Efficient implementation of coupled logic gates for quantum computation

Debbie W. Leung,[1,2] Isaac L. Chuang,[2] Fumiko Yamaguchi,[1] and Yoshihisa Yamamoto[1,3]
[1]*Quantum Entanglement Project, ICORP, JST, Edward L. Ginzton Laboratory, Stanford University, Stanford, California 94305-4085*
[2]*IBM Almaden Research Center, San Jose, California 94120*
[3]*NTT Basic Research Laboratories, 3-1 Morinosato-Wakamiya, Atsugi, Kanagawa 243-0198, Japan*
(Received 7 May 1999; published 16 March 2000)

Most natural Hamiltonians do not couple specific pairs of quantum bits and spurious couplings occur along with the intended one. We present an efficient scheme that couples any designated pair of spins in heteronuclear spin systems. The scheme is based on the existence of Hadamard matrices. For a system of n spins with pairwise coupling, the scheme concatenates cn intervals of system evolution and uses at most cn^2 pulses where $c \approx 1$. Our results demonstrate that, in many systems, selective recoupling is possible with linear overhead, contrary to common speculation that exponential effort is always required.

PACS number(s): 03.67.Lx

I. INTRODUCTION

Quantum computation requires the ability to perform coupled logic which can only originate from the natural couplings in the quantum systems involved. However, naturally available interactions do not couple specific pairs of quantum bits (qubits) as desired in most applications of quantum computation [1,2]. Rather, many couplings occur simultaneously along with the intended one. Moreover, the problem generally becomes worse with larger systems and stronger couplings, which are essential for quantum computation to be useful. This fundamental task to turn off spurious evolution is so difficult that, coercing a complex system to *do nothing* [3] – ceasing all evolution – can be just as difficult as making it do something computationally useful.

In this paper, we address a simpler instance of the above problem: how to stop the spurious coupling and to perform specific coupled logic gates when implementing quantum computation in nuclear spin systems using nuclear magnetic resonance (NMR) techniques [4–7]. This is particularly relevant because any two spins either couple all the time or never couple at all. The task of turning off all couplings is known in the art of NMR as *decoupling*; doing this for all but a select subset of couplings is known as *selective recoupling*. The basic idea is to interrupt the free evolution by carefully chosen pulses. These pulses are single qubit operations that transform the Hamiltonian in the time between pulses in such a manner that unwanted couplings in consecutive evolutions cancel out each other. Ingenious schemes have been found [8–11] but they do not address the problems relevant to quantum computation. In usual NMR applications, the structure of the spin systems is not known *a priori*. Therefore, pulse sequences are not designed to address individual spins. Moreover, the primary interest in these schemes is to reveal complex structures in the spectra rather than to achieve precise quantum evolutions. Quantum computation brings new requirements, and initial efforts [12] have been made to develop pulse sequences to satisfy these needs; however, to-date, schemes have necessitated resources (such as total number of pulses applied) exponential in the number of spins being controlled. Schemes for selective recoupling are generally difficult to find for a large system. Each pulse simultaneously affects many coupling terms in the Hamiltonian. To turn off all but one of the coupling terms, these pulses have to satisfy many simultaneous requirements.

In this paper, we present *efficient* schemes for decoupling and selective recoupling. For an n-spin system, in which any pair of spins can be coupled, our schemes concatenate cn time intervals and use fewer than cn^2 pulses, where $c \approx 1$ for most n with a strict upper bound $c \leqslant 2$. Our method exploits simplifications in the couplings when the spins have very different Zeeman frequencies. In this case, we show that the conditions for decoupling and selective recoupling are special orthogonality conditions, with solutions given by a class of well-known matrices called *Hadamard matrices*. These are generalizations of the well-known Hadamard transformation in quantum computation. The efficiency of the scheme originates from the existence of general Hadamard matrices in many dimensions.

The paper is structured as follows. In Sec. II, we review relevant concepts in NMR quantum computing and restate the problems precisely. In Sec. III, we first motivate the construction of the decoupling scheme with examples, and then derive conditions for decoupling and describe the general construction related to Hadamard matrices. Modifications of the decoupling scheme to perform selective recoupling are described. We conclude with various properties and limitations of the scheme. Important properties of Hadamard matrices are summarized in the Appendices.

II. NMR QUANTUM COMPUTING AND THE STATEMENT OF THE PROBLEM

In this section, we describe the NMR system and describe how a universal set of (nonfault tolerant) operations [13–15], namely, the single qubit operations and the controlled-NOT gate [16], can be realized using basic NMR primitives.

We shall consider a physical system that consists of a solution of identical molecules. Each molecule has n nonmagnetically equivalent nuclear spins that serve as qubits. A static magnetic field is applied externally along the $+\hat{z}$ direction. This magnetic field splits the energy levels of the spin states aligned with and against it. This is described in

the Hamiltonian by the Zeeman terms, which, in the energy eigenbasis, are given by

$$\mathcal{H}_Z = -\frac{1}{2}\sum_i \hbar\omega_i \sigma_z^{(i)}, \tag{1}$$

where i is the spin index, $\omega_i/2\pi$ is the *Zeeman frequency* for the ith spin, and $\sigma_z^{(i)}$ is the Pauli matrix operating on the ith spin. The convention $\hbar=1$ is used for the rest of the paper. The spins have very different Zeeman frequencies, a situation loosely termed as ''heteronuclear'' in this paper.

