupling in the interaction picture, $V_I(t)=U(t)V(t)U(t)^\dagger$, with $U(t)=T\exp(i\int_0^t H_0(\tau)d\tau)$, would be identical to the Ising coupling $V_I(t)=H_I$, or even to switch the coupling off and on using this method, i.e., $V_I(t)=0$ for a certain choice of $H_0(t)$. It turns out that this is impossible, since the ''transformed'' coupling must have the form

$$V_I(t)=J(t)\mathbf{S}_1\cdot[R(t)\mathbf{S}_2], \tag{45}$$

where $R(t)$ is a time-dependent rotation matrix. For $J\neq 0$, this clearly excludes the complete ''switching off'' of the interaction. Furthermore, the coupling Eq. (45) is still isotropic at every instant t.

In spite of the impossibility of using a Heisenberg system as an effective XY (or Ising) system by adding time-dependent fields, there are XY systems in nature which have been proposed for quantum computation.[19] In the case of Ising systems we have seen above that there is a very simple prescription for generating the XOR gate. We devote the rest of this section to demonstrating that XOR can also be obtained with XY coupling. For two spins with $s=\frac{1}{2}$, the XY Hamiltonian is given by

$$H_{XY}=J(S_1^xS_2^x+S_1^yS_2^y)=\frac{J}{2}\begin{pmatrix}0&0&0&0\\0&0&1&0\\0&1&0&0\\0&0&0&0\end{pmatrix}, \tag{46}$$

where for the matrix representation we chose the S^z basis. The corresponding time evolution operator is

$$U_{XY}(\phi=Jt)=\exp(itH_{XY})=\begin{pmatrix}1&&&\\&e^{i\phi S^x}&&\\&&&1\end{pmatrix}. \tag{47}$$

There is a qualitative difference between two qubits coupled via an XY and those coupled by a Heisenberg interaction: it is impossible to generate powers $U_{\rm swap}^{\alpha}$ $(0<\alpha<1)$ of the swap gate Eq. (4) with only one use of $U_{XY}(\phi)$ together with single-qubit operations. In particular, this is impossible for the ''square-root-of-swap'' gate $U_{\rm swap}^{1/2}$. In spite of this, we found that the CPF gate can be produced by the serial-pulse sequence

$$U_{\rm CPF}=e^{i\pi/4}e^{2i\pi\mathbf{n}_1\cdot\mathbf{S}_1/3}e^{2i\pi\mathbf{n}_2\cdot\mathbf{S}_2/3}\times U_{XY}(\pi/2)e^{i\pi S_1^y}U_{XY}(\pi/2)e^{-i\pi S_1^x/2}e^{-i\pi S_2^x/2}, \tag{48}$$

where $\mathbf{n}_1=(1,-1,1)/\sqrt{3}$ and $\mathbf{n}_2=(1,1,-1)/\sqrt{3}$. This is proof that XY systems with single-qubit interactions are in principle capable of universal quantum computation.

We now consider parallel switching with the XY dynamics,

$$H_{XY,B}=H_{XY}+\mathbf{B}_1\cdot\mathbf{S}_1+\mathbf{B}_2\cdot\mathbf{S}_2, \tag{49}$$

$$U_{XY,B}(t)=\exp(itH_{XY,B}). \tag{50}$$

As in the case of Heisenberg interactions, we first consider the CPF gate which can be used to assemble the XOR gate as shown in Eq. (8). We have not found a possibility to generate the CPF gate Eq. (5) with the XY Hamiltonian with applied magnetic fields with constant parameters $(N=1)$ using a numerical search.[24] If the switching is performed in two steps $(N=2)$, we find numerically that there are several possibilities to generate $U_{\rm CPF}$ in the form

$$U_{\rm CPF}=e^{i\phi}U_2U_1, \tag{51}$$

where $U_k=\exp[2\pi iH_{XY,B}(J^{(k)},B_x^{(k)},B_z^{(k)})]$, $k=1,2$. Note that all magnetic fields can be chosen homogeneous $(\mathbf{B}_1^{(k)}=\mathbf{B}_2^{(k)}\equiv\mathbf{B}^{(k)})$ and perpendicular to the y axis $(B_y=0)$. Here we give one possible realization which is found numerically $(\phi=-3\pi/4)$:

k	$J^{(k)}$	$B_x^{(k)}$	$B_z^{(k)}$
1	0.7500	**0.7906**	0.5728
2	**0.5000**	0.0000	0.2500

