

# Improved bounded-strength decoupling schemes for local Hamiltonians

Adam D. Bookatz

*Center for Theoretical Physics, Massachusetts Institute of Technology, Cambridge, MA, U.S.A.*

Martin Roetteler

*Microsoft Research, Quantum Architectures and Computation Group, Redmond, WA, U.S.A.*

Pawel Wocjan

*Department of Electrical Engineering and Computer Science,  
University of Central Florida, Orlando, FL, U.S.A*

We address the task of switching off the Hamiltonian of a system by removing all internal and system-environment couplings. We propose dynamical decoupling schemes, that use only bounded-strength controls, for quantum many-body systems with local system Hamiltonians and local environmental couplings. To do so, we introduce the combinatorial concept of balanced-cycle orthogonal arrays (BOAs) and show how to construct them from classical error-correcting codes. The derived decoupling schemes may be useful as a primitive for more complex schemes, e.g., for Hamiltonian simulation. For the case of  $n$  qubits and a 2-local Hamiltonian, the length of the resulting decoupling scheme scales as  $O(n \log n)$ , improving over the previously best-known schemes that scaled quadratically with  $n$ . More generally, using balanced-cycle orthogonal arrays constructed from families of BCH codes, we show that bounded-strength decoupling for any  $\ell$ -local Hamiltonian, where  $\ell \geq 2$ , can be achieved using decoupling schemes of length at most  $O(n^{\ell-1} \log n)$ .

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

## I. INTRODUCTION

Consider a quantum system of  $n$  interacting  $d$ -dimensional qudits with a time-independent (possibly unknown) Hamiltonian  $H$  acting on a Hilbert space  $\mathcal{H} \cong (\mathbb{C}^d)^{\otimes n}$ . We make the assumption that the system is  $\ell$ -local, i.e. that  $H$  can be written as the sum of operators, each of which acts only on  $\ell$  of the  $n$  qudits. In nature it is usually the case that  $\ell$  is small even when  $n$  is large. Without loss of generality, we also take  $H$  to be traceless, and for technical reasons, we assume that  $d$  is a prime power (which includes the important case of qubits, i.e.  $d = 2$ ).

We consider the task of *decoupling*, i.e. effectively switching off the Hamiltonian  $H$  (including removing any couplings to the environment) so that the system effectively evolves under the zero Hamiltonian. Such a task is important, for example, in the context of quantum memory, where one desires to preserve the state of a quantum system.

To achieve this task, we assume that the natural dynamics of the system can be modified by adjoining an open-loop (non-feedback) controller according to

$$H \mapsto H + H_c(t).$$

In practice, physical limitations restrict the types of control Hamiltonians available for use. We consider the realistic setting in which  $H_c(t)$  is only 1-local, i.e. due to our limited control of the system,  $H_c$  is the sum of operators that each act on only one qudit. We further impose the constraint that our control Hamiltonian  $H_c(t)$  is limited to be bounded-strength, i.e. a sufficiently smooth bounded function. This is in contrast to the setting of bang-bang control in which  $H_c(t)$  can be a discontinuous function that takes values of arbitrarily large norm. Our assumptions that the system Hamiltonian is an  $\ell$ -local Hamiltonian acting on a system of  $n$  interacting qudits and that the control Hamiltonian is a 1-local bounded-strength Hamiltonian reflect the typical composite nature of quantum systems and their coupling locality as well as the limitations in implementing external controls.

Viola and Knill proposed a general method for bounded-strength decoupling; see [1] and [2, Chapter 4]. Their method, often referred to as *Eulerian decoupling*, relies on Eulerian cycles in Cayley graphs of a control group — a certain finite group of control unitaries that can be implemented by switching on control Hamiltonians, from a finite set of available control operations, for a fixed time. The Eulerian cycle dictates which control Hamiltonians are applied in the different time-slots of the decoupling protocol.

The Eulerian method, as introduced in [1], does not make it possible to directly leverage the fact that the system Hamiltonian is  $\ell$ -local in order to obtain more efficient decoupling schemes. However, in the setting of bang-bang control there do exist efficient decoupling schemes that are specifically designed for composite quantum systems with  $\ell$ -local system Hamiltonians; see [3–5] and [2, Chapter 15]. In these schemes, the specification of which bang-bang

control unitaries are to be applied is chosen according to the entries of so-called *orthogonal arrays of strength  $\ell$* . They are matrices with the property that any submatrix formed by an arbitrary collection of  $\ell$  rows satisfies a certain balancedness condition.

The work [6] presented a particular construction of decoupling schemes merging the approaches of Eulerian (bounded-strength) decoupling together with orthogonal array (bang-bang) decoupling. This construction yields schemes that require only bounded-strength controls and exploit the composite structure of the quantum system (namely, the locality of the system Hamiltonian) to achieve decoupling with fewer control operations. To do so, these schemes introduce the concept of so-called *Eulerian orthogonal arrays*.

The purpose of the present paper is to further improve upon the method of [6] to obtain even more efficient bounded-strength decoupling schemes. To this end, we first generalize the Eulerian method due to [1] by showing that it is also possible to achieve decoupling with the help of so-called *balanced cycles*, which encompass Eulerian cycles as a special case. We then show that bounded-strength decoupling of composite quantum systems with local Hamiltonians can be accomplished based on the new concept of *balanced-cycle orthogonal arrays*.

Note that all the schemes discussed above can also be applied to the situation of a general open quantum system with joint Hamiltonian  $H$  acting on a quantum system that is coupled to an uncontrollable environment. Such a Hamiltonian has the form

$$H = H_S \otimes \mathbb{1}_B + \mathbb{1}_S \otimes H_B + \sum_{\alpha} S_{\alpha} \otimes B_{\alpha},$$

where the operators  $H_S$  and  $S_{\alpha}$  act on the system and where the operators  $H_B$  and  $B_{\alpha}$  act on the environment. We assume that the system Hamiltonian  $H_S$  and the operators  $S_{\alpha}$  are all  $\ell$ -local. The decoupling goal in this case is to effectively switch off the system Hamiltonian  $H_S$  and remove all couplings to the environment. If, using controls that act only on the system, one can effectively switch off all generic system Hamiltonians, then such an operation will switch off  $H_S$  and each  $S_{\alpha}$ , thereby accomplishing decoupling.<sup>1</sup> For notational simplicity, the remainder of the paper will therefore ignore the environment and treat only the case of effectively switching off an arbitrary  $\ell$ -local operator  $H$ .

## II. DESCRIPTION OF THE CONTROL-THEORETIC MODEL

Consider the group  $(\mathbb{F}_q, +)$ , the additive group of the finite field of order  $q = d^2$ , where  $d$  (the dimension of the qudits) is some prime power. For the remainder of this paper, let  $\rho : \mathbb{F}_q \rightarrow \mathcal{U}(d)$  be a faithful, irreducible, unitary, projective<sup>2</sup> representation that maps the elements of  $\mathbb{F}_q$  to  $d \times d$  unitary matrices, say  $\rho : g \mapsto U_g$ . That  $q$  cannot be smaller than  $d^2$  for such a representation will be justified later in Remark 2; that  $q = d^2$  suffices is justified by the explicit example shown below.

We assume that for every  $g \in \mathbb{F}_q$  we can implement  $U_g$  on any qudit of our system in the following sense: for every  $g$ , we can physically implement, over time  $\delta \in [0, \Delta]$ , a bounded-strength single-qudit Hamiltonian  $h_g(\delta)$ , corresponding to a single-qudit unitary evolution operator  $u_g(\delta)$ , such that  $U_g = u_g(\Delta)$  where  $\Delta$  is some fixed length of time. We assume that we can do this on any qudit and, moreover, that we can do so for each of the  $n$  qudits in parallel. Note that this assumption obeys the practical control limitations discussed earlier.

Of particular interest, in the case of qubits ( $d = 2, q = 4$ ) we can consider the representation  $\rho : \mathbb{F}_4 \rightarrow \mathcal{U}(2)$  that maps the four elements of  $\mathbb{F}_4$  to the four  $2 \times 2$  Pauli matrices  $\{\mathbb{1}, X, Y, Z\}$ . Thus, it is assumed that we can physically implement any Pauli operator on any qubit. Rather than assuming that  $q = 4$ , this paper will treat  $q$  more generally; however the reader is invited to think of the special case of qubits if desired. For non-qubits, with  $q > 4$ , we can generalize this example as follows. For a prime  $p$ , define  $\tilde{X} = \sum_{j=0}^{p-1} |j+1 \bmod p\rangle\langle j|$  and  $\tilde{Z} = \sum_{j=0}^{p-1} \omega^j |j\rangle\langle j|$ , where  $\omega$  is a  $p^{\text{th}}$  root of unity. For prime  $d = p$ , the map  $(a, b) \mapsto \tilde{X}^a \tilde{Z}^b$  defines a faithful, irreducible, unitary, projective representation from  $\mathbb{Z}_d \times \mathbb{Z}_d$  to  $\mathcal{U}(d)$ . For a prime power  $d = p^e$  (for some  $e$ ), map  $((a_1, b_1), \dots, (a_e, b_e)) \mapsto \tilde{X}^{a_1} \tilde{Z}^{b_1} \otimes \dots \otimes \tilde{X}^{a_e} \tilde{Z}^{b_e}$ .

A decoupling protocol is defined by specifying a sequence of control Hamiltonians (equivalently, control unitaries) to be applied. As shown in Fig. 1, we construct an  $n \times N$  array with entries from  $\mathbb{F}_q$ , which we regard as a sequence of  $N$  columns from  $\mathbb{F}_q^n$ . The  $j$ th column  $\vec{g}_j = (g_{1j}, \dots, g_{nj})^T$  corresponds to the  $j$ th time interval  $[(j-1)\Delta, j\Delta]$  of our protocol, during which we apply the control Hamiltonian

$$h_{\vec{g}_j}(\delta) = h_{g_{1j}}(\delta) \otimes \mathbb{1} \otimes \dots \otimes \mathbb{1} \quad + \dots + \quad \mathbb{1} \otimes \dots \otimes \mathbb{1} \otimes h_{g_{nj}}(\delta)$$

<sup>1</sup> The remaining Hamiltonian term of  $\mathbb{1}_S \otimes H_B$  is inconsequential, as it does not affect the system at all.

<sup>2</sup> Projective representations need only be homomorphisms up to phase, i.e. obey  $U_{g+h} \propto U_g U_h$  with proportionality rather than equality.

time slot	$0 - \Delta$	$\Delta - 2\Delta$	...	$(N-1)\Delta - N\Delta$	
qudit number	1	$g_{11}$	$g_{12}$	...	$g_{1N}$
	2	$g_{21}$	$g_{22}$	...	$g_{2N}$
	$\vdots$	$\vdots$	$\vdots$		$\vdots$
	$n$	$g_{n1}$	$g_{n2}$	...	$g_{nN}$
column vector	$\vec{g}_1$	$\vec{g}_2$	...	$\vec{g}_N$	
apply Hamiltonian	$h_{\vec{g}_1}(\delta)$	$h_{\vec{g}_2}(\delta)$	...	$h_{\vec{g}_N}(\delta)$	

FIG. 1: An  $n \times N$  array, with each entry  $g_{ij} \in \mathbb{F}_q$ , shown within the dashed lines. Rows correspond to qudit numbers, columns to time slots (each of width  $\Delta$ ). This array encapsulates the control sequence, with  $H_c(t) = h_{\vec{g}_j}(\delta)$  over  $\delta \in [0, \Delta)$  during the interval  $t \in [(j-1)\Delta, j\Delta)$ .

that gives rise to evolution  $u_{\vec{g}_j}(\delta) = u_{g_{1j}}(\delta) \otimes \cdots \otimes u_{g_{nj}}(\delta)$  over  $\delta \in [0, \Delta]$ . In other words, for each  $\delta \in [0, \Delta]$  and  $j = 1, \dots, N$ ,  $H_c(t) = h_{\vec{g}_j}(\delta)$  where  $t = (j-1)\Delta + \delta$ . The total time required to apply the entire sequence, i.e. the control cycle length, is therefore  $T_c = N\Delta$ , at which point the control sequence can be repeated. Observe that for any  $t = (j-1)\Delta + \delta$ , the unitary evolution  $U_c(t)$  corresponding to the control Hamiltonian consequently satisfies  $U_c(t) = u_{\vec{g}_j}(\delta)U_c((j-1)\Delta)$ .