Nuclear spins can interact via the dipolar coupling or the indirect coupling mediated by electrons [9,17]. If the molecules tumble fast and isotropically, dipolar coupling and the tensor part of the indirect coupling will be averaged away; otherwise, the physics can be more complicated. However, in the presence of a strong external magnetic field, only the *secular* part (the energy conserving terms that commute with $\mathcal{H}_Z$) is important [9,17]. For a heteronuclear system, the resulting coupling becomes

$$\mathcal{H}_c = \sum_{i<j} g_{ij}\sigma_z^{(i)}\otimes\sigma_z^{(j)}, \tag{2}$$

independent of the exact form of the original coupling. In Eq. (2), g_{ij} denotes the coupling constant between the ith and the jth spin.

Single qubit operations are performed by applying *pulsed* radio frequency (RF) magnetic fields along some direction $\hat{\eta}$ perpendicular to the static field. To address the ith spin, the frequency of the RF field is tuned to $\omega_i/2\pi$. When the ω_i's are very different, very short pulses can be used, so that during each pulse, all other evolutions are negligible except for the rotation operator $e^{-i(\theta/2)\vec{\sigma}^{(i)}\cdot\hat{\eta}}$, where θ is proportional to the pulse duration and the power. The Lie group of all single qubit operations can be generated by rotations about $\hat{x}$ and $\hat{y}$.

Coupled operations such as controlled phase shift or controlled-NOT acting on the ith and the jth spins can be performed given the primitive

$$ZZ_{ij} = e^{-i(\pi/4)\sigma_z^{(i)}\otimes\sigma_z^{(j)}}. \tag{3}$$

For instance, a controlled-NOT from the ith spin to the jth spin can be implemented by compositing the gates $e^{-i(\pi/4)\sigma_y^{(i)}}e^{i(\pi/4)\sigma_x^{(i)}}e^{i(\pi/4)\sigma_y^{(i)}}e^{-i(\pi/4)\sigma_x^{(j)}}e^{i(\pi/4)\sigma_y^{(j)}}ZZ_{ij}e^{-i(\pi/4)\sigma_y^{(j)}}$.

The ultimate goal is to be able to efficiently realize arbitrary quantum operations on an n-spin system with arbitrary couplings. In this paper, we consider a more limited objective, which can now be stated precisely, using the definitions of Eqs. (1)–(3): Given a heteronuclear system of n spins with free evolution $e^{-i(\mathcal{H}_Z+\mathcal{H}_c)t}$, controlled using typical RF pulses, how can ZZ_{ij} be implemented efficiently? Following NMR tradition, we refer to this task as ''recoupling.''

III. CONSTRUCTION OF THE SCHEMES

A problem closely related to recoupling is the following: Given a heteronuclear system of n spins with free evolution $e^{-i\mathcal{H}_c t}$, controlled using typical RF pulses, how can the identity I be implemented efficiently?

We refer to this task as ''decoupling.'' It is conceptually easier to first construct a decoupling scheme. The scheme is derived from Hadamard matrices, which will be reviewed. Modifications to implement selective recoupling will be described afterwards.

A. Decoupling scheme for two qubits

To motivate the general construction, we analyze the simplest example of decoupling two spins. From Eq. (2), the evolution operator for an arbitrary duration t is given by $\tau = e^{-ig_{12}t\sigma_z^{(1)}\otimes\sigma_z^{(2)}}$. We define X to be the gate σ_x, superscripted by the spin index where appropriate. In the notation defined in Sec. II, X is a rotation of $\theta=\pi$ along $\hat{x}$ up to an irrelevant overall phase. $X^{(i)}$ is physically performed by an RF pulse at frequency ω_i. The important observation is

$$X^{(2)}(\sigma_z^{(1)}\otimes\sigma_z^{(2)})X^{(2)} = -\sigma_z^{(1)}\otimes\sigma_z^{(2)} \tag{4}$$

and therefore

$$X^{(2)}\tau X^{(2)} \tag{5}$$

$$= X^{(2)}e^{-ig_{12}t\sigma_z^{(1)}\otimes\sigma_z^{(2)}}X^{(2)} \tag{6}$$

$$= e^{-ig_{12}t\sigma_z^{(1)}\otimes(X^{(2)}\sigma_z^{(2)}X^{(2)})} \tag{7}$$

$$= e^{-ig_{12}t\sigma_z^{(1)}\otimes(-\sigma_z^{(2)})} \tag{8}$$

$$= \tau^{-1}, \tag{9}$$

where Eq. (7) is obtained using the Taylor series expansion of the matrix exponents and the fact $(X^{(2)})^2=I$. This observation implies that adding the gate $X^{(2)}$ before and after the evolution τ results in τ^{-1}, so that the sequence of events $X^{(2)}\tau X^{(2)}\tau = I$ has no net coupling although the spins are actually coupled all the time. This is called refocusing in NMR, and clearly illustrates how single qubit operations can transform the Hamiltonian so that unwanted couplings in consecutive evolutions cancel out each other [18].