(52)

The total switching time for CPF, assuming equal bounds $M_J=M_B\equiv M$ for J and B, is $t_{{\rm CPF},p}^{XY}=1.291\times 2\pi\hbar/M$, compared to $t_{{\rm CPF},s}^{XY}=2.167\times 2\pi\hbar/M$ for the serial-pulse sequence defined in Eq. (48).

In order to produce the XOR gate Eq. (7) we can implement the basis change Eq. (8) using the single-qubit rotation V. This procedure requires a total of four steps for the XOR gate. Another way of achieving XOR is the following sequence which we found numerically and which takes only three steps:

$$U_{\rm XOR}=\exp(3i\pi/4)U_3U_2U_1, \tag{53}$$

with the following parameters:

k	$J^{(k)}$	$B_{1x}^{(k)}$	$B_{2x}^{(k)}$	$B_{1y}^{(k)}$	$B_{2y}^{(k)}$	$B_{1z}^{(k)}$	$B_{2z}^{(k)}$
1	1.802	0.615	**2.045**	0.020	0.316	0.794	0.130
2	**3.344**	0.348	0.718	0.259	0.493	1.583	1.062
3	**1.903**	1.193	0.705	0.413	−0.305	0.589	0.604

(54)

The total switching time of $t_{{\rm XOR},p}^{XY}=7.29\times 2\pi\hbar/M$ (compared to $2.67\times 2\pi\hbar/M$ using CPF and a basis change) indicates that Eq. (54) is not an optimal solution.

VI. REQUIREMENTS FOR PARALLEL SWITCHING

The parallel switching mechanism presented in the Secs. IV and V relies on the following essential assumptions.

(a) Each of the parameters in the Hamiltonian can be varied independently. That is, the coupling can be varied independent of the magnetic fields in the Hamiltonian Eq. (1).

(b) We know the exact relation between the externally controlled parameters (such as the electric and magnetic field or a gate voltage) and the parameters in the Hamiltonian.

(c) The switching is synchronous, with all parameters p_i varying with the same time profile $p_i(t)=\tilde{p}_if(t)$. The change of parameters does not have to be steplike, but can be chosen to have some smooth pulse form. Also, any pulse magnitudes $\tilde{p}_i$ are allowed.

Whether the above requirements can be fulfilled depends on the underlying microscopic mechanisms which are responsible for the effective Hamiltonian, such as the Heisenberg Hamiltonian, Eq. (1). In our previous work[16] we have used the model Hamiltonian

$$H=\frac{1}{2m}\sum_{i=1,2}\left[\left(\mathbf{p}_i-\frac{e}{c}\mathbf{A}(\mathbf{r}_i)\right)^2+ex_iE+\frac{m\omega_0^2}{2}\left(\frac{1}{4a^2}(x_i^2-a^2)^2+y_i^2\right)\right]+\frac{e^2}{\kappa|\mathbf{r}_1-\mathbf{r}_2|}, \quad (55)$$

with $\mathbf{A}(\mathbf{r})=B(-y,x,0)/2$ to describe the orbital dynamics of electrons in coupled quantum dots. Here, $\mathbf{r}_i$ and $\mathbf{p}_i$ denote the location and momentum of the electron i which is moving in two dimensions in a double-well potential V with characteristic energy $\hbar\omega_0$ and a magnetic field B perpendicular to the 2D electron system and an electric field E parallel to the coupling axis of the two wells. The distance between the quantum dots is denoted by $2a$, the effective mass and the charge of the electron by m and e, and the dielectric constant of the material by κ. As we pointed out earlier,[16] the spin-orbit interaction $H_{so}=(\omega_0^2/2m_0c^2)\mathbf{S}\cdot\mathbf{L}$ is very small for an electron in a parabolically confined quantum dot. Note, however, that this expression for the spin-orbit coupling contains the bare electron mass m_0, instead of m, the effective electron mass,[25] and therefore the spin-orbit coupling in GaAs is about $m_0/m\simeq 15$ times smaller than estimated in Ref. 16. For a quantum dot with confining energy $\hbar\omega_0=3$ meV, we obtain $H_{so}/\hbar\omega_0\approx 10^{-8}$.

