Efficient Decoupling Schemes Based on Hamilton Cycles

Martin Rötteler*
Institute for Quantum Computing, University of Waterloo
Waterloo, Ontario, Canada, N2L 3G1
(Dated: February 1, 2008)

Decoupling the interactions in a spin network governed by a pair-interaction Hamiltonian is a well-studied problem. Combinatorial schemes for decoupling and for manipulating the couplings of Hamiltonians have been developed which use selective pulses. In this paper we consider an additional requirement on these pulse sequences: as few *different* control operations as possible should be used. This requirement is motivated by the fact that optimizing each individual selective pulse will be expensive, i. e., it is desirable to use as few different selective pulses as possible. For an arbitrary d-dimensional system we show that the ability to implement only two control operations is sufficient to turn off the time evolution. In case of a bipartite system with local control we show that four different control operations are sufficient. Turning to networks consisting of several d-dimensional nodes which are governed by a pair-interaction Hamiltonian, we show that decoupling can be achieved if one is able to control a number of different control operations which is logarithmic in the number of nodes.

PACS numbers: 03.67.Lx, 03.65.Fd, 03.67.-a

I. INTRODUCTION

The problem of simulating pair-interaction Hamiltonians has been studied intensively [1, 2, 3, 4, 5, 6]. It has been shown that starting from a given entangling bipartite Hamiltonian any bipartite Hamiltonian can be simulated [2]. This can be extended to networks of qubits [1, 3, 6] and even to networks of higher dimensional systems [4, 5]. The underlying idea is to control the system by applying hard pulses to the individual nodes of the network. This parallels the methods developed for universal control of open quantum systems [7, 8, 9, 10]. Decoupling of arbitrary interactions is an important primitive for the simulation. This can be achieved by using combinatorial constructions such as triples of Hadamard matrices [3] and orthogonal arrays [11]. The control operations in these schemes are local and have to be applied selectively to the nodes. In the following we give a brief account of the general setting.

We assume that H is a pair-interaction Hamiltonian of a system which consists of N coupled spin-$\frac{1}{2}$ particles. Let $\sigma_\alpha^{(i)}$, where $\alpha \in \{x, y, z\}$ and $i \in \{1, \ldots, N\}$ denote the Pauli operators acting locally on qubit i. We can write H in the form

$$H = \sum_{k=1}^{N} \sum_{\alpha} r_\alpha^{(k)} \sigma_\alpha^{(k)} + \sum_{k,\ell=1}^{N} \sum_{\alpha,\beta} J_{\alpha,\beta}^{k,\ell} \sigma_\alpha^{(k)} \otimes \sigma_\beta^{(\ell)}, \quad (1)$$

with indices $\alpha, \beta \in \{x, y, z\}$. Hence the coupling strength between the different qubits in this N-spin network is given by $J_{\alpha,\beta}^{k,\ell}$. The problem at hand is to decouple interactions in a Hamiltonian of the form eq. (1), or more generally to simulate another Hamiltonian $\tilde{H}$ by the given one. The framework for these simulations is average Hamiltonian theory [12, 13].

A special case is given by a system which has $\sigma_z\sigma_z$ interactions only. Here selective σ_x pulses applied to the nodes are sufficient to turn off the interactions and hence to simulate any desired Hamiltonian [1, 3].

For general pair-interaction Hamiltonians the decoupling problem is harder. Nevertheless, in [11] it was shown how to achieve decoupling using orthogonal arrays which are objects studied in combinatorial theory. The approach taken in [11] generalizes schemes obtained from Hamadard matrices [1, 3]. All these methods can be thought of as generalizations of well-known techniques for decoupling and refocusing used in nuclear-magnetic-resonance theory [12, 13]. In higher-dimensional systems decoupling can be achieved by means of selective pulses which are derived from orthogonal arrays [4, 11]. The selective pulses employed in these schemes will be quite demanding in experimental realizations. Hence it would be desirable to have as few different selective pulses as possible in order to minimize the optimization overhead necessary to implement each one of them. This motivates the question to search for decoupling schemes in which the pulses can be arranged in such a way that only few different pulses are used.

After a brief introduction into the framework we will consider schemes for one d-dimensional node which will work with two different pulses, schemes for a bipartite system of two d-dimensional nodes which will work with four different pulses, and finally schemes for networks of n nodes which are d-dimensional. The latter schemes make use of $O(\log n)$ different pulses.

