Kerdock Codes Determine Unitary 2-Designs

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

Abstract—The non-linear binary Kerdock codes are known to be Gray images of certain extended cyclic codes of length \( N = 2^m \) over \( \mathbb{Z}_4 \). We show that exponentiating these \( \mathbb{Z}_4 \)-valued codewords by \( i = \sqrt{-1} \) produces stabilizer states, that are quantum states obtained using only Clifford unitaries. These states are also the common eigenvectors of commuting Hermitian matrices forming maximal commutative subgroups (MCS) of the Pauli group. We use this quantum description to simplify the derivation of the classical weight distribution of Kerdock codes. Next, we organize the stabilizer states to form \( N + 1 \) mutually unbiased bases and prove that automorphisms of the Kerdock code permute their corresponding MCS, thereby forming a subgroup of the Clifford group. When represented as symplectic matrices, this subgroup is isomorphic to the projective special linear group \( \text{PSL}(2, N) \). We show that this automorphism group acts transitively on the Pauli matrices, which implies that the ensemble is Pauli mixing and hence forms a unitary 2-design. The Kerdock design described here was originally discovered by Cleve et al. (2016), but the connection to classical codes is new which simplifies its description and translation to circuits significantly. Sampling from the design is straightforward, the translation to circuits uses only Clifford gates, and the process does not require ancillary qubits. Finally, we also develop algorithms for optimizing the synthesis of unitary 2-designs on encoded qubits, i.e., to construct logical unitary 2-designs. Software implementations are available at https://github.com/nrenga/symplectic-arch18a which we use to provide empirical gate complexities for up to 16 qubits.

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 t-designs

I. INTRODUCTION

Quantum computers promise enormous computational speedups over the best classical supercomputers in certain problems. It has been established that even constant-depth quantum circuits provide an advantage over classical computation [2]. Today these devices are moving out of the lab and becoming generally programmable [3]. Since quantum computers are noisy, they will most likely employ quantum error-correcting codes (QECCs) to ensure reliability of computation. Classical error-correcting codes inspired the discovery of the first QECC by Shor [4], the development of CSS codes by Calderbank, Shor and Steane [5], [6], and the development of stabilizer codes [7], [8] by Calderbank, Rains, Shor and Sloane and by Gottesman. A QECC protects \( m - k \) logical qubits by embedding them in a system comprising \( m \) physical qubits. If 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. The most common QECCs are stabilizer QECCs, that are derived from commutative subgroups of the Heisenberg-Weyl group \( \text{HW}_N \) (also known as the Pauli group), and the simplest quantum circuits are composed of unitary operators from the Clifford group \( \text{Cliff}_N \) (see Section III for formal definitions). Note that \( N = 2^m \) throughout this paper. The Clifford group normalizes \( \text{HW}_N \), so each element of \( \text{Cliff}_N \) induces an automorphism of \( \text{HW}_N \) under conjugation. Since \( \text{HW}_N \) elements can be efficiently represented as binary length-\( 2m \) vectors, Clifford operators can be efficiently represented as \( 2m \times 2m \) binary symplectic matrices that preserve the group structure of \( \text{HW}_N \) under the binary mapping. A central theme in this paper is that beyond inspiring the construction of QECCs, interactions between the classical and quantum worlds still prove mutually beneficial for other purposes, especially via the binary representations of \( \text{HW}_N \) and \( \text{Cliff}_N \).

Prior to running applications, a quantum computer needs to be assessed for its quality, in terms of the fidelity of the quantum operations executed on the system. The randomized benchmarking protocol, introduced by Emerson et al. [9], [10], is a well-established scheme that estimates the fidelity of the noise in the system by twirling the underlying channel through a randomized sequence of gates and calculating the fidelity of the resulting depolarizing channel. The depolarizing channel can be interpreted as the quantum analogue of the binary symmetric channel in classical communication theory. Since the fidelity is shown to be an invariant of this twirling process, the protocol indeed estimates the fidelity of the actual noise (under some additional assumptions). This protocol works on the physical operations in the computer, so the fidelity estimates then need to be translated into the quality of the logical operations (on the protected qubits) for an error-corrected quantum computer. Since this translation might not be reliable, the procedure has recently been extended to the logical randomized benchmarking protocol [11] that directly estimates the fidelity of the logical operations more reliably.