We now extract the essential features of the above decoupling scheme by rewriting the sequence $X^{(2)}\tau X^{(2)}\tau$ as

$$e^{-ig_{12}t(+\sigma_z^{(1)})\otimes(-\sigma_z^{(2)})}e^{-ig_{12}t(+\sigma_z^{(1)})\otimes(+\sigma_z^{(2)})}, \tag{10}$$

and referring to τ and $X^{(2)}\tau X^{(2)}$ as time intervals. We note the following facts.

(1) Since the matrix exponents commute, negating the coupling for exactly half of the total time is sufficient to cancel out the coupling.

(2) Since the coupling is bilinear in $\sigma_z^{(1)}$ and $\sigma_z^{(2)}$, it is unchanged (negated) when the signs of $\sigma_z^{(1)}$ and $\sigma_z^{(2)}$ agree (disagree).

(3) The sign of $\sigma_z^{(i)}$ is $(-)$ or $(+)$ depending on whether $X^{(i)}$ gates are applied before and after the interval. In other words, the sign of σ_z for each spin in each time interval is controlled by inserting X gates for that spin before and after that interval.

In summary, the most crucial point leading to decoupling is that the signs of the σ_z matrices of the coupled spins, controlled by the X gates, disagree for half of the total time elapsed.

B. Sign matrix and decoupling criteria

Following the observations in the previous decoupling scheme, we generalize the result to n qubits in this section. We consider schemes that concatenate a certain number of equal-time intervals and use X gates to control the signs of σ_z for each spin. The essential information on the signs can be represented by a ''sign matrix'' defined as follows. The sign matrix of a pulse scheme for n spins with m time intervals is the $n\times m$ matrix with the (i,a) entry being the *sign* of $\sigma_z^{(i)}$ in the ath time interval. We denote any sign matrix for n spins by S_n. For example, the sequence in Eq. (10) can be represented by the sign matrix

$$S_2=\begin{bmatrix} + & + \\ + & - \end{bmatrix}. \tag{11}$$

Each column represents a time interval and each row represents a sequence of m intervals for a particular spin. The entry ''$-$'' represents an interval that is preceded and followed by X gates for the spin involved. Therefore, each sign matrix corresponds to a sequence of events for the whole system. Following the discussion in Sec. III A, decoupling is achieved whenever any two rows in the sign matrix disagree in exactly half of the entries (all couplings are negated for exactly half of the time). The general construction of the decoupling scheme is now reduced to finding sign matrices satisfying the above criteria.

As an illustration, we construct a decoupling scheme for four spins. We first find a correct sign matrix and then derive the corresponding pulse sequence. For example, a possible sign matrix is given by

$$S_4=\begin{bmatrix} + & + & + & + \\ + & + & - & - \\ + & - & - & + \\ + & - & + & - \end{bmatrix}, \tag{12}$$

in which any two rows disagree in exactly two entries. The sequence corresponding to S_4 can be obtained by converting each column to a time interval before and after which X pulses are applied to spins (rows) given by $-$'s. No pulses are applied to spins (rows) with $+$'s. The resulting sequence,

$$\tau(X^{(3)}X^{(4)}\tau X^{(3)}X^{(4)})(X^{(2)}X^{(3)}\tau X^{(2)}X^{(3)}) \times(X^{(2)}X^{(4)}\tau X^{(2)}X^{(4)}), \tag{13}$$

is the identity by construction and this can also be verified directly. Note that $\mathcal{H}_c$ in $\tau=e^{-i\mathcal{H}_c t}$ now denotes the sum of six possible coupling terms for four spins. Note also Eq. (13) is written in such a way that it corresponds visually to the sign matrix, though the evolutions are actually in reverse time order relative to S_4. However, such ordering is irrelevant for commuting evolutions. Since $X^{(i)}X^{(i)}=I$, Eq. (13) can be simplified to

$$\tau(X^{(3)}X^{(4)}\tau X^{(4)})(X^{(2)}\tau X^{(3)})(X^{(4)}\tau X^{(2)}X^{(4)}). \tag{14}$$

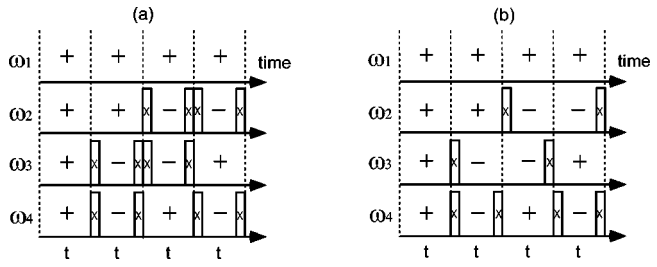

FIG. 1. (a) Pulse sequence corresponding to Eq. (13). From S_4, each ''$-$'' sign in the ith row and ath column translates to two X pulses at ω_i before and after the ath time interval. (b) Pulse sequence obtained from simplifying (a). This corresponds to Eq. (14), and can be constructed directly from S_4 by translating each change of sign in the ith row to an X pulse at ω_i. A ''$-$'' sign at the end of the row also gives rise to an X pulse at end of the last time interval.

This simplified pulse sequence can also be obtained directly from Eq. (12) by converting columns to time intervals and inserting $X^{(i)}$ between intervals whenever the ith row changes sign or whenever a $-$ sign reaches either end of the row. The relation between the sequences in Eq. (13) and Eq. (14) and S_4 is illustrated in Fig. 1.