Concerning condition (a), we have found that the spin-spin coupling J can be controlled by several external ''knobs.'' The gate voltage V applied between the coupled quantum dots controls the height of the barrier for tunneling of an electron from one dot into the other and therefore strongly influences the exchange coupling J between the electronic spins. In a similar manner, J depends on the inter-dot distance $2a$. We have also found[16] that an external magnetic field B perpendicular to the 2DEG causes a strong change (even a sign reversal) of J. Not surprisingly, an electric field E applied along the coupling direction of the dots also changes the exchange coupling, which can be understood as an effect of level detuning. When switching on a magnetic field, the effect of the field on J could be compensated by changing another independent control parameter, e.g., the electric field. In practice, one has to know the functional dependence $J(V,a,B,E)$ in the range where it is used, see also (b).

While a magnetic field perpendicular to the 2DEG strongly influences the exchange J, we can argue that sufficiently weak in-plane magnetic fields have little influence on J. Classically, the motion of a particle in a plane is not affected by a magnetic field in the plane, since the Lorentz force is orthogonal to the plane. Quantum mechanically, we can describe a particle in a magnetic field confined to a plane by the Hamiltonian

$$H=\frac{1}{2m}\left(\mathbf{p}-\frac{e}{c}\mathbf{A}\right)^2+\frac{m\omega^2}{2}z^2, \quad (56)$$

where the vector potential $\mathbf{A}=B(0,-z,0)$ corresponds to a magnetic field of magnitude B along the x axis and the confinement in the z direction is modeled by a harmonic potential with frequency ω. In this gauge, the Hamiltonian can be rewritten in the form

$$H=\frac{p_x^2+p_z^2}{2m}+\frac{p_y^2}{2\bar{m}}+\frac{m\bar{\omega}^2}{2}(z-z_0)^2, \quad (57)$$

with the renormalized effective mass in the y direction, $\bar{m}=m(1+4\omega_L^2/\omega^2)$, the renormalized confining energy $\hbar\bar{\omega}=\hbar\omega\sqrt{1+4\omega_L^2/\omega^2}$, and a shift in the confining potential $z_0=2p_y\omega_L/m\bar{\omega}^2$ which depends on the momentum p_y in the y direction and the Larmor frequency $\omega_L=eB/2mc$. Note that the corrections due to the magnetic field in the resulting 2D Hamiltonian

$$H_{2D}=\frac{p_x^2}{2m}+\frac{p_y^2}{2\bar{m}} \quad (58)$$

are of the order ω_L^2/ω^2 or $(a_z/l_B)^4$, where $l_B=\sqrt{\hbar c/eB}$ denotes the magnetic length and $a_z=\sqrt{\hbar/m\omega}$ the confinement length. Usually, we are interested in the case of strong confinement and moderate magnetic fields where $a_z\ll l_B$, therefore $\bar{m}\approx m$ up to small corrections. In this case, an in-plane magnetic field does not affect the orbital degrees of freedom of the 2D electrons.