II. DECOUPLING SCHEMES

The underlying model of the decoupling schemes described in this paper is average Hamiltonian theory [13],

*Electronic address: mroetteler@iqc.ca

the necessary parts of which we briefly describe next. Assume that the Hamiltonian H is of the form (1). We can apply the sequence

$$e^{-i\tau_n H} V_n \dots e^{-i\tau_2 H} V_2 e^{-i\tau_1 H} V_1, \tag{2}$$

with relative times $\tau_i \in \mathbf{R}$ and local unitaries V_i for $i = 1, \dots, n$. Note that the requirement $\prod_{i=1}^n V_i = \mathbf{1}$ is necessary in order for average Hamiltonian theory to hold and to determine the terms in the Magnus expansion [14] of the piece-wise constant evolution given in eq. (2). We can rewrite (2) in the form

$$(V_n \dots V_1)^\dagger e^{-i\tau_n H} \dots (V_2 V_1)^\dagger e^{-i\tau_2 H} (V_2 V_1)\, V_1^\dagger e^{-i\tau_1 H} V_1,$$

i. e., as a product in which all factors are given by Hamiltonians $H_j = U_j H U_j^\dagger$, where $U_j := \prod_{k=1}^j V_k$ (ordered from the right). Hence, the time evolution is divided into n intervals in each of which we have a conjugated time evolution $U_j^\dagger e^{-i\tau_k H} U_j$ with respect to the basis given by U_j, i. e., this is the "toggling-frame" form of the sequence [13]. We can still rewrite this using $U_j = \prod_{k=1}^j V_k$ and obtain the new sequence

$$U_n^\dagger e^{-i\tau_n H} U_n U_{n-1}^\dagger \dots U_2^\dagger e^{-i\tau_2 H} U_2 U_1^\dagger e^{-i\tau_1 H} U_1. \tag{3}$$

This is the form of the pulse sequence we actually work with in the following. The effective Hamiltonian corresponding to eq. (3), i. e., the first term in the Magnus expansion, is given by $\sum_{i=1}^n U_i^\dagger H U_i$. If the unitary operators U_i applied in the toggling-frame have the property that for each pair (k, l) of nodes the respective local operations applied to spins k and l run through the elements of a unitary operator basis $\mathcal{B}$ [15, 16, 17] of the subsystem given by k and l, then we obtain that the time evolution of the system is stopped. Indeed, on the subsystem we then obtain the average Hamiltonian [4]

$$\frac{1}{|\mathcal{B}|} \sum_{U \in \mathcal{B}} U^\dagger H U = \frac{1}{d} \mathrm{tr}(H) \mathbf{1}_d,$$

which is zero since $\mathrm{tr}(H) = 0$. Unitary operator bases $\mathcal{B}$ exist in any dimension. Indeed, let $d \geq 2$ be the dimension of the system, we explicitly define a basis for the vector space of $\mathbf{C}^{d \times d}$ matrices: let $\omega_d = \exp(2\pi i/d)$, $\sigma_x = \sum_{i=0}^{d-1} |i\rangle \langle i+1|$, $\sigma_z = \sum_{i=0}^{d-1} \omega_d^i |i\rangle \langle i|$, where all indices are computed modulo d. Then $\mathcal{B} = \{\sigma_x^i \sigma_z^j : i, j = 0, \dots, d-1\}$ is an operator basis which will be referred to as the Pauli basis.

We continue with an observation on the sequence (3): while the matrices U_i have to run through the list of all elements of the operator basis $\mathcal{B}$, the list of quotients $U_{i+1} U_i^\dagger$ can be considerably smaller. The following example shows that for a system consisting of two d dimensional subsystems it is enough to be able to apply four different operators in order to switch off the time evolution.

Example. In Figure 1 we have shown how to label the elements of the Pauli basis for a d dimensional system in such a way that we reach all elements by just multiplying one generator at a time. It is also shown how the elements of an operator basis for a bipartite system can be arranged. This corresponds to an enumeration of the elements of $\mathbf{Z}_d^4 = \langle S \rangle / (\langle S \rangle \cap \mathbf{C}^*)$, where $S := \{\sigma_x^{(1)}, \sigma_z^{(1)}, \sigma_x^{(2)}, \sigma_z^{(2)}\}$. This enumeration can be cast in terms of Hamilton cycles in Cayley graphs (for the basic notions of graph theory we refer to [18]). Let G be a group and let S be a set of generators of G. Then the Cayley graph $\Gamma(G, S) = (V, E)$ is the directed graph with vertices $V = \{v_g : g \in G\}$ labeled by the group elements. The edges E are as follows: there is a directed edge from v_g to v_h if there exists $s \in S$ such that $h = sg$. Each Cayley graph is regular of degree $|S|$ and its structure depends on the specific choice of the generating set S.