The above scheme can be generalized to decouple n spins with m time intervals as follows: Construct the $n\times m$ sign matrix S_n, with entries $+$ or $-$, such that *any* two rows disagree in exacly half of the entries. For each $-$ sign in the ith row and the ath column, apply $X^{(i)}$ before and after the ath time interval.

Because of the pulses, the sign of the σ_z matrix for each spin in each time interval is as given by the sign matrix. The σ_z matrices of any two spins therefore have opposite signs for half of the time, during which their coupling is negated, and the evolution is always cancelled.

For n spins, $n\times m$ sign matrices that correspond to decoupling schemes do not necessarily exist for arbitrary m, but they always exist for large and special values of m. A possible structure is

$$S_n=\begin{bmatrix} + & \cdots & + & + & \cdots & + & + & \cdots & + & + & \cdots & + \\ + & \cdots & + & + & \cdots & + & - & \cdots & - & - & \cdots & - \\ & \cdots & & & \cdots & & & \cdots & & & \cdots & \\ + & \cdots & + & - & \cdots & - & + & \cdots & + & - & \cdots & - \\ & \cdots & & & \cdots & & & \cdots & & & \cdots & \\ + & \cdots & - & + & \cdots & - & + & \cdots & - & + & \cdots & - \end{bmatrix}, \tag{15}$$

in which intervals are bifurcated when rows (spins) are added. Such bifurcation takes place whenever it is impossible to add an extra row that is orthogonal to all the existing ones (''depletion''). If such depletion occurs frequently, the sign matrix will have an exponential number of columns, and

decoupling will take an exponential number of steps as n increases. The challenge is to find the correct sign matrices with a subexponential number of columns.

C. Equivalent decoupling criteria

The criteria for a sign matrix S_n to represent a valid decoupling scheme is that any two rows disagree in exactly half of the entries. It is useful to rephrase this complicated criteria concisely. Suppose $\pm$ is replaced by ± 1 in S_n. If S_n satisfies the decoupling criteria, any two rows have zero inner product and therefore $S_n S_n^T = nI$. Conversely, any $n \times m$ matrix M with entries ± 1 satisfying $MM^T = nI$ is a valid sign matrix giving a decoupling scheme that requires m time intervals. We now present very efficient solutions to this simple criteria, namely the Hadamard matrices.

D. Hadamard matrices and decoupling scheme

Hadamard matrices have applications in many areas such as the construction of designs, error correcting codes, and Hadamard transformations [19–23].

A Hadamard matrix of order n, denoted by $H(n)$, is an $n \times n$ matrix with entries ± 1, such that

$$H(n)H(n)^T = nI. \tag{15}$$

The rows are pairwise orthogonal, therefore any two rows agree in exactly half of the entries. Likewise columns are pairwise orthogonal. We identify ''± 1'' with ''$\pm$'' throughout the paper. It is immediate that each $H(n)$ is a valid sign matrix giving a decoupling scheme for n spins using only n time intervals.

For example, S_2 and S_4 in Eqs. (11) and (12) are possible $H(2)$ and $H(4)$. An example of $H(12)$ is given by

$$H(12) = \begin{bmatrix}
+ & + & + & + & + & + & - & + & + & + & + & + \\
+ & + & + & - & - & + & + & - & + & - & - & + \\
+ & + & + & + & - & - & + & + & - & + & - & - \\
+ & - & + & + & + & - & + & - & + & - & + & - \\
+ & - & - & + & + & + & + & - & - & + & - & + \\
+ & + & - & - & + & + & + & + & - & - & + & - \\
- & + & + & + & + & + & - & - & - & - & - & - \\
+ & - & + & - & - & + & - & - & - & + & + & - \\
+ & + & - & + & - & - & - & - & - & - & + & + \\
+ & - & + & - & + & - & - & + & - & - & - & + \\
+ & - & - & + & - & + & - & + & + & - & - & - \\
+ & + & - & - & + & - & - & - & + & + & - & -
\end{bmatrix}. \tag{16}$$

Whenever $H(n)$ exists, there is a decoupling scheme for n spins concatenating only n time intervals. However, $H(n)$ may or may not exist for a given n (see Appendix A). For an arbitrary integer n, let $\overline{n}$ be the smallest integer that satisfies $n \leqslant \overline{n}$ with *known* $H(\overline{n})$. To construct a decoupling scheme for n spins when $H(n)$ does not necessarily exist, we start with $H(\overline{n})$ and take S_n to be any $n \times \overline{n}$ submatrix of $H(\overline{n})$. In other words, S_n is formed by choosing n rows from $H(\overline{n})$, which still achieves decoupling because subsets of rows of $H(\overline{n})$ are still pairwise orthogonal. The resulting decoupling scheme for n spins requires $\overline{n}$ time intervals.

As an example, S_9 can be chosen to be the first nine rows of $H(12)$ in Eq. (16):

$$S_9 = \begin{bmatrix}
+ & + & + & + & + & + & - & + & + & + & + & + \\
+ & + & + & - & - & + & + & - & + & - & - & + \\
+ & + & + & + & - & - & + & + & - & + & - & - \\
+ & - & + & + & + & - & + & - & + & - & + & - \\
+ & - & - & + & + & + & + & - & - & + & - & + \\
+ & + & - & - & + & + & + & + & - & - & + & - \\
- & + & + & + & + & + & - & - & - & - & - & - \\
+ & - & + & - & - & + & - & - & - & + & + & - \\
+ & + & - & + & - & - & - & - & - & - & + & +
\end{bmatrix}. \tag{17}$$

Note that the scheme is efficient if $\overline{n} - n \ll n$. A detailed analysis of the efficiency will be given after we present the recoupling scheme.