The condition (b) can be fulfilled in two ways. Either we have a theoretical description of the dependence of the Hamiltonian parameters $(J,\mathbf{B}_i)$ on the control parameters (V, a, B, E) or this relation is first mapped out in experiment and the obtained data are used later for the control of the device. A good approximate description is possible in the case of adiabatic switching. In order to demonstrate this, we cast the microscopic Hamiltonian into the form $H(t)=H_0+V(t)$. Then we find the instantaneous eigenstates $|n(t)\rangle$ and the corresponding instantaneous eigenvalues $\epsilon_n(t)$ by solving the time-independent Schrödinger equation for fixed time t. The instantaneous eigenstate $|n(t)\rangle$ is a good approximation for the time evolution of the initial state $|n(0)\rangle$, provided the adiabaticity criterion

$$\left|\frac{\langle m|\partial_t V|n\rangle}{\epsilon_m-\epsilon_n}\right|\ll\frac{1}{\tau_s} \quad (59)$$

is met, where τ_s denotes the switching time. Equation (59) means that the change of the external control parameters during the switching time should be much smaller than the level spacing in the microscopic Hamiltonian. In the case of coupled quantum dots in the adiabatic regime, $J(t)=\epsilon_t(t)-\epsilon_s(t)$ is the level spacing between the instantaneous singlet and triplet energies.

Note also that if $V(t)$ respects some symmetry, there can be selection rules that make Eq. (59) less stringent. In the case of two coupled quantum dots with an applied homogeneous magnetic field, the total spin is conserved by $V(t)$ and therefore only transitions to higher orbital levels of the quantum dots are relevant. Therefore, the less stringent condition $1/\tau_s\approx|\dot{V}/V|\ll\Delta\bar{\epsilon}/\hbar$ is sufficient for adiabatic switching.[16] Here, $\Delta\bar{\epsilon}$ denotes the orbital level distance averaged over the switching time. Since in this case the Zeeman energy is independent of the space coordinates, it commutes with the orbital Hamiltonian and does not affect adiabaticity. The case of inhomogeneous magnetic fields is more intricate. The lack of a selection rule enforces the more stringent adiabaticity condition[16] $1/\tau_s\approx|\dot{V}/V|\ll\bar{J}/\hbar\ll\Delta\bar{\epsilon}/\hbar$, where $\bar{J}$ de-

notes the average exchange coupling during the switching. In addition to this, the Zeeman term does not commute with the orbital Hamiltonian in the case of inhomogeneous fields and therefore also influences J. Due to these difficulties, we presently do not know how to calculate the parameter J in Eq. (1) in the presence of an inhomogeneous field, $\mathbf{B}_1 \neq \mathbf{B}_2$.

The condition of synchronous switching (c) is mainly a technical issue. We would like to stress that the choice of the pulse form has a decisive influence on whether the adiabaticity condition Eq. (59) can be satisfied or not. It is quite easy to see that a rectangular pulse is unsuitable because it has infinite derivatives. Both Gaussian $[\exp(-t^2/\Delta t^2)]$ and exponential $[\exp(-|t|/\Delta t)]$ pulses are far better than a rectangular pulse. The exponential pulse has the advantage that $|\dot{V}/V|$ is independent of t compared to the Gaussian pulse where $|\dot{V}/V| \propto t$. However, the exponential pulse has the disadvantage that it has a cusp at $t=0$ which causes algebraically decaying tails in its Fourier spectrum. We can combine the advantages of both pulses by using the sech pulse, $\mathrm{sech}(t/\Delta t) = 1/\cosh(t/\Delta t)$. Since all the pulses have to be cut off at some finite time $\pm \tau_s/2$, we choose the width of the pulse Δt smaller than the actual switching time τ_s, i.e., we choose $\alpha = \tau_s/\Delta t > 1$. By substituting the sech pulse into the adiabaticity condition Eq. (59), we obtain the condition $\tau_s \gg \alpha\hbar/\Delta\overline{\epsilon}$ in the case where the spin is conserved (homogeneous magnetic field) and $\tau_s \gg \alpha\hbar/\overline{J}$ otherwise.