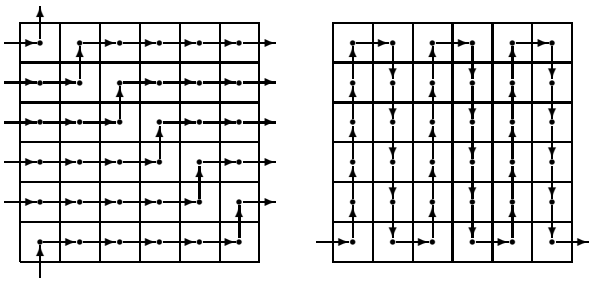

FIG. 1: Decoupling of a Hamiltonian on $\mathbf{C}^d$ can be achieved using two different pulses (the case $d = 6$ is shown). Pulses correspond to elements in $\mathbf{Z}_d^2$ which is generated up to phases by σ_x and σ_z. The left square shows the sequence in which the pulses have to be applied. In each square a horizontal move $\rightarrow$ corresponds to multiplication with $\sigma_x^{(i)}$ and a vertical move $\uparrow$ to multiplication with $\sigma_z^{(i)}$ for $i = 1, 2$. An alternative sequence is given in the right square. Decoupling of a bipartite Hamiltonian on $\mathbf{C}^d \otimes \mathbf{C}^d$ can be achieved using four different pulses. Here pulses correspond to elements in $\mathbf{Z}_d^4 = \mathbf{Z}_d^2 \times \mathbf{Z}_d^2$ generated by $\sigma_x^{(i)}$, $\sigma_z^{(i)}$ for $i = 1, 2$. A cyclic sequence can be obtained by performing one step in the first copy of $\mathbf{Z}_d^2$ followed by one full cycle in the second copy and so on.

A tour through the vertices of a graph which visits each vertex precisely once is called a Hamilton path. In case there is an edge between the end node and the start node we can close the cycle and obtain a Hamilton cycle. The sequences shown in Figure 1 define Hamilton cycles in the Cayley graph $\Gamma(\mathbf{Z}_d^4, S)$.

While for graphs like the Cayley graph of $\mathbf{Z}_d^4$ Hamilton cycles can easily constructed directly, the general question whether Hamilton cycles exist in arbitrary Cayley graphs is open [19]. In general the problem to decide whether a given graph contains a Hamilton cycle is a difficult problem and of interest in computer science and optimization. It is one of the classical NP complete problems [20], i. e., it is believed that no polynomial time exists for this problem.

For the rest of the paper we use the fact that there are Hamilton cycles in the Cayley graphs $\Gamma(G, S)$ for the abelian groups $G = \mathbf{Z}_d^{2n}$ and the set S of generators is given by the $2n$ coordinate vectors. These can be obtained by generalizing the construction given in Fig. 1.

III. ORTHOGONAL ARRAYS

In the design of statistical experiments [21] which depend on several factors one is often forced to work with an incomplete subset of the set of all possible combinations of factors. Orthogonal arrays provide a way to plan such experiments systematically. An orthogonal array is a (in general non-square) matrix with entries from a finite set S of symbols. The properties of an array are determined by a set of characteristic parameters for which the notation $OA(N, n, s, t)$ is used [22]. An $n \times N$ matrix A with entries from the set S is an orthogonal array with $s := |S|$ levels and strength t iff every $t \times N$ subarray of A contains each possible t-tuple of elements in $|S|$ precisely once as a column of A. The shorthand notation for this is that A is an $OA(N, n, s, t)$.

The rows of this matrix are also called *factors* and correspond to nodes of the network. The columns are also called *runs* and correspond to the time slots of the scheme, i. e., to the pulses to be applied. The most important parameter is the *strength* t of the array. In the context of simulation of pair-interaction Hamiltonians the strength has to be $t = 2$.

In [11] it has been shown that given an orthogonal array $OA(N, n, 4, 2)$, an arbitrary and possibly unknown Hamiltonian H, which describes the pair-interactions in an n qubit network, can be decoupled using N pulses.

