Kerdock Codes Determine Unitary 2-Designs

Trung Can, Narayanan Rengaswamy, Robert Calderbank, and Henry D. Pfister

***Abstract*—The non-linear binary codes constructed by Nordstrom-Robinson (1967), Kerdock (1972), Preparata (1968), Goethals (1974), and Delsarte-Goethals (1975) contain more codewords than any known linear code of comparable length and minimum distance. Each code can be constructed very simply as the Gray image of an extended cyclic code of length $N = 2^m$ over $\mathbb{Z}_4$. The complex lines obtained by exponentiating the $\mathbb{Z}_4$-valued codewords are shown to be stabilizer states. They are eigenvectors of maximal commutative subgroups of the Heisenberg-Weyl (Pauli) group HW_N that is fundamental to quantum error correction. This *quantum* description is used to simplify the derivation of certain *classical* weight distributions.**

The Kerdock code of length N over $\mathbb{Z}_4$ is shown to determine $N + 1$ mutually unbiased eigenbases, and the corresponding maximal commutative subgroups partition the non-identity Hermitian Pauli matrices. Automorphisms of the Kerdock code determine elements of the Clifford group Cliff_N that is fundamental to quantum computation. These Clifford elements are unitary matrices that act by conjugation, permuting the $N + 1$ maximal commutative subgroups. They determine a group of symplectic matrices isomorphic to the projective special linear group PSL$(2, N)$, and the simplicity of this representation makes it easy to demonstrate transitivity on Pauli matrices. This property is shown to be equivalent to that of the Clifford elements forming a unitary 2-design. The *Kerdock* unitary 2-design described here was originally discovered by Cleve, Leung, Liu and Wang (2016), but the connection to classical codes is new and the description of the design and translation to circuits is simplified significantly. The translation uses only Clifford gates, and empirical evidence for up to 16 qubits suggests that the gate complexity is $O(m \log m \log \log m)$, which is better than the unconditional guarantee provided by Cleve et al. by a factor $O(\log m)$. Algorithms are developed for optimizing the synthesis of unitary 2-designs on protected qubits, i.e., to construct *logical* unitary 2-designs. Software implementations are available at https://github.com/nrenga/symplectic-arxiv18a.

***Index Terms*—Heisenberg-Weyl group, Pauli group, quantum computing, Clifford group, symplectic geometry, Kerdock codes, Delsarte-Goethals codes, Gray map, stabilizer states, mutually unbiased bases, unitary k-designs**

I. Introduction

Classical error-correcting codes inspired the discovery of the first quantum error-correcting code (QECC) by Shor [1], the development of CSS codes by Calderbank and Shor [2] and by Steane [3], and the development of stabilizer codes by Calderbank, Rains, Shor and Sloane [4] and by Gottesman [5]. A quantum error-correcting code protects $m-k$ logical qubits by embedding them in a system comprising m physical qubits. In fault-tolerant computation, any desired operation on the $m - k$ logical (protected) qubits must be implemented as a physical operation on the m physical qubits that preserves the code space. Section II introduces the Heisenberg-Weyl group HW_N (also known as the Pauli group), its commutative subgroups, and the Clifford group Cliff_N, which are fundamental to quantum computation. Note that $N = 2^m$ throughout this paper.

Recall that Hermitian matrices that commute can be simultaneously diagonalized. The Kerdock and Delsarte-Goethals binary codes are unions of cosets of the first order Reed-Muller (RM) code RM$(1, m)$, the cosets are in one-to-one correspondence with symplectic forms, and the weight distribution of a coset is determined by the rank of the symplectic form (see [6, Chapter 15] for more details). Section III-A reviews the $\mathbb{Z}_4$ description of these codes given in [7]. Section III-B shows that when we exponentiate codewords in these cosets of RM$(1, m)$ we obtain a basis of common eigenvectors for a *maximal* commutative subgroup of Hermitian Pauli matrices. The operators that project onto individual lines in a given eigenbasis are invariants of the corresponding subgroup [8], and the weight distribution of each code is determined by the inner product of the corresponding eigenvectors (see [Section III, Lemma 9]). When calculating weight distributions, this property makes it possible to avoid using Dickson's Theorem [6, Chapter 15] to choose an appropriate representation of the symplectic form. The correspondence between classical and quantum worlds simplifies the calculation (of the weight distribution) given in [6] significantly.

Eigenvectors of maximal commutative subgroups of HW_N are called *stabilizer states*. The Clifford group Cliff_N consists of all unitary matrices that normalize HW_N. Clifford elements act by conjugation on HW_N, permuting the maximal commutative subgroups, and fixing the ensemble of stabilizer states (see Section IV). The Clifford group is highly symmetric, and it approximates the full unitary group in a way that can be made precise by comparing irreducible representations [8], [9]. Kueng and Gross [10] have shown that the ensemble of stabilizer states is a complex projective 3-design; given a polynomial of degree at most 3, the integral over the N-sphere can be calculated by evaluating the polynomial at stabilizer states, and taking a finite sum. Stabilizer states also find application as measurements in the important classical problem of phase retrieval, where an unknown vector is to be recovered from the magnitudes of the measurements (see Kueng, Zhu and Gross [11]). A third application is unsourced multiple access, where there is a large number of devices (messages) each of which transmits (is transmitted) infrequently. This provides a model for machine-to-machine communication in the Internet-of-Things (IoT), including the special case of radio-frequency identification (RFID), as well as neighbor discovery in ad-hoc

T. Can is currently with the Department of Mathematics, California Institute of Technology, Pasadena, CA 91125, USA. Most of this work was conducted while he was with the Department of Mathematics, Duke University, Durham, North Carolina 27708, USA. Email: tcan@caltech.edu

N. Rengaswamy, R. Calderbank and H. D. Pfister are with the Department of Electrical and Computer Engineering, Duke University, Durham, North Carolina 27708, USA. Email: {narayanan.rengaswamy, robert.calderbank, henry.pfister}@duke.edu

wireless networks. Here, Thompson and Calderbank [12] have shown that stabilizer states associated with Delsarte-Goethals codes support a fast algorithm for unsourced multiple access that scales to 2^{100} devices (arbitrary 100-bit messages).

Section IV constructs the $N+1$ eigenbases (of stabilizer states) determined by the Kerdock code of length N over $\mathbb{Z}_4$, and shows that the corresponding maximal commutative subgroups partition the non-identity Hermitian Pauli matrices. The eigenbases are mutually unbiased, so that unit vectors u, v in different eigenbases satisfy $|\langle \mathsf{u}, \mathsf{v} \rangle| = N^{-\frac{1}{2}}$, and hence each eigenbasis looks like noise to the other eigenbases. The Kerdock ensemble of $N(N+1)$ complex lines is extremal; Calderbank et al. [13] have shown that any collection of unit vectors for which pairwise inner products have absolute value 0 or $N^{-\frac{1}{2}}$ has size at most N^2+N, and that any extremal example must be a union of eigenbases. The group of Clifford symmetries of this ensemble, represented as binary symplectic matrices, is shown to be isomorphic to the projective special linear group $\mathrm{PSL}(2,N)$. We note that the Kerdock ensemble also appears in the work of Tirkkonen et al. [14].

Unitary k-designs are finite ensembles of unitary matrices that approximate the Haar distribution over unitary matrices. Section V makes this precise by discussing linear maps called *twirls* over the full unitary ensemble and the finite ensemble. When the two linear maps coincide the finite ensemble is a unitary k-design. It is easy to analyze protocols that randomly sample unitary matrices with respect to the Haar measure, but sampling is infeasible, hence the interest in finite ensembles of unitary matrices that approximate the Haar distribution. Cliff_N is known to be a unitary 3-design [15], and the proof by Webb involves the concepts of Pauli mixing and Pauli 2-mixing, which we introduce in Section V.

Cleve et al. [16] have recently found a *subgroup* of Cliff_N that is a unitary 2-design. Section V uses the *classical* Kerdock and Delsarte-Goethals codes to simplify the construction of this *quantum* unitary 2-design and its translation to circuits. A graph $\mathbb{H}_N$ is defined on (scalar multiples of) non-identity (Hermitian) Pauli matrices, where two matrices (vertices) are joined (by an edge) if and only if they commute. This graph is shown to be *strongly regular*; every vertex has the same degree, and the number of vertices joined to two given vertices depends only on whether the two vertices are joined or not joined. The automorphism group of this graph is the binary symplectic group $\mathrm{Sp}(2m,\mathbb{F}_2)$. A subgroup of Cliff_N containing HW_N is proven to be Pauli mixing if it acts transitively on vertices, and Pauli 2-mixing if it acts transitively on edges and on non-edges. These properties imply that Pauli mixing ensembles are unitary 2-designs and Pauli 2-mixing ensembles are unitary 3-designs [15]. The Clifford symmetries of the Kerdock ensemble (of stabilizer states), again represented as symplectic matrices, are shown to be transitive on the vertices of $\mathbb{H}_N$ and hence a unitary 2-design.

T. Can [17] has developed an algorithm that factors a $2m \times 2m$ binary symplectic matrix into a product of at most 6 elementary symplectic matrices of the type shown in Table I. The target symplectic matrix maps the dual basis $X_N = E([I_m \mid 0]), Z_N = E([0 \mid I_m])$ (see Section II for notation) to a dual basis X_N', Z_N', and row and column operations by the elementary matrices return X_N', Z_N' to the original pair X_N, Z_N. Section V uses this decomposition to simplify the translation of the Kerdock unitary 2-design into circuits. The elementary symplectic matrices appearing in the product can be related to the Bruhat decomposition of the symplectic group (see [18]). When the algorithm is run in reverse it produces a random Clifford matrix that can serve as an approximation to a random unitary matrix. This is an instance of the subgroup algorithm [19] for generating uniform random variables. The algorithm has complexity $O(m^3)$ and uses $O(m^2)$ random bits, which is order optimal given the order of the symplectic group $\mathrm{Sp}(2m,\mathbb{F}_2)$ (cf. [20]). We note that the problem of selecting a unitary matrix uniformly at random finds application in machine learning (see [21] and the references therein). The algorithm developed by Can is similar to that developed by Jones, Osipov and Rokhlin [22] in that it alternates (partial) Hadamard matrices and diagonal matrices; the difference is that the unitary 3-design property of the Clifford group provides randomness guarantees.

There are many applications of unitary 2-designs. The first is quantum data hiding (the LOCC model described in [23]) where the objective is to hide classical information from two parties who each share part of the data but are only allowed to perform local operations and classical communication. The data hiding protocol can be implemented by sampling randomly from the full unitary group but it is sufficient to sample randomly from a unitary 2-design. Other applications of unitary 2-designs are the randomized benchmarking of quantum circuits [24], [25], fidelity estimation of quantum channels [26], quantum state and process tomography [27], and more recently minimax quantum state estimation [28]. In quantum information theory, they have been used extensively in the analysis of decoupling of quantum systems [29]–[32].

In prior work [33], the authors have developed a mathematical framework for synthesizing physical circuits that implement *logical* Clifford operators for stabilizer codes. Circuit synthesis is enabled by representing the desired physical Clifford operator as a $2m \times 2m$ binary symplectic matrix. For an $[\![m, m-k]\!]$ stabilizer code, every logical Clifford operator is shown to have $2^{k(k+1)/2}$ symplectic solutions, and these are enumerated efficiently using symplectic transvections, thus enabling optimization with respect to a suitable metric. See https://github.com/nrenga/symplectic-arxiv18a for implementations. It is now well-known that different codes yield efficient implementations of different logical operators. A transversal implementation, albeit naturally fault-tolerant, might not always be desirable since it generally requires each logical qubit to be encoded in a different code block, and that has a significant impact on the rate and hence the amount of physical resources necessary for performing reliable computation. Hence, a compiler for a quantum computer might usefully switch between several codes [34] *dynamically*, depending on the current state of the system. The above algorithm enables the compiler to be able to determine logical operators for a code quickly depending on the input circuit (on *protected* qubits).

Section VI provides a proof of concept implementation of the Kerdock unitary 2-design on protected (logical) qubits using our logical Clifford synthesis algorithm in [33]. This finds application in the recent logical randomized benchmarking protocol [35], where the authors show that this procedure is more accurate in assessing the quality of an error-correction implementation, compared to the standard approach of physical randomized benchmarking [24]. The protocol requires a unitary 2-design on the logical qubits, and they use the full Clifford group for this purpose which is much larger than the Kerdock unitary 2-design described here.

In summary, the purpose of this paper is to emphasize that interactions between the classical and quantum domains still prove mutually beneficial, as much as they helped inspire the first QECC more than two decades back. Specifically, we make four main *theoretical* contributions.

1) Use of quantum concepts to simplify the calculation of classical weight distributions of several families of non-linear binary codes [6], [36]–[42].
2) Elementary description of symmetries of the Kerdock code, and the $N^2 + N$ stabilizer states determined by this code [12], [14], [43], [44].
3) Demonstration that the symmetry group of the Kerdock code is a unitary 2-design, and introduction of elementary methods for circuit synthesis. Provide strong empirical evidence, for up to 16 qubits, that our Clifford-gate-complexity is $O(m \log m \log\log m)$, which is better by a factor $O(\log m)$ compared to the unconditional complexity of Cleve et al. while employing only Clifford gates [16].
4) Proof of concept construction of logical unitary 2-designs on the protected qubits of a stabilizer code [33], [35].

We also provide *software* implementations of all algorithms, at https://github.com/nrenga/symplectic-arxiv18a.

II. The Heisenberg-Weyl and Clifford Groups

Quantum error-correcting codes serve to protect qubits involved in quantum computation, and this section summarizes the mathematical framework introduced in [2], [4], [5], [45], and described more completely in [46] and [33]. In this framework for fault-tolerant quantum computation, Clifford operators on the N-dimensional complex space afforded by m qubits are represented as $2m \times 2m$ binary symplectic matrices. This is an exponential reduction in size, and the symplectic matrices serve as a binary control plane for the quantum computer.

Remark 1: Throughout the paper, we adopt the convention that all binary vectors are row vectors, and $\mathbb{Z}_4$-, real- or complex-valued vectors are column vectors, where $\mathbb{Z}_4$ is the ring of integers modulo 4. The values $\imath^{\kappa}$, where $\imath \triangleq \sqrt{-1}, \kappa \in \mathbb{Z}_4$, are called *quaternary phases*.