Randomized benchmarking requires that the sequence of gates be sampled from an ensemble of unitaries that form a unitary 2-design. A unitary t-design is an ensemble of unitaries, bestowed with a probability distribution, that ap-

*These two authors contributed equally to this work. This work was presented in part at the 2019 IEEE International Symposium on Information Theory [1].

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.renga@gmail.com, robert.calderbank, henry.pfister]@duke.edu

This work was supported in part by the National Science Foundation (NSF) under Grant Nos. 1718494 and 1908730. Any opinions, findings, conclusions, and recommendations expressed in this material are those of the authors and do not necessarily reflect the views of these sponsors.

Copyright (c) 2017 IEEE. Personal use of this material is permitted. However, permission to use this material for any other purposes must be obtained from the IEEE by sending a request to pubs-permissions@ieee.org.
proximates the Haar distribution on the unitary group up to the t-th moment. Section [VI] 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 t-design. It is easy to analyze protocols that randomly sample unitary matrices with respect to the Haar measure, but such 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 [12], and the proof by Webb involves the concepts of Pauli mixing and Pauli 2-mixing, which we introduce in Section [VI]. However, Cliff_N has size $2^{m^2 + 2m} \prod_{j=1}^m (4^j - 1)$ (up to scalars $e^{2\pi i \theta}, \theta \in \mathbb{R}$) which is much larger than the lower bound of $\approx 2^{4m}$ for any unitary 2-design, established by Gross, Audenaert and Eisert [13], and by Roy and Scott [14]. They also discuss the existence of Clifford ensembles that saturate this bound. Although random circuits are known to be exact or approximate unitary 2-designs [15, 16], deterministic constructions of such ensembles facilitate practical realizations. Cleve et al. [17] have recently found an explicit subgroup of Cliff_N that is a unitary 2-design. The central contribution of this paper is to use the classical Kerdock codes to simplify the construction of this quantum unitary 2-design and its translation to circuits (see Section [VI]).

There are many other applications of unitary 2-designs. The first is quantum data hiding (the LOCC model described in [13]), 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 fidelity estimation of quantum channels [19], quantum state and process tomography [20], and more recently minimax quantum state estimation [21]. In quantum information theory, they have been used extensively in the analysis of decoupling [14, 16, 22, 23].

The next section discusses the flow of ideas in the rest of the paper, and points to related work and applications.

## II. MAIN IDEAS AND DISCUSSION

The first result in the paper is to use the (quantum) commutative subgroups of HW_N to simplify the derivation of weight distributions for the (classical) Kerdock codes.

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 [24] Chapter 15) for more details). Section [IV-A] reviews the Z_4 description of these codes given in [25]. Section [IV-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 [26], and the distance distribution of the code is determined by the inner product of pairs of such eigenvectors (see [Section [IV] Lemma[10]]). When calculating weight distributions, this property makes it possible to avoid using Dickson’s Theorem [24 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 [24] significantly. In order to demonstrate this simplicity, we provide the proof of the weight distribution here. For most parts of the proof, we only need a brief description of the Kerdock set, Kerdock code, and the Gray map. See Section [IV] for formal definitions, constructions, and results used in the following proof.