According to average Hamiltonian theory [7-9], the resulting system evolution under  $H + H_c(t)$  can be effectively approximated by

$$U(t) \approx e^{-i\bar{H}^{(0)}t}$$

at times  $t$  that are integer multiples of  $T_c$ , i.e.  $t = mT_c$  for any  $m \in \mathbb{N}$ , where

$$\bar{H}^{(0)} = \frac{1}{T_c} \int_{t=0}^{T_c} U_c(t)^\dagger H U_c(t) dt$$

is time-independent and where  $U_c(t)$  is the time evolution due to  $H_c(t)$  alone. The goal of decoupling, therefore, is to choose  $U_c(t)$  such that  $\bar{H}^{(0)} = 0$  for any  $H$ . It is in this sense that we effectively switch off the Hamiltonian  $H$ . We refer the reader to [10] for a detailed description of the above control-theoretic model and the resulting effective time-evolution. We note, in particular, that although the approximation above is to leading order (in the Magnus expansion of  $U_c(t)^\dagger H U_c(t)$ ), the second-order term may be eliminated by designing the control Hamiltonian to satisfy  $U_c(t) = U_c(T_c - t)$  [9].

The efficiency of the protocol developed in this paper is obtained by exploiting the composite structure of the Hamiltonian, namely the fact that  $H$  was assumed to be a *local* Hamiltonian. By definition, an  $\ell$ -local Hamiltonian  $H$  on  $n$  qudits can be written as  $H = \sum_k H_k$ , where each  $H_k$  acts non-trivially on at most  $\ell$  of the  $n$  qudits. In particular, the  $\ell = 2$  case corresponds to Hamiltonians with only pairwise interactions. Our goal is to create a protocol that decouples each  $H_k$  simultaneously, and therefore decouples  $H$ . To see that this would work, observe that for any protocol  $U_c(t)$ ,

$$\bar{H}^{(0)} = \frac{1}{T_c} \int U_c(t)^\dagger H U_c(t) dt = \sum_k \frac{1}{T_c} \int U_c(t)^\dagger H_k U_c(t) dt = \sum_k \bar{H}_k^{(0)}.$$

### III. BALANCED CYCLES

The success of the decoupling protocol introduced in this paper will rely on some basic group theory, which we introduce now. Let  $\mathcal{G}$  be an Abelian group with a generating set  $\mathcal{S} \subset \mathcal{G}$ , i.e. any element of  $\mathcal{G}$  can be written as a sum of elements from  $\mathcal{S}$ .

**Definition 1 (Cayley graph).** The *Cayley graph*,  $\Gamma(\mathcal{G}, \mathcal{S})$ , of  $\mathcal{G}$  with respect to  $\mathcal{S}$  is a directed graph whose vertices are labeled by the group elements and whose edges are labeled by the generators. More precisely, there is a directed edge labeled  $s$  from vertex  $g \in \mathcal{G}$  to vertex  $h \in \mathcal{G}$  iff  $h = s + g$  for the generator  $s \in \mathcal{S}$ .

**Definition 2 (Cycle).** A *cycle*,  $\mathcal{L}$ , on  $\Gamma(\mathcal{G}, \mathcal{S})$  is a traversal on  $\Gamma$  that starts and ends on the same vertex. We describe the cycle by the ordered list  $\mathcal{L}_{\mathcal{G}} = (g_0, \dots, g_{N-1})$  of elements from  $\mathcal{G}$ , indicating the order in which the elements are visited, with the understanding that the cycle visits  $g_N = g_0$  immediately after visiting  $g_{N-1}$ . All the cycles in this paper visit every vertex at least once, so we assume without loss of generality that the first vertex is the identity element,  $e$ , of  $\mathcal{G}$ . With this assumption we may equivalently represent the cycle  $\mathcal{L}_{\mathcal{G}}$  by specifying the edges traversed, i.e.  $\mathcal{L}_{\mathcal{S}} = (s_1, \dots, s_N)$ , where  $g_j = s_j + g_{j-1}$  for  $j = 1, \dots, N$ ; note that we differentiate between these representations by the subscript on  $\mathcal{L}$ , but they both refer to the same cycle.

Note that a cycle may visit vertices more than once and may traverse edges multiple times. We will be interested not only in the vertices, but also the specific labels leaving each vertex; we denote by  $g \xrightarrow{s}$  the  $s$ -labeled edge leaving vertex  $g$ .

**Definition 3 (Balanced cycle).** We say that  $\mathcal{L}$  is a *balanced cycle* if  $\forall s \in \mathcal{S}, \exists \mu_s > 0$  such that  $\forall g \in \mathcal{G}, g \xrightarrow{s}$  occurs exactly  $\mu_s$  times; in other words, the cycle is balanced if it is balanced with respect to each label  $s \in \mathcal{S}$  in the sense that it leaves each  $g$  via label  $s$  an equal number of times (independent of  $g$ ). Consequently, each  $g$  will appear in  $\mathcal{L}$  precisely  $\lambda = \sum_{s \in \mathcal{S}} \mu_s$  times, independent of  $g$ . Because a Cayley graph is a regular directed graph, it always has a balanced cycle whose length is then necessarily  $N = \lambda|\mathcal{G}|$ .

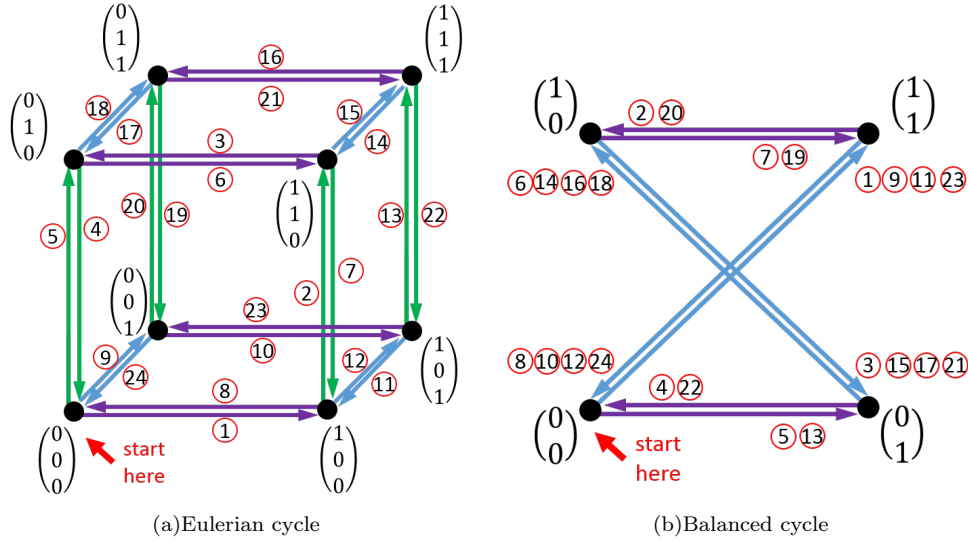


FIG. 2: (a) An Eulerian cycle on the Cayley graph  $\Gamma(\mathbb{Z}_2^3, \left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right\})$ , i.e. a balanced cycle in which each edge label leaves each vertex precisely once. Vertices correspond to the eight elements of  $\mathbb{Z}_2^3$ . Edge labels correspond to the three generators, namely  $\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$  (purple),  $\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$  (green), and  $\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$  (blue). The cycle starts at  $\begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$  and follows the path indicated (in ascending numerical order) by the circled integers (red). (b) A balanced cycle on the Cayley graph  $\Gamma(\mathbb{Z}_2^2, \left\{ \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\})$ . Vertices correspond to the four elements of  $\mathbb{Z}_2^2$ . Edge labels correspond to the two generators, namely  $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$  (purple) and  $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$  (blue). The cycle starts at  $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$  and follows the path indicated (in ascending numerical order) by the circled integers (red). Observe that the cycle is indeed balanced: for each of the two edge labels, the edges leave each vertex the same number of times, irrespective of vertex. Specifically, the  $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$  label leaves each vertex precisely  $\mu_{\begin{pmatrix} 0 \\ 1 \end{pmatrix}} = 2$  times, while the  $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$  label leaves each vertex precisely  $\mu_{\begin{pmatrix} 1 \\ 1 \end{pmatrix}} = 4$  times.

An important special case of a balanced cycle is an *Eulerian cycle* on  $\Gamma(\mathcal{G}, \mathcal{S})$ , for which  $\mu_s = 1$  for every  $s \in \mathcal{S}$ . Examples of an Eulerian cycle and a non-Eulerian balanced cycle are shown in Fig. 2(a) and Fig. 2(b) respectively. In [1], Eulerian cycles were used to define decoupling protocols that avoided the discontinuous nature of bang-bang

decoupling. More generally, one can define decoupling protocols based on balanced cycles (of which Eulerian decoupling is a special case), to which we now turn our attention. Note, however, that this balanced-cycle decoupling protocol will not be the goal of this paper. Indeed, such a protocol will not exploit the composite structure of the Hamiltonian. Later we will utilize the balanced-cycle decoupling on  $\ell$ -qudit subsystems of a larger  $n$  qudit space to develop more efficient protocols; in the current section, however, we may regard  $\ell$  as the size of the entire system.

In exploiting the  $\ell$ -local nature of  $H$ , we will find that we are primarily interested in the group

$$\mathcal{G} = \mathbb{F}_q^\ell = \{(a_1, \dots, a_\ell)^T : a_i \in \mathbb{F}_q\}$$

with some generating set  $\mathcal{S}$  and the representation

$$\rho^{\otimes \ell} : \mathcal{G} \rightarrow \mathcal{U}(d^\ell)$$

defined from our representation  $\rho : \mathbb{F}_q \rightarrow \mathcal{U}(d)$ . Specifically, if  $g = (a_1, \dots, a_\ell)^T \in \mathcal{G}$  and  $\rho(a_i) = U_{a_i}$  then  $\rho^{\otimes \ell}(g) = U_g = U_{a_1} \otimes \dots \otimes U_{a_\ell}$ . By our assumptions above, we can physically implement  $U_g$  by applying the control unitary  $u_g(\delta)$  (equivalently, the control Hamiltonian  $h_g(\delta)$ ) for time  $\Delta$ . For example, in the case of qubits ( $q = 4$ ), the group  $\mathbb{F}_4$ , whose elements we denote<sup>3</sup> as  $\{0, 1, \alpha, \alpha + 1\}$ , is generated by the set  $S_4 = \{1, \alpha\}$ . We choose  $\mathcal{S} = \{1^1, \alpha^1, \dots, 1^\ell, \alpha^\ell\}$ , which is a generating set of  $2\ell$  elements for the group  $\mathcal{G} = \mathbb{F}_4^\ell$ , where  $x^i$  here denotes the column  $(0, \dots, 0, x, 0, \dots, 0)^T$  with  $x \in \mathbb{F}_q$  in the  $i$ th position. In this case we assume  $\rho(a_i) = U_{a_i}$  is a Pauli matrix, so  $\rho^{\otimes \ell}(g)$  is a tensor product of Pauli matrices.

The purpose for the group theory used in this paper resides in the following observation [2, Chapter 4]. We define the operator  $\Pi_{\mathcal{G}}$  to act on matrices  $A$  as

$$\Pi_{\mathcal{G}}(A) = \frac{1}{|\mathcal{G}|} \sum_{g \in \mathcal{G}} U_g^\dagger A U_g. \quad (1)$$

Note that for every matrix  $A$ ,  $\Pi_{\mathcal{G}}(A)$  commutes with all  $U_g$  ( $g \in \mathcal{G}$ ). Thus, by Schur's lemma, since  $\rho$  is irreducible<sup>4</sup>, we have  $\Pi_{\mathcal{G}}(A) = \frac{\text{tr}(A)}{D} \mathbb{1}$  (where  $D$  is the dimension of the Hilbert space). In particular then, if  $\text{tr}(A) = 0$  then  $\Pi_{\mathcal{G}}(A) = 0$ .

**Protocol 1 (Bounded-strength balanced-cycle decoupling).** Let  $\mathfrak{L}$  be a balanced cycle on  $\Gamma(\mathcal{G}, \mathcal{S})$  of length  $N = |\mathcal{G}| \sum_{\delta} \mu_{\delta} = \lambda |\mathcal{G}|$ , with group element representation  $\mathfrak{L}_{\mathcal{G}} = (g_0, \dots, g_{N-1})$  and generator representation  $\mathfrak{L}_{\mathcal{S}} = (\delta_1, \dots, \delta_N)$ . For  $j = 1, \dots, N$ , set  $U_c(0) = U_{\varepsilon} = \mathbb{1}$  and

$$U_c((j-1)\Delta + \delta) = u_{\delta_j}(\delta) U_c((j-1)\Delta), \quad \delta \in [0, \Delta].$$

Note that because<sup>5</sup>  $U_{\delta_j} U_{g_{j-1}} = U_{\delta_j + g_{j-1}} = U_{g_j}$ , this implies  $U_c(j\Delta) = U_{g_j}$  (for  $j = 0, \dots, N$ ), i.e.

$$U_c((j-1)\Delta + \delta) = u_{\delta_j}(\delta) U_{g_{j-1}}, \quad \delta \in [0, \Delta]. \quad (2)$$

The control cycle length is thus  $T_c = N\Delta = |\mathcal{G}|\lambda\Delta$ .