A single qubit is a 2-dimensional Hilbert space, and a quantum state v is a superposition of the two states $e_0 \triangleq [1,0]^T, e_1 \triangleq [0,1]^T$ which form the *computational basis*. Thus $\mathsf{v} = \alpha e_0 + \beta e_1$, where $\alpha, \beta \in \mathbb{C}$ satisfy $|\alpha|^2 + |\beta^2| = 1$ as per the Born rule [47, Chapter 3]. The *Pauli* matrices are

$$I_2,\ X \triangleq \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},\ Z \triangleq \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix},\ Y \triangleq \imath XZ = \begin{bmatrix} 0 & -\imath \\ \imath & 0 \end{bmatrix}, \quad (1)$$

where $\imath \triangleq \sqrt{-1}$ and I_2 is the 2×2 identity matrix [48, Chapter 10]. We may express an arbitrary *pure* quantum state v as

$$\mathsf{v} = (\alpha_0 I_2 + \alpha_1 X + \imath\alpha_2 Z + \alpha_3 Y)\ e_0,\ \text{ where } \alpha_i \in \mathbb{R}. \quad (2)$$

We describe m-qubit states by (linear combinations of) m-fold Kronecker products of computational basis states, or equivalently by m-fold Kronecker products of Pauli matrices.

Given row vectors $a, b \in \mathbb{F}_2^m$ define the m-fold Kronecker product

$$D(a,b) \triangleq X^{a_1} Z^{b_1} \otimes \cdots \otimes X^{a_m} Z^{b_m} \in \mathbb{U}_N,\ \ N \triangleq 2^m, \quad (3)$$

where $\mathbb{U}_N$ denotes the group of all $N \times N$ unitary operators. The *Heisenberg-Weyl group* HW_N (also called the *m-qubit Pauli group*) consists of all operators $\imath^{\kappa} D(a,b)$, where $\kappa \in \mathbb{Z}_4 \triangleq \{0,1,2,3\}$. The order is $|HW_N| = 4N^2$ and the *center* of this group is $\langle \imath I_N \rangle \triangleq \{I_N, \imath I_N, -I_N, -\imath I_N\}$, where I_N is the $N \times N$ identity matrix. Multiplication in HW_N satisfies the identity

$$D(a,b)D(a',b') = (-1)^{a'b^T + b'a^T} D(a',b')D(a,b). \quad (4)$$

The standard *symplectic inner product* in $\mathbb{F}_2^{2m}$ is defined as

$$\langle [a,b],[a',b'] \rangle_{\mathrm{s}} \triangleq a'b^T + b'a^T = [a,b]\ \Omega\ [a',b']^T, \quad (5)$$

where the symplectic form $\Omega \triangleq \begin{bmatrix} 0 & I_m \\ I_m & 0 \end{bmatrix}$ (see [4], [33]). Therefore, two operators $D(a,b)$ and $D(a',b')$ commute if and only if $\langle [a,b],[a',b'] \rangle_{\mathrm{s}} = 0$.

The homomorphism $\gamma\colon HW_N \to \mathbb{F}_2^{2m}$ defined by

$$\gamma(\imath^{\kappa} D(a,b)) \triangleq [a,b]\ \forall\ \kappa \in \mathbb{Z}_4 \quad (6)$$

has kernel $\langle \imath I_N \rangle$ and allows us to represent elements of HW_N (up to multiplication by scalars) as binary vectors.

The *Clifford group* Cliff_N consists of all unitary matrices $g \in \mathbb{C}^{N \times N}$ for which $gD(a,b)g^{\dagger} \in HW_N$ for all $D(a,b) \in HW_N$, where $g^{\dagger}$ is the Hermitian transpose of g [46]. Cliff_N is the *normalizer* of HW_N in the unitary group $\mathbb{U}_N$. The Clifford group contains HW_N and its size is $|\mathrm{Cliff}_N| = 4 \cdot 2^{m^2+2m} \prod_{j=1}^{m} (4^j - 1)$ [4]. We regard operators in Cliff_N as *physical* operators acting on quantum states in $\mathbb{C}^N$, to be implemented by quantum circuits. Every operator $g \in \mathrm{Cliff}_N$ induces an automorphism of HW_N by conjugation. Note that the inner automorphisms induced by matrices in HW_N preserve every conjugacy class $\{\pm D(a,b)\}$ and $\{\pm \imath D(a,b)\}$, because (4) implies that elements in HW_N either commute or anti-commute. Matrices $D(a,b)$ are symmetric or anti-symmetric according as $ab^T = 0$ or 1, hence the matrix

$$E(a,b) \triangleq \imath^{ab^T} D(a,b) \quad (7)$$

is Hermitian. Note that $E(a,b)^2 = I_N$. The automorphism induced by a Clifford element g satisfies

$$gE(a,b)g^{\dagger} = \pm E\left([a,b]F_g\right),\ \text{ where }\ F_g = \begin{bmatrix} A_g & B_g \\ C_g & D_g \end{bmatrix} \quad (8)$$

is a $2m \times 2m$ binary matrix that preserves symplectic inner products: $\langle [a,b]F_g, [a',b']F_g \rangle_{\mathrm{s}} = \langle [a,b],[a',b'] \rangle_{\mathrm{s}}$. Hence F_g is

TABLE I

A GENERATING SET OF SYMPLECTIC MATRICES AND THEIR CORRESPONDING UNITARY OPERATORS. The number of 1s in Q and P directly relates to number of gates involved in the circuit realizing the respective unitary operators (see [33, Appendix I]). The N coordinates are indexed by binary vectors $v \in \mathbb{F}_2^m$, and e_v denotes the standard basis vector in $\mathbb{C}^N$ with an entry 1 in position v and all other entries 0. Here H_{2^k} denotes the Walsh-Hadamard matrix of size 2^k, $U_k = \mathrm{diag}\,(I_k, 0_{m-k})$ and $L_{m-k} = \mathrm{diag}\,(0_k, I_{m-k})$.

Symplectic Matrix F_g	Clifford Operator g
$\Omega = \begin{bmatrix} 0 & I_m \\ I_m & 0 \end{bmatrix}$	$H_N = H_2^{\otimes m}$
$L_Q = \begin{bmatrix} Q & 0 \\ 0 & Q^{-T} \end{bmatrix}$	$\ell_Q : e_v \mapsto e_{vQ}$
$T_P = \begin{bmatrix} I_m & P \\ 0 & I_m \end{bmatrix}; P = P^T$	$t_P \;=\; \mathrm{diag}\left(\imath^{vPv^T \bmod 4}\right)$
$G_k = \begin{bmatrix} L_{m-k} & U_k \\ U_k & L_{m-k} \end{bmatrix}$	$g_k = H_{2^k} \otimes I_{2^{m-k}}$

called a *binary symplectic matrix* and the symplectic property reduces to $F_g \Omega F_g^T = \Omega$, or equivalently

$$A_g B_g^T = B_g A_g^T,\; C_g D_g^T = D_g C_g^T,\; A_g D_g^T + B_g C_g^T = I_m. \tag{9}$$

(See [49] for an extensive discussion on general symplectic geometry and quantum mechanics.) The symplectic property encodes the fact that the automorphism induced by g must respect commutativity in HW_N. Let $\mathrm{Sp}(2m, \mathbb{F}_2)$ denote the group of symplectic $2m \times 2m$ matrices over $\mathbb{F}_2$. The map $\phi\colon \mathrm{Cliff}_N \to \mathrm{Sp}(2m, \mathbb{F}_2)$ defined by

$$\phi(g) \triangleq F_g \tag{10}$$

is a homomorphism with kernel HW_N, and every Clifford operator projects onto a symplectic matrix F_g. Thus, HW_N is a normal subgroup of Cliff_N and $\mathrm{Cliff}_N / HW_N \cong \mathrm{Sp}(2m, \mathbb{F}_2)$. This implies that the size is $|\mathrm{Sp}(2m, \mathbb{F}_2)| = 2^{m^2} \prod_{j=1}^{m} (4^j - 1)$ (also see [4]). Table I lists elementary symplectic transformations F_g, that generate the binary symplectic group $\mathrm{Sp}(2m, \mathbb{F}_2)$, and the corresponding unitary automorphisms $g \in \mathrm{Cliff}_N$, which together with HW_N generate Cliff_N. (See [33, Appendix I] for a discussion on the Clifford gates and circuits corresponding to these transformations.)

We use commutative subgroups of HW_N to define resolutions of the identity. A *stabilizer* is a subgroup S of HW_N generated by commuting Hermitian matrices $\pm E(a, b)$, with the additional property that if $E(a, b) \in S$ then $-E(a, b) \notin S$ [48, Chapter 10]. The operators $\frac{I_N \pm E(a,b)}{2}$ project onto the ± 1 eigenspaces of $E(a, b)$, respectively.

Remark 2: Since all elements of S are unitary, Hermitian and commute with each other, they can be diagonalized simultaneously with respect to a common orthonormal basis, and their eigenvalues are ± 1 with algebraic multiplicity $N/2$. We refer to such a basis as the *common eigenbasis* or simply *eigenspace* of the subgroup S, and to the subspace of eigenvectors with eigenvalue $+1$ as the *+1 eigenspace* of S.

If the subgroup S is generated by $E(a_i, b_i), i = 1, \ldots, k$, then the operator

$$\frac{1}{2^k} \prod_{i=1}^{k} (I_N + E(a_i, b_i)) \tag{11}$$

projects onto the 2^{m-k}-dimensional subspace $V(S)$ fixed pointwise by S, i.e., the $+1$ eigenspace of S. The subspace $V(S)$ is the *stabilizer code* determined by S. We use the notation $[\![m, m-k]\!]$ code to represent that $V(S)$ encodes $m-k$ *logical* qubits into m *physical* qubits.

Let $\gamma(S)$ denote the subspace of $\mathbb{F}_2^{2m}$ formed by the binary representations of the elements of S using the homomorphism γ in (6). A generator matrix for $\gamma(S)$ is

$$G_S \triangleq [a_i, b_i]_{i=1,\ldots,k} \text{ s.t. } G_S\; \Omega\; G_S^T = 0, \tag{12}$$

where 0 is the $k \times k$ matrix with all entries zero.

Given a stabilizer S with generators $E(a_i, b_i), i = 1, \ldots, k$, we can define 2^k subgroups $S_{\epsilon_1 \cdots \epsilon_k}$ where the index $(\epsilon_1 \cdots \epsilon_k)$ represents that $S_{\epsilon_1 \cdots \epsilon_k}$ is generated by $\epsilon_i E(a_i, b_i)$, for $\epsilon_i \in \{\pm 1\}$. Note that the operator

$$\Pi_{\epsilon_1 \cdots \epsilon_k} \triangleq \frac{1}{2^k} \prod_{i=1}^{k} (I_N + \epsilon_i E(a_i, b_i)) \tag{13}$$

projects onto $V(S_{\epsilon_1 \cdots \epsilon_k})$, and that

$$\sum_{(\epsilon_1, \ldots, \epsilon_k) \in \{\pm 1\}^k} \Pi_{\epsilon_1 \cdots \epsilon_k} = I_N. \tag{14}$$

Hence the subspaces $V(S_{\epsilon_1 \cdots \epsilon_k})$, or equivalently the subgroups $S_{\epsilon_1 \cdots \epsilon_k}$, provide a resolution of the identity, and elements (errors) in HW_N simply permute these subspaces (under conjugation).

Given an $[\![m, m-k]\!]$ stabilizer code, it is possible to perform encoded quantum computation in any of the subspaces $V(S_{\epsilon_1 \cdots \epsilon_k})$ by synthesizing appropriate logical Clifford operators (see [33] for algorithms). If we think of these subspaces as *threads*, then a computation starts in one thread and jumps to another when an error (from HW_N) occurs. Quantum error-correcting codes enable error control by identifying the jump that the computation has made. Identification makes it possible to modify the computation in flight instead of returning to the initial subspace and restarting the computation. The idea of tracing these threads is called as *Pauli frame tracking* in the literature (see [50] and references therein).

In this paper we focus on stabilizers S of dimension $k = m$ that are disjoint from $Z_N \triangleq \{E(0, b) \colon b \in \mathbb{F}_2^m\}$. In this case S is a *maximal commutative subgroup* of HW_N and $\gamma(S)$ is called a *maximal isotropic subspace* of $\mathbb{F}_2^{2m}$. The generator matrix G_S has rank m and can be row-reduced to the form $[I_m \mid P]$, or $[0 \mid I_m]$ if $S = Z_N$. Hence we will denote these subgroups as $E([I_m \mid P])$ and $E([0 \mid I_m])$, respectively. The condition $G_S \Omega G_S^T = 0$ implies $P = P^T$, and any element of $\gamma(S)$ can be expressed in the form $[a, aP]$ for some $a \in \mathbb{F}_2^m$. Note that $E([I_m \mid 0]) = X_N \triangleq \{E(a, 0) \colon a \in \mathbb{F}_2^m\}$. Since $\dim\; V(S) = 2^{m-m} = 1$, the subgroup S fixes exactly one vector. However, the eigenspace of $S = S_{1 \cdots 1}$ has dimension N since the $+1$ eigenvectors of $S_{\epsilon_1 \cdots \epsilon_m}$ are also (± 1) eigenvectors of S. The eigenvectors in these N-dimensional spaces are called *stabilizer states* [51].

III. Weight Distributions of Kerdock Codes

Kerdock codes were first constructed as non-linear binary codes [37], as was the Goethals code [39] and the Delsarte-Goethals codes [41]. In this Section, we describe the Kerdock and Delsarte-Goethals codes as linear codes over $\mathbb{Z}_4$, the ring of integers modulo 4. These $\mathbb{Z}_4$-linear codes were constructed by Hammons et al. [7] as Hensel lifts of binary cyclic codes, and this description requires Galois rings. The description given in Section III-A requires finite field arithmetic, but is entirely binary and follows [43]. Our construction of unitary 2-designs in Section V uses the matrices that are defined in Section III-A. In Section III-B, we make a connection between the Kerdock and Delsarte-Goethals codes and maximal commutative subgroups of HW_N via stabilizer states, use this relation to compute inner products between stabilizer states, and hence calculate weight distributions of Kerdock codes.

A. Kerdock and Delsarte-Goethals Sets

The finite field $\mathbb{F}_{2^m}$ is obtained from the binary field $\mathbb{F}_2$ by adjoining a root α of a primitive irreducible polynomial $p(x)$ of degree m. The elements of $\mathbb{F}_{2^m}$ are polynomials in α of degree at most $m-1$, with coefficients in $\mathbb{F}_2$, and we will identify the polynomial $z_0 + z_1\alpha + \ldots + z_{m-1}\alpha^{m-1}$ with the binary (row) vector $[z_0, z_1, \ldots, z_{m-1}]$.