E. Recoupling scheme

Recall that we have to remove $\mathcal{H}_Z$ along with the unwanted coupling in the recoupling scheme. We first construct a scheme that freezes all evolution–removes both $\mathcal{H}_Z$ and $\mathcal{H}_c$. We need the following property of Hadamard matrices. Note that permutations or negations of rows or columns of Hadamard matrices leave the orthogonality condition invariant. Two Hadamard matrices are called equivalent if one can be transformed to the other by a series of such operations. Each Hadamard matrix is equivalent to a *normalized* one, which has only $+$'s in the first row and column. For instance, $H(12)$ in Eq. (16) can be *normalized* by negating the seventh row and column

$$H(12) = \begin{bmatrix}
+ & + & + & + & + & + & + & + & + & + & + & + \\
+ & + & + & - & - & + & - & - & + & - & - & + \\
+ & + & + & + & - & - & - & + & - & + & - & - \\
+ & - & + & + & + & - & - & - & + & - & + & - \\
+ & - & - & + & + & + & - & - & - & + & - & + \\
+ & + & - & - & + & + & - & + & - & - & + & - \\
+ & - & - & - & - & - & - & + & + & + & + & + \\
+ & - & + & - & - & + & + & - & - & + & + & - \\
+ & + & - & + & - & - & + & - & - & - & + & + \\
+ & - & + & - & + & - & + & + & - & - & - & + \\
+ & - & - & + & - & + & + & + & + & - & - & - \\
+ & + & - & - & + & - & + & - & + & + & - & -
\end{bmatrix}. \tag{18}$$

To remove both $\mathcal{H}_Z$ and $\mathcal{H}_c$, note that the Zeeman term for the ith spin is linear in $\sigma_z^{(i)}$, and negating $\sigma_z^{(i)}$ for half of the time results in no net Zeeman evolution for the ith spin. Therefore, Zeeman evolution for all spins can be removed if the sign matrix has identically zero row sum. Such a sign matrix can be constructed by starting with a *normalized* $H(\overline{n})$ and excluding the first row of $H(\overline{n})$ in the sign matrix. Since a normalized $H(\overline{n})$ has only $+$'s in the first row, all other rows have zero row sums by orthogonality. Such construction is possible unless $n=\overline{n}$, in which case construction should start with $H(\overline{n+1})$. For instance, the last nine rows of the normalized $H(12)$ in Eq. (18) is a valid S_9.

To implement selective recoupling between the ith and the jth spins, the sign matrix should have equal ith and jth rows but any other two rows should be orthogonal. The coupling term $g_{ij}\sigma_z^{(i)}\otimes\sigma_z^{(j)}$ never changes sign and that coupling is implemented selectively, while all other couplings are removed. The sign matrix can be obtained from a normalized $H(\overline{n})$ by first excluding the first row and taking the second row of $H(\overline{n})$ to be the ith and jth row of S_n. The other $n-2$ rows of S_n can be chosen from the remaining $\overline{n}-2$ rows of $H(\overline{n})$. This scheme also removes $\mathcal{H}_Z$ and requires no more than $\overline{n}$ time intervals. To implement ZZ_{ij}, the duration of each interval t is chosen to satisfy $g_{ij}\overline{n}t=\pi/4$. Note that the total time used to implement ZZ_{ij} is the shortest possible, since the coupling is always ''on.''

For example, starting from the normalized $H(12)$, S_9 performing ZZ_{34} can be chosen as

$$S_9=\begin{bmatrix} + & + & + & + & - & - & - & + & - & + & - & - \\ + & - & + & + & + & - & - & - & + & - & + & - \\ + & + & + & - & - & + & - & - & + & - & - & + \\ + & + & + & - & - & + & - & - & + & - & - & + \\ + & - & - & + & + & + & - & - & - & + & - & + \\ + & + & - & - & + & + & - & + & - & - & + & - \\ + & - & - & - & - & - & - & + & + & + & + & + \\ + & - & + & - & - & + & + & - & - & + & + & - \\ + & + & - & + & - & - & + & - & - & - & + & + \end{bmatrix}. \tag{19}$$