We now show that in this case the pulse sequence can be arranged in such a way that only a minimal number of different pulses have to be applied. First, we briefly recall some basic facts about error correcting codes [23] since they will feature in the subsequent constructions of orthogonal arrays. A linear code over the finite field $\mathbf{F}_q$ is a k-dimensional subspace of the vector space $\mathbf{F}_q^n$. The metric on the space $\mathbf{F}_q^n$ is called the Hamming weight which for $x = (x_1, \ldots, x_n) \in \mathbf{F}_q^n$ is defined by $\mathrm{wt}(x) := |\{i \in \{1, \ldots, n\} : x_i \neq 0\}|$. The minimum distance of a linear code C is defined by $d = d_{\min} := \min\{\mathrm{wt}(c) : c \in C\}$. As a shorthand we abbreviate this by saying that C is an $[n, k, d]_q$ code. We need one more definition which is the dual code $C^\perp$ of C defined by $C^\perp := \{x \in \mathbf{F}_q^n : x \cdot y = 0 \text{ for all } y \in \mathbf{F}_q^n\}$.

The following theorem [22, Theorem 4.6] establishes a connection between orthogonal arrays and error correcting codes. In fact this is one of the most prolific construction for orthogonal arrays known.

Theorem 1 *Let C be a linear $[n, k, d]_q$ code over $\mathbf{F}_q$. Let $d^\perp$ be the minimum distance of $C^\perp$. Arrange the codewords of C into the columns of a matrix $A \in \mathbf{F}_q^{n \times q^k}$. Then A is an $OA(q^k, n, q, d^\perp - 1)$.*

Each column of the orthogonal array corresponds to one of the pulses U_i in eq. (3) and we want to keep the set $\{U_{i+1}U_i^\dagger\}$ as small as possible. We are going to show next that for the arrays constructed from Theorem 1 this is always possible.

IV. DECOUPLING USING GRAY CODES

We illustrate Theorem 1 by a scheme for a small network consisting of 5 qubits. The finite field needed for this case is the field $\mathbf{F}_4 = \{0, 1, \omega, \overline{\omega}\}$ of four elements in which the relation $1 + \omega + \overline{\omega} = 0$ holds. The following is a generator matrix for the quadratic residue code [23] C over $\mathbf{F}_4$ with parameters $[5, 2, 4]$.

$$\begin{bmatrix} 1 & 0 & 1 & \overline{\omega} & \overline{\omega} \\ 0 & 1 & \overline{\omega} & \overline{\omega} & 1 \end{bmatrix}$$

The dual code $C^\perp$ of this code again is defined over $\mathbf{F}_4$ and has parameters $[5, 3, 3]$. By taking all $4^2 = 16$ code-words in C as the columns of a matrix we obtain an $OA(16, 5, 4, 2)$. We now address the question how to arrange the columns of this 4×16 matrix. First, recall the Gray codes [24, 25] are Hamilton cycles for the groups $\mathbf{F}_2^n$ where the generator sets are the coordinate functions. For $\mathbf{F}_2^4$ a particular Gray code is given by the following sequence of binary strings:

$$\begin{bmatrix} 0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1 \\ 0&0&0&0&1&1&1&1&1&1&1&1&0&0&0&0 \\ 0&0&1&1&1&1&0&0&0&0&1&1&1&1&0&0 \\ 0&1&1&0&0&1&1&0&0&1&1&0&0&1&1&0 \end{bmatrix}. \quad (4)$$

Observe that from column c_i to c_{i+1} exactly one position is flipped. Overall we obtain a cyclic sequence which runs through all 16 elements of $\mathbf{F}_2^4$ exactly once. The order defined by the Gray code also defines an order of the vectors in $\mathbf{F}_4^2$. To obtain the corresponding elements in $\mathbf{F}_4^2$ we make the identification $(0,0) \mapsto 0$, $(0,1) \mapsto 1$, $(1,0) \mapsto \omega$, and $(1,1) \mapsto \overline{\omega}$. Using this identification we can now map all elements of $\mathbf{F}_4^2$ to elements of $\mathbf{F}_4^5$ using the linear code C. We obtain the following scheme for a system of five qubits:

$$\begin{bmatrix} 0&0&0&0&1&1&1&1&\overline{\omega}&\overline{\omega}&\overline{\omega}&\overline{\omega}&\omega&\omega&\omega&\omega \\ 0&1&\overline{\omega}&\omega&\omega&\overline{\omega}&1&0&0&1&\overline{\omega}&\omega&\omega&\overline{\omega}&1&0 \\ 0&\overline{\omega}&\omega&1&0&\overline{\omega}&\omega&1&\overline{\omega}&0&1&\omega&\overline{\omega}&0&1&\omega \\ 0&\overline{\omega}&\omega&1&\omega&1&0&\overline{\omega}&\omega&1&0&\overline{\omega}&0&\overline{\omega}&\omega&1 \\ 0&1&\overline{\omega}&\omega&1&0&\omega&\overline{\omega}&\omega&\overline{\omega}&1&0&\overline{\omega}&\omega&0&1 \end{bmatrix}$$