The *Frobenius map* $f\colon \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ is defined by $f(x) \triangleq x^2$, and the *trace map* $\mathrm{Tr}\colon \mathbb{F}_{2^m} \to \mathbb{F}_2$ is defined by

$$\mathrm{Tr}(x) \triangleq x + x^2 + \ldots + x^{2^{m-1}}. \tag{15}$$

Since $(x+y)^2 = x^2 + y^2$ for all $x, y \in \mathbb{F}_{2^m}$, the trace is linear over $\mathbb{F}_2$. The trace inner product $\langle x, y\rangle_{\mathrm{tr}} = \mathrm{Tr}(xy)$ defines a symmetric bilinear form, so there exists a binary symmetric matrix W for which $\mathrm{Tr}(xy) = xWy^T$. In fact

$$W_{ij} = \mathrm{Tr}\left(\alpha^i\alpha^j\right),\ i, j = 0, 1, \ldots, m-1. \tag{16}$$

The matrix W is non-singular since the trace inner product is non-degenerate (if $\mathrm{Tr}(xz) = 0$ for all $z \in \mathbb{F}_{2^m}$ then $x = 0$). Observe that W is a Hankel matrix, since if $i+j = h+k$ then $\mathrm{Tr}(\alpha^i\alpha^j) = \mathrm{Tr}(\alpha^h\alpha^k)$. The matrix W can be interpreted as the primal-to-dual-basis conversion matrix for $\mathbb{F}_{2^m}$, with the primal basis being $\{1, \alpha, \alpha^2, \ldots, \alpha^{m-1}\}$ (see [16]).

The Frobenius map $f(x) = x^2$ is linear over $\mathbb{F}_2$, so there exists a binary matrix R for which $f(x) \equiv xR$. Since

$$\begin{aligned} f(x_0 + x_1\alpha + \ldots + x_{m-1}\alpha^{m-1}) & \\ = x_0 + x_1\alpha^2 + \ldots + x_{m-1}\alpha^{2(m-1)}, & \end{aligned} \tag{17}$$

the rows of R are the vectors representing the field elements $\alpha^{2i}, i = 0, \ldots, m-1$.

We write multiplication by $z \in \mathbb{F}_{2^m}$ as a linear transformation $xz \equiv xA_z$. For $z = 0$, $A_0 = 0$, and for $z = \alpha^i$ the matrix $A_z = A^i$ for $i = 0, 1, \ldots, 2^m - 2$, where A is the matrix that represents multiplication by the primitive element α. The matrix A is the *companion matrix* of the primitive irreducible polynomial $p(x) = p_0 + p_1x + \ldots + p_{m-1}x^{m-1} + x^m$ over the binary field. Thus

$$A \triangleq \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ & \vdots & & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ p_0 & p_1 & p_2 & \cdots & p_{m-1} \end{bmatrix}, \tag{18}$$

and we have chosen A rather than A^T as the companion matrix since we are representing field elements in $\mathbb{F}_{2^m}$ by row vectors (rather than column vectors).

Lemma 3: The matrices A_z, W, and R^i, for $i \in [m]$, satisfy:

(a) $A_zA_x = A_xA_z = A_{xz}$;
(b) $A_x + A_z = A_{x+z}$;
(c) $A_zW = WA_z^T$;
(d) $R^iA_x^{2^i} = A_xR^i$, $R^iA_x^2 = A_x^{2^{1-i}}R^i$, and $R^{-i}A_x^{-2} = A_x^{-2^{1+i}}R^{-i}$;
(e) $R^iW = W(R^{-i})^T$ and $W^{-1}R^{-i}W = (R^i)^T$.

Proof: Identities (a) through (d) follow directly from the arithmetic of $\mathbb{F}_{2^m}$. Specifically, for (c), observe that

$$(xA_z)Wy^T = \mathrm{Tr}((xz)y) = \mathrm{Tr}(x(yz)) = xW(yA_z)^T,$$

and (d) can be proven similarly. To prove part (e) we observe $\mathrm{Tr}(x) = \mathrm{Tr}(x^2)$ and verify that for all $x, y \in \mathbb{F}_{2^m}$,

$$(xR^i)Wy^T = \mathrm{Tr}(x^{2^i}y) = \mathrm{Tr}(xy^{2^{-i}}) = xW(R^{-i})^Ty^T. \ \blacksquare$$

Definition 4: For $0 \le r \le (m-1)/2$ and for $\underline{z} = (z_0, z_1, \ldots, z_r) \in \mathbb{F}_{2^m}^{r+1}$ define the bilinear form $\beta_{\underline{z},r}(x, y) \triangleq \mathrm{Tr}[z_0xy + z_1(x^2y + xy^2) + \ldots + z_r(x^{2^r}y + xy^{2^r})]$. Note that $\beta_{\underline{z},r}(x, y)$ is represented by the binary symmetric matrix

$$P_{\underline{z},r} \triangleq A_{z_0}W + \sum_{i=1}^{r}[A_{z_i}W(R^i)^T + R^iWA_{z_i}^T]. \tag{19}$$

The *Delsarte-Goethals set* $P_{\mathrm{DG}}(m, r)$ consists of all such matrices $P_{\underline{z},r}$. The *Kerdock set* $P_{\mathrm{K}}(m) \triangleq P_{\mathrm{DG}}(m, 0)$ consists of all matrices $P_z \triangleq P_{\underline{z},0}$, where $\underline{z} = (z), z \in \mathbb{F}_{2^m}$.

Lemma 5: The Delsarte-Goethals set $P_{\mathrm{DG}}(m, r)$ is an $m(r+1)$-dimensional vector space of symmetric matrices. If $z \neq 0$ then $\mathrm{rank}(P_{\underline{z},r}) \ge m - 2r$. Matrices in the Kerdock set $P_{\mathrm{K}}(m)$ are non-singular.

Proof: Closure under addition follows from part (b) of Lemma 3. Observe $\mathrm{Tr}(x) = \mathrm{Tr}(x^2) = \cdots = \mathrm{Tr}(x^{1/2})$. If x is in the nullspace of $P_{\underline{z},r}$, i.e., using its vector representation $xP_{\underline{z},r} = 0$, then $\beta_{\underline{z},r}(x, y) = 0$ for all $y \in \mathbb{F}_{2^m}$ and we obtain

$$\begin{aligned} 0 &= \mathrm{Tr}[z_0xy + z_1(x^2y + xy^2) + \ldots + z_r(x^{2^r}y + xy^{2^r})] \\ &= \mathrm{Tr}[(z_0x)^{2^r}y^{2^r} + (z_1^{2^r}x^{2^{r+1}}y^{2^r} + (z_1x)^{2^{r-1}}y^{2^r}) + \ldots \\ &\qquad \ldots + (z_r^{2^r}x^{2^{2r}}y^{2^r} + (z_rx)y^{2^r})] \\ &= \mathrm{Tr}[y^{2^r}((z_0x)^{2^r} + (z_1^{2^r}x^{2^{r+1}} + (z_1x)^{2^{r-1}}) + \ldots \\ &\qquad \ldots + (z_r^{2^r}x^{2^{2r}} + z_rx))]. \end{aligned}$$

This holds for all y, so $(z_0x)^{2^r} + (z_1^{2^r}x^{2^{r+1}} + (z_1x)^{2^{r-1}}) + \ldots + (z_r^{2^r}x^{2^{2r}} + z_rx)$ must be identically 0, i.e., x is a root of the polynomial. Since the polynomial has at most 2^{2r} roots, the nullspace of $P_{\underline{z},r}$ has dimension at most $2r$, which implies that $\text{rank}(P_{\underline{z},r}) \geq m - 2r$. ■

Remark 6: Note that since the dimension of the vector space of all binary $m \times m$ symmetric matrices is $m(m+1)/2$, the set $P_{\text{DG}}(m, (m-1)/2)$ contains *all* possible symmetric matrices. For the remainder of this paper we represent a general symmetric matrix as simply P, thereby dropping the subscripts $\underline{z}, r$ unless necessary. We will continue to represent Kerdock matrices as P_z.

B. Delsarte-Goethals Codes and Weight Distributions

Hammons et al. [7] showed that the classical nonlinear Kerdock and Delsarte-Goethals codes defined by quadratic forms in [37], [40] are images of linear codes over $\mathbb{Z}_4$ under the Gray map. In this Section, we begin by reviewing this construction using the Kerdock and Delsarte-Goethals sets of matrices, and demonstrate that exponentiating these $\mathbb{Z}_4$-valued codewords entry-wise by $\imath$ produces stabilizer states. For stabilizer states of $E([I_m \mid P_{\underline{z}_1,r}])$ and $E([I_m \mid P_{\underline{z}_2,r}])$, we calculate their Hermitian inner products using the trace of certain projection operators, and show that the distribution of inner products depends on $\text{rank}(P_{\underline{z}_1,r} + P_{\underline{z}_2,r})$. Then, since $\text{rank}(P_z) \in \{0, m\}$ for all $P_z \in P_{\text{K}}(m)$, we compute the weight distribution of Kerdock codes by relating these Hermitian inner products to the histogram of values in the difference between two $\mathbb{Z}_4$-valued codewords. In order to calculate the weight distribution of Delsarte-Goethals codes, we would need to determine the distribution of ranks in the Delsarte-Geothals sets $P_{\text{DG}}(m, r)$. While this question is straightforward for the Kerdock sets it remains open for general Delsarte-Goethals sets and will be investigated in future work.

Definition 7: The $\mathbb{Z}_4$-linear *Delsarte-Goethals code* is given by

$$\text{DG}(m, r) \triangleq \{[xPx^T + 2wx^T + \kappa]_{x \in \mathbb{F}_2^m} : P \in P_{\text{DG}}(m, r), \\ w \in \mathbb{F}_2^m, \kappa \in \mathbb{Z}_4\}. \tag{20}$$

This code has size $2^{m(r+1)+m+2}$ and is of *type* $4^{m+1}2^{mr}$ [42, Section 12.1]. The *Kerdock code* $\text{K}(m) \triangleq \text{DG}(m, 0)$.

Here the notation $[xPx^T + 2wx^T + \kappa]_{x \in \mathbb{F}_2^m}$ represents a $\mathbb{Z}_4$-valued column vector with each entry $xPx^T + 2wx^T + \kappa \pmod 4$ indexed by the vector $x \in \mathbb{F}_2^m$.

Definition 8: For $u, v \in \mathbb{Z}_4^N$ the *Lee weight* (of u) is defined as $w_L(u) \triangleq n_1(u) + 2n_2(u) + n_3(u)$, where $n_\kappa(u)$ denotes the number of entries of u with value κ, and the *Lee distance* (between u and v) is defined as $d_L(u, v) \triangleq w_L(u - v)$.

Figure 1 defines the *Gray* map which assigns integers modulo 4 or quaternary phases (see Remark 1) to binary pairs. For a vector, the map is applied to each entry and concatenated row-wise to return a row vector, thereby adhering to our convention for binary vectors (see Remark 1). Distance around the circle defines the Lee metric on $\mathbb{Z}_4^N$ and Gray encoding is an isometry from ($\mathbb{Z}_4^N$, Lee metric) to ($\mathbb{Z}_2^{2N}$, Hamming metric). However, since $\mathfrak{g}(1+3) \neq \mathfrak{g}(1) + \mathfrak{g}(3)$, the Gray map is non-linear. Hence the *binary* Kerdock and Delsarte-Goethals codes obtained by Gray-mapping the codewords in $\text{K}(m)$ and $\text{DG}(m, r)$, respectively, are *non-linear* (see [42, Chapter 12]).

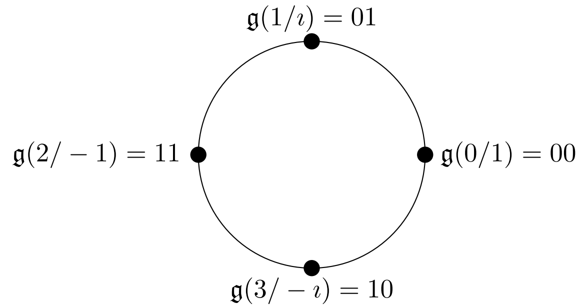

Fig. 1. The Gray map assigning integers modulo 4 or quaternary phases to binary pairs (that are length-2 row vectors).

The Gray map is also an isometry from (length-N vectors of quaternary phases, Euclidean metric) to ($\mathbb{Z}_2^{2N}$, Hamming metric). This is formalized in the following lemma.

Lemma 9: Let $\mathsf{u}, \mathsf{v} \in \mathbb{C}^N$ be two length-N vectors of quaternary phases. Then

$$\langle \mathsf{u} - \mathsf{v}, \mathsf{u} - \mathsf{v} \rangle = 2d_H(\mathfrak{g}(\mathsf{u}), \mathfrak{g}(\mathsf{v})), \tag{21}$$

where d_H denotes the Hamming distance.

Next, we prove a lemma establishing the relation between $\text{DG}(m, r)$ and the common eigenspace of $E([I_m \mid P])$ determined by a binary symmetric matrix P (see Remark 6). Note that we denote the maximal commutative subgroup determined by the rows of $[I_m \mid P]$ as $E([I_m \mid P])$, and that we do not normalize eigenvectors (stabilizer states) in this Section, since the Gray map needs to be applied to quaternary phases.

Lemma 10: Given a binary symmetric matrix P, the (column) vectors $[\imath^{xPx^T + 2wx^T}]_{x \in \mathbb{F}_2^m}$ are common eigenvectors of the maximal commutative subgroup $E([I_m \mid P])$. Each eigenvector has Euclidean length $\sqrt{N} = 2^{m/2}$.

Proof: It is possible to prove this result by direct calculation, i.e., by calculating $E(a, aP) \cdot [\imath^{xPx^T + 2wx^T}]_{x \in \mathbb{F}_2^m}$ for some $a \in \mathbb{F}_2^m$, but the following argument uses the mathematical framework described in Section II. Note that

$$[\imath^{xPx^T + 2wx^T}]_{x \in \mathbb{F}_2^m} = \sum_{x \in \mathbb{F}_2^m} \imath^{xPx^T + 2wx^T} e_x, \tag{22}$$

where e_x denotes the standard basis vector in $\mathbb{C}^N$ with a 1 in the position x and 0 elsewhere.

The columns $[\imath^{2wx^T}]_{x \in \mathbb{F}_2^m} = [(-1)^{wx^T}]_{x \in \mathbb{F}_2^m}$ of the Walsh-Hadamard matrix H_N, where $w \in \mathbb{F}_2^m$ indexes the column, are common eigenvectors of the maximal commutative subgroup $X_N = E([I_m \mid 0])$. The Clifford operator $t_P = \text{diag}\left(\imath^{xPx^T}\right)$ corresponds to the binary symplectic matrix $T_P = \begin{bmatrix} I_m & P \\ 0 & I_m \end{bmatrix}$ (see Table I). Hence conjugation by t_P maps $E([I_m \mid 0])$ to $E([I_m \mid P])$, i.e., $t_P E(a, 0) t_P^\dagger = E(a, aP)$, and so the common eigenvectors of $E([I_m \mid P])$ are

$$t_P \cdot [\imath^{2wx^T}]_{x \in \mathbb{F}_2^m} = [\imath^{xPx^T + 2wx^T}]_{x \in \mathbb{F}_2^m}.$$

It is easily verified that for any $a \in \mathbb{F}_2^m$,

$$\left(t_P E(a, 0) t_P^\dagger\right) \; t_P \cdot [\imath^{2wx^T}]_{x \in \mathbb{F}_2^m} = \pm[\imath^{xPx^T + 2wx^T}]_{x \in \mathbb{F}_2^m}.$$

■

Now we have the following important observation. Given $\mathsf{v} \in \mathbb{C}^N$, define

$$S_{\mathsf{v}} \triangleq \{g \in HW_N \colon g\mathsf{v} = \alpha\mathsf{v}, \text{ where } \alpha \in \mathbb{C} \text{ and } |\alpha| = 1\}. \tag{23}$$

Lemma 11:

(a) S_{v} is commutative.