F. Efficiency

The decoupling and recoupling schemes require $\overline{n}$ time intervals. They require at most $n\overline{n}$ pulses, since $XX=I$ and the X pulses are only used in pairs. The remaining question is, how does $\overline{n}$ depend on n? If Hadamard matrices exist and can be constructed for all orders, $\overline{n}=n$. However, some Hadamard matrices are missing, either because no construction methods are known or they simply cannot exist. Therefore, $\overline{n}=cn$, where $c\geqslant 1$. We will use some facts about the existence of Hadamard matrices in the following, leaving the details in Appendix A for interested readers. $H(n)$ exists only for $n=1$, $n=2$, or $n\equiv 0 \bmod 4$. Hadamard conjectured that $H(n)$ exists for every $n\equiv 0 \bmod 4$. This famous conjecture is verified for all $n<428$. Therefore, $\overline{n}-n\leqslant 3$ $\forall\ n<428$. We argue for *arbitrary n* that the schemes are still very efficient. First of all, we prove that $c<2$. For each n, there exists r such that $2^{r-1}\leqslant n<2^r$. Since $H(2^r)$ exists by Sylvester's construction, $cn=\overline{n}\leqslant 2^r<2n$. We now show that c is close to the ideal value 1 in most cases, due to the existence of Hadamard matrices of orders other than powers of 2. This is why the full connection to Hadamard matrices is useful. First of all, $\overline{n}-n\leqslant 31$ $\forall n\leqslant 10000$. In Fig. 2, c as a function of n is plotted for $n\leqslant 10000$. Within this technologically relevant range of n, c deviates significantly from 1 only for a few exceptional values of n *when* n is small. For completeness, we present arguments for $c\approx 1$ for *arbitrarily large n* in Appendix B. This is based on Paley's construction and the prime number theorem. Finally, if Hadamard's conjecture is proven, $\overline{n}-n\leqslant 3$ $\forall n$.

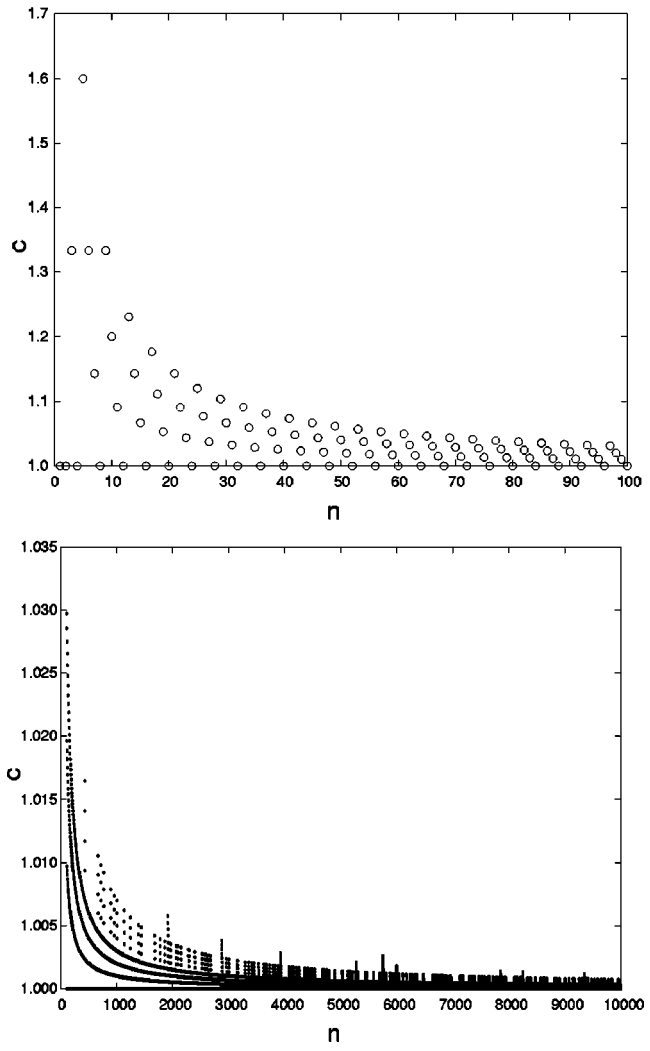

FIG. 2. Plots of c vs n, where $cn=\overline{n}$ is the minimun number of time intervals required to perform decoupling or selective recoupling for an n-spin system. c for $n\leqslant 100$ and $101\geqslant n\leqslant 10\,000$ are plotted separately.

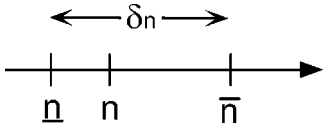

FIG. 3. The gap δ_n between two existing orders of Hadamard matrices.

IV. CONCLUSION

We reduce the problem of decoupling and selective recoupling in heteronuclear spin systems to finding sign matrices, which is further reduced to finding Hadamard matrices. While the most difficult task of constructing Hadamard matrices is not discussed in this paper, solutions already exist in the literature. Even more important is that the connection to Hadamard matrices results in very efficient schemes.

Some properties of the scheme are as follows. First of all, the scheme is optimal in the following sense. The rows of Hadamard matrices and their negations form the codewords of the first-order Reed-Muller codes, which are *perfect codes* [21,22]. It follows that, for each Hadamard matrix, it is impossible to add an extra row that is orthogonal to all the existing ones. Therefore, for a given n, $\overline{n}$ is in fact the minimum number of time intervals necessary for decoupling or recoupling, if one is restricted to the class of schemes considered. Second, the scheme applies for arbitrary duration of the time intervals. This is a consequence of the commutivity of all the terms in the Hamiltonian, which in turn comes from the large separations of the Zeeman frequencies compared to the coupling constants. Spin systems can be chosen to satisfy this condition. Finally, disjoint pairs of spins can be coupled in parallel.