VII. APPLICATIONS

We will now give a detailed description of how a system of three coupled quantum dots could be controlled in order to test the functionality of three-bit quantum error correction in that system. We denote the maximal coupling and magnetic field that can be applied by $J_{\max}$ and $B_{\max}$. If only one of the parameters J_{ij}, $\mathbf{B}_i$ can be made nonzero at a given instant, then the following serial-pulse sequence has to be applied:

step	duration	parameter	value
1	$\tau_B/4$	B_y^2	$B_{\max}$
2	$\tau_J/4$	J_{12}	$J_{\max}$
3	$\tau_B/2$	B_z^1	$B_{\max}$
4	$\tau_J/4$	J_{12}	$J_{\max}$
5	$\tau_B/4$	B_z^1	$B_{\max}$
6	$\tau_B/4$	B_z^2	$-B_{\max}$
7	$\tau_B/4$	B_y^2	$-B_{\max}$
8	$\tau_B/4$	B_y^3	$B_{\max}$
9	$\tau_J/4$	J_{13}	$J_{\max}$
10	$\tau_B/2$	B_z^1	$B_{\max}$
11	$\tau_J/4$	J_{13}	$J_{\max}$
12	$\tau_B/4$	B_z^1	$B_{\max}$
13	$\tau_B/4$	B_z^3	$-B_{\max}$
14	$\tau_B/4$	B_y^3	$-B_{\max}$
15	τ_n	B_x	random
16–29	repeat	1–14	

(60)

where $\tau_J = 2\pi\hbar/J_{\max}$ and $\tau_B = 2\pi\hbar/g\mu_B B_{\max}$. Step 15 describes the artificial introduction of noise into the system by applying a random magnetic field in the x direction, causing random spin flips in a time $\tau_n \lesssim \pi/g\mu_B\overline{B_x}$, where $\overline{B_x}$ denotes the mean amplitude of the random B field. After step 29 is completed, qubits 2 and 3 are measured and qubit 1 is flipped (by applying $B_x^1 = B_{\max}$ for time $\tau_B/2$) if both measurements yield 1 (spin down). The total switching time for steps 1 to 29 then amounts to $\tau_s = 6\tau_B + 2\tau_J + \tau_n$.

In a device where parallel pulses are possible, i.e., where the conditions (a)–(c) from Sec. VI are fulfilled, the following pulse sequence can be applied with the same effect:

i	τ_i	J_{12}	B_{1x}	B_{2x}	B_{1y}	B_{2y}	B_{1z}	B_{2z}
1	$0.464\,\tau$	0.402	-0.054	1	0.442	0.419	-0.905	0.851
2	$0.617\,\tau$	1	-0.356	0.559	-0.622	0.396	0.572	0.176
		J_{13}	B_{1x}	B_{3x}	B_{1y}	B_{3y}	B_{1z}	B_{3z}
3	$0.464\,\tau$	0.402	-0.054	1	0.442	0.419	-0.905	0.851
4	$0.617\,\tau$	1	-0.356	0.559	-0.622	0.396	0.572	0.176
			B_{1x}	B_{2x}	B_{3x}			
5	τ_n		rnd	rnd	rnd			
6			1					
|	$2.162\,\tau$	repeat	|					
9			4					

(61)

We have assumed that the maximal Zeeman energy is equal to the maximal coupling, $g\mu_B B_{\max} = J_{\max} \equiv M$, and defined $\tau \equiv \tau_B = \tau_J$. All parameters are given in units of M. The parameters in every step can be multiplied by any pulse shape $f(t)$ with $\int_0^{\tau_i} f(t)dt = 1$, where τ_i denotes the duration of step i. Note that in every step, the pulse shape has to be the same for all parameters. Parameters that are omitted in Eq. (61) are set to zero. The total switching time in this parallelized version amounts to $\tau_p = 4.3252\,\tau + \tau_n$, compared to $\tau_s = 8\tau + \tau_n$ in the case of serial switching.

VIII. CONCLUSION

We have studied the minimal requirements for the implementation of the XOR gate, the conditional phase flip (CPF) gate, the encoding circuit E used for three-bit error correction, and the teleportation encoder E_T, all for Heisenberg-coupled spins with $s=\frac{1}{2}$. In addition to this, we have also considered anisotropic spin-spin coupling as described in the XY model. Two different methods for generating quantum gates with a time-dependent Hamiltonian have been discussed and compared, the ''conventional'' serial pulse method and a new method involving parallel pulses.