(b) There is a 1-N correspondence between maximal commutative subgroups of HW_N and stabilizer states.

Proof:

(a) If $E(a,b), E(a',b') \in S_{\mathsf{v}}$ then

$$E(a,b)E(a',b')\mathsf{v} = \alpha\alpha'\mathsf{v} = \alpha'\alpha\mathsf{v} = E(a',b')E(a,b)\mathsf{v}.$$

(b) If v is a stabilizer state then S_{v} is a maximal commutative subgroup of HW_N. ∎

Remark 12: All stabilizer states of maximal commutative subgroups of HW_N *disjoint* from Z_N can be obtained by exponentiating Delsarte-Goethals codewords, then multiplying the vector of quaternary phases by $N^{-\frac{1}{2}}$. The maximal commutative subgroups $E([I_m \mid P_z])$ determined by the Kerdock matrices P_z intersect trivially. Given a non-identity Hermitian Pauli matrix $E(a,b)$, it follows that there is a sign $\epsilon \in \{\pm 1\}$ such that $\epsilon E(a,b)$ is in one of the $N+1$ subgroups determined by all $P_z \in P_{\mathrm{K}}(m)$ and $Z_N = E([0 \mid I_m])$.

Therefore stabilizer states connect the *classical* world of Kerdock and Delsarte-Goethals codes and the *quantum* world of maximal commutative subgroups of the Pauli group HW_N. This synergy has proven successful in several applications [10]–[12], [14], [43], [44] and our construction of a unitary 2-design here, from stabilizer states, is another instance.

Remark 13: Note that in Lemma 10 we only considered $\kappa = 0$ while exponentiating codewords $c_{\mathsf{u}} \in \mathrm{DG}(m,r)$. This is to ensure that the resulting eigenvector corresponds to a ± 1 eigenvalue (and not a value in $\{\pm 1, \pm\imath\}$). However, we will consider all $\kappa \in \mathbb{Z}_4$ while calculating the weight distribution.

Given $P \in P_{\mathrm{DG}}(m,r)$, we scale the common eigenvectors of $E([I_m \mid P])$ by $\sqrt{N}$ to obtain a set $V(P)$ of length-N vectors of quaternary phases. (Note the similarity to the notation $V(S)$ used in Section II, and observe that here we consider all eigenvectors, albeit unnormalized, and not just the $+1$ eigenspace.) Therefore, if we can compute the Hermitian inner products between these unnormalized stabilizer states then we can use Lemma 9 to calculate the weight distribution of Kerdock and Delsarte-Goethals codes. Note that despite being non-linear codes the weight and distance distributions of these codes coincide, as shown in [6, Chapter 15].

Lemma 14: Let $P_1, P_2 \in P_{\mathrm{DG}}(m,r)$ be distinct. Fix $\mathsf{v} \in V(P_2)$ and let u run through $V(P_1)$. If $\mathrm{rank}(P_1 + P_2) = k$ then

$$|\langle \mathsf{u}, \mathsf{v}\rangle|^2 = \begin{cases} 2^{2m-k} & \text{for } 2^k \text{ eigenvectors } \mathsf{u}, \\ 0 & \text{for } 2^m - 2^k \text{ eigenvectors } \mathsf{u}. \end{cases} \tag{24}$$

Proof: Let $Q = [I_m \mid P_1] \cap [I_m \mid P_2]$ represent a basis for the subspace formed by intersecting the spaces generated by $[I_m \mid P_1]$ and $[I_m \mid P_2]$. Then $\dim(Q) = m - k$. Let $[a_1, b_1], \ldots, [a_{m-k}, b_{m-k}]$ be a basis for Q, and complete to bases for P_1 and P_2 by adding vectors $[c_j, d_j], j = m-k+1, \ldots, m$ and $[c'_j, d'_j], j = m-k+1, \ldots, m$ respectively. Since v is fixed, using (13), there are *fixed* $f_i, t_j \in \{\pm 1\}$ such that

$$\left(\frac{1}{\sqrt{N}}\mathsf{v}\right)\left(\frac{1}{\sqrt{N}}\mathsf{v}^\dagger\right) = \prod_{i=1}^{m-k} \frac{(I_N + f_i E(a_i,b_i))}{2} \prod_{j=m-k+1}^{m} \frac{(I_N + t_j E(c'_j, d'_j))}{2},$$

and since the only constraint for u is to be from $V(P_1)$,

$$\left(\frac{1}{\sqrt{N}}\mathsf{u}\right)\left(\frac{1}{\sqrt{N}}\mathsf{u}^\dagger\right) = \prod_{i=1}^{m-k} \frac{(I_N + e_i E(a_i,b_i))}{2} \prod_{j=m-k+1}^{m} \frac{(I_N + s_j E(c_j, d_j))}{2},$$

where $e_i, s_i \in \{\pm 1\}$ are variable. Since $|\langle \mathsf{u}, \mathsf{v}\rangle|^2 = \mathrm{Tr}(\mathsf{u}\mathsf{u}^\dagger\mathsf{v}\mathsf{v}^\dagger)$ it only remains to calculate $\mathrm{Tr}(\mathsf{u}\mathsf{u}^\dagger\mathsf{v}\mathsf{v}^\dagger)$. If $e_i = f_i \ \forall\, i$, then

$$(I_N + e_i E(a_i,b_i))(I_N + f_i E(a_i,b_i)) = 2(I_N + e_i E(a_i,b_i))$$

so that

$$\mathrm{Tr}(\mathsf{u}\mathsf{u}^\dagger\mathsf{v}\mathsf{v}^\dagger) = 2^{m-k}\mathrm{Tr}\Bigg(\prod_{i=1}^{m-k}(I_N + e_i E(a_i,b_i)) \times \prod_{j=m-k+1}^{m}(I_N + s_j E(c_j,d_j)) \times \prod_{j=m-k+1}^{m}(I_N + t_j E(c'_j,d'_j))\Bigg).$$

Expanding the right hand side, the only term with nonzero trace is the identity with trace 2^m. Hence in this case $\mathrm{Tr}(\mathsf{u}\mathsf{u}^\dagger\mathsf{v}\mathsf{v}^\dagger) = 2^{2m-k}$. The k eigenvalues s_j can be freely chosen, so there are 2^k eigenvectors in this case.

If $e_i \neq f_i$ for some i, then

$$(I_N + e_i E(a_i,b_i))(I_N + f_i E(a_i,b_i)) = 0$$

and $\mathrm{Tr}(\mathsf{u}\mathsf{u}^\dagger\mathsf{v}\mathsf{v}^\dagger) = 0$. There are $2^m - 2^k$ such eigenvectors.

Finally, if $k = m$ then $\mathrm{Tr}(\mathsf{u}\mathsf{u}^\dagger\mathsf{v}\mathsf{v}^\dagger) = \mathrm{Tr}(I_N) = 2^m \ \forall\, \mathsf{u}$. ∎

Corollary 15: For $P_1, P_2 \in P_{\mathrm{K}}(m)$, since $\mathrm{rank}(P_1 + P_2) \in \{0, m\}$ the inner products are

$$|\langle \mathsf{u}, \mathsf{v}\rangle|^2 = \begin{cases} 0 & \text{if } P_1 = P_2 \text{ and } \mathsf{u} \neq \mathsf{v} \\ 2^m & \text{if } P_1 \neq P_2, \\ 2^{2m} & \text{if } (P_1 = P_2 \text{ and}) \ \mathsf{u} = \mathsf{v}. \end{cases} \tag{25}$$

The following theorem is the only result in this Section that is restricted to Kerdock codes (and requires m to be odd).

Theorem 16: Let m be odd. The weight distribution $A_i, i = 0, \ldots, 2^{m+1}$ of the classical binary Kerdock code of length 2^{m+1} is as follows.

i	0	$2^m - 2^{(m-1)/2}$	2^m	$2^m + 2^{(m-1)/2}$	2^{m+1}
A_i	1	$2^{2m+1} - 2^{m+1}$	$2^{m+2} - 2$	$2^{2m+1} - 2^{m+1}$	1

Proof: We explicitly use Corollary 15 and Lemma 9 to calculate the weight distribution. Fix a vector v of quaternary phases obtained by exponentiating a codeword

$$c_{\mathsf{v}} = [xP_2x^T + 2w_2x^T + \kappa_2]_{x \in \mathbb{F}_2^m}$$

in the $\mathbb{Z}_4$-linear Kerdock code. Consider any vector u of quaternary phases obtained by exponentiating a second codeword

$$c_{\mathsf{u}} = [xP_1x^T + 2w_1x^T + \kappa_1]_{x \in \mathbb{F}_2^m}.$$

Note that Lemmas 10 and 14 considered $\kappa_1 = \kappa_2 = 0$ so that the eigenvalues are ± 1 (and not in $\{\pm 1, \pm \imath\}$), but we have to account for these factors here.

Let n_j be the number of indices $x \in \mathbb{F}_2^m$ for which $(c_{\mathsf{u}})_x - (c_{\mathsf{v}})_x = j$, for $j \in \mathbb{Z}_4$. Since the Gray map preserves the Lee metric, the Hamming distance between the Gray images of c_{u} and c_{v} is $d_H(\mathfrak{g}(c_{\mathsf{u}}), \mathfrak{g}(c_{\mathsf{v}})) = n_1 + 2n_2 + n_3$. Since $n_0 + n_1 + n_2 + n_3 = 2^m$ we simply have to relate n_0 and n_2 to obtain $d_H(\mathfrak{g}(c_{\mathsf{u}}), \mathfrak{g}(c_{\mathsf{v}}))$. Observe that $\langle \mathsf{u}, \mathsf{v} \rangle = (n_0 - n_2) + (n_1 - n_3)\imath$. Lemma 9 implies

$$\begin{aligned} & 2^{m+1} - 2\mathrm{Re}[\langle \mathsf{u}, \mathsf{v} \rangle] = 2d_H(\mathfrak{g}(c_{\mathsf{u}}), \mathfrak{g}(c_{\mathsf{v}})) \\ & \Rightarrow d_H(\mathfrak{g}(c_{\mathsf{u}}), \mathfrak{g}(c_{\mathsf{v}})) = 2^m - (n_0 - n_2). \end{aligned} \tag{26}$$

Now we observe three distinct cases for the codeword $c_{\mathsf{u}} - c_{\mathsf{v}}$. Note that there are 2^{2m+2} codewords in $\mathrm{K}(m)$.

(i) $P_1 = P_2, w_1 = w_2$: If $\kappa_1 - \kappa_2 = 0$ then we have the all-zeros codeword, and if $\kappa_1 - \kappa_2 = 2$ then we have the all-ones codeword. However, if $\kappa_1 - \kappa_2 \in \{1, 3\}$ then $n_0 - n_2 = 0$ and this determines two codewords of weight 2^m (more precisely, at distance 2^m from c_{v}).

(ii) $P_1 = P_2, w_1 \neq w_2$: From Corollary 15, irrespective of κ_1, κ_2, we have $\langle \mathsf{u}, \mathsf{v} \rangle = 0$, which implies $n_0 - n_2 = 0$ and hence the distance is 2^m. This determines another $(2^m - 1)2^2 = 2^{m+2} - 4$ codewords of weight 2^m.

(iii) $P_1 \neq P_2$: From Corollary 15 we have $|\langle \mathsf{u}, \mathsf{v} \rangle|^2 = 2^m$, which implies $(n_0 - n_2)^2 + (n_1 - n_3)^2 = 2^m$. Since m is odd, and n_j are non-negative integers, direct calculation shows that this means $(n_0 - n_2)^2 = (n_1 - n_3)^2 = 2^{m-1}$ and therefore $n_0 - n_2 = \pm 2^{(m-1)/2}$. More formally, since the Gaussian integers $\mathbb{Z}[\imath]$ are a unique factorization domain, we have $(n_0 - n_2) + (n_1 - n_3)\imath = (\pm 1 \pm \imath)2^{(m-1)/2}$. Thus we have weights $2^m \pm 2^{(m-1)/2}$. We have $2^{2m+2} - 2^{m+2}$ codewords remaining and it is easy to see that the signs occur equally often. Hence there are $2^{2m+1} - 2^{m+1}$ codewords of each weight. ∎

IV. Mutually Unbiased Bases from $P_{\mathrm{K}}(m)$

In this Section, we will organize all stabilizer states determined by $P_z \in P_{\mathrm{K}}(m)$, and I_N, into a matrix to form mutually unbiased bases and analyze its symmetries. This symmetry group will eventually lead to the construction of the unitary 2-design. We first state a result that holds for stabilizer states determined by matrices from general Delsarte-Goethals sets.

Definition 17: Given a collection M of unit vectors in $\mathbb{C}^N$ (Grassmannian lines) the *chordal distance* $\mathrm{chor}(S)$ is given by

$$\mathrm{chor}(M) \triangleq \min_{(\mathsf{u},\mathsf{v}) \in M} \sqrt{1 - |\langle \mathsf{u}, \mathsf{v} \rangle|^2}. \tag{27}$$

It follows from Lemma 14 that the Delsarte-Goethals set $P_{\mathrm{DG}}(m, r)$ determines $2^{m(r+2)}$ complex lines (stabilizer states) in $\mathbb{C}^N$ with chordal distance $\sqrt{1 - 2^{-(m-2r)}}$ (cf. [52]).

Definition 18: Two $N \times N$ unitary matrices U and V are said to be *mutually unbiased* if $|\langle \mathsf{u}, \mathsf{v} \rangle| = N^{-\frac{1}{2}}$ for all columns u of U, and all columns v of V. Each matrix is interpreted as an orthonormal basis and collections of such unitary matrices that are pairwise mutually unbiased are called *mutually unbiased bases* (MUBs). Vectors in each orthonormal basis look like noise to the other bases (due to the small inner product).

Corollary 15, when applied to normalized eigenvectors, shows that the N eigenbases determined by the Kerdock set $P_{\mathrm{K}}(m)$ are mutually unbiased (also see Remark 12). Let $\mathcal{B}_{\mathrm{K}}(m)$ denote the collection of these N eigenbases (of $E([I_m \mid P])$ for all $P \in P_{\mathrm{K}}(m)$) along with the eigenbasis I_N of $E([0 \mid I_m])$. This is a set of $N+1$ mutually unbiased bases and they determine an ensemble of $N(N+1)$ complex lines (stabilizer states) that is extremal [13]. In this Section we provide an elementary description of their group of Clifford symmetries.