Hence there are four basic pulses $\pi_1, \ldots, \pi_4$ corresponding to those columns in (4) which are elementary vectors $e_1, \ldots, e_4$, i. e., columns 2, 4, 8, and 16. The corresponding operators are $\pi_1 = \mathbf{1}_2 \otimes \sigma_1 \otimes \sigma_3 \otimes \sigma_3 \otimes \sigma_1$, $\pi_2 = \mathbf{1}_2 \otimes \sigma_2 \otimes \sigma_1 \otimes \sigma_1 \otimes \sigma_2$, $\pi_3 = \sigma_1 \otimes \mathbf{1}_2 \otimes \sigma_1 \otimes \sigma_3 \otimes \sigma_3$, $\pi_4 = \sigma_2 \otimes \mathbf{1}_2 \otimes \sigma_2 \otimes \sigma_1 \otimes \sigma_1$. The order in which they have to be applied can be read off from the transitions in (4), i. e., we obtain the following pulse sequence:

$$\pi_1, \pi_2, \pi_1, \pi_3, \pi_1, \pi_2, \pi_1, \pi_4, \pi_1, \pi_2, \pi_1, \pi_3, \pi_1, \pi_2, \pi_1, \pi_4.$$

We now turn to the question how to generalize this to more general networks and show that pulse sequences obtained from linear codes have the property that the number of different pulses grows logarithmically with the

number of spins. In order to apply Theorem 1 we have to find linear codes over $\mathbf{F}_4$ for which the minimum distance of the dual code is at least 3.

Let q be a prime power and let $m \in \mathbf{N}$. The Hamming code $H_{q,m}$ of length $n := (q^m-1)/(q-1)$ is a single-error correcting linear code with parameters $[n, n-m, 3]_q$. The corresponding dual code $H_{q,m}^{\perp}$ has parameters $[n, m, q^{m-1}]$. By specializing $q = 4$ and by using Theorem 1 for $H_{4,m}^{\perp}$ we therefore obtain orthogonal arrays with parameters $OA(N, n, 4, 2)$, where $n = (4^m-1)/3$ and $N = 4^{n-m}$ for any choice of $m \in \mathbf{N}$.

The procedure to obtain a pulse sequence for a network of n spin-$\frac{1}{2}$ particles, where n_0 is an arbitrary natural number, i. e., not necessarily of the form $n = (4^m - 1)/3$ is as follows: first let $m \in \mathbf{N}$ be the unique integer such that $n_0 \leq \frac{4^m-1}{3} \leq 4n_0$. Then construct the orthogonal array with parameters $OA(4^m, (4^m-1)/3, 4, 2)$. The columns of this orthogonal array are codewords of $H_{4,m}^{\perp} \subseteq \mathbf{F}_4^{(4^m-1)/3}$. We will use only the first n_0 rows of this $\frac{4^m-1}{3} - m \times \frac{4^m-1}{3}$ array. Since $H_{4,m}^{\perp} \cong \mathbf{F}_4^m$, we can find the desired Hamilton cycle by choosing a Gray code on $\mathbf{F}_2^{2m}$, i. e., we can decouple using $2m$ different pulses.

Higher Dimensional Systems.— So far we have only considered spin-$\frac{1}{2}$ particles, i. e., networks consisting of qubits. Methods exist to decouple Hamiltonians also in case the dimension of the individual nodes is greater than two [4, 5]. Basically, for one node of dimension $d \geq 2$ the requirement to switch off the time evolution of this node is to apply all d^2 elements of a unitary operator basis $\{U_{i,j} : i, j = 0, \ldots, d-1\}$. For any pair of nodes we have to apply all d^4 elements of a tensor product basis $\{U_{i,j} \otimes U_{k,\ell} : i, j, k, \ell = 0, \ldots, d-1\}$. These pulses can be arranged like in the previous schemes using orthogonal arrays. By combining the construction of orthogonal arrays from Hamming codes over the alphabet $\mathbf{F}_{2^{2\alpha}}$, where $\alpha \in \mathbf{N}$, together with the Gray codes for $\mathbf{F}_{2^{2m}}$, which can be constructed as in Figure 1, we obtain schemes for networks of $n = (2^{2m} - 1)/3$ nodes (each of dimension 2^{α}) which use only $4 \log n$ different pulses.