In [27], the *Kerdock set* $P_k(m)$ is defined to be a collection of $N$ binary $m \times m$ symmetric matrices that is characterized by the following properties: it is closed under binary addition, and if $P, Q \in P_k(m)$ are distinct, then $P + Q$ is non-singular. The codewords of the length-$N$ $Z_4$-linear Kerdock code $K(m)$ can be expressed as $[xP \cdot x + 2wx^T + \kappa]$ (mod 4), where $x \in F_2^m$ chooses the symbol index in a codeword, and the codeword is determined by the choice of $\omega \in F_2^m, P \in P_k(m)$ and $\kappa \in Z_4 = \{0, 1, 2, 3\}$. One can obtain complex vectors of quaternary phases $\{1, i, -1, -i\}$ by raising $i = \sqrt{-1}$ to the integer powers in the $Z_4$-valued codeword vector. We will refer to this operation as exponentiating the codeword by $i$. The *Gray map* is an isometry from (length-$N$ vectors of quaternary phases, Euclidean metric) to $\mathbb{Z}_2^N$, (Hamming metric) defined by $g(1) \triangleq 00, g(i) \triangleq 01, g(-1) \triangleq 11, \text{ and } g(-i) \triangleq 10$. Note that the domain of the map can equivalently be taken as $Z_4$ in which case the metric is the Lee metric (defined in Section [IV-B]). The codewords of the *binary non-linear* Kerdock code of length $2m+1$ are obtained as Gray images of the $Z_4$-valued codewords described above.

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

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

**Proof:** We explicitly use Lemma[10] and Corollary[16] to calculate the weight distribution. Fix a vector $v$ of quaternary phases obtained by exponentiating a codeword

$$c_v = [xP \cdot x + 2wx^T + \kappa]_x \in F_2^m$$

in the $Z_4$-linear Kerdock code. Consider any vector $u$ of quaternary phases obtained by exponentiating a second codeword

$$c_u = [xP \cdot x^T + 2wx^T + \kappa]_x \in F_2^m.$$  

(Lemmas[11] and [15] consider $\kappa_1 = \kappa_2 = 0$ so that the eigenvalues are $\pm 1$ (and not in $\{\pm 1, \pm i\}$, but we account for these factors here.)

Let $n_j$ be the number of indices $x \in F_2^m$ for which $(c_u)x - (c_v)x = j$, for $j \in Z_4$. Since the Gray map preserves the Lee metric, the Hamming distance between the Gray images of $c_u$ and $c_v$ is $d_H(g(c_u), g(c_v)) = n_1 + 2n_2 + n_3$. Since $n_0 + n_1 + n_2 + n_3 = 2m$ we simply have to relate
Now we observe three distinct cases for the codeword $c_u - c_v$.

(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 $c_j$).

(ii) $P_1 = P_2, w_1 \neq w_2$: From Corollary 10 irrespective of $\kappa_1, \kappa_2$, we have $\langle u, v \rangle = 0$, 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 10 we have $|\langle u, v \rangle|^2 = 2^m$, which implies $(n_0 - n_2)^2 + (n_1 - n_3)^2 = 2^m$. Since $m$ is odd, and $n_2$ 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 $\mathbb{Z}[i]$ are a unique factorization domain, we have $(n_0 - n_2)^2 + (n_1 - n_3)^2 = (\pm 1 \pm i)(2^{m-1}/2)$ and this gives weights $2^m \pm 2^{(m-1)/2}$. Thus, 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 $2^{2m+1} - 2^{m+2}$ codewords of each weight.

Lemma 11 shows that the (normalized) length-$N$ vectors of quaternary phases obtained by exponentiating Pauli, or more generally Delsarte-Goethals, codewords are common eigenvectors of maximal commutative subgroups of $HW_N$. These eigenvectors are called stabilizer states in the quantum information literature (28) (also see end of Section III). They can equivalently be described as those quantum states that scales to $|\psi(\kappa)|^2 = 1/|\kappa|^2$.

According to Kerdock, these states are approximated by a family of diagonal 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 group of binary symplectic matrices $Sp(2m, \mathbb{F}_2)$. A subgroup of $C^{\infty}$ 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 [12]. 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. Since the Clifford symmetries include all Hermitian Paulis, in addition to $PSL(2, N)$, the size of the Kerdock unitary 2-design is $N^5 - N^3 \approx 2^{5m}$, which almost saturates the bound by Gross et al. [13] discussed above. The next step is to translate these symmetry elements into circuits for, say, randomized benchmarking.