A. The Kerdock MUBs

Recollect from Section III-A that the Kerdock matrices are $P_z = A_z W$, where W is the binary symmetric and Hankel matrix that satisfies $\mathrm{Tr}(xy) = xWy^T$ and A_z represents multiplication by z, both in $\mathbb{F}_{2^m}$. Using the result of Lemma 10, define N mutually unbiased bases

$$M_z \triangleq t_{P_z} H_N = \mathrm{diag}\left(\imath^{xP_z x^T}\right) H_N, \ z \in \mathbb{F}_{2^m}, \tag{28}$$

where $[H_N]_{x,y} \triangleq \frac{1}{\sqrt{N}}(-1)^{xy^T}$, for $x, y \in \mathbb{F}_2^m$, is the Walsh-Hadamard matrix of order N. Note that $M_0 = H_N$ and that all columns of M_z have Euclidean length $\frac{1}{\sqrt{N}}$. Complete the MUBs by appending the matrix $M_\infty \triangleq I_N$. The common eigenspaces of the maximal commutative subgroup $E([I_m \mid P_z])$ are the columns of M_z and the common eigenspaces of $E([0 \mid I_m])$ are the standard unit coordinate vectors. Hence the set of *Kerdock MUBs*

$$\mathcal{B}_{\mathrm{K}}(m) \triangleq \{I_N, M_z \colon z \in \mathbb{F}_{2^m}\} \tag{29}$$

is a maximal collection of mutually unbiased bases [13].

B. Symmetries of Kerdock MUBs

Let M be the $N \times N(N+1)$ matrix given by

$$M \triangleq [\ M_\infty \ \mid \ M_0 \ \mid \ \cdots \ \mid \ M_z \ \mid \ \cdots\ ]. \tag{30}$$

Note that $M_\infty = I_N$ and $M_0 = H_N$.

Definition 19: A *symmetry* of M is a pair (U, G) such that $UMG = M$, where U is an $N \times N$ unitary matrix, and G is a generalized permutation matrix, i.e., $G = \Pi D$ where Π is a permutation matrix and D is a diagonal matrix of quaternary phases.

Observe that for any such symmetry, G can undo the action of U if and only if U induces a (generalized) permutation on the columns of M. Moreover, since U is unitary it has to preserve inner products, so Corollary 15 implies that U can only permute the bases M_z and permute columns within each basis, or equivalently permute the corresponding maximal commutative subgroups and permute elements within each subgroup, respectively, by conjugation.

Lemma 20: For any symmetry (U, G) of M, the unitary matrix U is an element of the Clifford group Cliff_N.

Proof: A Pauli matrix $E(a,b) \in E([I_m \mid P_z])$ that fixes M_z can be written as $E(a,b) = \sum_{\mathsf{v} \in M_z} \epsilon_{\mathsf{v}} \mathsf{v}\mathsf{v}^\dagger$, where $\epsilon_{\mathsf{v}} = \pm 1$ for all v. Since U permutes the eigenbases M_z, it follows that $U\mathsf{v} \in M_{z'}$, for some $z' \in \mathbb{F}_{2^m} \cup \{\infty\}$, is fixed by $UE(a,b)U^\dagger$ which must again be a Pauli matrix. Hence U is a Clifford element. ∎

We first observe the symmetries induced by elements of HW_N.

1) Pauli Matrices $E(a,0)$ and $E(0,a)$: The group $E([I_m \mid 0])$ of Pauli matrices $E(a,0)$ fixes each column of $M_0 = H_N$ and acts transitively on the columns of each of the other N blocks. The group $E([0 \mid I_m])$ of Pauli matrices $E(0,a)$ fixes each column of $M_\infty = I_N$ and acts transitively on the columns of each of the remaining blocks.

Definition 21: The *projective special linear group* $\mathrm{PSL}(2, 2^m)$ is the group of all transformations

$$f(z) = \frac{az+b}{cz+d}, \text{ where } a,b,c,d \in \mathbb{F}_{2^m}, ad+bc = 1, \quad (31)$$

acting on the projective line $\mathbb{F}_{2^m} \cup \{\infty\}$. The transformation f is associated with the action of the 2×2 matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ on 1-dimensional spaces, since

$$f\colon \begin{bmatrix} z \\ 1 \end{bmatrix} \mapsto \begin{bmatrix} az+b \\ cz+d \end{bmatrix} \equiv \begin{bmatrix} 1 \\ 0 \end{bmatrix} \text{ or } \begin{bmatrix} \frac{az+b}{cz+d} \\ 1 \end{bmatrix}.$$

The *projective linear group* $\mathrm{P\Gamma L}(2, 2^m)$ is the group of all transformations

$$f(z) = \frac{az^{2^{-i}}+b}{cz^{2^{-i}}+d}, \text{ where } a,b,c,d \in \mathbb{F}_{2^m}, ad+bc = 1, \quad (32)$$

and $i \in \{0, 1, \ldots, m-1\}$. The orders are

$$\begin{aligned} |\mathrm{PSL}(2,2^m)| &= (N+1)N(N-1) = 2^{3m} - 2^m, \\ |\mathrm{P\Gamma L}(2,2^m)| &= (N+1)N(N-1)m. \end{aligned} \quad (33)$$

Now we analyze the symmetries induced by elements of the binary symplectic group $\mathrm{Sp}(2m, \mathbb{F}_2)$.

2) Clifford Symmetries of M: The group $\mathrm{PSL}(2, 2^m)$ is generated by the transformations $z \mapsto z + x, z \mapsto zx$, and $z \mapsto 1/z$. The group $\mathrm{P\Gamma L}(2, 2^m)$ is $\mathrm{PSL}(2, 2^m)$ enlarged by the Frobenius automorphisms $z \mapsto z^{2^{-i}} \equiv zR^{-i}$ discussed in Section III-A. We realize each of these transformations as a symmetry of M. We recall that $A_z W A_z^T = A_z^2 W$ from part (c) of Lemma 3, and for convenience we work with maximal commutative subgroups $E([I_m \mid A_z^2 W])$, i.e., the Kerdock matrices are $P_z = A_z^2 W$. Note that every field element $\beta \in \mathbb{F}_{2^m}$ is a square, so this is equivalent to $P_z = A_z W$.

(i) $z \mapsto z + x$ becomes $[I_m \mid A_z^2 W] \mapsto [I_m \mid A_{x+z}^2 W]$:

$$\begin{aligned} [I_m \mid A_z^2 W] \begin{bmatrix} I_m & A_x^2 W \\ 0 & I_m \end{bmatrix} &= [I_m \mid (A_z^2 + A_x^2) W] \\ &\equiv [I_m \mid (A_{x+z}^2) W]. \end{aligned} \quad (34)$$

(ii) $z \mapsto xz$ becomes $[I_m \mid A_z^2 W] \mapsto [I_m \mid A_{xz}^2 W]$:

$$\begin{aligned} [I_m \mid A_z^2 W] \begin{bmatrix} A_x^{-1} & 0 \\ 0 & A_x^T \end{bmatrix} &= [A_x^{-1} \mid A_z^2 W A_x^T] \\ &= [A_x^{-1} \mid A_x A_z^2 W] \\ &\equiv [I_m \mid A_{xz}^2 W]. \end{aligned} \quad (35)$$

(iii) $z \mapsto 1/z$ becomes $[I_m \mid A_z^2 W] \mapsto [I_m \mid A_{z^{-1}}^2 W]$:

$$\begin{aligned} [I_m \mid A_z^2 W] \begin{bmatrix} 0 & I_m \\ I_m & 0 \end{bmatrix} \begin{bmatrix} W^{-1} & 0 \\ 0 & W^T \end{bmatrix} & \\ = [A_z^2 W \mid I_m] \begin{bmatrix} W^{-1} & 0 \\ 0 & W \end{bmatrix} & \\ = [A_z^2 \mid W] & \\ \equiv [I_m \mid A_{z^{-1}}^2 W]. & \end{aligned} \quad (36)$$

Note that if we start with $z = 0$, i.e., the subgroup $E([I_m \mid 0])$, then since W is invertible the final subgroup is $E([0 \mid I_m])$, interpreted as $z = \infty$.

(iv) $z \mapsto z' \triangleq z^{2^{-i}}$ becomes $[I_m \mid A_z^2 W] \mapsto [I_m \mid A_{z'}^2 W]$:

$$\begin{aligned} [I_m \mid A_z^2 W] \begin{bmatrix} R^{-i} & 0 \\ 0 & (R^i)^T \end{bmatrix} &= [R^{-i} \mid A_z^2 W (R^i)^T] \\ &= [R^{-i} \mid A_z^2 R^{-i} W] \\ &\equiv [I_m \mid A_{z'}^2 W]. \end{aligned} \quad (37)$$

Let $\mathfrak{P}_{\mathrm{K},m}$ be the group of symplectic transformations generated by (i), (ii) and (iii) above, and let $\mathfrak{P}_{\mathrm{K},m}^*$ be the group $\mathfrak{P}_{\mathrm{K},m}$ enlarged by the generators (iv). Thus, using notation in Table I, we have

$$\mathfrak{P}_{\mathrm{K},m} \triangleq \langle T_{A_x^2 W},\ L_{A_x^{-1}},\ \Omega L_{W^{-1}}; x \in \mathbb{F}_{2^m} \rangle \cong \mathrm{PSL}(2, 2^m), \quad (38)$$

$$\mathfrak{P}_{\mathrm{K},m}^* \triangleq \langle T_{A_x^2 W},\ L_{R^{-i} A_x^{-1}},\ \Omega L_{W^{-1}}; x \in \mathbb{F}_{2^m} \rangle \cong \mathrm{P\Gamma L}(2, 2^m). \quad (39)$$

Although $T_W^2 = I_{2m}$, in the unitary group we have $t_W^2 = E(0, d_W)$. Therefore the corresponding Clifford elements will generate a group larger than $\mathrm{PSL}(2, 2^m)$ and $\mathrm{P\Gamma L}(2, 2^m)$. Each symplectic matrix in the above groups can be transformed into a quantum circuit (or simply a unitary matrix) by expressing it as a product of standard symplectic matrices from Table I (see [33, Section II]).

Remark 22: Note that $\Omega \notin \mathfrak{P}_{\mathrm{K},m}$ but $\Omega L_{W^{-1}} \in \mathfrak{P}_{\mathrm{K},m}$, which means H_N does not permute columns of M but $H_N \ell_{W^{-1}}$ does. Hence, for example, to map $[0, a]$ to $[a, 0]$ one sequence would be $(\Omega L_{W^{-1}}) \cdot L_{A_b^{-1}}$, where b satisfies $a W^{-1} A_b^{-1} = a$. This does not force $A_b^{-1} = W$.

Lemma 23: Any element of $\mathfrak{P}_{\mathrm{K},m}$ can be described as a product of at most 4 basis symplectic matrices given in Section IV-B2.

Proof: Using the results in this Section, a general block permutation $[I_m \mid A_z^2 W] \mapsto [I_m \mid A_{\frac{az+b}{cz+d}}^2 W]$ is realized as

$$\begin{aligned} [I_m \mid A_z^2 W] \begin{bmatrix} A_d^2 & A_b^2 W \\ W^{-1} A_c^2 & (A_a^2)^T \end{bmatrix} &= [A_{cz+d}^2 \mid A_{az+b}^2 W] \\ &\equiv \left[I_m \mid A_{\frac{az+b}{cz+d}}^2 W \right]. \end{aligned}$$

It can be verified that the above is a valid symplectic matrix and satisfies all conditions in (9). We now show that this matrix can be decomposed as a product of 4 basis matrices.

We use the results in Lemma 3 and observe the following:

$$\begin{bmatrix} A_x^{-2} & 0 \\ 0 & (A_x^2)^T \end{bmatrix} \begin{bmatrix} 0 & W^T \\ W^{-1} & 0 \end{bmatrix} = \begin{bmatrix} 0 & A_x^{-2} W \\ W^{-1} A_x^2 & 0 \end{bmatrix};$$

$$\begin{bmatrix} I_m & A_y^2 W \\ 0 & I_m \end{bmatrix} \begin{bmatrix} 0 & A_x^{-2} W \\ W^{-1} A_x^2 & 0 \end{bmatrix} = \begin{bmatrix} A_{xy}^2 & A_x^{-2} W \\ W^{-1} A_x^2 & 0 \end{bmatrix};$$

$$\begin{bmatrix} A_{xy}^2 & A_x^{-2} W \\ W^{-1} A_x^2 & 0 \end{bmatrix} \begin{bmatrix} I_m & A_w^2 W \\ 0 & I_m \end{bmatrix} = \begin{bmatrix} A_{xy}^2 & A_{wxy+x^{-1}}^2 W \\ W^{-1} A_x^2 & (A_{wx}^2)^T \end{bmatrix}$$

Hence we set $x \triangleq c, w \triangleq \frac{a}{c}, y \triangleq \frac{d}{c}$ so that $wxy + x^{-1} = \frac{ad+1}{c} = b$ and the resultant matrix matches the general symplectic matrix given above. ■

Corollary 24: Let $a, b, c, d \in \mathbb{F}_{2^m}$ be such that $ad + bc = 1$. The isomorphism $\tau\colon \mathrm{PSL}(2, 2^m) \to \mathfrak{P}_{\mathrm{K},m}$ can be defined as

$$\tau\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) \triangleq T_{A_{d/c}^2 W} \cdot L_{A_c^{-2}} \cdot \Omega L_{W^{-1}} \cdot T_{A_{a/c}^2 W}. \quad (40)$$

Observe that this provides a systematic procedure to sample from the group $\mathfrak{P}_{\mathrm{K},m}$. By choosing $\alpha, \beta, \delta \in \mathbb{F}_{2^m}$ uniformly at random, a symmetry element can be constructed as

$$F_{\alpha,\beta,\delta} \triangleq T_{A_\alpha W} \cdot L_{A_\beta} \cdot (\Omega L_{W^{-1}} \cdot T_{A_\delta W}). \quad (41)$$

The first two factors provide transitivity on the Hermitian matrices of all maximal commutative subgroups except $Z_N = E([0 \mid I_m])$, and the last factor enables exchanging any subgroup $E([I_m \mid P_z])$ with $E([0 \mid I_m])$ (see Lemma 31).

We complete this Section by observing that the symmetry group can be enlarged by including the Frobenius automorphisms R from Section III-A.