**Theorem 1.** *The above balanced-cycle protocol performs bounded-strength decoupling.*

<sup>3</sup> Here the reader may prefer to equivalently think of the Abelian group as  $\{1, z, x, y = xz = zx\}$  with generating set  $S_4 = \{z, x\}$ . Then we can use  $\mathcal{S} = \{z^{(1)}, x^{(1)}, \dots, z^{(\ell)}, x^{(\ell)}\}$  and  $\rho(x) = X, \rho(y) = Y$ , and  $\rho(z) = Z$ . Be aware, however, that the group operation used throughout the paper is denoted by  $+$  rather than by multiplication, since it is inherited from the finite field.

<sup>4</sup> Schur's lemma guarantees this directly when  $\ell = 1$ . But then it also applies for  $\ell = 2$  since then for any matrix  $A = \sum_i B_i \otimes C_i$ , we have  $\Pi_{\mathcal{G}}(A) = \frac{1}{|\mathcal{G}|} \sum_i \sum_{a_1, a_2 \in \mathbb{F}_q} U_{a_1}^\dagger B_i U_{a_1} \otimes U_{a_2}^\dagger C_i U_{a_2} \propto \sum_i \text{tr} B_i \text{tr} C_i = \text{tr} \sum_i B_i \otimes C_i = \text{tr} A$ , and similarly for larger  $\ell$ .

<sup>5</sup> up to phase, since  $\rho$  is a projective representation; since we will only ever conjugate by  $U_c$ , the overall phase is irrelevant and we shall simply ignore it.

*Proof.* Since  $\mathcal{D}$  is a balanced cycle,  $g \xrightarrow{\bullet \Delta}$  occurs exactly  $\mu_\Delta$  times for every  $g, \Delta$  pair. Thus  $u_\Delta(\delta)U_g$  appears exactly  $\mu_\Delta$  times in the protocol for each  $\Delta, g$ , and so we have, for any traceless  $d^\ell \times d^\ell$  Hamiltonian  $H$ ,

$$\begin{aligned} \bar{H}^{(0)} &= \frac{1}{T_c} \int_{t=0}^{T_c} U_c(t)^\dagger H U_c(t) dt \\ &= \frac{1}{T_c} \sum_g U_g^\dagger \left[ \sum_\Delta \mu_\Delta \int_{\delta=0}^\Delta u_\Delta(\delta)^\dagger H u_\Delta(\delta) d\delta \right] U_g \\ &= \Pi_{\mathcal{G}}(F_{\mathcal{S}}(H)) \end{aligned}$$

where  $\Pi_{\mathcal{G}}$  is defined in Eq. (1) and  $F_{\mathcal{S}}$  is defined by

$$F_{\mathcal{S}}(H) = \sum_\Delta \frac{\mu_\Delta}{\lambda \Delta} \int_{\delta=0}^\Delta u_\Delta(\delta)^\dagger H u_\Delta(\delta) d\delta. \quad (3)$$

Recall that  $\Pi_{\mathcal{G}}$  suppresses traceless matrices. Assuming that  $H$  is traceless, and observing that  $F_{\mathcal{S}}$  is trace-preserving, we have that  $\Pi_{\mathcal{G}}(F_{\mathcal{S}}(H)) = 0$ . We conclude that  $\bar{H}^{(0)} = 0$ , i.e. the protocol succeeds at decoupling.  $\square$

**Remark 1.** For simplicity, we have assumed that  $\rho$  is irreducible. Then this protocol works for any traceless time-independent  $H$ , even if  $H$  is unknown. It is possible to define protocols in which  $\rho$  is not irreducible, in which case  $\Pi_{\mathcal{G}}$  need not suppress all traceless matrices. However, in such a case, one must take special care to ensure that  $\Pi_{\mathcal{G}}$  still suppresses  $F_{\mathcal{S}}(H)$  for the Hamiltonians of interest. See [10] for examples in a similar context, as well as Example 3 later in this paper.

**Remark 2.** Although Protocol 1 performs bounded-strength decoupling, it would generally not be an efficient protocol were it applied to the entire system (i.e. if  $\ell$  were the number of qudits of the entire system). Assuming that  $\rho$  is irreducible, the representation  $\rho^{\otimes \ell} : \mathcal{G} \rightarrow \mathcal{U}(d^\ell)$  necessitates that  $|\mathcal{G}|$ , and therefore  $T_c$ , are exponential in  $\ell$ . Indeed, suppose we have a representation from  $\mathcal{G}$  to  $\mathcal{U}(D)$  such that for any  $D \times D$  matrix  $A$ ,  $\Pi_{\mathcal{G}}(A) = \frac{\text{tr}(A)}{D} \mathbb{1}_D$  as we used in Theorem 1. Consider sending the bipartite entangled state  $|\psi\rangle = \frac{1}{\sqrt{D}} \sum_{j=1}^D |j\rangle \otimes |j\rangle$ , or more precisely,  $\Psi = |\psi\rangle\langle\psi|$ , through the channel  $\mathcal{I} \otimes \Pi_{\mathcal{G}}$  (where  $\mathcal{I}$  is the identity channel on a  $D$ -dimensional space) obtaining

$$\sum_{g \in \mathcal{G}} \frac{1}{|\mathcal{G}|} (\mathbb{1}_D \otimes U_g^\dagger) \Psi (\mathbb{1}_D \otimes U_g) = (\mathcal{I} \otimes \Pi_{\mathcal{G}})(\Psi) = \frac{1}{D^2} \mathbb{1}_D \otimes \mathbb{1}_D = \frac{1}{D^2} \mathbb{1}_{D^2}.$$

The matrix rank of the right-hand side is  $D^2$ . Using the fact that  $\text{rank}(A+B) \leq \text{rank}(A) + \text{rank}(B)$  and that for each  $g$ ,  $\text{rank}(\frac{1}{|\mathcal{G}|} (\mathbb{1} \otimes U_g^\dagger) \Psi (\mathbb{1} \otimes U_g)) = \text{rank}(\Psi) = 1$ , the rank of the left-hand side is at most  $|\mathcal{G}|$ ; thus,  $|\mathcal{G}| \geq D^2$ . Therefore, for the representation  $\rho^{\otimes \ell} : \mathcal{G} \rightarrow \mathcal{U}(d^\ell)$  to succeed in the proof of Theorem 1, we require that  $|\mathcal{G}| \geq d^{2\ell}$ , which is exponential in  $\ell$ . Incidentally, by considering the case of  $\ell = 1$ , we have justified why we could not have chosen  $q$  less than  $d^2$  in our irreducible representation  $\rho : \mathbb{F}_q \rightarrow \mathcal{U}(d)$ .

Observe that the key to this protocol working is the fact that each  $u_\Delta(\delta)U_g$  shows up an equal number of times, independent of  $g$ , i.e.  $\forall \Delta \in \mathcal{S} \exists \mu_\Delta > 0$  such that  $\forall g \in \mathcal{G}$ ,  $g \xrightarrow{\bullet \Delta}$  occurs  $\mu_\Delta$  times (independent of  $g$ ). In an Eulerian cycle,  $\mu_\Delta = 1$  for every  $\Delta$ , which is certainly sufficient. All else being equal, given the choice between Eulerian and other balanced cycles, we would choose Eulerian cycles as they will minimize  $N$  and therefore  $T_c$ . However, we will see that when considering the composite properties of a system (specifically that interactions are local), we will be able to exploit the notion of balanced cycles to come up with a much more efficient protocol.

#### IV. BALANCED-CYCLE ORTHOGONAL ARRAYS

In Section II and Fig. 1, we indicated how we view our decoupling scheme as an array. For the protocol to be efficient, we shall ensure that this array corresponds to what we call a *balanced-cycle orthogonal array* (BOA). A BOA is a special type of orthogonal array (OA), which we first define. We refer the reader to [11] for a thorough introduction to OAs, particularly their relationship to linear codes (of which we shall later make use).

0	1	1	0	0	1	1	0
0	0	1	1	0	0	1	1
0	1	0	1	0	1	0	1
0	0	0	0	1	1	1	1
0	1	1	0	1	0	0	1
0	0	1	1	1	1	0	0
0	1	0	1	1	0	1	0

FIG. 3: Example of a  $OA_2(8, 7, 2, 2)$ , i.e. a  $OA_\lambda(N, n, q, \ell)$  with  $N = 8$  columns and  $n = 7$  rows on the finite field  $\mathbb{F}_q = \mathbb{Z}_2$  of order  $q = 2$ . Any subarray defined by any  $\ell = 2$  rows contains each 2-tuple precisely  $\lambda = 2$  times. For example, rows 5 and 7 (highlighted) form a  $2 \times 8$  subarray in which  $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$ ,  $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ ,  $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ , and  $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$  each occur precisely twice. Note that typically in this paper,  $q = d^2$  (for example, for qubits  $q = 4$ ), but for simplicity, the example in this figure uses  $q = 2$ .

For notational consistency, we point out that throughout the remainder of this paper we adopt the notation that  $\mathcal{G}$  and  $\mathcal{S}$  refer specifically to the group  $\mathbb{F}_q^\ell$  and a generating set for  $\mathbb{F}_q^\ell$ , respectively. Elements of  $\mathcal{G}$  will be denoted using script  $\mathfrak{g}$ , elements of  $\mathcal{S}$  will be denoted using script  $\mathfrak{s}$ , and cycles on  $\mathcal{G}$  will be denoted  $\mathfrak{L}$ . When other groups (such as  $\mathbb{F}_q$  or  $\mathbb{F}_q^n$ ) are being considered, other notation (such as  $g$ ,  $m$ ,  $S$ ,  $s$  and  $\mathcal{L}$ ) will be used instead.

**Definition 4 (Orthogonal array).** An  $OA_\lambda(N, n, q, \ell)$  *orthogonal array* on the alphabet  $\mathbb{F}_q$  is an  $n \times N$  array where each of the  $N$  columns is a vector from  $\mathbb{F}_q^n$  such that every  $\ell \times N$  subarray (obtained by only considering a selection of just  $\ell$  of the  $n$  rows) contains each possible  $\ell$ -tuple of elements of  $\mathbb{F}_q$  (i.e. contains each  $c \in \mathbb{F}_q^\ell$ ) precisely  $\lambda$  times as a column. The number  $\ell$  is called the *strength* of the OA.

**Remark 3.** To relate these numbers to those appearing elsewhere in this paper,

- $N$  will correspond to number of steps in the decoupling protocol (i.e. the length of our balanced cycle),
- $n$  will correspond to the number of  $d$ -dimensional qudits describing the system,
- $q = d^2$  (e.g. for qubits,  $d = 2$  and  $q = 4$ ),
- $\ell$  is the locality of the Hamiltonian (e.g. for pairwise interactions,  $\ell = 2$ ), and
- $\lambda = N/q^\ell$  will be the same  $\lambda$  as in our discussion of balanced cycles,  $\lambda = \sum_{\mathfrak{s}} \mu_{\mathfrak{s}}$ .

**Remark 4.** Note that the order of the columns in the OA is irrelevant to whether the array is an OA. Moreover, if  $A = [\vec{a}_i]$  is an  $OA_\lambda(N, n, q, \ell)$  with columns  $\vec{a}_1, \dots, \vec{a}_N$  then the matrix  $A'$ , whose columns consist of precisely  $r$  copies of each  $\vec{a}_i$  (in any order), is an  $OA_{r\lambda}(rN, n, q, \ell)$ . Note, however, that while the order of the columns does not affect the OA property of the array, when defining balanced-cycle orthogonal arrays (which we do next), we will be highly concerned with the order of the columns in the array.

An example of an  $OA_2(8, 7, 2, 2)$  is shown in Fig. 3. Orthogonal arrays have been used to construct bang-bang decoupling schemes (see [3–5] and [2, Chapter 15]). In order to construct a bounded-strength scheme, we introduce the notion of a balanced-cycle orthogonal array, defined as follows.