T. Can has developed an algorithm [35] 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 II. The target symplectic matrix maps the (Hadamard) dual basis $X_N = E([I_m \mid 0]), Z_N = E([0 \mid I_m])$ (see Section III for notation) to a dual basis $X_N', Z_N'$. Then, row and column operations by the elementary matrices return $X_N', Z_N'$ to the original pair $X_N, Z_N$ thereby producing a decomposition of the target symplectic matrix.

Section VI 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 $Sp(2m, \mathbb{F}_2)$ (see [37]). 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 \( \{38\} \) 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 \( \text{Sp}(2m, \mathbb{F}_2) \) (cf. \( \{39\} \)). We note that the problem of selecting a unitary matrix uniformly at random finds application in machine learning (see \( \{40\} \) and the references therein). The algorithm developed by Can is similar to that developed by Jones, Osipov and Rokhlin \( \{41\} \) in that it alternates (partial) Hadamard matrices and diagonal matrices; the difference is that the unitary 3-design property of the Clifford group \( \{12\} \) provides randomness guarantees.

Finally, Section \( \text{VII} \) constructs logical unitary 2-designs that can be applied in the logical randomized benchmarking protocol of Combes et al. \( \{11\} \). In prior work \( \{42\} \), we have developed a mathematical framework for synthesizing all physical circuits that implement a logical Clifford operator (on the encoded qubits) for stabilizer codes (up to equivalence classes and ignoring stabilizer freedom). Circuit synthesis is enabled by representing the desired physical equivalence classes and ignoring stabilizer freedom). 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 \( \text{https://github.com/nrenga/symplectic-arxiv18a} \) for implementations.

It is now well-known that different codes yield efficient (e.g., low-depth) implementations of different logical operators. However, computing environments can change dynamically so that qubits or qubit links might have varying fidelity, and thus low-depth alone might not be desirable. Under such circumstances it is necessary to leverage all degrees of freedom in implementing a logical operator, and a compiler might use the above framework for this purpose. More generally, a compiler might usefully switch between several codes \( \{43\} \) dynamically, depending on the state of the system. Then this algorithm enables the compiler to be able to determine logical operators for a code quickly depending on the user-input circuit (on the protected qubits).

Section \( \text{VII} \) provides a proof of concept implementation of the Kerdock unitary 2-design on the protected (logical) qubits of the \([6,4,2]\) CSS code using the above logical Clifford synthesis algorithm. The logical randomized benchmarking protocol requires a unitary 2-design on the logical qubits, and Combes et al. use the full Clifford group for this purpose, which is much larger than the Kerdock design as shown above.

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 \( \{24\}, \{44\} - \{59\} \).
2) Elementary description of symmetries of the Kerdock code, and the \( N^2 + N \) stabilizer states determined by this code \( \{27\}, \{43\}, \{55\}, \{61\} \).
3) Demonstration that the symmetry group of the Kerdock code is a unitary 2-design and that sampling from it is straightforward. Introduction of elementary methods for translation to circuits without using ancillary qubits.
4) Provide a proof of concept construction for unitary 2-designs on the logical qubits of a stabilizer code \( \{11\}, \{42\} \).

We also provide software implementations of all algorithms, at \( \text{https://github.com/nrenga/symplectic-arxiv18a} \). Using this utility, we provide empirical estimates of the gate complexity for circuits obtained from the Kerdock design. We believe this paves the way for employing this design in several applications, specifically in randomized benchmarking \( \{10\}, \{52\} \).

III. 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 \( \{5\}, \{7\}, \{8\}, \{33\}, \{34\} \), and described more completely in \( \{54\} \) and \( \{42\} \). 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 2: 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 \( i^2 \), where \( i \triangleq \sqrt{-1}, \kappa \in \mathbb{Z}_4 \), are called quaternary phases. A single qubit is a 2-dimensional Hilbert space, and a quantum state \( \psi \) is a superposition of the two states \( \psi_0 \triangleq [1, 0]^T, \psi_1 \triangleq [0, 1]^T \) which form the computational basis. Thus \( \psi = \alpha \psi_0 + \beta \psi_1 \), where \( \alpha, \beta \in \mathbb{C} \) satisfy \( |\alpha|^2 + |\beta|^2 = 1 \) as per the Born rule \( \{55\} \) Chapter 3). The Pauli matrices are