Lemma 25: An arbitrary element from $\mathfrak{P}_{\mathrm{K},m}^*$ specified by $a, b, c, d \in \mathbb{F}_{2^m}$ and $i \in \{0, \ldots, m-1\}$ takes the form

$$F = \begin{bmatrix} R^{-i} A_d^2 & R^{-i} A_b^2 W \\ W^{-1} R^{-i} A_c^2 & (R^i)^T (A_a^2)^T \end{bmatrix}, \quad (42)$$

with $ad + bc = 1$, and realizes the block permutation

$$[I_m \mid A_z^2 W] \longmapsto \left[I_m \mid A_{\frac{az'+b}{cz'+d}}^2 W\right],\ z' \triangleq z^{2^{-i}}. \quad (43)$$

Proof: See Appendix A. ■

V. Unitary 2-Designs from the Kerdock MUBs

In this Section, we show that the unitary transformations determined by $\mathfrak{P}_{\mathrm{K},m}$, along with Pauli matrices $D(a,b) \in HW_N$, form a unitary 2-design. We first define a graph on Pauli matrices, where Clifford elements act as graph automorphisms. We then show that a group of automorphisms that acts transitively on vertices forms a unitary 2-design. Finally we show that a group of automorphisms that acts transitively on vertices, on edges, and on non-edges forms a unitary 3-design.

Definition 26: The *Heisenberg-Weyl graph* $\mathbb{H}_N$ has $N^2 - 1$ vertices, labeled by pairs $\pm E(a,b)$ with $[a,b] \neq [0,0]$ where vertices labeled $\pm E(a,b)$ and $\pm E(c,d)$ are joined if $E(a,b)$ commutes with $E(c,d)$. We use $[a,b]$ to represent the vertex labeled $\pm E(a,b)$ and $[a,b]$ — $[c,d]$ to represent an edge between two vertices.

Remark 27: Elements of the Clifford group act by conjugation on HW_N, inducing automorphisms of the graph $\mathbb{H}_N$. We shall distinguish two types of edges in $\mathbb{H}_N$. *Type* 1 edges connect vertices from the same maximal commutative subgroup $E([I_m \mid P_z]), z \in \mathbb{F}_{2^m}$, or from $E([0 \mid I_m])$. *Type* 2 edges connect vertices from different maximal commutative subgroups.

To see that $\mathrm{Aut}(\mathbb{H}_N) = \mathrm{Sp}(2m, \mathbb{F}_2)$, determine a symplectic matrix to reduce an arbitrary graph automorphism to an automorphism π that fixes $[e_i, 0], [0, e_i], i = 1, \ldots, m$, then show that π fixes every vertex. This essentially amounts to solving for a symplectic matrix satisfying a linear system.

Definition 28 ([53, Def. 2.4]): A *strongly regular graph* with parameters (n, t, λ, μ) is a graph with n vertices, where each vertex has degree t, and where the number of vertices joined to a pair of distinct vertices x, y is λ or μ according as x, y are joined or not joined respectively.

Lemma 29: The Heisenberg-Weyl graph $\mathbb{H}_N$ is strongly regular with parameters

$$n = N^2 - 1,\ t = \frac{N^2}{2} - 2,\ \lambda = \frac{N^2}{4} - 3,\ \mu = \frac{N^2}{4} - 1. \quad (44)$$

Proof: A vertex $[c,d]$ joined to a given vertex $[a,b]$ is a solution to $[a,b]\Omega[c,d]^T = 0$ (due to (4)). This is a linear system with a single constraint, and after eliminating the solutions $[0,0]$ and $[a,b]$ we are left with $t = \frac{N^2}{2} - 2$ distinct vertices $[c,d]$ joined to $[a,b]$.

Given vertices $[a,b], [c,d]$ a vertex $[e,f]$ joined to both $[a,b]$ and $[c,d]$ is a solution to a linear system with two independent constraints. When $[a,b]$ is not joined to $[c,d]$, we only need to eliminate the solution $[0,0]$. When $[a,b]$ is joined to $[c,d]$ we need to eliminate $[0,0], [a,b]$ and $[c,d]$. ■

Remark 30: The number of edges in $\mathbb{H}_N$ is $(N^2-1)(\frac{N^2}{2} - 2)$. The number of type-1 edges is $(N+1)(N-1)(N-2)/2$ and the number of type-2 edges is $(N^2-1)(\frac{N^2}{2} - N)/2$.

Lemma 31:

(a) The symplectic group $\mathrm{Sp}(2m, \mathbb{F}_2)$ acts transitively on vertices, on edges, and on non-edges of $\mathbb{H}_N$.

(b) The groups $\mathfrak{P}_{\mathrm{K},m}$ and $\mathfrak{P}_{\mathrm{K},m}^*$ act transitively on vertices of $\mathbb{H}_N$.

Proof: Part (a) is well-known in symplectic geometry, and can also be proven by direct calculation using symplectic matrices.

(b) Since $\mathfrak{P}_{\mathrm{K},m}$ acts transitively on maximal commutative subgroups $E([0 \mid I_m]), E([I_m \mid P_z]), z \in \mathbb{F}_{2^m}$ (see (34) and (36)), we need only show that $\mathfrak{P}_{\mathrm{K},m}$ is transitive on a particular subgroup, say $E([I_m \mid 0])$. If $a, b \in \mathbb{F}_{2^m}$ then there exists $c \in \mathbb{F}_{2^m}$ such that $b = ac$, and it follows from (35) that the symplectic matrix $\begin{bmatrix} A_c & 0 \\ 0 & A_{c^{-1}}^T \end{bmatrix}$ maps $[a, 0]$ to $[b, 0]$. ■

Remark 32: The groups $\mathfrak{P}_{\mathrm{K},m}$ and $\mathfrak{P}_{\mathrm{K},m}^*$ are not transitive on edges of $\mathbb{H}_N$ because they cannot mix type-1 and type-2 edges.

Definition 33 ([15] [54, Chap. 7]): Let k be a positive integer. An ensemble $\mathcal{E} = \{p_i, U_i\}_{i=1}^n$, where the unitary matrix U_i is selected with probability p_i, is said to be a *unitary k-design* if for all linear operators $X \in (\mathbb{C}^N)^{\otimes k}$

$$\sum_{(p,U) \in \mathcal{E}} p\ U^{\otimes k} X (U^\dagger)^{\otimes k} = \int_{\mathbb{U}_N} d\eta(U)\ U^{\otimes k} X (U^\dagger)^{\otimes k}, \quad (45)$$

where $\eta(\cdot)$ denotes the Haar measure on the unitary group $\mathbb{U}_N$. The linear transformations determined by each side of (45) are called *k-fold twirls*. A unitary k-design is defined by the property that the ensemble twirl coincides with the full unitary twirl.

We define the *Kerdock twirl* to be the linear transformation of $(\mathbb{C}^N)^{\otimes 2}$ determined by the uniformly weighted ensemble consisting of $\phi^{-1}(\mathfrak{P}_{\mathrm{K},m})$ along with Pauli matrices $D(a,b)$, where $\phi\colon \mathrm{Cliff}_N/HW_N \to \mathrm{Sp}(2m,\mathbb{F}_2)$ (from Section II). Similarly, we define the 2-fold action (in (45)) of the ensemble determined by $\mathfrak{P}^*_{\mathrm{K},m}$ as the *enlarged Kerdock twirl*.

Definition 34: An ensemble $\mathcal{E} = \{p_i, U_i\}_{i=1}^n$ of Clifford elements U_i is *Pauli mixing* if for every vertex $[a,b]$ the distribution $\{p_i, U_i E(a,b) U_i^\dagger\}$ is uniform over vertices of $\mathbb{H}_N$. The ensemble $\mathcal{E}$ is *Pauli 2-mixing* if it is Pauli mixing and if for every edge (resp. non-edge) $([a,b],[c,d])$ the distribution $\{p_i, (U_i E(a,b) U_i^\dagger, U_i E(c,d) U_i^\dagger)\}$ is uniform over edges (resp. non-edges) of $\mathbb{H}_N$.

Theorem 35: Let G be a subgroup of the Clifford group containing all $D(a,b) \in HW_N$, and let $\mathcal{E} = \{\frac{1}{|G|}, U\}_{U\in G}$ be the ensemble defined by the uniform distribution. If G acts transitively on vertices of $\mathbb{H}_N$ then $\mathcal{E}$ is a unitary 2-design, and if G acts transitively on vertices, edges and non-edges then $\mathcal{E}$ is a unitary 3-design.

Proof: Transitivity means a single orbit so that random sampling from G results in the uniform distribution on vertices, edges, or non-edges. Hence transitivity on vertices implies $\mathcal{E}$ is Pauli mixing and transitivity on vertices, edges and non-edges implies $\mathcal{E}$ is Pauli 2-mixing. It now follows from [15] or [16] that Pauli mixing (resp. Pauli 2-mixing) implies $\mathcal{E}$ is a unitary 2-design (resp. unitary 3-design). ■

Corollary 36: Random sampling from the Clifford group gives a unitary 3-design and random sampling from the groups $\mathfrak{P}_{\mathrm{K},m}, \mathfrak{P}^*_{\mathrm{K},m}$ followed by a random Pauli matrix $D(a,b)$ gives unitary 2-designs.

Puchała and Miszczak have developed a useful Mathematica® package `IntU` [55] for symbolic integration with respect to the Haar measure on unitaries. For small m, we used this utility to verify the equality in (45) explicitly for our Kerdock 2-design.

Sampling uniformly from the groups $\mathfrak{P}_{\mathrm{K},m}$ can be achieved using the *systematic* procedure shown in (41). The resultant symplectic matrix can be transformed into a quantum circuit (or simply a unitary matrix) by expressing it as a product of standard symplectic matrices from Table I (see [33, Section II]). Although our unitary 2-design is equivalent to that discovered by Cleve et al. [16], the methods we use to translate design elements to circuits are very different and much simpler. While they use sophisticated methods from finite fields to propose a circuit translation that is *tailored* for the design, our algorithm from [17] (whose details are discussed in [33, Appendix II]) is a *general purpose* procedure that can be used to translate *arbitrary* symplectic matrices to circuits. They have been able to show Clifford-gate-complexity $O(m \log m \log\log m)$ assuming the extended Riemann hypothesis is true, or $O(m \log^2 m \log\log m)$ unconditionally, both of which are *near-linear* when compared to the $O(m^2)$ gate-complexity for general Clifford elements. Although their methods come with explicit guarantees, we

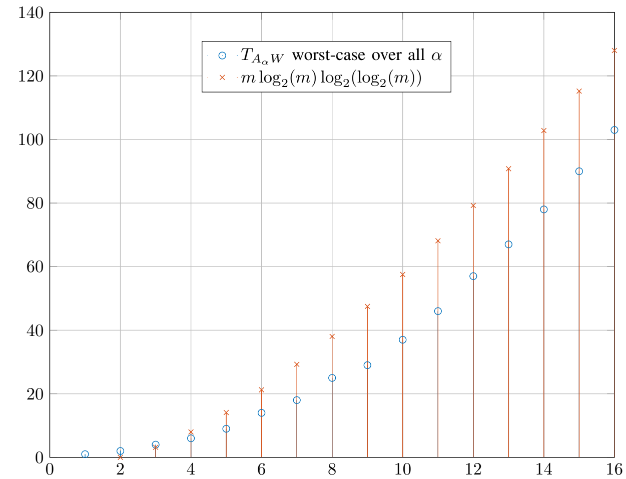

Fig. 2. The gate complexities for the element $T_{A_\alpha W}$ in (41) for varying m.

show strong empirical evidence here that our gate complexities scale as $O(m \log m \log\log m)$ unconditionally.

In our sampling procedure (41) we have three elementary forms $T_{A_\alpha W}, L_{A_\beta}$, and Ω, which translate to phase and controlled-Z gates, permutations and controlled-NOT gates, and Hadamard gates on all qubits, respectively (see [33, Appendix I]). Note that $L_{W^{-1}}$ has the same elementary form as L_{A_β}, although W is fixed for a given m. The Hadamard gates add only $O(m)$ complexity. Figures 2, 3, and 4 plot the *worst-case* complexities of the gates $T_{A_\alpha W}, L_{A_\beta}$, and $L_{W^{-1}}$ obtained using our procedure [1]. The only form that seems to grow a little faster than $O(m \log m \log\log m)$ is L_{A_β}, but a factor 1.5 appears to contain the growth, *independent* of m. A curious data point is $m = 15$ in Fig. 4, where the matrix W has zeros everywhere except the anti-diagonal, which translates to a single permutation of the qubits. Since the decomposition in (41) involves a *constant* number of factors, the overall complexity is that of the factor with largest order term. However, it is not clear if our circuits can always be organized to give a depth of $O(\log m)$ just as Cleve et al.

Hence, we have provided an alternative perspective to the *quantum* unitary 2-design discovered by Cleve et al. by establishing a connection to *classical* Kerdock codes, and simplified the description of the design as well as its translation to circuits. Since we also appear to achieve a slightly better Clifford-gate-complexity, by a factor $O(\log m)$, and provide implementations for our methods, we believe this paves the way for employing this 2-design in several applications, specifically in randomized benchmarking [24], [25].

VI. Logical Unitary 2-Designs

In this Section, we apply our synthesis algorithm [33] to logical randomized benchmarking, which was recently proposed by Combes et al. [35] as a more precise protocol to reliably estimate performance metrics for an error correction implementation, as compared to the standard approach of physical randomized benchmarking. Using this procedure, they are able

[1] Implementations online: https://github.com/nrenga/symplectic-arxiv18a

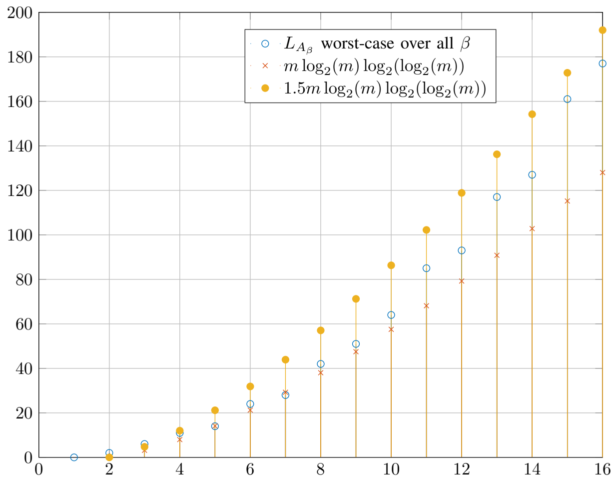

Fig. 3. The gate complexities for the element L_{A_β} in (41) for varying m.