We outline possible simplifications of the scheme for systems with restricted range of coupling. For example, a linear spin system with n spins but only k-nearest neighbor coupling can be decoupled by a scheme for k spins only. The ith row of the $n\times\overline{k}$ sign matrix can be chosen to be the rth row of $H(\overline{k})$, where $i\equiv r \bmod k$. Selective recoupling can be implemented using a decoupling scheme for $k+1$ spins. The sign matrix is constructed as in decoupling using $H(\overline{k+1})$ but the rows for the spins to be coupled are chosen to be the $(k+1)$th row different from all existing rows [27]. This method involving periodic boundary conditions generalizes to other spatial structures. The size of the scheme depends on k and the exact spatial structure but not on n.

The schemes have a few limitations. First of all, it only applies to systems in which spins can be individually addressed by short pulses and coupling has the simplified form given by Eq. (2). These conditions are essential to the simplicity of the scheme. They can all be satisfied if the Zeeman frequencies have large separations. Second, generalizations to include couplings of higher order than bilinear remain to be developed. Furthermore, in practice, RF pulses are inexact and have finite durations, leading to imperfect transformations and residual errors.

We have limited the discussion to quantum computation in solution NMR. The schemes can be modified for certain solid state NMR implementations [28]. In this case, complications arise from the extra couplings between different quantum computers in the ensemble. Such couplings are both homonuclear and heteronuclear in nature. Moreover, the transformed Hamiltonians in different time intervals do not commute. However, traditional sequences such as WHH [29,11] can still be combined with the current schemes, and with rapid repetition of the combined sequence, spurious couplings can be reduced.

The present discussion is only one example of a more general issue, that the naturally occuring Hamiltonian in a system does not directly give rise to convenient quantum logic gates or other computations, such as simulation of quantum systems [30]. Efficient conversion of the given system Hamiltonian to a useful form is necessary and is an important challenge for future research.

ACKNOWLEDGMENTS

This work was supported by DARPA under Contract No. DAAG55-97-1-0341 and Nippon Telegraph and Telephone Corporation (NTT). D.L. acknowledges support from the IBM Fellowship Program. We thank Nino Yannoni and Mark Sherwood for useful discussions on NMR pulse sequences, Hoi-Fung Chau and Kai-Man Tsang for discussions on the prime number theorem for arithmetic progressions, and Hoi-Fung Chau, Hoi-Kwong Lo, Alex Pines, Xinlan Zhou, and Lieven Vandersypen for helpful comments.

APPENDIX A: EXISTENCE PROPERTIES OF HADAMARD MATRICES

The following is a list of useful facts about the existence properties of Hadamard matrices.

1. *Necessary conditions*. $H(n)$ exists only for $n=1$, $n=2$, or $n\equiv 0 \bmod 4$. This is obvious if the matrix is normalized, and the columns are permuted so that the first three rows become

$$\begin{bmatrix} + & \cdots & + & + & \cdots & + & + & \cdots & + & + & \cdots & + \\ + & \cdots & + & + & \cdots & + & - & \cdots & - & - & \cdots & - \\ + & \cdots & + & - & \cdots & - & + & \cdots & + & - & \cdots & - \end{bmatrix}.$$

2. *Hadamard's conjecture* [24]. $H(n)$ exists for every $n\equiv 0 \bmod 4$. This famous conjecture is verified for all $n<428$.

3. *Sylvester's construction* [25]. If $H(n)$ and $H(m)$ exist, then $H(nm)$ can be constructed as $H(n)\otimes H(m)$. In particular, $H(2^r)$ can be constructed as $H(2)^{\otimes r}$, which is proportional to the matrix representation of the Hadamard transformation for r qubits.

4. *Paley's construction* [26]. Let q be an odd prime power. If $q\equiv 3 \bmod 4$, then $H(q+1)$ exists; if $q\equiv 1 \bmod 4$, then $H(2(q+1))$ exists.

5. *Numerical facts* [19]. For an arbitrary integer n, let $\underline{n}$ and $\overline{n}$ be the largest and smallest integers that satisfy $\underline{n}<n\leqslant\overline{n}$ with *known* $H(\overline{n})$ and $H(\underline{n})$. We define the ''gap'' δ_n to be $\overline{n}-\underline{n}$ (see Fig. 3). For $n\leqslant 1000$, $H(n)$ is known for every possible order except for six cases, and the maximum

gap is eight. For $n \leqslant 10\,000$, $H(n)$ is unknown for 192 possible orders and the maximum gap is 32.

APPENDIX B: UPPER BOUNDS FOR $\overline{n}$

An argument for $c \approx 1$ for large n is presented using Paley's construction (mentioned in Appendix A), known results on primes in intervals and the prime number theorem for arithmetic progressions.

Let $\pi(x)$ be the number of primes that satisfies $2 \leqslant p \leqslant x$. For $x < 67$, $x/(\ln x - 1/2) < \pi(x) < x/(\ln x - 3/2)$ [31]. It follows that there exists a prime between n and $n(1+\epsilon)$ for $\epsilon > 2/\ln n$. Applying Paley's construction, $H(p+1)$ or $H(2(p+1))$ exists depending on whether $p \equiv 3 \bmod 4$ or $p \equiv 1 \bmod 4$. Therefore, $\overline{n} \leqslant n(1+\epsilon)+1$ or $\overline{n} \leqslant 2[n(1+\epsilon)+1]$, respectively.