\[
I_2, \quad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad Y = iXZ = \begin{bmatrix} 0 & i \\ -i & 0 \end{bmatrix},
\]

where \( i \triangleq \sqrt{-1} \) and \( I_2 \) is the 2 \( \times \) 2 identity matrix \( \{56\} \) Chapter 10]. We may express an arbitrary pure quantum state \( \psi \) as

\[
\psi = (\alpha_0 I_2 + \alpha_1 X + \alpha_2 Z + \alpha_3 Y) e_0, \quad \text{where } \alpha_\iota \in \mathbb{R} \quad (3)
\]

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

\[
D(a, b) \triangleq X^{a_1}Z^{b_1} \otimes \cdots \otimes X^{a_m}Z^{b_m} \in \mathbb{U}_N, \quad N \triangleq 2^m, \quad (4)
\]

where \( \mathbb{U}_N \) denotes the group of all \( N \times N \) unitary operators. The Heisenberg-Weyl group \( \text{HW}_N \) (also called the \( m \)-qubit Pauli group) consists of all operators \( \kappa^\dagger D(a, b) \), where \( \kappa \in \mathbb{Z}_4 \triangleq \{0, 1, 2, 3\} \). The order is \( |\text{HW}_N| = 4N^2 \) and the center of this group is \( \langle iI_n \rangle \triangleq \{I_n, iI_n, -I_n, -iI_n\}, \) where \( I_n \) is...
the $N \times N$ identity matrix. Multiplication in $\text{HW}_N$ satisfies the identity
\begin{equation}
D(a, b)D(a', b') = (-1)^{a'b^T + b'a^T} D(a', b')D(a, b).
\end{equation}
The standard symplectic inner product in $\mathbb{F}_2^{2m}$ is defined as
\[
\langle [a, b], [a', b'] \rangle_s = a^T b + b^T a = [a, b] \Omega [a', b']^T,
\] where the symplectic form $\Omega = \begin{bmatrix} 0 & I_m \\ I_m & 0 \end{bmatrix}$.

Therefore, two operators $D(a, b)$ and $D(a', b')$ commute if and only if $\langle [a, b], [a', b'] \rangle_s = 0$.

The homomorphism $\gamma : \text{HW}_N \to \mathbb{F}_2^{2m}$ defined by
\[
\gamma(\pi^a D(a, b)) = [a, b] \quad \forall \kappa \in \mathbb{Z}_4
\] has kernel $\langle I_N \rangle$ and allows us to represent elements of $\text{HW}_N$ (up to multiplication by scalars) as binary vectors.

The Clifford group $\text{Cliff}_N$ consists of all unitary matrices $g \in \mathbb{C}^{N \times N}$ for which $gD(a, bg^\dagger) \in \text{HW}_N$ for all $D(a, b) \in \text{HW}_N$, where $g^\dagger$ is the Hermitian transpose of $g$ [54]. $\text{Cliff}_N$ is the normalizer of $\text{HW}_N$ in the unitary group $\text{U}_N$. The Clifford group contains $\text{HW}_N$ and its size is $|\text{Cliff}_N| = 2^{m^2 + 2m} \prod_{j=1}^{m} (4^j - 1)$ (up to scalars $2^{2m\theta}$, $\theta \in \mathbb{R}$) [7]. We regard operators in $\text{Cliff}_N$ as physical operators acting on quantum states in $\mathbb{C}^N$, to be implemented by quantum circuits. Every operator $g \in \text{Cliff}_N$ induces an automorphism of $\text{HW}_N$ by conjugation. Note that the inner automorphisms induced by matrices in $\text{HW}_N$ preserve every conjugacy class $\{\pm D(a, b)\}$ and $\{\pm \text{D}(a, b)\}$, because $a, b$ are symmetric or anti-symmetric according as $ab^T = 0$ or 1, hence the matrix
\[
E(a, b) = \pi a^T b^T D(a, b)
\] is Hermitian. Note that $E(a, b)^2 = I_N$. The automorphism induced by a Clifford element $g$ satisfies
\[
gE(a, b)g^\dagger = \pm E([a, b]F_g),\quad \text{where } F_g = \begin{bmatrix} A_g & B_g \\ C_g & D_g \end{bmatrix}
\] is a $2m \times 2m$ binary matrix that preserves symplectic inner products: $\langle [a, b], [a', b'] \rangle_s = \langle [a, b], [a', b'] \rangle_s$. Hence $F_g$ is called a binary symplectic matrix and the symplectic property reduces to $F_g^T \Omega F_g^T = \Omega$, or equivalently
\[
A_g B_g^T = B_g A_g^T, \quad C_g D_g^T = D_g C_g^T, \quad A_g D_g^T + B_g C_g^T = I_m.
\]