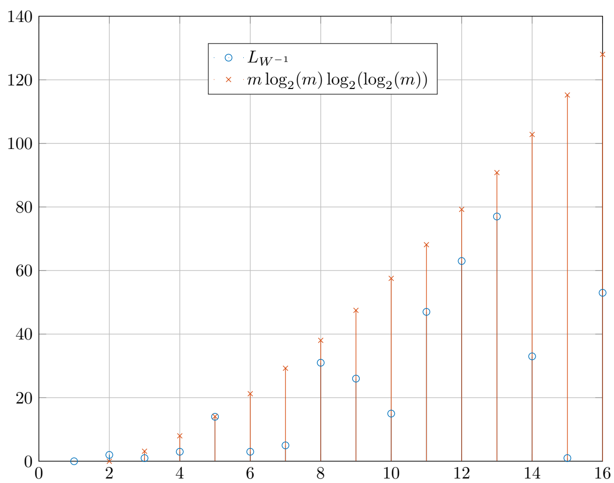

Fig. 4. The gate complexities for the element $L_{W^{-1}}$ in (41) for varying m.

to quantify the effects of imperfect logical gates, crosstalk, and correlated errors, which are typically ignored. They use the full logical Clifford group to perform benchmarking as this group forms a (logical) unitary 2-design. Our construction can be used to implement their protocol with a much smaller 2-design ($\mathfrak{P}_{\mathrm{K},m}$) and our synthesis algorithm can be used to realize the design at the logical level.

Here we show by example that we can efficiently translate *any* unitary 2-design of Clifford elements into a *logical* unitary 2-design, i.e., for a given $[\![m, m-k]\!]$ stabilizer code, produce m-qubit physical Clifford circuits that form a unitary 2-design on the $m-k$ protected qubits. As a proof of concept, we translate our Kerdock design $\mathfrak{P}_{\mathrm{K},m-k}$ on the $m-k=4$ logical qubits of the $[\![6,4,2]\!]$ CSS code [45], [56] into their physical 6-qubit implementations. The stabilizers of this code are

$$\begin{aligned} S &\triangleq \langle X^{\otimes 6}, Z^{\otimes 6} \rangle \\ &= \langle E(111111, 000000), E(000000, 111111) \rangle. \end{aligned} \tag{46}$$

The logical Pauli operators are

$$\left. \begin{array}{l} \bar{X}_1 \triangleq E(110000, 000000) \\ \bar{X}_2 \triangleq E(101000, 000000) \\ \bar{X}_3 \triangleq E(100100, 000000) \\ \bar{X}_4 \triangleq E(100010, 000000) \end{array} \right| \begin{array}{l} \bar{Z}_1 \triangleq E(000000, 010001) \\ \bar{Z}_2 \triangleq E(000000, 001001) \\ \bar{Z}_3 \triangleq E(000000, 000101) \\ \bar{Z}_4 \triangleq E(000000, 000011) \end{array} . \tag{47}$$

Consider $\mathbb{F}_{16}$ constructed by adjoining to $\mathbb{F}_2$ a root α of the primitive polynomial $p(x) = x^4 + x + 1$. Consider the element F_{abcd} in $\mathfrak{P}_{\mathrm{K},4}$ identified by the tuple $(a = \alpha^3, b = \alpha^8, c = \alpha^7, d = 0)$, or equivalently $(a, b, c, d, i = 0)$ in $\mathfrak{P}^*_{\mathrm{K},4}$. In this case the matrices defined in Section III-A are

$$\begin{aligned} W &= \begin{bmatrix} 0&0&0&1\\0&0&1&0\\0&1&0&0\\1&0&0&1 \end{bmatrix}, W^{-1} = \begin{bmatrix} 1&0&0&1\\0&0&1&0\\0&1&0&0\\1&0&0&0 \end{bmatrix}, \\ R &= \begin{bmatrix} 1&0&0&0\\0&0&1&0\\1&1&0&0\\0&0&1&1 \end{bmatrix}, \quad A = \begin{bmatrix} 0&1&0&0\\0&0&1&0\\0&0&0&1\\1&1&0&0 \end{bmatrix}. \end{aligned} \tag{48}$$

Then, using the isomorphism in Corollary 24 and the direct form in Lemma 23, we can express the element in $\mathfrak{P}_{\mathrm{K},4}$ as

$$\begin{aligned} F_{abcd} &= T_{A_0^2 W} \cdot L_{A_{\alpha^7}^{-2}} \cdot \Omega L_{W^{-1}} \cdot T_{A_{\alpha^{11}}^2 W} \\ &= I_8 \cdot L_{(A^7)^{-2}} \cdot \Omega L_{W^{-1}} \cdot T_{(A^{11})^2 W} \end{aligned} \tag{49}$$

$$\begin{aligned} &= \begin{bmatrix} 0 & A_{\alpha^8}^2 W \\ W^{-1} A_{\alpha^7}^2 & (A_{\alpha^3}^2)^T \end{bmatrix} \\ &= \begin{bmatrix} 0 & A^{16} W \\ W^{-1} A^{14} & (A^6)^T \end{bmatrix} \end{aligned} \tag{50}$$

$$= \left[\begin{array}{cccc|cccc} 0&0&0&0&0&0&1&0\\ 0&0&0&0&0&1&0&0\\ 0&0&0&0&1&0&0&1\\ 0&0&0&0&0&0&1&1\\ \hline 1&0&1&1&0&1&1&0\\ 0&1&0&0&0&1&0&1\\ 1&0&0&0&1&0&1&0\\ 1&0&0&1&1&1&0&1 \end{array} \right]. \tag{51}$$

Using the explicit decomposition in (49), we map the elementary symplectic matrices to standard Clifford gates (as discussed in [33]) and get the following circuit (`CKT1`).[2]

'Permute'	[4,1,2,3]
'CNOT'	[1,2]
'Permute'	[4,3,2,1]
'CNOT'	[1,4]
'H'	[1,2,3,4]
'P'	[1,2,3,4]
'CZ'	[1,3]
'CZ'	[2,4]
'CZ'	[3,4]

Here the indices corresponding to 'Permute' imply the cycle permutation (1432), i.e., the first qubit has been replaced by the fourth, the fourth by the third, the third by the second,

[2]We list circuits instead of giving their circuit representation to align with the `MATLAB`® cell array format we adopt in our implementations.

and the second by the first. (Note that we do not simplify circuits to their optimal form here but simply report the results of our synthesis algorithm.) An alternative procedure is to directly input the final symplectic matrix (51) to the symplectic decomposition algorithm in [17] (also see [33, Section II]), yielding the following circuit (CKT2).

'Permute'	[3,2,1,4]
'CNOT'	[4,3]
'CNOT'	[1,4]
'H'	[1,2,3,4]
'P'	[1,2,3,4]
'CZ'	[1,3]
'CZ'	[2,4]
'CZ'	[3,4]

The difference in depth of the two circuits is very small in this case, but we found that for about half of the elements in $\mathfrak{P}_{\mathrm{K},4}$ the explicit form in Corollary 24 had smaller depth, while for those remaining, the direct decomposition was better.

Next we translate this logical circuit into its physical implementation for the $[\![6,4,2]\!]$ CSS code. We apply our synthesis algorithm [33], which can be summarized as follows.

1) Compute the action of either of the above circuits on the Pauli matrices X_i, Z_i, for $i = 1,2,3,4$, under conjugation, i.e., compute $gE(e_i,0)g^\dagger, gE(0,e_i)g^\dagger$ where g represents the circuit.
2) Translate these into logical constraints on the desired physical circuit $\bar{g}$ by interpreting X_i, Z_i above as their logical equivalents $\bar{X}_i, \bar{Z}_i$.
3) Rewrite the above conditions as linear constraints on the desired symplectic matrix $F_{\bar{g}}$ using (8). Add constraints to normalize (or just centralize) the stabilizer S.
4) Solve for all symplectic solutions, compute their corresponding circuits and identify the best solution in terms of smallest depth, with respect to the decomposition in [17] (also discussed in [33, Section II]).
5) Verify the constraints imposed in step 2 and check for any sign violations (due to signs in (8)). In case of violations, identify a Pauli matrix to fix the signs.

Using this algorithm, we computed the circuit with smallest depth (relative to other solutions decomposed using the same algorithm) and obtained the following solution (CKT3).

'Permute'	[1,6,3,5,4,2]
'CNOT'	[3,1]
'CNOT'	[4,1]
'CNOT'	[5,1]
'CNOT'	[6,1]
'CNOT'	[6,4]
'CNOT'	[6,5]
'CNOT'	[4,5]
'CNOT'	[3,6]
'CNOT'	[2,3]
'H'	[1,2,3,4,5,6]
'P'	[3,4,5]
'CZ'	[1,3]
'CZ'	[1,4]
'CZ'	[1,5]
'CZ'	[2,6]
'CZ'	[3,5]
'CZ'	[4,5]
'CZ'	[4,6]
'CZ'	[5,6]
'H'	[1,2]
'CNOT'	[2,3]
'CNOT'	[2,4]
'CNOT'	[2,5]
'CNOT'	[2,6]
'Z'	[2,6]

We used the same procedure to translate all 4080 elements of $\mathfrak{P}_{\mathrm{K},4}$ into their (smallest depth) physical implementations for the $[\![6,4,2]\!]$ code, and the synthesis took about 25 minutes on a laptop running the Windows 10 operating system (64-bit) with an Intel® Core™ i7-5500U @ 2.40GHz processor and 8GB RAM. Note that for this case each element of $\mathfrak{P}_{\mathrm{K},4}$ translates to $2^{k(k+1)/2} = 8$ symplectic solutions during the above procedure, and we need to compare depth after calculating circuits for all solutions. In future work, we will try to optimize directly for depth without computing all solutions as this procedure is expensive for codes with large redundancy (k). However, since this translation needs to be done only once for a given set $\mathfrak{P}_{\mathrm{K},m-k}$ and an $[\![m, m-k]\!]$ stabilizer code, the circuits can be precomputed and stored in memory.

VII. Conclusion

In this paper we provided a simpler calculation of the Hamming weight distribution of the classical binary non-linear Kerdock codes by appealing to the connection with maximal commutative subgroups of the Heisenberg-Weyl group from the quantum domain. Using this connection, we also described the group of Clifford symmetries of the mutually unbiased bases determined by the Kerdock sets of symmetric matrices. We then used this result in the classical domain to construct small unitary 2-designs. Finally, we demonstrated an efficient procedure for translating any unitary 2-design consisting of Clifford elements into a logical unitary 2-design for a given stabilizer code. Through this work, we have reiterated that interactions between the classical and quantum domains can be mutually beneficial, both theoretically and practically.

References

[1] P. W. Shor, "Scheme for reducing decoherence in quantum computer memory," *Phys. Rev. A*, vol. 52, no. 4, pp. R2493–R2496, 1995.

[2] A. R. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist," *Phys. Rev. A*, vol. 54, pp. 1098–1105, Aug 1996.

[3] A. M. Steane, "Simple quantum error-correcting codes," *Phys. Rev. A*, vol. 54, no. 6, pp. 4741–4751, 1996.

[4] A. Calderbank, E. Rains, P. Shor, and N. Sloane, "Quantum error correction via codes over GF(4)," *IEEE Trans. Inform. Theory*, vol. 44, pp. 1369–1387, Jul 1998.

[5] D. Gottesman, *Stabilizer codes and quantum error correction*. PhD thesis, California Institute of Technology, 1997.

[6] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. North-Holland, Amsterdam, 1977.

[7] A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, "The $\mathbb{Z}_4$-Linearity of Kerdock, Preparata, Goethals, and Related Codes," *IEEE Trans. Inform. Theory*, vol. 40, no. 2, pp. 301–319, 1994.

[8] H. Weyl, *The Classical Groups: Their Invariants and Representations*, vol. 1. Princeton University Press, 1997.

[9] K. Koike and I. Terada, "Young-diagrammatic methods for the representation theory of the classical groups of type Bn, Cn, Dn," *J. Algebr.*, vol. 107, pp. 466–511, May 1987.

[10] R. Kueng and D. Gross, "Qubit stabilizer states are complex projective 3-designs," *arXiv preprint arXiv:1510.02767*, 2015. [Online]. Available: https://arxiv.org/abs/1510.02767.

[11] R. Kueng, H. Zhu, and D. Gross, "Low rank matrix recovery from Clifford orbits," *arXiv preprint arXiv:1610.08070*, 2016. [Online]. Available: https://arxiv.org/abs/1610.08070.

[12] A. Thompson and R. Calderbank, "Compressed Neighbour Discovery using Sparse Kerdock Matrices," in *Proc. IEEE Int. Symp. Inform. Theory*, pp. 2286–2290, Jun 2018. [Online]. Available: http://arxiv.org/abs/1801.04537.

[13] A. Calderbank, P. Cameron, W. Kantor, and J. Seidel, "$\mathbb{Z}_4$-Kerdock Codes, Orthogonal Spreads, and Extremal Euclidean Line-Sets," *Proc. London Math. Soc.*, vol. 75, pp. 436–480, Sep 1997.

[14] O. Tirkkonen, C. Boyd, and R. Vehkalahti, "Grassmannian codes from multiple families of mutually unbiased bases," in *Proc. IEEE Int. Symp. Inform. Theory*, pp. 789–793, Jun 2017.

[15] Z. Webb, "The Clifford Group forms a Unitary 3-Design," *arXiv preprint arXiv:1510.02769*, 2016. [Online]. Available: https://arxiv.org/abs/1510.02769.

[16] R. Cleve, D. Leung, L. Liu, and C. Wang, "Near-linear constructions of exact unitary 2-designs," *arXiv preprint arXiv:1501.04592*, 2016. [Online]. Available: https://arxiv.org/abs/1501.04592.

[17] T. Can, "The Heisenberg-Weyl group, finite symplectic geometry, and their applications," Senior Thesis, Duke University, May 2018.

[18] D. Maslov and M. Roetteler, "Shorter Stabilizer Circuits via Bruhat Decomposition and Quantum Circuit Transformations," *IEEE Trans. Inform. Theory*, vol. 64, no. 7, pp. 4729–4738, 2018.

[19] P. Diaconis and M. Shahshahani, "The subgroup algorithm for generating uniform random variables," *Prob. Eng. Inf. Sci.*, vol. 1, no. 1, pp. 15–32, 1987.

[20] R. Koenig and J. A. Smolin, "How to efficiently select an arbitrary Clifford group element," *J. Math. Phys.*, vol. 55, p. 122202, Dec 2014.

[21] K. Choromanski, F. Fagan, C. Gouy-Pailler, A. Morvan, T. Sarlos, and J. Atif, "TripleSpin - a generic compact paradigm for fast machine learning computations," *arXiv preprint arXiv:1605.09046*, 2016. [Online]. Available: http://arxiv.org/abs/1605.09046.

[22] P. W. Jones, A. Osipov, and V. Rokhlin, "A randomized approximate nearest neighbors algorithm," *Appl. Comput. Harmon. Anal.*, vol. 34, no. 3, pp. 415–444, 2013.

[23] D. DiVincenzo, D. Leung, and B. Terhal, "Quantum Data Hiding," *IEEE Trans. Inform. Theory*, vol. 48, no. 3, pp. 580–598, 2002.

[24] E. Magesan, J. M. Gambetta, and J. Emerson, "Characterizing quantum gates via randomized benchmarking," *Phys. Rev. A*, vol. 85, no. 4, p. 042311, 2012.