**Definition 5 (Balanced-cycle orthogonal array).** A  $BOA(N, n, q, \ell)$  *balanced-cycle orthogonal array* on the alphabet  $\mathbb{F}_q$  is an  $n \times N$  array,  $A$ , where each of the  $N$  columns is a vector from  $\mathbb{F}_q^n$  such that every  $\ell \times N$  subarray (obtained by only considering a selection of just  $\ell$  of the  $n$  rows) defines a balanced cycle on the Cayley graph of  $\mathcal{G} = \mathbb{F}_q^\ell$  with respect to some generating set for  $\mathcal{G}$  (which may depend on the subarray). Specifically, if the entries of  $A$  are denoted  $a_{ij}$  (with  $1 \leq i \leq n$  and  $0 \leq j \leq N - 1$ ), then for every choice of  $\ell$  distinct integers  $i_1, \dots, i_\ell \in \{1, \dots, n\}$ , there is a generating set  $\mathcal{S}$  for  $\mathcal{G}$  (which may, in general, depend on  $i_1, \dots, i_\ell$ ) such that if  $\mathfrak{g}_j = (a_{i_1 j}, \dots, a_{i_\ell j})^T$  denotes the  $j$ th column of  $A$  restricted to rows  $i_1, \dots, i_\ell$ , then  $\mathfrak{L}_{\mathcal{G}} = (\mathfrak{g}_0, \dots, \mathfrak{g}_{N-1})$  defines a balanced cycle on  $\Gamma(\mathcal{G}, \mathcal{S})$ .

An example of a BOA is shown in Fig. 4. We defer the proof that BOAs exist to Sec. V. The remainder of the current section defines a decoupling protocol based on BOAs and proves that it works to decouple  $\ell$ -local Hamiltonians in  $n$  qudit systems ( $\ell \leq n$ ). Working with  $\ell$  qudits (rather than  $n$  qudits), along with the promise that  $H$  is  $\ell$ -local, will enable us to give an efficient protocol.

	①	②	③	④	⑤	⑥	⑦	⑧	⑨	⑩	⑪	⑫	⑬	⑭	⑮	⑯	⑰	⑱	⑲	⑳	㉑	㉒	㉓	㉔
0	1	1	0	0	0	1	1	0	0	1	1	1	1	1	1	0	0	0	0	0	1	1	0	
0	0	1	1	0	1	1	0	0	0	0	0	0	1	1	1	1	1	1	0	1	1	0	0	
0	1	0	1	0	1	0	1	0	0	1	1	1	0	0	0	1	1	1	0	1	0	1	0	
0	0	0	0	0	0	0	0	0	1	1	0	1	1	0	1	1	0	1	1	1	1	1	1	
0	1	1	0	0	0	1	1	0	1	0	1	0	0	1	0	1	0	1	1	1	0	0	1	
0	0	1	1	0	1	1	0	0	1	1	0	1	0	1	0	1	0	1	0	1	0	0	1	
0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	

FIG. 4: Example of a  $BOA(24, 7, 2, 2)$ , i.e. a  $BOA(N, n, q, \ell)$  with  $N = 24$  columns and  $n = 7$  rows on the finite field  $\mathbb{F}_q = \mathbb{Z}_2$  of order  $q = 2$ . Any subarray defined by any  $\ell = 2$  rows defines a balanced cycle on the Cayley graph  $\Gamma(\mathcal{G}, \mathcal{S})$  of  $\mathcal{G} = \mathbb{F}_q^\ell = \mathbb{Z}_2^2$  with respect to some generating set  $\mathcal{S}$  (which may depend on the subarray). For example, rows 5 and 7 (highlighted) form a  $2 \times 24$  subarray that defines the balanced cycle shown in Fig. 2(b). The circled integers (red) correspond to the steps taken by the balanced cycle as shown in that figure. Note that typically in this paper,  $q = d^2$  (for example, for qubits  $q = 4$ ), but for simplicity, the BOA example shown here uses  $q = 2$ . The method by which this BOA was constructed is detailed in Example 1 of Sec. VIII.

**Protocol 2 (Efficient, bounded-strength balanced-cycle decoupling based on BOAs).** Let  $A = [\vec{a}_j]_{j=0, \dots, N-1}$  be a  $BOA(N, n, q, \ell)$  whose columns are denoted by the vectors  $\vec{a}_j = (a_{1j}, \dots, a_{nj})^T$ , where  $a_{ij} \in \mathbb{F}_q$  is the  $(i, j)$  entry of  $A$ . For  $j = 1, \dots, N$ , let  $\vec{b}_j = \vec{a}_j - \vec{a}_{j-1}$  be the transitions between the columns, treating  $\vec{a}_N = \vec{a}_0 = 0$ . For  $j = 1, \dots, N$ , set  $U_c(0) = \mathbb{1}$  and

$$U_c((j-1)\Delta + \delta) = u_{\vec{b}_j}(\delta) U_c((j-1)\Delta), \quad \delta \in [0, \Delta];$$

note that this implies that  $U_c(j\Delta) = U_{\vec{a}_j}$  (for  $j = 0, \dots, N$ ). The control cycle length is thus  $T_c = N\Delta$ .

**Theorem 2.** *The above protocol performs bounded-strength decoupling.*

*Proof.*  $H$  is an  $\ell$ -local Hamiltonian,  $H = \sum_k H_k$  with each  $H_k$  acting non-trivially on at most  $\ell$  qudits. Consider a term  $H_k$ , which acts non-trivially only on qudits denoted  $i_1, \dots, i_\ell$  and write  $H_k = h_k \otimes \mathbb{1}_{n-\ell}$ , where  $h_k$  is understood to be a  $d^\ell \times d^\ell$  matrix acting only on these  $\ell$  qudits and  $\mathbb{1}_{n-\ell}$  is the identity matrix on the other  $n - \ell$  qudits. By definition of a BOA, the  $\ell \times N$  subarray of  $A$  restricted to rows  $i_1, \dots, i_\ell$  defines a balanced cycle  $\mathcal{L}$  on  $\Gamma(\mathcal{G}, \mathcal{S})$  where  $\mathcal{S}$  is some generating set of  $\mathcal{G} = \mathbb{F}_q^\ell$ . The idea of the proof is to observe that the protocol involving the columns  $\vec{a}_j$  for decoupling  $H_k$  is equivalent to a protocol involving the subarray's columns for decoupling  $h_k$ ; since the subarray defines a balanced cycle, we can then invoke Protocol 1 to successfully decouple  $h_k$  and therefore  $H_k$ .

Let  $g_j = (a_{i_1 j}, \dots, a_{i_\ell j})^T$  denote the  $j$ th column of  $A$  restricted to rows  $i_1, \dots, i_\ell$  and let  $s_j = g_j - g_{j-1} = (b_{i_1 j}, \dots, b_{i_\ell j})^T$ , where  $b_{ij}$  is the  $i$ th entry of  $\vec{b}_j$ . Then the cycle  $\mathcal{L}$  is represented as  $\mathcal{L}_{\mathcal{G}} = (g_0, \dots, g_{N-1})$  and  $\mathcal{L}_{\mathcal{S}} = (s_1, \dots, s_N)$ .

As in the proof of Theorem 1, we are interested in  $U_c(t)^\dagger H_k U_c(t)$ . The control unitary at time  $t = (j-1)\Delta + \delta$  is

$$U_c((j-1)\Delta + \delta) = u_{\vec{b}_j}(\delta) U_c((j-1)\Delta) = u_{\vec{b}_j}(\delta) U_{\vec{a}_{j-1}} = (u_{b_{i_1 j}}(\delta) \otimes \dots \otimes u_{b_{i_\ell j}}(\delta)) (U_{a_{i_1(j-1)}} \otimes \dots \otimes U_{a_{i_\ell(j-1)}}).$$

Thus, when conjugating  $H_k = h_k \otimes \mathbb{1}_{n-\ell}$  by  $U_c((j-1)\Delta + \delta)$ , all of the unitaries not acting on the  $\ell$ -qudit subspace of  $h_k$  will commute through  $H_k$  and cancel, leaving only those corresponding to the  $\ell$ -qudit subspace, i.e. those corresponding to the labels  $s_j$  and  $g_j$ . Explicitly,

$$\begin{aligned} U_c((j-1)\Delta + \delta)^\dagger H_k U_c((j-1)\Delta + \delta) &= \left[ \left( U_{a_{i_1(j-1)}}^\dagger \otimes \dots \otimes U_{a_{i_\ell(j-1)}}^\dagger \right) \left( u_{b_{i_1 j}}(\delta)^\dagger \otimes \dots \otimes u_{b_{i_\ell j}}(\delta)^\dagger \right) h_k \right. \\ &\quad \left. \left( u_{b_{i_1 j}}(\delta) \otimes \dots \otimes u_{b_{i_\ell j}}(\delta) \right) \left( U_{a_{i_1(j-1)}} \otimes \dots \otimes U_{a_{i_\ell(j-1)}} \right) \right] \otimes \mathbb{1}_{n-\ell} \\ &= U_{g_{j-1}}^\dagger u_{s_j}(\delta)^\dagger h_k u_{s_j}(\delta) U_{g_{j-1}} \otimes \mathbb{1}_{n-\ell}. \end{aligned}$$

Thus, the protocol of applying  $U_c$  to  $H_k$  is effectively the same as applying a protocol  $u_{s_j}(\delta) U_{g_{j-1}}$  to  $h_k$ , following the balanced cycle  $\mathcal{L}$ . Since this is precisely the scheme defined in Protocol 1 applied to  $h_k$  (see Eq. (2)), we conclude



from Theorem 1 that it decouples  $h_k$ . Consequently,  $\bar{H}_k^{(0)} = \bar{h}_k^{(0)} \otimes \mathbb{1}_{n-\ell} = 0$ . This occurs for every term  $H_k$  in  $H = \sum_k H_k$ , whence  $H$  itself is decoupled:  $\bar{H}^{(0)} = \sum_k \bar{H}_k^{(0)} = 0$ .  $\square$

**Remark 5.** Once we have a BOA scheme that can decouple a system of  $n$  qudits, the same scheme can be used (with the same BOA and therefore same length  $N$ ) for a system of  $n' < n$  qudits. This can be accomplished by simply ignoring  $n - n'$  of the qudits, i.e. by having  $U_c$  act as  $\mathbb{1}$  on these  $n - n'$  extra qudits (rather than as dictated by the original protocol). The proof of Theorem 2 remains unaffected because  $H_k$  acts trivially on these extra qudits, i.e. they are not acted upon by  $h_k$ .

Theorem 2 showed that decoupling protocols based on BOAs work, with control cycle length proportional to the BOA parameter  $N$ . We next show that BOAs can indeed be constructed and, moreover, that the construction gives rise to an *efficient* decoupling protocol, in the sense that  $N$  does not increase exponentially with  $n$ .

## V. CONSTRUCTION OF BALANCED-CYCLE ORTHOGONAL ARRAYS

The existence of balanced-cycle orthogonal arrays follows naturally from constructions of orthogonal arrays generated using classical linear codes, which we shall define shortly. We first give a brief outline of our BOA construction. This construction is via the generator matrix  $G$  of a linear code, which is a linear mapping from  $\mathbb{F}_q^k$  to  $\mathbb{F}_q^n$  for some  $k \leq n$ . If we enumerate all elements of  $\mathbb{F}_q^k$  in an arbitrary order and consider their image under  $G$ , this will form an OA of strength  $\ell$  (for an appropriately chosen  $k$ ). To obtain a BOA, we do this enumeration according to the prescription of an Eulerian cycle on  $\mathbb{F}_q^k$ . In doing so, we can guarantee that we always obtain a balanced cycle when we consider any submatrix of  $\ell$  rows, ultimately ensuring that any  $\ell$ -local Hamiltonian term on those corresponding qudits will be decoupled. We now prove this, starting with a definition of a classical linear code.

**Definition 6 (Classical linear code).** A *classical linear*  $[n, k]_q$  code,  $C$ , is a  $k$ -dimensional subspace of the vector space  $\mathbb{F}_q^n$ . For any vector  $x = (x_1, \dots, x_n)^T \in \mathbb{F}_q^n$ , define  $\text{wt}(x) = |\{i \in \{1, \dots, n\} : x_i \neq 0\}|$ . The *distance* of a linear code  $C$  is defined to be  $\min\{\text{wt}(c) : c \in C, c \neq o\}$ , where  $o$  denotes the zero vector. An  $[n, k]_q$  linear code can be described by a *generator matrix*  $G$  of size  $n \times k$  with entries from  $\mathbb{F}_q$ .  $G$  maps the vectors  $m \in \mathbb{F}_q^k$  onto the elements (*code words*) of  $C$  so that  $C = G[\mathbb{F}_q^k] = \{Gm \in \mathbb{F}_q^n : m \in \mathbb{F}_q^k\}$ .

The dual code  $C^\perp$  of  $C$  is defined by  $C^\perp = \{y \in \mathbb{F}_q^n : x \cdot y = 0 \forall x \in C\}$  with the dot product  $x \cdot y = \sum_{i=1}^n x_i y_i$ . The dual code is also a classical linear code, namely an  $[n, n - k]_q$  code with some distance  $\delta^\perp$  that we will refer to as the *dual distance*. Orthogonal arrays can be constructed from linear codes, as the following theorem [11, Theorem 4.6] establishes.