The main results of our work are the parallel pulses for the conditional phase flip [Eq. (38)] and XOR [Eq. (42)] using Heisenberg dynamics, and the corresponding results [Eq. (52) and Eq. (54)] for XY dynamics. The direct parallel-pulse sequence Eq. (44) for the three-bit encoder E was found; however, it is possible that a faster pulse sequence for this gate can be found with more numerical effort.

The following results for serial switching have been found: There is an analog of the known circuit Eq. (6) for CPF (cf. Fig. 3) for systems with XY coupling, which is given in Eq. (48). For Heisenberg coupling, we have proved that the known circuit Eq. (6) is optimal in the sense that CPF cannot be obtained with one ''square-root-of-swap'' gate. For the proof we invoked the set $\mathcal{P}(U)$ of all product states that are mapped onto product states by a quantum gate U; $\mathcal{P}(U)$ helps to distinguish quantum gates modulo concatenation of single-qubit gates. The same tool was also used to prove that the encoder E for quantum error correction cannot be generated with serial switching with fewer than four ''square-root-of-swap'' gates. The same is true for the encoder E_T for the teleportation of one qubit.

The results for the parallel-pulse XOR for isotropic Heisenberg interactions and the results for CPF and XOR for XY interactions, Eqs. (42), (52), and (54), and for the three-bit encoder Eq. (44) were all found using the computer algorithm described in Sec. IV. This algorithm searches for a (parallel) pulse sequence for an arbitrary quantum gate operating on any number of qubits. The number of qubits and the complexity of the pulse sequence that can be studied are only limited by the available computational resources.

Quantum computations are very often presented in the form of quantum circuits, i.e., as a sequence of gates belonging to a small set of universal gates. Our examples of parallel-pulse gates illustrate that such quantum circuits are in general not the most efficient way of performing a quantum computation. The reason for this is that standard quantum circuits only allow the use of a small fraction of the possible time evolutions that can be generated by the underlying Hamiltonian. While for the two- and three-qubit gates we have studied here we could optimize the switching time by typically a factor of about 2 by using parallel pulses, it can be speculated that for gates operating on many qubits or whole quantum computations, switching times could be reduced by a much larger amount. Note also that the parallel pulses we have studied here represent only a small subset of the possible time evolutions themselves, since we have been restricted to very simple discretized pulses of up to three time steps.

While quantum circuits are very intuitive and provide an excellent framework for the theoretical study of quantum algorithms and their connection to classical algorithms, the representation of quantum gates or whole computations as parallel pulse sequences may turn out to be more efficient for a number of physical implementations.

ACKNOWLEDGMENTS

We would like to thank C.H. Bennett, A. Imamoglu, B.M. Terhal, and A.V. Thapliyal for interesting discussions. This work was supported by the Swiss National Science Foundation. D.P.D. acknowledges the funding under Grant No. ARO DAAG55-98-C-0041. G.B. acknowledges the hospitality and financial support from the IBM T.J. Watson Research Center, where much of this work was completed.

*Electronic address: burkard@ubaclu.unibas.ch
†Electronic address: loss@ubaclu.unibas.ch
‡Electronic address: divince@watson.ibm.com
§Electronic address: smolin@watson.ibm.com