[25] J. Helsen, J. J. Wallman, S. T. Flammia, and S. Wehner, "Multi-qubit Randomized Benchmarking Using Few Samples," *arXiv preprint arXiv:1701.04299*, 2017. [Online]. Available: http://arxiv.org/abs/1701.04299.

[26] C. Dankert, R. Cleve, J. Emerson, and E. Livine, "Exact and approximate unitary 2-designs and their application to fidelity estimation," *Phys. Rev. A*, vol. 80, no. 1, p. 012304, 2009.

[27] A. J. Scott, "Optimizing quantum process tomography with unitary 2-designs," *arXiv preprint arXiv:0711.1017*, 2007. [Online]. Available: http://arxiv.org/abs/0711.1017.

[28] M. Quadeer, M. Tomamichel, and C. Ferrie, "Minimax quantum state estimation under Bregman divergence," *arXiv preprint arXiv:1808.08984*, 2018. [Online]. Available: http://arxiv.org/abs/1808.08984.

[29] P. Hayden, M. Horodecki, A. Winter, and J. Yard, "A decoupling approach to the quantum capacity," *arXiv preprint arXiv:quant-ph/0702005*, 2007. [Online]. Available: http://arxiv.org/abs/quant-ph/0702005.

[30] A. Roy and A. J. Scott, "Unitary designs and codes," *Designs, Codes Cryptogr.*, vol. 53, no. 1, pp. 13–31, 2009.

[31] O. Szehr, F. Dupuis, M. Tomamichel, and R. Renner, "Decoupling with unitary approximate two-designs," *New J. Phys.*, vol. 15, no. 5, p. 053022, 2013.

[32] Y. Nakata, C. Hirche, C. Morgan, and A. Winter, "Unitary 2-designs from random X- and Z-diagonal unitaries," *J. Math. Phys.*, vol. 58, no. 5, p. 052203, 2017.

[33] N. Rengaswamy, R. Calderbank, H. D. Pfister, and S. Kadhe, "Synthesis of Logical Clifford Operators via Symplectic Geometry," in *Proc. IEEE Int. Symp. Inform. Theory*, pp. 791–795, Jun 2018. [Online]. Available: http://arxiv.org/abs/1803.06987.

[34] J. T. Anderson, G. Duclos-Cianci, and D. Poulin, "Fault-Tolerant Conversion between the Steane and Reed-Muller Quantum Codes," *Phys. Rev. Lett.*, vol. 113, no. 8, p. 080501, 2014. [Online]. Available: http://arxiv.org/abs/1403.2734.

[35] J. Combes, C. Granade, C. Ferrie, and S. T. Flammia, "Logical Randomized Benchmarking," *arXiv preprint arXiv:1702.03688*, 2017. [Online]. Available: http://arxiv.org/abs/1702.03688.

[36] A. W. Nordstrom and J. P. Robinson, "An optimum nonlinear code," *Inform. and Control*, vol. 11, no. 5-6, pp. 613–616, 1967.

[37] A. Kerdock, "A class of low-rate nonlinear binary codes," *Inform. and Control*, vol. 20, pp. 182–187, Mar 1972.

[38] F. P. Preparata, "A class of optimum nonlinear double-error correcting codes," *Inform. and Control*, vol. 13, no. 13, pp. 378–400, 1968.

[39] J. Goethals, "Two dual families of nonlinear binary codes," *Electronic Letters*, vol. 10, no. 23, p. 471, 1974.

[40] J.-M. Goethals, "Nonlinear codes defined by quadratic forms over GF(2)," *Inform. and Control*, vol. 31, pp. 43–74, May 1976.

[41] P. Delsarte and J. M. Goethals, "Alternating bilinear forms over GF(q)," *J. Comb. Theory, Ser. A*, vol. 19, no. 1, pp. 26–50, 1975.

[42] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*. Cambridge University Press, 2003.

[43] R. Calderbank and S. Jafarpour, "Reed Muller Sensing Matrices and the LASSO," *arXiv preprint arXiv:1004.4949*, Apr 2010. [Online]. Available: http://arxiv.org/abs/1004.4949.

[44] A. Thompson and R. Calderbank, "Sparse near-equiangular tight frames with applications in full duplex wireless communication," in *IEEE Glob. Conf. Signal Inf. Process.*, pp. 868–872, Nov 2017.

[45] D. Gottesman, "A Theory of Fault-Tolerant Quantum Computation," *arXiv preprint arXiv:quant-ph/9702029*, 1997. [Online]. Available: http://arxiv.org/pdf/quant-ph/9702029.pdf.

[46] D. Gottesman, "An Introduction to Quantum Error Correction and Fault-Tolerant Quantum Computation," *arXiv preprint arXiv:0904.2557*, 2009. [Online]. Available: http://arxiv.org/abs/0904.2557.

[47] M. M. Wilde, *Quantum Information Theory*. Cambridge University Press, 2013.

[48] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge University Press, 2010.

[49] M. A. De Gosson, *Symplectic Geometry and Quantum Mechanics*, vol. 166. Springer Science & Business Media, 2006.

[50] C. Chamberland, P. Iyer, and D. Poulin, "Fault-tolerant quantum computing in the Pauli or Clifford frame with slow error diagnostics," *Quantum*, vol. 2, p. 43, 2018. [Online]. Available: https://arxiv.org/pdf/1704.06662.pdf.

[51] J. Dehaene and B. De Moor, "Clifford group, stabilizer states, and linear and quadratic operations over GF(2)," *Phys. Rev. A*, vol. 68, p. 042318, Oct 2003.

[52] A. Calderbank, R. Hardin, E. Rains, P. Shor, and N. Sloane, "A Group-Theoretic Framework for the Construction of Packings in Grassmannian Spaces," *J. Algebr. Comb.*, vol. 9, no. 2, pp. 129–140, 1999.

[53] P. J. Cameron and J. H. Van Lint, *Designs, Graphs, Codes and their Links*, vol. 3. Cambridge University Press, 1991.

[54] J. Watrous, *The Theory of Quantum Information*. Cambridge University Press, 2018.

[55] Z. Puchała and J. A. Miszczak, "Symbolic integration with respect to the haar measure on the unitary groups," *Bulletin of the Polish Academy of Sciences Technical Sciences*, vol. 65, no. 1, pp. 21–27, 2017.

[56] R. Chao and B. W. Reichardt, "Fault-tolerant quantum computation with few qubits," *arXiv preprint arXiv:1705.05365*, 2017. [Online]. Available: http://arxiv.org/pdf/1705.05365.pdf.

Appendix A
Proof of Lemma 25

We proceed as in the proof of Lemma 23 to derive the general form of an element in $\mathfrak{P}^*_{\mathrm{K},m}$. Introducing the new generators $L_{R^{-i}}$, and using identities from Lemma 3, we calculate

$$\begin{bmatrix} R^{-i}A_x^{-2} & 0 \\ 0 & (R^i)^T(A_x^2)^T \end{bmatrix}\begin{bmatrix} 0 & W^T \\ W^{-1} & 0 \end{bmatrix}$$
$$= \begin{bmatrix} 0 & R^{-i}A_x^{-2}W \\ (R^i)^T W^{-1}A_x^2 & 0 \end{bmatrix};$$
$$\begin{bmatrix} I_m & A_y^2W \\ 0 & I_m \end{bmatrix}\begin{bmatrix} 0 & R^{-i}A_x^{-2}W \\ (R^i)^T W^{-1}A_x^2 & 0 \end{bmatrix}$$
$$= \begin{bmatrix} A_y^2W(R^i)^TW^{-1}A_x^2 & R^{-i}A_x^{-2}W \\ (R^i)^TW^{-1}A_x^2 & 0 \end{bmatrix};$$
$$\begin{bmatrix} A_y^2W(R^i)^TW^{-1}A_x^2 & R^{-i}A_x^{-2}W \\ (R^i)^TW^{-1}A_x^2 & 0 \end{bmatrix}\begin{bmatrix} I_m & A_w^2W \\ 0 & I_m \end{bmatrix}$$
$$= \begin{bmatrix} A_y^2(W(R^i)^TW^{-1})A_x^2 & A_y^2(W(R^i)^TW^{-1})A_x^2A_w^2W + R^{-i}A_x^{-2}W \\ (R^i)^TW^{-1}A_x^2 & (R^i)^TW^{-1}A_x^2A_w^2W \end{bmatrix}$$
$$= \begin{bmatrix} A_y^2R^{-i}A_x^2 & A_y^2R^{-i}A_{wx}^2W + R^{-i}A_x^{-2}W \\ W^{-1}R^{-i}A_x^2 & (R^i)^T(A_{wx}^2)^T \end{bmatrix}$$
$$\triangleq F.$$

In this case the relations between a, b, c, d and x, y, z, w that will yield the desired map are unclear. Hence, we first determine the transformation on $[I_m \mid A_z^2W]$ in terms of x, y, z and w. Again, we repeatedly invoke identities from Lemma 3.

$$\begin{aligned}
&[I_m \mid A_z^2W]F \\
&= [A_y^2R^{-i}A_x^2 + A_z^2R^{-i}A_x^2 \mid (A_y^2R^{-i}A_{wx}^2 + R^{-i}A_x^{-2})W \\
&\qquad\qquad + A_z^2W(R^i)^T(A_{wx}^2)^T] \\
&= [A_{y+z}^2R^{-i}A_x^2 \mid (A_{y+z}^2R^{-i}A_{wx}^2 + R^{-i}A_x^{-2})W],
\end{aligned}$$

where we have simplified the last term as

$$A_z^2W(R^i)^T(A_{wx}^2)^T = A_z^2R^{-i}W(A_{wx}^2)^T = A_z^2R^{-i}A_{wx}^2W.$$

Now we have the following simplifications for the three terms.

$$\begin{aligned}
A_{y+z}^2R^{-i}A_x^2 &= A_{y+z}^2A_x^{2^{i+1}}R^{-i}, \\
A_{y+z}^2R^{-i}A_{wx}^2 &= A_{y+z}^2A_{wx}^{2^{i+1}}R^{-i}, \\
R^{-i}A_x^{-2} &= A_x^{-2^{i+1}}R^{-i}.
\end{aligned}$$

Applying this back we get

$$\begin{aligned}
&[I_m \mid A_z^2W]F \\
&= \left[A_{y+z}^2A_x^{2^{i+1}}R^{-i} \mid \left(A_{y+z}^2A_{wx}^{2^{i+1}} + A_x^{-2^{i+1}}\right)R^{-i}W\right] \\
&\equiv \left[I_m \mid R^iA_x^{-2^{i+1}}A_{y+z}^{-2}\left(A_{y+z}^2A_{wx}^{2^{i+1}} + A_x^{-2^{i+1}}\right)R^{-i}W\right] \\
&= \left[I_m \mid R^i\left(A_w^{2^{i+1}} + A_{y+z}^{-2}A_x^{-2\cdot 2^{i+1}}\right)R^{-i}W\right] \\
&= \left[I_m \mid A_w^2W + R^iA_{y+z}^{-2}A_x^{-2\cdot 2^{i+1}}R^{-i}W\right] \\
&= \left[I_m \mid A_w^2W + A_{y+z}^{-2^{1-i}}R^iA_x^{-2\cdot 2^{i+1}}R^{-i}W\right] \\
&= \left[I_m \mid A_w^2W + A_{y+z}^{-2^{1-i}}\left(R^iA_{x^{2^{i+1}}}^{-2}R^{-i}\right)W\right] \\
&= \left[I_m \mid A_w^2W + A_{y+z}^{-2^{1-i}}A_{x^{2^{i+1}}}^{-2^{1-i}}W\right] \\
&= \left[I_m \mid \left(A_w^2 + A_{(y+z)^{-2^{-i}}x^{-2}}^2\right)W\right] \\
&= \left[I_m \mid A_{w+(y+z)^{-2^{-i}}x^{-2}}^2W\right].
\end{aligned}$$

Now we define $x \triangleq c, w \triangleq \frac{a}{c}$ and $y \triangleq \left(\frac{d}{c}\right)^{2^i}$. Then we get

$$\begin{aligned}
w + (y+z)^{-2^{-i}}x^{-2} &= \frac{a}{c} + \left(z + \left(\frac{d}{c}\right)^{2^i}\right)^{-2^{-i}}\frac{1}{c^2} \\
&= \frac{a}{c} + \left(z^{2^{-i}} + \left(\frac{d}{c}\right)^{2^i\cdot 2^{-i}}\right)^{-1}\frac{1}{c^2} \\
&= \frac{1}{c}\left[a + \frac{1}{cz^{2^{-i}} + c\cdot\frac{d}{c}}\right] \\
&= \frac{1}{c}\left[\frac{acz^{2^{-i}} + ad + 1}{cz^{2^{-i}} + d}\right] \\
&= \frac{az^{2^{-i}} + \left(\frac{ad+1}{c}\right)}{cz^{2^{-i}} + d} \\
&= \frac{az^{2^{-i}} + b}{cz^{2^{-i}} + d}\ ;\ b = \frac{ad+1}{c}.
\end{aligned}$$

Hence we have proved that F performs the permutation

$$[I_m \mid A_z^2W] \longmapsto \left[I_m \mid A_{\frac{az'+b}{cz'+d}}^2W\right],\ z' \triangleq z^{2^{-i}}.$$

We note that the above definitions for x, w, y also satisfy the special case of $i = 0$ that corresponds to the proof in Lemma 23. We now substitute these back in F and observe the following simplifications.

$$\begin{aligned}
(A_y^2R^{-i})A_x^2 &= R^{-i}A_y^{2^{-i+1}}A_x^2 = R^{-i}A_{y^{2^{-i}}x}^2 = R^{-i}A_d^2, \\
(A_y^2R^{-i})A_{wx}^2 + R^{-i}A_x^{-2} &= R^{-i}A_{d/c}^2A_a^2 + R^{-i}A_{c^{-1}}^2 = R^{-i}A_b^2, \\
W^{-1}R^{-i}A_x^2 &= W^{-1}R^{-i}A_c^2 = (R^i)^TW^{-1}A_c^2, \\
(R^i)^T(A_{wx}^2)^T &= (R^i)^T(A_a^2)^T.
\end{aligned}$$

These imply that the general form of an element in $\mathfrak{P}^*_{\mathrm{K},m}$ is

$$\begin{aligned}
F &= \begin{bmatrix} A_y^2R^{-i}A_x^2 & (A_y^2R^{-i}A_{wx}^2 + R^{-i}A_x^{-2})W \\ W^{-1}R^{-i}A_x^2 & (R^i)^T(A_{wx}^2)^T \end{bmatrix} \\
&= \begin{bmatrix} R^{-i}A_d^2 & R^{-i}A_b^2W \\ W^{-1}R^{-i}A_c^2 & (R^i)^T(A_a^2)^T \end{bmatrix}. \qquad \blacksquare
\end{aligned}$$