**Theorem 3 (OAs from linear codes).** Let  $C$  be a linear  $[n, k]_q$  code with dual distance  $\delta^\perp$ . The  $n \times q^k$  matrix  $[Gm]_{m \in \mathbb{F}_q^k}$ , whose columns are the  $q^k$  vectors  $Gm \in \mathbb{F}_q^n$  ( $\forall m \in \mathbb{F}_q^k$ ), is an OA( $q^k, n, q, \ell$ ) with strength  $\ell = \delta^\perp - 1$ .

Let  $C$  be an  $[n, k]_q$  with dual distance  $\delta^\perp = \ell + 1$  and generating matrix  $G$ . Let  $\mathcal{L}$  be an Eulerian cycle on the Cayley graph  $\Gamma(\mathbb{F}_q^k, S_q^{(k)})$ , where  $S_q^{(k)}$  is a generating set for  $\mathbb{F}_q^k$ ; thus, we can write  $\mathcal{L}_{\mathbb{F}_q^k} = (m_0, \dots, m_{N-1})$  with transitions  $\mathcal{L}_{S_q^{(k)}} = (s_1, \dots, s_N)$  and  $N = q^k |S_q^{(k)}|$ . Because  $d$  is a prime power, say  $d = p^e$  for some prime  $p$ , the minimal generating set is of size  $|S_q^{(k)}| = 2ke$ . We are interested in the image of the cycle in the codespace; thus, consider the Eulerian cycle, denoted  $G\mathcal{L}$ , on  $\Gamma(G[\mathbb{F}_q^k], G[S_q^{(k)}])$ , where  $G[\mathbb{F}_q^k] = C \subset \mathbb{F}_q^n$  is the image of  $\mathbb{F}_q^k$  under  $G$ , i.e. is the codespace. In other words,  $G\mathcal{L}_{\mathbb{F}_q^k} = (Gm_0, \dots, Gm_{N-1})$  and  $G\mathcal{L}_{S_q^{(k)}} = (Gs_1, \dots, Gs_N)$ .

To avoid possible confusion, we emphasize here that although we will use  $G\mathcal{L}$  to construct a BOA, neither  $\mathcal{L}$  nor  $G\mathcal{L}$  will serve as the balanced cycle to which Theorem 1 applies (which is why we have used the notation  $\mathcal{L}$  rather than  $\mathfrak{L}$ ). Rather, for our efficient decoupling scheme, we construct an array  $A_{G\mathcal{L}}$ , dictated by  $G\mathcal{L}$ , and prove that the result is a BOA by showing that if we consider any subarray of  $\ell$  rows, it gives rise to some balanced cycle  $\mathfrak{L}$  on  $\mathcal{G} = \mathbb{F}_q^\ell$ . The notation and relationships of the various groups and cycles used in this paper is sketched in Fig. 5.

We turn  $G\mathcal{L}$  into an array  $A_{G\mathcal{L}}$  in the obvious way as follows. Each element  $Gm_j$  of  $G\mathcal{L}_{\mathbb{F}_q^k}$  is a column vector in  $\mathbb{F}_q^n$ . Therefore we may associate to  $G\mathcal{L}$  the  $n \times N$  matrix  $A_{G\mathcal{L}} = [Gm]_{m \in \mathcal{L}_{\mathbb{F}_q^k}}$  with elements  $a_{ij} = (Gm_j)_i$ , so that the  $j$ th column of  $A_{G\mathcal{L}}$  is the vector  $Gm_j$ , and the columns are arranged in the order of the Eulerian cycle  $G\mathcal{L}$ . Note that since we assumed that Eulerian cycles always start with the (additive) identity element, i.e. the zero vector  $o \in \mathbb{F}_q^k$ , and since  $G$  maps the zero vector to the zero vector ( $Go = o \in \mathbb{F}_q^n$ ), the first column of  $A_{G\mathcal{L}}$  is the zero vector of  $\mathbb{F}_q^n$ .

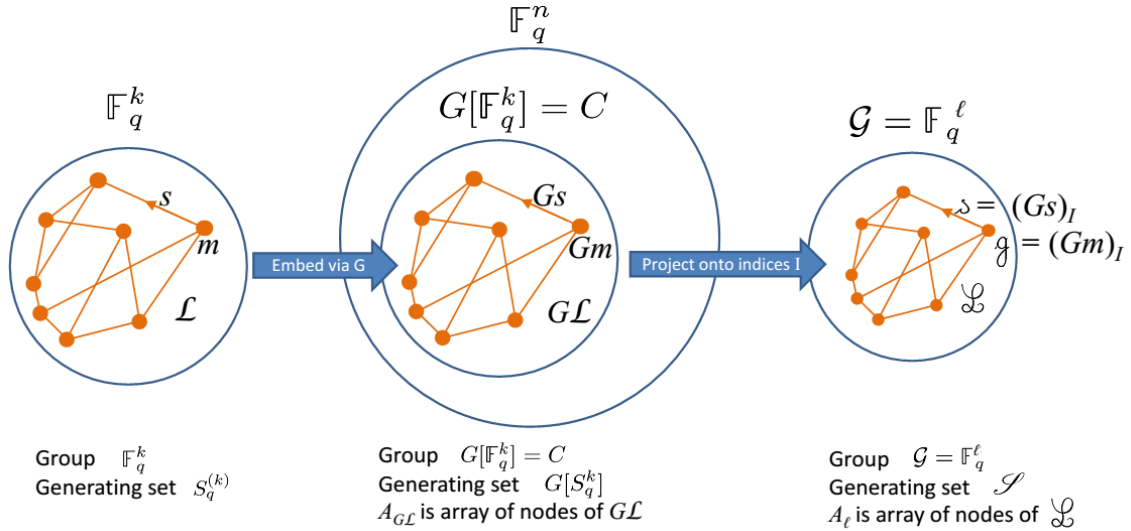


FIG. 5: Names and relationships between various groups and cycles in the BOA construction. The graph is a schematic of a Cayley graph. As explained in the text, the BOA,  $A_{G\mathcal{L}}$ , is the array form of  $G\mathcal{L}$ , which is the result of mapping an Eulerian cycle  $\mathcal{L}$  under the linear code generating matrix  $G$ . As a BOA,  $A_{G\mathcal{L}}$  has the property that if one considers a subarray of  $\ell$  rows, the result describes a balanced cycle. Specifically, let  $I \subset \{1, 2, \dots, n\}$  be a subset of  $\ell$  indices.  $(Gm)_I$  denotes the  $\ell$ -tuple of elements of  $Gm$  (itself an  $n$ -tuple) corresponding to the indices  $I$ . The cycle  $\mathcal{L}$ , composed of nodes  $(Gm)_I$  (in the same order in which  $\mathcal{L}$  was composed of  $m$ ), is shown to be a balanced cycle.

**Lemma 1.**  $A_{G\mathcal{L}}$  is an  $OA_{N/q^\ell}(N, n, q, \ell)$  with  $N = q^k |S_q^{(k)}|$ .

*Proof.* By Theorem 3, an array whose  $q^k$  columns are the vectors of the codespace is an OA. The columns of  $A_{G\mathcal{L}}$  are precisely  $|S_q^{(k)}|$  copies of each vector in the codespace, and therefore (using Remark 4),  $A_{G\mathcal{L}}$  is an OA.  $\square$

Let  $s \in S_q^{(k)}$ .  $Gs \in \mathbb{F}_q^n$ , so  $Gs = ((Gs)_1, \dots, (Gs)_n)^T$ , where we use the notation  $(Gs)_i \in \mathbb{F}_q$  to denote the  $i$ th component of the column vector  $Gs$ . Fix  $\ell$  distinct numbers  $i_1, \dots, i_\ell \in \{1, \dots, n\}$  and write  $I = \{i_1, \dots, i_\ell\}$ . Let  $(Gs)_I$  denote the  $\ell$ -tuple  $((Gs)_{i_1}, \dots, (Gs)_{i_\ell})^T$ . Let  $\mathcal{S} = \{(Gs)_I : s \in S_q^{(k)}\}$ .

**Lemma 2.**  $\mathcal{S}$  is a generating set for  $\mathcal{G} = \mathbb{F}_q^\ell$ .

*Proof.* Let  $\mathfrak{g} \in \mathcal{G}$ . By definition, since  $A_{G\mathcal{L}} = [Gm]_{m \in \mathcal{L}_{\mathbb{F}_q^k}}$  is an OA of strength  $\ell$ , the  $\ell \times N$  subarray obtained by only considering rows  $i_1, \dots, i_\ell$  contains each possible  $\ell$ -tuple of elements of  $\mathbb{F}_q$ , and therefore contains  $\mathfrak{g}$ . Thus,  $\exists Gm$  such that  $(Gm)_I = \mathfrak{g}$ . Since  $S_q^{(k)}$  is a generating set for  $\mathbb{F}_q^k$ ,  $\exists u_1, \dots, u_r \in S_q^{(k)}$  such that  $m = u_1 + \dots + u_r$ , and therefore  $Gm = Gu_1 + \dots + Gu_r$ . But then  $(Gu_j)_I \in \mathcal{S}$  for every  $j = 1, \dots, r$  and  $\mathfrak{g} = (Gm)_I = (Gu_1)_I + \dots + (Gu_r)_I$ , whence  $\mathcal{S}$  generates  $\mathcal{G}$ .  $\square$

Recall  $A_{G\mathcal{L}} = [Gm]_{m \in \mathcal{L}_{\mathbb{F}_q^k}}$  and consider the  $\ell \times N$  submatrix  $A_\ell = [g_j]$  of  $A_{G\mathcal{L}}$ , whose  $j$ th column is  $g_j = (Gm_j)_I \in \mathcal{G}$ . Define the ordered list  $\mathfrak{L}_\mathcal{G} = (g_0, \dots, g_{N-1})$ . Although  $\mathfrak{L}_\mathcal{G}$  depends on  $I$ , we suppress mention of this for notational simplicity.

**Lemma 3.**  $\mathfrak{L}_\mathcal{G}$  is a balanced cycle on  $\Gamma(\mathcal{G}, \mathcal{S})$ .

*Proof.* Each  $\mathfrak{g} \in \mathcal{G}$  is present in  $\mathfrak{L}_\mathcal{G}$  an equal number of times because  $A_{G\mathcal{L}}$  is an OA of strength  $\ell$ . The transitions in this cycle are  $\delta_j = g_j - g_{j-1} = (Gm_j)_I - (Gm_{j-1})_I = (Gs_j)_I \in \mathcal{S}$ , so the transition representation  $\mathfrak{L}_\mathcal{G} = (\delta_1, \dots, \delta_N)$  consists of generators from  $\mathcal{S}$ ;  $\mathfrak{L}_\mathcal{G}$  is therefore a cycle on the Cayley graph  $\Gamma(\mathcal{G}, \mathcal{S})$ . Moreover, because  $\mathcal{L}$  is an Eulerian cycle and  $A_{G\mathcal{L}}$  is an OA,  $\mathfrak{L}_\mathcal{G}$  is a balanced cycle (although not an Eulerian cycle): informally, each  $Gm \xrightarrow{Gs}$  occurs in

$G\mathcal{L}$  an equal (non-zero) number of times (namely once, independent of  $Gm$ ) for each  $Gs$ , so each  $g \xrightarrow{\Delta}$  occurs in  $\mathcal{L}$  an equal (non-zero) number of times (independent of  $g = (Gm)_I$ , since  $A_{G\mathcal{L}}$  is an OA) for each  $s = (Gs)_I$ .

Explicitly, consider any  $g \in \mathcal{G}$  and  $s \in \mathcal{S}$ . Let  $M_g = \{m \in \mathbb{F}_q^k : (Gm)_I = g\}$ .  $\mathcal{L}_{\mathbb{F}_q^k}$  is an Eulerian cycle so each element in  $\mathbb{F}_q^k$  shows up precisely  $|S_q^{(k)}|$  times in  $\mathcal{L}_{\mathbb{F}_q^k}$ . In particular, therefore, each  $m \in M_g$  appears precisely  $|S_q^{(k)}|$  times in  $\mathcal{L}_{\mathbb{F}_q^k}$ , and consequently,  $g$  shows up in  $\mathcal{L}$  precisely  $|M_g||S_q^{(k)}|$  times. But  $A_{G\mathcal{L}}$  is an OA of strength  $\ell$ , so  $|M_g||S_q^{(k)}|$  must then be independent of  $g$ , and therefore  $|M_g|$  is also independent of  $g$ . Since  $s \in \mathcal{S}$ , let  $S_s = \{s \in S_q^{(k)} : (Gs)_I = s\}$ . This set is non-empty by definition of  $\mathcal{S}$ . In general,  $|S_s|$  may depend on  $s$ . Now,  $\forall m \in M_g$  and  $\forall s \in S_s$ , the Eulerian property of  $\mathcal{L}$  guarantees that  $Gm \xrightarrow{Gs}$  occurs precisely once in  $G\mathcal{L}$ . Therefore,  $g \xrightarrow{\Delta}$  occurs in  $\mathcal{L}$  precisely  $|S_s||M_g| \geq 1$  times, which is independent of  $g$ . Thus  $\mathcal{L}$  is a balanced cycle.  $\square$

Together, the above lemmas prove the existence of BOAs and how to construct them from classical linear codes.