Conclusions and Discussion.— We have shown that pulse sequences for decoupling in networks of qubits and higher-dimensional systems can be arranged in such a way that the number of different pulses needed is small. Using orthogonal arrays derived from Hamming codes over finite fields it has been shown that the number of different operations can be chosen to be of the order $O(\log n)$, where n is the number of nodes in the network. The method presented in this paper is based on Hamilton cycles in the Cayley graph of the group defined by the columns of an orthogonal array. The related graph theoretical concept of Eulerian cycles has been used recently for the problem of designing robust schemes for decoherence control [26, 27]. Since in this case the Hamiltonian of the system can be arbitrary, i. e., not necessarily of pair-interaction type, the task to decouple from an environment leads to a different control scenario. It would be of interest to determine whether the methods described in this paper can also be used to derive efficient schemes for robust Eulerian dynamical coupling.

The author thanks E. Knill, R. Laflamme, and P. Zanardi for valuable discussions. This work was supported in part by NSA and ARDA under the ARDA Quantum Computing Program. The author also acknowledges support by CFI, ORDCF, and MITACS.

[1] J. A. Jones and E. Knill, J. Magn. Res. **141**, 323 (1999).
[2] C. H. Bennett, J. I. Cirac, M. S. Leifer, D. W. Leung, N. Linden, S. Popescu, and G. Vidal, Phys. Rev. A **66**, 012305 (2002).
[3] D. Leung, Journal of Modern Optics **49**, 1199 (2002).
[4] Wocjan, P. and Rötteler, M. and Janzing, D. and Beth, Th., Phys. Rev. A **65**, 042309 (2002).
[5] M. A. Nielsen, M. J. Bremner, J. L. Dodd, A. M. Childs, and C. M. Dawson, Phys. Rev. A **66**, 022317 (2002).
[6] J. L. Dodd, M. A. Nielsen, M. J. Bremner, and R. T. Thew, Phys. Rev. A **65**, 040301 (2002).
[7] L. Viola and S. Lloyd, Phys. Rev. A **58**, 2733 (1998).
[8] L. Viola, E. Knill, and S. Lloyd, Phys. Rev. Lett. **82**, 2417 (1999).
[9] L. Viola, S. Lloyd, and E. Knill, Phys. Rev. Lett. **83**, 4888 (1999).
[10] P. Zanardi, Phys. Rev. A **63**, 012301 (2001).
[11] M. Stollsteimer and G. Mahler, Phys. Rev. A **64**, 052301 (2001).
[12] C. P. Slichter, *Principles of Magnetic Resonance* (Springer, 1990), 3rd ed.
[13] R. R. Ernst, G. Bodenhausen, and A. Wokaun, *Principles of nuclear magnetic resonance in one and two dimension* (Clarendon Press, Oxford, 1987).
[14] U. Haeberlen, *High resolution NMR in solids, Selective Averaging* (Academic Press, New York, 1976).
[15] J. Schwinger, Proc. Nat. Acad. Sci. U.S.A. **46**, 570 (1960).
[16] E. Knill (1996), LANL preprint quant-ph/9608048.
[17] A. Klappenecker and M. Rötteler, IEEE Trans. Inform. Theory **48**, 2392 (2002).
[18] C. Godsil and G. Royle, *Algebraic Graph Theory*, vol. 207 of *Graduate Texts in Mathematics* (Springer, 2001).
[19] S. J. Curran and J. A. Gallian, Discrete Mathematics **156**, 1 (1996).
[20] C. H. Papadimitriou and K. Steiglitz, *Combinatorial Optimization* (Prentice-Hall, New Jersey, 1982).
[21] Th. Beth, D. Jungnickel, and H. Lenz, *Design Theory*, vol. I (Cambridge University Press, 1999), 2nd ed.
[22] A. S. Hedayat, N. J. A. Sloane, and J. Stufken, *Orthogonal Arrays*, Springer Series in Statistics (Springer, 1999).
[23] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes* (North-Holland, 1977).
[24] E. N. Gilbert, Bell Systems Tech. J. **37**, 815 (1958).
[25] C. Savage, SIAM Review **39**, 605 (1997).
[26] L. Viola and E. Knill, Phys. Rev. Lett. **90**, 037901 (2003).
[27] L. Viola (2004), arXiv preprint quant–ph/0404038.