The worse of the upper bounds $\overline{n} \leqslant 2[n(1+\epsilon)+1]$ resulting from $p \equiv 1 \bmod 4$ can be improved. Note that there are at least r primes between n and $n(1+\epsilon)^r$. If the primes that equal $3 \bmod 4$ and $1 \bmod 4$ are randomly and uniformly distributed, the probability to find a prime which equals $3 \bmod 4$ between n and $n(1+\epsilon)^r$ is larger than $1-2^{-r}$. This assumption is true due to the prime number theorem for arithmetic progressions [32]. Let $\pi(x,a,q)$ denote the number of primes in the arithmetic progression $\{a, a+q, a+2q, \ldots\}$ which satisfies $2 \leqslant p \leqslant x$. It is known that $\pi(x,3,4) \approx \pi(x,1,4)$. Therefore, with probability larger than $1-2^{-r}$, $\overline{n} \leqslant n(1+\epsilon)^r + 1$, implying $c \leqslant (1+\epsilon)^r + 1/n \approx 1$ for large n.

[1] D. DiVincenzo, Science **270**, 255 (1995).
[2] A. Ekert and R. Jozsa, Rev. Mod. Phys. **68**, 733 (1996).
[3] R. Josza, in *Proceedings of First NASA International Conference on Quantum Computation and Quantum Communication, Palm Springs, FL, 1998*, edited by C. Williams (Springer Verlag, New York, 1999); e-print quant-ph/9805086.
[4] N. Gershenfeld and I. Chuang, Science **275**, 350 (1997).
[5] D. Cory, A. Fahmy, and T. Havel, Proc. Natl. Acad. Sci. USA **94**, 1634 (1997).
[6] D. Cory, M. Price, and T. Havel, Physica D **120**, 82 (1998); e-print quant-ph/9709001.
[7] I. Chuang, N. Gershenfeld, M. Kubinec, and D. Leung, Proc. R. Soc. London, Ser. A **454**, 447 (1998).
[8] R. R. Ernst, G. Bodenhausen, and A. Wokaun, *Principles of Nuclear Magnetic Resonance in One and Two Dimensions* (Oxford University Press, Oxford, 1994).
[9] C. Slichter, *Principles of Magnetic Resonance* (Springer, Berlin, 1990).
[10] P. Mansfield, *Pulsed NMR in Solids*, Progress in Nuclear Magnetic Resonance Spectroscopy Vol. 8 (Pergamon Press, Oxford, 1971).
[11] M. Mehring, *Principles of High Resolution NMR in Solids* (Springer, Berlin, 1983).
[12] N. Linden, H. Barjat, R. Carbajo, and R. Freeman, e-print quant-ph/9811043. Homonuclear systems were considered, in contrast to the present discussion.
[13] D. DiVincenzo, Phys. Rev. A **51**, 1015 (1995).
[14] A. Barenco, Proc. R. Soc. London, Ser. A **449**, 679 (1995).
[15] D. Deutsch, A. Barenco, and A. Ekert, Proc. R. Soc. London, Ser. A **449**, 669 (1995).
[16] A. Barenco, C. Bennett, R. Cleve, D. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. Smolin, and H. Weinfurter, Phys. Rev. A **52**, 3457 (1995).
[17] A. Abragam, *The Principles of Nuclear Magnetism* (Oxford University Press, Oxford, 1961).
[18] Refocusing has been used in many demonstrations of quantum information processing, for instance, see I. Chuang, L. Vandersypen, X. Zhou, D. Leung, and S. Lloyd, Nature (London) **393**, 143 (1998); and M. Nielsen, E. Knill, and R. Laflamme, *ibid.* **395**, 52 (1998).
[19] *The CRC Handbook of Combinatorial Designs* edited by C. Colbourn and J. Dinitz (CRC Press, Boca Raton, FL, 1996).
[20] http://www.research.att.com/~njas/hadamard/index.ht-ml
[21] J. van Lint and R. Wilson, *A Course in Combinatorics* (Cambridge University Press, Cambridge, 1992).
[22] F. MacWilliams and N. Sloane, *The Theory of Error-Correcting Codes* (North-Holland, Amsterdam, 1977).
[23] For the Walsh-Hadamard transformation commonly used in quantum computation, see for instance, L. Grover, Phys. Rev. Lett. **80**, 4329 (1998); and A. Steane, *ibid.* **77**, 793 (1996).
[24] J. Hadamard, Bull. Sci. Math., **17**, 240 (1893).
[25] J. Sylvester, Philos. Mag. **34**, 461 (1867).
[26] R. E. A. C. Paley, J. Math. Phys. **12**, 311 (1933).
[27] With a periodic sign matrix, setting the jth row to be the ith row also recouples the jth and the $(i+k)$th spins when $j > i$. Similar problems occur when $j < i$. Therefore a row different from all existing ones is used. This is not necessary in linear systems using a more complicated scheme, but it is necessary for other structures such as a planar system.
[28] F. Yamaguchi and Y. Yamamoto, Appl. Phys. A: Mater. Sci. Process. **68**, 1 (1999).
[29] J. Waugh, L. Huber, and U. Haeberlen, Phys. Rev. Lett. **20**, 180 (1968).
[30] B. Terhal and D. DiVincenzo, Phys. Rev. A **61**, 022301 (2000).
[31] J. Rosser and L. Schoenfeld, Ill. J. Math. **6**, 64 (1962).
[32] H. Davenport, *Multiplicative Number Theory* (Springer-Verlag, New York, 1967).