**Theorem 4.** *Let  $C$ ,  $\mathcal{L}$ , and  $A_{G\mathcal{L}}$  be as above, i.e.  $C$  is an  $[n, k]_q$  code with dual distance  $\delta^\perp = \ell + 1$  and generating matrix  $G$ ,  $\mathcal{L}$  is an Eulerian cycle on the Cayley graph  $\Gamma(\mathbb{F}_q^k, S_q^{(k)})$ , written  $\mathcal{L}_{\mathbb{F}_q^k} = (m_0, \dots, m_{N-1})$  and  $\mathcal{L}_{S_q^{(k)}} = (s_1, \dots, s_N)$ , and  $A_{G\mathcal{L}} = [Gm]_{m \in \mathcal{L}_{\mathbb{F}_q^k}}$  is an OA whose columns are the vectors  $Gm_j$ . Then  $A_{G\mathcal{L}}$  is a BOA( $N, n, q, \ell$ ) with  $N = q^k |S_q^{(k)}|$ .*

*Proof.* For every choice of  $\ell$  distinct integers  $I = \{i_1, \dots, i_\ell\} \subset \{1, \dots, n\}$ , the set  $\mathcal{S} = \{(Gs)_I : s \in S_q^{(k)}\}$  is a generating set for  $\mathcal{G}$  (by Lemma 2) such that if  $g_j$  denotes the  $j$ th column of  $A_{G\mathcal{L}}$  restricted to rows  $i_1, \dots, i_\ell$ , then (by Lemma 3)  $\mathcal{L}_{\mathcal{G}} = (g_0, \dots, g_{N-1})$  defines a balanced cycle on  $\Gamma(\mathcal{G}, \mathcal{S})$ .  $\square$

For  $n$  interacting qudits of dimension  $d = p^e$  (for some prime  $p$  and positive integer  $e$ ) that obey an  $\ell$ -local Hamiltonian, this construction therefore allows

$$N = q^k |S_q^{(k)}| = q^k 2k\ell e \quad (4)$$

where  $k$  is the dimension of the code used and  $q = d^2$ . Observe that the BOA decoupling protocol (Protocol 2) for this BOA construction has a control cycle length of  $T_c = N\Delta = d^{2k} 2k\ell e \Delta$  where  $\Delta$  is some fixed length of time. For example, in the qubit ( $d = 2$ ) case discussed above,  $|S_4^{(k)}| = 2k$ , whence  $T_c = N\Delta$  with  $N = (2k)4^k$ . To maximize efficiency for a given  $n$  and  $\ell$ , one should select a code that minimizes  $k$  (equivalently, select a dual code that maximizes  $k^\perp = n - k$ ).

There exist many good families of classical linear codes. For instance, for 2-local interactions, we can (as was done in [12] for OAs) rely on  $[n, k]_q$  Hamming codes with dual distance 3 such that  $k = \log_q((q-1)n+1)$ ; our scheme then has  $N$  scaling like  $n \log(n)$ . This protocol is therefore much more efficient than a naive protocol of applying balanced-cycle decoupling (including Eulerian decoupling) without exploiting the  $\ell$ -local structure of the Hamiltonian, which would have a control cycle length that scales exponentially with  $n$ . It is also more efficient than the method of [6], which required  $N = d^{4k}$ , i.e. whose scaling for this case ( $\ell = 2$ , using Hamming codes) is quadratic in  $n$ . Next, we address codes for BOA construction with values of  $\ell$  greater than 2.

## VI. BOA DECOUPLING SCHEMES FROM BCH CODES

In this section we show how to construct schemes that achieve decoupling for  $\ell$ -local Hamiltonians on  $\mathcal{H} \cong (\mathbb{C}^d)^{\otimes n}$  for arbitrary  $\ell$ ,  $n$ , and prime power  $d$ . Besides the machinery of balanced-cycle orthogonal arrays (BOAs) that was introduced in the previous sections, our construction relies on BCH codes as a particular vehicle to construct good BOAs. The choice of BCH codes results from the fact that they are among the best known codes for the particular situation where the distance is a fixed, small number and the goal is to maximize the overall code dimension. Using the dual of a BCH code when constructing the corresponding orthogonal arrays, we obtain schemes with a designed OA strength (i.e. locality  $\ell$ ) while having a small  $N$  in the corresponding decoupling protocol. We begin by briefly recalling some basics about BCH codes; for more details on finite fields and BCH codes see, for example, the textbooks [13–15].

**Definition 7 (BCH code).** Let  $\alpha$  be a primitive  $n$ -th root of unity in the finite field  $\mathbb{F}_{q^m}$ , where  $q$  is a prime power,  $n \geq 2$ , and  $m \geq 1$ . A *BCH code* over  $\mathbb{F}_q$  of length  $n$  and designed distance  $D$ , where  $2 \leq D \leq n$ , is a cyclic polynomial code defined by the zeros

$$\alpha^b, \alpha^{b+1}, \dots, \alpha^{b+D-2},$$

where  $b \geq 1$  is a positive integer.

The generator polynomial  $g(x)$  of the cyclic code introduced in Definition 7 is given by  $g(x) = \text{lcm}(M_b(x), M_{b+1}(x), \dots, M_{b+D-2}(x))$ , where  $M_i(x)$  denotes the minimal polynomial of  $\alpha^i$  over  $\mathbb{F}_q$ . Note that even though the zeros of the code lie in an extension field  $\mathbb{F}_{q^m}$  over  $\mathbb{F}_q$ , the BCH code itself is a cyclic code over the ground field  $\mathbb{F}_q$ . Furthermore, it is known that a BCH code defined this way has a distance  $\delta$  that is at least  $D$ , which is why  $D$  is sometimes called the ‘‘designed distance.’’ Note that the actual distance  $\delta$  of the code might exceed  $D$ . The possible lengths of BCH codes are quite restricted, as any admissible length  $n$  must be a divisor of the order of the multiplicative group of  $\mathbb{F}_{q^m}$ , i.e. must be a divisor of  $q^m - 1$ . In the following we restrict ourselves to the case where  $n = q^m - 1$ , which is called the case of *primitive BCH codes*. Furthermore we only consider the case where  $b = 1$ , which is called the case of *narrow-sense BCH codes*. We denote these codes by  $\text{BCH}(\mathbb{F}_{q^m}/\mathbb{F}_q, D)$ , and we note that they always exist.

For any linear error-correcting code  $C = [n, k, \delta]_q$  of length  $n$ , dimension  $k$ , and distance  $\delta$ , an *extension*  $C' = [n+1, k, \delta']_q$  can be defined by adding another coordinate and an overall parity check. At the level of parity check matrices, this corresponds to appending the parity check matrix  $M$  of  $C$  with an all-zeros column  $\mathbf{0}$  and an all-ones row  $\mathbf{1}^T$  so that  $C'$  has the new parity check matrix  $\begin{bmatrix} \mathbf{1}^T & 1 \\ M & \mathbf{0} \end{bmatrix}$ . For binary codes, the distance of the extension is easy to characterize: if  $\delta \equiv 0 \pmod{2}$  then  $\delta' = \delta$  and if  $\delta \equiv 1 \pmod{2}$  then  $\delta' = \delta + 1$ . In general over larger alphabets, however, it is possible that the distance increases even when  $\delta$  is even. When applying an extension to the BCH codes introduced above, we use the notation  $\text{BCH}^{\text{ext}}(\mathbb{F}_{q^m}/\mathbb{F}_q, D)$ . We make use of the following theorem about such codes.

**Theorem 5.** *Let  $\mathbb{F}_q$  be a finite field and let  $\text{BCH}^{\text{ext}}(\mathbb{F}_{q^m}/\mathbb{F}_q, D) = [n, k, \delta]_q$  be the extension of the primitive narrow-sense BCH code with designed distance  $D$  constructed in Definition 7, so  $n = q^m$  and  $\delta \geq D$ . Assume that  $D \leq q^{\lceil m/2 \rceil} + 2$ . Then the dimension  $k$  of the code satisfies  $k \geq n - m \lceil \frac{q-1}{q}(D-2) \rceil - 1 \geq n - m(D-2) - 1$ .*

See [16] for a proof of Theorem 5 that leverages the fact that the extended primitive narrow-sense BCH codes are subfield subcodes of the Reed-Solomon codes. See also [15, Problem 8.12] and [17]. By combining Theorem 5 with the construction of Theorem 4 we now obtain the following result regarding bounded-strength decoupling for  $\ell$ -local Hamiltonians.

**Theorem 6.** *For any  $\ell \geq 2$ ,  $n \geq (\ell-1)^2$ , and  $q = d^2$  with  $d \geq 2$  a prime power, there exists a BOA( $N, n, q, \ell$ ) whose length  $N$  scales as  $N = O(n^{\ell-1} \log n)$ . That is, there exists a bounded-strength BOA decoupling scheme to switch off  $\ell$ -local Hamiltonians on  $n$  interacting  $d$ -dimensional qudits that uses  $N = O(n^{\ell-1} \log n)$  time slices.*

*Proof.* First, note that if  $n$  is not of the special form  $n = q^m$  where  $m \geq 1$ , then we can always embed the  $n$  qudits into a larger system of  $q^m$  qudits with  $m = \lceil \log_q(n) \rceil$ , construct a scheme for the larger system, and ignore the additional qudits (as per Remark 5). This increases  $n$  by a factor of at most  $q$  and therefore doesn’t affect the statement of the theorem, i.e. we can without loss of generality assume that  $n = q^m$  where  $m \geq 1$ .

Now, we consider the code  $C$  that is the *dual* of a  $k^\perp$ -dimensional  $\text{BCH}^{\text{ext}}(\mathbb{F}_{q^m}/\mathbb{F}_q, D)$  code with designed distance  $D = \ell + 1$ . Thus  $C$  has length  $n$ , dual distance  $\delta^\perp \geq D = \ell + 1$ , and, according to Theorem 5, dimension  $k = n - k^\perp \leq m(D-2) + 1 = m(\ell-1) + 1$ . By Theorem 3, this means that we can construct an  $n \times N_{OA}$  orthogonal array of strength  $\delta^\perp - 1 \geq \ell$  from this code, where  $N_{OA} = q^k \leq q^{m(\ell-1)+1} = qn^{\ell-1}$ . According to Theorem 4, the corresponding BOA has an overhead that scales at most logarithmically in  $n$  since from Eq. (4) we obtain the following bound on the length of the bounded-strength decoupling scheme corresponding to the BOA:  $N_{BOA} = q^k |S_q^{(k)}| = q^k 2ke \leq [qn^{\ell-1}] [2(m(\ell-1) + 1)e] = 2qen^{\ell-1} [(\ell-1) \log_q n + 1] = O(n^{\ell-1} \log n)$ . This establishes the claimed bound.  $\square$

In physical systems, the locality  $\ell$  is generally a small fixed number, so the requirement of  $n \geq (\ell-1)^2$  is inconsequential asymptotically, while for small  $n$ , one can (by Remark 5) always artificially increase  $n$  to satisfy it. Our main focus in Theorem 6 is on the asymptotic cost for fixed locality  $\ell$  as the number  $n$  of qudits grows. It should be noted that, depending on the particular choice of  $q$ ,  $\ell$ , and  $n$ , further improvements over the bound in Theorem 6 are possible; see e.g., [17, 18]. This in turn leads to further improvements in the length of the decoupling schemes constructed via Theorem 4. For instance, for 2-local qubit Hamiltonians we saw at the end of Sec. V that Hamming codes can be used to construct BOA decoupling schemes of length  $N = 2[3n+1] \log_4[3n+1]$ , giving a slight improvement over schemes constructed from primitive BCH codes which lead to a scaling of  $N \leq 8n[\log_4(n) + 1]$ .