[1] P.W. Shor, in *Proceedings of the 35th Annual Symposium on the Foundations of Computer Science* (IEEE Press, Los Alamitos, CA, 1994), p. 124.
[2] R.P. Feynman, Int. J. Theor. Phys. **21**, 467 (1982).
[3] D.P. DiVincenzo, Science **270**, 255 (1995).
[4] A. Barenco, C.H. Bennett, R. Cleve, D.P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J.A. Smolin, and H. Weinfurter, Phys. Rev. A **52**, 3457 (1995).
[5] J.I. Cirac and P. Zoller, Phys. Rev. Lett. **74**, 4091 (1995); C. Monroe, D.M. Meekhof, B.E. King, W.M. Itano, and D.J. Wineland, *ibid.* **75**, 4714 (1995).
[6] Q.A. Turchette, C.J. Hood, W. Lange, H. Mabuchi, and H.J. Kimble, Phys. Rev. Lett. **75**, 4710 (1995).
[7] D. Cory, A. Fahmy, and T. Havel, Proc. Natl. Acad. Sci. USA **94**, 1634 (1997); I.L. Chuang, N. Gershenfeld, and K. Kubinec, Phys. Rev. Lett. **80**, 3408 (1998); J.A. Jones, M. Mosca, and R.H. Hansen, Nature (London) **393**, 344 (1998).
[8] D. Loss and D.P. DiVincenzo, Phys. Rev. A **57**, 120 (1998).
[9] B.E. Kane, Nature (London) **393**, 133 (1998).
[10] D.V. Averin, Solid State Commun. **105**, 659 (1998); A. Shnirman, G. Schön, and Z. Hermon, Phys. Rev. Lett. **79**, 2371 (1997).
[11] L.B. Ioffe, V.B. Geshkenbein, M.V. Feigel'man, A.L. Fauchère, and G. Blatter, Nature (London) **398**, 679 (1999).
[12] A. Barenco, D. Deutsch, A. Ekert, and R. Josza, Phys. Rev. Lett. **74**, 4083 (1995); R. Landauer, Science **272**, 1914 (1996); J.A. Brum and P. Hawrylak, Superlattices Microstruct. **22**, 431 (1997); P. Zanardi and F. Rossi, Phys. Rev. Lett. **81**, 4752 (1998).
[13] P.W. Shor, Phys. Rev. A **52**, R2493 (1995); A.M. Steane, Phys. Rev. Lett. **77**, 793 (1996); D.P. DiVincenzo and P.W. Shor, *ibid.* **77**, 3260 (1996); E. Knill and R. Laflamme, Phys. Rev. A **55**, 900 (1997); D. Gottesman, *ibid.* **54**, 1862 (1996).
[14] D.G. Cory, M.D. Price, W. Mass, E. Knill, R. Laflamme, W.H. Zurek, T.F. Havel, and S.S. Somaroo, Phys. Rev. Lett. **81**, 2152 (1998).
[15] G.D. Sanders, K.W. Kim, and W.C. Holton, Phys. Rev. A **59**, 1098 (1999).

[16] G. Burkard, D. Loss, and D.P. DiVincenzo, Phys. Rev. B **59**, 2070 (1999).
[17] D.P. DiVincenzo, J. Appl. Phys. **85**, 4785 (1999) (cond-mat/9810295).
[18] D.P. DiVincenzo and D. Loss, J. Magn. Magn. Mater. (to be published) (cond-mat/9901137).
[19] A. Imamoğlu, D.D. Awschalom, G. Burkard, D.P. DiVincenzo, D. Loss, M. Sherwin, and A. Small, quant-ph/9904096.
[20] G. Brassard, Physica D **120**, 43 (1998) (quant-ph/9605035).
[21] D.P. DiVincenzo, Proc. R. Soc. London, Ser. A **454**, 261 (1998).
[22] For M qubits, the set of product state is defined as $\mathcal{P}=\{|\Psi\rangle\in\mathcal{H}=\mathcal{H}_2^{\otimes M}||\Psi\rangle=|\phi_1\rangle\otimes\cdots\otimes|\phi_M\rangle;|\phi_i\rangle\in\mathcal{H}_2\}$.
[23] For compactness, we have truncated our numerical results after the third or fourth decimal. If desired, much higher precision can be obtained with our numerical algorithm.
[24] In the special case where $B_{ix}=B_{iy}=0$, this can be demonstrated by applying the same procedure as for the Heisenberg interaction, showing that the corresponding four equations have no solution.
[25] The spin-orbit coupling $H_{so}=\Sigma_i(\hbar/2im_0mc^2)\mathbf{S}_i\cdot(\boldsymbol{\nabla}_iV\times\boldsymbol{\nabla}_i)$ for a band electron in a slowly varying potential V contains both the bare mass m_0 (from the magnetic moment of the electron) and the effective mass m (since the velocity of the electron is derived from the band structure). In our case, the effective mass is canceled because $V=m\omega^2r^2/2$.