$\ell \setminus N$	64	384	2 048	10 240	49 152	229 376	1 048 576
2	2–5 <sup>a</sup>	6–21 <sup>a</sup>	22–85 <sup>a</sup>	86–341 <sup>a</sup>	342–1 365 <sup>a</sup>	1 366–5 461 <sup>a</sup>	5 462–21 845 <sup>a</sup>
3	-	3–6 <sup>b</sup>	7–17 <sup>c</sup>	18–41 <sup>c</sup>	42–126 <sup>c</sup>	127–288 <sup>c</sup>	289–756 <sup>c</sup>
4	-	-	4–5	6–11 <sup>d</sup>	12–21 <sup>e</sup>	22–43	44–85
5	-	-	-	5–6	7–12 <sup>f</sup>	13–20	21–27
6	-	-	-	-	6–7	8–9	10–17
7	-	-	-	-	-	7–8	9–10
8	-	-	-	-	-	-	8–9

TABLE I: Table of the best known balanced-cycle orthogonal arrays (BOAs) for qubit ( $d = 2$ ) systems, indicating the number of qubits that can be decoupled by a BOA scheme for the given locality and length. Shown are the locality  $\ell$  of the underlying Hamiltonian from 2 up to 8 and length  $N = 4^k 2k$  of the BOA cycles from 64 up to 1 048 576, corresponding to the values  $k = 2, \dots, 8$  in Eq. (4) with  $q = 4$  and  $e = 1$ . Each entry in the table denotes the range of the number  $n$  of qubits that can be achieved by a BOA scheme of the corresponding locality and length. For instance, the entry 7–17 at location (3, 2 048) indicates that in order to decouple a 3-local Hamiltonian on a system with  $n$  qubits, where  $n \in \{7, \dots, 17\}$ , the best known BOA schemes have 2 048 time steps. If the number of qubits is one higher, e. g.,  $n = 18$ , then the currently best known BOA scheme would require 10 240 time steps. Superscripts indicate if the dual codes  $[n, k^\perp, \delta^\perp]_4$  underlying the BOAs were obtained by a particular construction: a) all codes for  $\ell = 2$  were obtained from the Hamming code family  $[n, n - k, 3]_4$  with  $k = \log_4(3n + 1)$ ; b) the code  $[6, 3, 4]_4$  is the Hexacode [13]; c) the codes with parameters  $[17, 13, 4]_4$ ,  $[41, 36, 4]_4$ ,  $[126, 120, 4]_4$ ,  $[288, 281, 4]_4$ , and  $[756, 748, 4]_4$  are based on caps in finite projective spaces which are sets of points of which no three are collinear, see [18]; d) the code  $[11, 6, 5]_4$  is a quadratic residue code, see [11, 5.13] and [13]; e) the code  $[21, 15, 5]_4$  is the Kschischang-Pasupathy code, see [20]; and f) the code  $[12, 6, 6]_4$  is a quadratic residue code, see [11, 5.13] and [13]. All other codes in the table are based on the database of best known linear codes that is available in Magma [19].

$\ell \setminus N$	324	4 374	52 488	590 490	6 377 292	66 961 566
2	2–10 <sup>a</sup>	11–91 <sup>a</sup>	92–820 <sup>a</sup>	821–7 381 <sup>a</sup>	7 382–66 430 <sup>a</sup>	66 431–597 871 <sup>a</sup>
3	-	3–10 <sup>b</sup>	11–82 <sup>b</sup>	83–212 <sup>b</sup>	213–840 <sup>b</sup>	841–6 723 <sup>b</sup>
4	-	-	4–10	11–20	21–72	73–96
5	-	-	-	5–10	11–16	17–73
6	-	-	-	-	6–10	11–17
7	-	-	-	-	-	7–10

TABLE II: Table of the best known balanced-cycle orthogonal arrays (BOAs) for qutrit ( $d = 3$ ) systems, indicating the number of qutrits that can be decoupled by a BOA scheme for the given locality and length. Shown are the locality  $\ell$  of the underlying Hamiltonian from 2 up to 7 and length  $N = 9^k 2k$  of the BOA cycles from 324 up to 66 961 566, corresponding to the values  $k = 2, \dots, 7$  in Eq. (4) with  $q = 9$  and  $e = 1$ . Each entry in the table denotes the range of the number  $n$  of qutrits that can be achieved by a BOA scheme of the corresponding locality and length. Superscripts indicate if the dual codes  $[n, k^\perp, \delta^\perp]_9$  underlying the BOAs were obtained by a particular construction: a) all codes for  $\ell = 2$  were obtained from the Hamming code family  $[n, n - k, 3]_9$  with  $k = \log_9(8n + 1)$ ; and b) the codes with parameters  $[10, 7, 4]_9$ ,  $[82, 78, 4]_9$ ,  $[212, 207, 4]_9$ ,  $[840, 834, 4]_9$ , and  $[6 723, 6 716, 4]_9$  are based on caps in finite projective spaces, see [18]. All other codes in the table are based on the database of best known linear codes that is available in Magma [19].

## VII. TABLES OF BEST KNOWN BOA SCHEMES FOR SMALL SYSTEMS

In the following, we present a summary of the best known BOA schemes for qubit ( $d = 2$ ,  $q = 4$ ) and qutrit ( $d = 3$ ,  $q = 9$ ) systems for a variety of small localities  $\ell$  and system sizes  $n$ . All schemes are obtained by our main construction in Theorem 4, where the underlying classical linear codes are either taken from the literature or from the Magma [19] database of best known linear codes which can be accessed using the Magma command `BestDimensionLinearCode(<field>, <length>, <distance>)`.

Recall from Remark 5 that if we have a BOA decoupling scheme for  $n$  qudits, it can also be used for smaller systems of  $n' < n$  qudits. Therefore, the best known BOA for  $n$  qudits is also the best known BOA for all  $n' < n$  qudits unless a better BOA scheme for  $n'$  is known. Table I summarizes the best known schemes for systems of  $n$  qubits ( $d = 2$ ), for small values of  $n$ , that can be obtained from good linear codes. Similarly, Table II summarizes the best known schemes for systems of  $n$  qutrits ( $d = 3$ ), for small values of  $n$ .



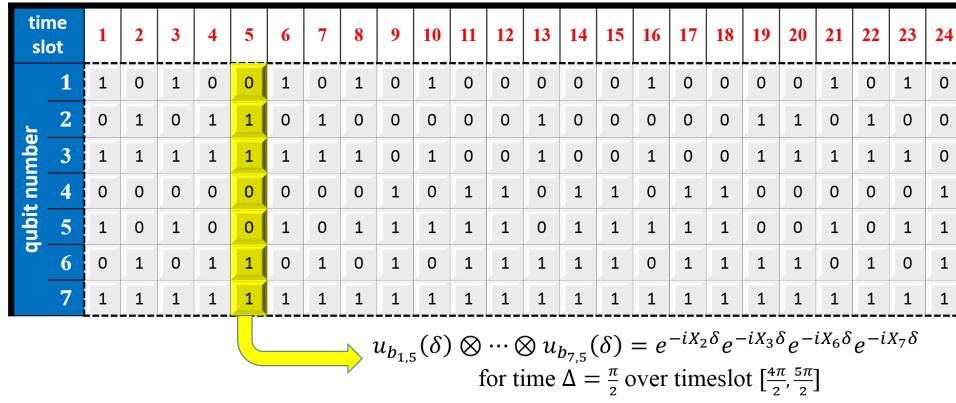


FIG. 6: A  $7 \times 24$  array defining the decoupling protocol in Example 1 in the format of Fig. 1. Rows correspond to qubit numbers, columns correspond to time slots (each of width  $\Delta = \frac{\pi}{2}$ ), and entries correspond to unitary operators on qubits according to Eq. 5. As per Protocol 2, the control cycle evolution is  $U_c((j-1)\Delta + \delta) = u_{\vec{b}_j}(\delta)U_c((j-1)\Delta)$ ,  $\delta \in [0, \Delta]$ , where  $\vec{b}_j$  is the  $j$ th column. For example, because  $\vec{b}_5 = (0, 1, 1, 0, 0, 1, 1)^T$ , we have  $u_{\vec{b}_5}(\delta) = u_0 \otimes u_1 \otimes u_1 \otimes u_0 \otimes u_0 \otimes u_1 \otimes u_1(\delta) = e^{-iX_2\delta} e^{-iX_3\delta} e^{-iX_6\delta} e^{-iX_7\delta}$ .

our choice of Eq. 5, which was chosen to be consistent with our representation  $\rho$ . For example, in time slot 5, the transition column is  $\vec{b}_5 = (0, 1, 1, 0, 0, 1, 1)^T$ , which corresponds to the unitary

$$u_{\vec{b}_5}(\delta) = e^{-iX_2\delta} e^{-iX_3\delta} e^{-iX_6\delta} e^{-iX_7\delta}$$

where  $X_i$  denotes the Pauli  $X$  operator on the  $i$ th qubit. As per Protocol 2, the control cycle evolution is  $U_c((j-1)\Delta + \delta) = u_{\vec{b}_j}(\delta)U_c((j-1)\Delta)$ ,  $\delta \in [0, \Delta]$ , where  $\vec{b}_j$  is the  $j$ th column in Fig. 6. This protocol will decouple any 2-local 7-qubit diagonal Hamiltonian.

We emphasize that in this simple diagonal-Hamiltonian example, we were able to use  $q = d = 2$  (for reasons that will be addressed in Example 3). If the Hamiltonian were not known to be diagonal, this would not in general have been possible, and we would have needed to instead use a  $[7, k]_q$  code for  $q = 4$ .

**Example 2 (2-local decoupling using a Hamming code).** Consider an arbitrary 2-local Hamiltonian  $H$  on a system of 5 qubits. Then  $H$  can be decoupled by applying a BOA derived from the code dual to a  $[5, 3, 3]_4$  Hamming code, namely the  $[5, 2]_4$  code over  $\mathbb{F}_4$  with the generator matrix

$$G = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & \alpha^2 \\ \alpha^2 & \alpha^2 \\ \alpha^2 & 1 \end{bmatrix},$$

where  $\alpha$  is a primitive element of order 3 of  $\mathbb{F}_4$ . Note that we arrange the code words as *column* vectors, consistent with the notation used throughout this paper and some – but not all – of the literature. Since here  $k = 2$ ,  $d = 2$ , and  $e = 1$ , the corresponding BOA has a total number of time steps given by  $N = d^{2k}2ke = 64$ . When arranged into the columns of a  $5 \times 64$  matrix, each of the 64 control Hamiltonians that are applied in this scheme corresponds to one of the 16 code words of the  $[5, 2]_4$  code.

**Example 3 (5-local decoupling of a diagonal Hamiltonian using a BCH code).** Recall from Remark 1 that if one is interested in decoupling a Hamiltonian of a particular form, it may not be necessary for  $\rho$  to be irreducible, and in such a case it may be possible to choose a code over a field  $\mathbb{F}_q$  for which  $q$  is less than  $d^2$ . Consider a diagonal (i.e.,  $Z$ -only) 5-local Hamiltonian  $H$  on a system of 16 qubits. Then  $H$  can be decoupled by applying a BOA derived from the dual code of a  $\text{BCH}^{\text{ext}}(\mathbb{F}_2^4/\mathbb{F}_2, 6) = [16, 7, 6]_2$ , i.e. from a code over  $\mathbb{F}_2$  with parameters  $[16, 9]_2$  and generator

matrix

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

Due to the special structure of the Hamiltonian, we are able to choose  $q = d = 2$  (rather than  $q = d^2 = 4$ ) in this case. Since  $k = 9$ ,  $d = 2$ ,  $e = 1$ , and the Hamiltonian is  $Z$  only, the corresponding BOA has a total number of time steps given by  $N = d^k k e = 4608$ . When arranged into the columns of an  $16 \times 4608$  matrix, each of the 4608 control Hamiltonians that are applied in this scheme corresponds to one of the 512 code words of the  $[16, 9]_2$  code.

To construct our protocol from this code we first choose a generating set  $S_2^{(9)}$  for  $\mathbb{F}_2^9$ , such as the  $k = 9$  standard basis vectors  $\{(1, 0, 0, \dots)^T, (0, 1, 0, 0, \dots)^T, \dots\}$ . We then find an Eulerian cycle  $\mathcal{L}$  on the Cayley graph  $\Gamma(\mathbb{F}_2^9, S_2^{(9)})$  and map it to an Eulerian cycle  $G\mathcal{L}$  on the Cayley graph  $\Gamma(G[\mathbb{F}_2^9], G[S_2^{(9)}])$  using the generator matrix above. Our choice of  $S_2^{(9)}$  as being the standard basis vectors would dictate that the transition labels  $\vec{b} = Gs$ , for  $s \in S_2^{(9)}$ , are simply the columns of  $G$ . Our BOA consists of the  $2^9 = 512$  16-bit code words, each appearing exactly 9 times according to the order specified by  $G\mathcal{L}$ . To use the BOA as a decoupling scheme, we may choose

$$\rho : \{0, 1\} \rightarrow \{\mathbb{1}, X\}, \quad \text{with} \quad \rho(0) = \mathbb{1}, \quad \rho(1) = X$$

and choose the corresponding single-qubit control unitaries to be

$$u_0(\delta) = \mathbb{1}, \quad u_1(\delta) = e^{-iX\delta}, \quad \text{over time } \delta \in [0, \frac{\pi}{2}].$$

Observe that (ignoring global phase)  $u_0(\frac{\pi}{2}) = \mathbb{1} = \rho(0)$  and  $u_1(\frac{\pi}{2}) = X = \rho(1)$ . The multi-qubit control unitaries are defined by  $u_{\vec{b}} = u_{b_1} \otimes \dots \otimes u_{b_{16}}$  (for  $\vec{b} \in \{0, 1\}^{16}$ ). For example, if  $s = (1, 0, 0, \dots)^T$ , then  $\vec{b} = Gs$  is the first column of  $G$  and  $u_{\vec{b}} = e^{-iX_1\delta} e^{-iX_{10}\delta} e^{-iX_{13}\delta} e^{-iX_{14}\delta} e^{-iX_{15}\delta} e^{-iX_{16}\delta}$  acting non-trivially on qubits 1, 10, 13, 14, 15, and 16. The control scheme in Protocol 2 is thus specified.

We now prove that this example works, even though  $\rho$  is reducible (i.e. even though we are choosing  $q = 2$  rather than  $q = 4$ ). As per the argument in the proof of Theorem 2, we need only focus on a single 5-local term of  $H$  (so assume without loss of generality that  $H$  consists of only one such term), we can ignore all but the 5 qubits on which it acts non-trivially, and we need only speak of the 5-qubit unitaries  $u_{\delta}(\delta)$  that act on those qubits and correspond to  $\delta \in \mathcal{S}$  (where  $\mathcal{S}$  is the generator set for  $\mathbb{F}_2^5$  derived from the BOA for those 5 qubits). According to the proof of Theorem 1, our scheme works if and only if  $\Pi_{\mathcal{G}}(F_{\mathcal{S}}(H)) = 0$ . Here, however,  $\rho$  is not irreducible, so  $\Pi_{\mathcal{G}}$  will not suppress all traceless operators; indeed,  $X$ -only operators commute with each  $U_{\mathcal{g}}$  and are therefore unmodified by  $\Pi_{\mathcal{G}}$ .

To show that  $\Pi_{\mathcal{G}}(F_{\mathcal{S}}(H)) = 0$  nevertheless holds, observe from Eq. (3) that each term in  $F_{\mathcal{S}}(H)$  is of the form  $u_{\delta}^{\dagger} H u_{\delta}$ . Now,  $H$  is diagonal, i.e. a tensor product of only  $\mathbb{1}$  and  $Z$ , and  $u_{\delta}(\delta)$  is a tensor product of only  $\mathbb{1}$  and  $e^{-iX\delta}$ . Therefore, because  $e^{iX\delta} Z e^{-iX\delta} = \cos(2\delta)Z + \sin(2\delta)Y$ , we see that  $u_{\delta}^{\dagger} H u_{\delta}$  can be expanded as a sum of tensor products of  $\mathbb{1}$ ,  $Z$  and  $Y$ . Moreover, because  $H$  is traceless and conjugation by a unitary is trace-preserving, this sum cannot contain a term proportional to the identity,  $\mathbb{1}^{\otimes 5}$ . Thus, each of these terms consists of at least one operator (which for notational purposes we take to be on the first qubit) that is a  $Z$  or a  $Y$ , i.e. each can be written in the form  $\sigma \otimes A$ , where  $\sigma \in \{Y, Z\}$  and  $A$  is some 4-fold tensor product of operators from  $\{\mathbb{1}, Y, Z\}$ . Our protocol is defined by



a BOA of strength 5, so any subset of 5 rows of the BOA consists of all  $2^5$  5-tuples in  $\mathbb{F}_2^5$  repeated an equal number of times. Thus the sum in  $\Pi_G$  involves conjugating by each  $U_g$  where  $U_g$  ranges over all  $2^5$  possible tensor products that can be formed on 5 qubits using  $\mathbb{1}$  and  $X$ . Focusing on the first qubit, we can equivalently say that the  $U_g$  range over all possible  $\mathbb{1} \otimes B$  and  $X \otimes B$ , where  $B$  ranges over  $\{B_2 \otimes B_3 \otimes B_4 \otimes B_5 : B_i \in \{\mathbb{1}, X\}\}$ . Conjugating  $\sigma \otimes A$  by  $\mathbb{1} \otimes B$  yields either  $\sigma \otimes A$  or  $-\sigma \otimes A$ , whereas conjugating instead by  $X \otimes B$  yields the same result but with the opposite sign (since  $\sigma \in \{Y, Z\}$ ). In other words,  $(\mathbb{1} \otimes B)(\sigma \otimes A)(\mathbb{1} \otimes B) + (X \otimes B)(\sigma \otimes A)(X \otimes B) = 0$ . Thus, the sum in  $\Pi_G$  cancels in pairs, i.e.  $\Pi_G(F_{\mathcal{S}}(H))$  is indeed 0.

## IX. CONCLUSION

We have shown how to use bounded-strength controls to decouple  $n$  interacting qudits of dimension  $d = p^e$  (for some prime  $p$  and positive integer  $e$ ) that obey an  $\ell$ -local Hamiltonian. The system may be either closed or open (i.e. coupled to an environment), as long as both the system Hamiltonian and the environmental couplings are  $\ell$ -local on the system. The decoupling scheme is described using a balanced-cycle orthogonal array, which we introduced and showed how to construct from classical linear codes. To determine the best possible scheme based on our method, we have to find the best linear error-correcting code  $C^\perp = [n, k^\perp]_q$  of length  $n$  and distance at least  $\ell + 1$ . By *the best*, we mean  $k^\perp$  should be maximized for the given system size ( $n$ ) and locality ( $\ell$ ). The construction in the present paper yields a decoupling scheme that uses  $N = d^{2k} 2ke$  time slices (of fixed length) where  $k = n - k^\perp$ .

Finding the best code is a key problem in the theory of error-correcting codes; extensive code tables have been compiled for small distances. For the important case of qubits with 2-local interactions, for example, one can use Hamming codes over  $\mathbb{F}_4$  such that  $k = \log_4(3n + 1)$ , whence  $N$  scales like  $n \log n$ . For higher degrees of locality, we can use families of BCH codes to construct the decoupling schemes. The designed distance of these codes is chosen based on the locality  $\ell$  of the Hamiltonian, leading to a scaling of  $N$  as  $n^{\ell-1} \log n$ . An open question is whether the schemes so derived are optimal in the asymptotic sense, i.e. whether, for fixed  $\ell$  and qudit dimension  $d$ , a better scaling with  $n$  is possible. We note that it is known [21] that when using bang-bang pulses, time at least  $\Omega(n)$  is necessary to decouple general 2-body Hamiltonians, whereas our bounded-strength scheme takes time  $O(n \log n)$  using Hamming codes for such Hamiltonians. Another interesting open question is to develop a theory for systems with mixed qudit dimensions. All schemes derived here are decoupling schemes up to first order, and while it is easy to extend this to second order using symmetry, it would be interesting to find schemes that also achieve decoupling to higher orders. Finally, we mention as an avenue for future research the application of the derived bounded-strength decoupling schemes for the purpose of Hamiltonian simulation.

## Acknowledgments

This work was supported in part by the ARO grant Contract Number W911NF-12-0486, as well as by the National Science Foundation Science and Technology Center for Science of Information under grant CCF-0939370. P.W. gratefully acknowledges the support from the NSF CAREER Award CCF-0746600. We thank Madhu Sudan and Sergey Yekhanin for discussions on BCH codes, in particular regarding the proof of the bound in Theorem 5.

- 
- [1] L. Viola and E. Knill, "Robust dynamical decoupling of quantum systems with bounded controls," *Phys. Rev. Lett.*, vol. 90, p. 037901, 2003. <http://link.aps.org/doi/10.1103/PhysRevLett.90.037901>
  - [2] D. A. Lidar and T. A. Brun, Eds., *Quantum error correction*. Cambridge University Press, 2013.
  - [3] M. Stollsteimer and G. Mahler, "Suppression of arbitrary internal coupling in a quantum register," *Phys. Rev. A*, vol. 64, p. 052301, 2001. <http://link.aps.org/doi/10.1103/PhysRevA.64.052301>
  - [4] P. Wocjan, M. Roetteler, D. Janzing, and T. Beth, "Simulating hamiltonians in quantum networks: Efficient schemes and complexity bounds," *Phys. Rev. A*, vol. 65, p. 042309, 2002. <http://link.aps.org/doi/10.1103/PhysRevA.65.042309>
  - [5] M. Roetteler and P. Wocjan, "Equivalence of decoupling schemes and orthogonal arrays," *Information Theory, IEEE Transactions on*, vol. 52, no. 9, pp. 4171–4181, 2006. <http://dx.doi.org/10.1109/TIT.2006.880059>
  - [6] P. Wocjan, "Efficient decoupling schemes with bounded controls based on eulerian orthogonal arrays," *Phys. Rev. A*, vol. 73, p. 062317, 2006. <http://link.aps.org/doi/10.1103/PhysRevA.73.062317>
  - [7] R. R. Ernst, G. Bodenhausen, and A. Wokaun, *Principles of nuclear magnetic resonance in one and two dimensions*. Clarendon Press Oxford, 1987, vol. 14.

- [8] J. Waugh, L. Huber, and U. Haeberlen, "Approach to high-resolution nmr in solids," *Physical Review Letters*, vol. 20, no. 5, pp. 180–182, 1968. <http://dx.doi.org/10.1103/PhysRevLett.20.180>
- [9] U. Haeberlen, High resolution NMR in solids: Selective averaging, *Advances in magnetic resonance: Suppl. 1*. Academic Press, 1976, vol. 1.
- [10] A. D. Bookatz, P. Wocjan, and L. Viola, "Hamiltonian quantum simulation with bounded-strength controls," *New Journal of Physics*, vol. 16, no. 4, p. 045021, 2014. <http://dx.doi.org/10.1088/1367-2630/16/4/045021>
- [11] A. S. Hedayat, N. J. A. Sloane, and J. Stufken, *Orthogonal arrays: theory and applications*. Springer Science & Business Media, 1999.
- [12] M. Roetteler, "Dynamical decoupling schemes derived from Hamilton cycles," *Journal of Mathematical Physics*, vol. 49, p. 042106, 2008. <http://dx.doi.org/10.1063/1.2904471>
- [13] F. J. MacWilliams and N. J. A. Sloane, *The Theory of error-correcting codes*. North-Holland, 1977.
- [14] S. Lin and D. J. Costello, *Error Control Coding*. Prentice Hall, 2004.
- [15] R. M. Roth, *Introduction to Coding Theory*. Cambridge University Press, 2006.
- [16] M. Sudan, 2001, Lecture notes for *Algorithmic Introduction to Coding Theory* (MIT 6.897). <http://people.csail.mit.edu/madhu/FT01/>
- [17] S. Yekhanin and I. Dumer, "Long nonbinary codes exceeding the Gilbert-Varshamov bound for any fixed distance," *IEEE Transactions on Information Theory*, vol. 50, no. 10, pp. 2357–2362, 2004. <http://dx.doi.org/10.1109/TIT.2004.834744>
- [18] Y. Edel and J. Bierbrauer, "Large caps in small spaces," *Designs, Codes, and Cryptography*, vol. 23, no. 2, pp. 197–212, 2001. <http://dx.doi.org/10.1023/A%3A1011216716700>
- [19] W. Bosma, J. J. Cannon, and C. Playoust, "The Magma algebra system I: The user language," *Journal of Symbolic Computation*, vol. 24, no. 3–4, pp. 235–265, 1997. <http://dx.doi.org/10.1006/jsco.1996.0125>
- [20] F. R. Kschischang and S. Pasupathy, "Some ternary and quaternary codes and associated sphere packings," *IEEE Trans. Inf. Theory*, vol. 38, no. 2, pp. 227–246, 1992. <http://dx.doi.org/10.1109/18.119683>
- [21] D. Janzing, P. Wocjan, and T. Beth, "Complexity of decoupling and time reversal for  $n$  spins with pair interactions: Arrow of time in quantum control," *Phys. Rev. A*, vol. 66, p. 042311, 2002. <http://link.aps.org/doi/10.1103/PhysRevA.66.042311>