(See [57] 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 $\text{HW}_N$. Let $\text{Sp}(2m, \mathbb{F}_2)$ denote the group of symplectic $2m \times 2m$ matrices over $\mathbb{F}_2$. The map $\phi : \text{Cliff}_N \to \text{Sp}(2m, \mathbb{F}_2)$ defined by
\[
\phi(g) = F_g
\] is a homomorphism with kernel $\langle I_N \rangle$, in every Clifford operator projects onto a symplectic matrix $F_g$. Thus, $\text{HW}_N$ is a normal subgroup of $\text{Cliff}_N$ and $\text{Cliff}_N/\text{HW}_N \cong \text{Sp}(2m, \mathbb{F}_2)$. This implies that the size is $|\text{Sp}(2m, \mathbb{F}_2)| = 2^{m^2} \prod_{j=1}^{m} (4^j - 1)$ (also see [7]). Table I lists elementary symplectic transformations $F_g$, that generate the binary symplectic group $\text{Sp}(2m, \mathbb{F}_2)$, and the corresponding unitary automorphisms $g \in \text{Cliff}_N$, which together with $\text{HW}_N$ generate $\text{Cliff}_N$. (See [42] Appendix I for a discussion on the Clifford gates and circuits corresponding to these transformations.)

We use commutative subgroups of $\text{HW}_N$ to define resolutions of the identity. A stabilizer is a subgroup $S$ of $\text{HW}_N$ generated by commuting Hermitian matrices of the form $\pm E(a, b)$, with the additional property that if $E(a, b) \in S$ then $-E(a, b) \not\in S$ [56]. The operators $\frac{1}{2^k} \pm E(a, b)$ project onto the $\pm 1$ eigenspaces of $E(a, b)$, respectively.

Remark 3: 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 $\pm 1$ 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 $\pm 1$ as the $\pm 1$ eigenspace of $S$.

If the subgroup $S$ is generated by $E(a_i, b_i), i = 1, \ldots, k$, then the operator
\[
\frac{1}{k} \prod_{i=1}^{k} (I_N + E(a_i, b_i))
\] projects onto the $2^{m-k}$-dimensional subspace $V(S)$ fixed pointwise by $S$, i.e., the $\pm 1$ eigenspace of $S$. The subspace $V(S)$ is the stabilizer code determined by $S$. We use the notation $[m, m-k]$ 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 $\gamma$ in [7]. A generator matrix for $\gamma(S)$ is
\[
G_S = [a_{i}, b_{i}]_{i=1}^{k} \in \mathbb{F}_2^{k \times 2m} \text{ s.t. } G_S \Omega G_S^T = 0,
\] 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 $S_{e_1 \cdots e_k}$ is generated by $e_i E(a_i, b_i)$, for $e_i \in \{ \pm 1 \}$. Note that the operator
\[
\Pi_{e_1 \cdots e_k} \triangleq \frac{1}{2^k} \prod_{i=1}^{k} (I_N + e_i E(a_i, b_i))
\]  
(14)
projects onto $V(S_{e_1 \cdots e_k})$, and that
\[
\sum_{(e_1, \ldots, e_k) \in \{ \pm 1 \}^k} \Pi_{e_1 \cdots e_k} = I_N.
\]  
(15)
Hence the subspaces $V(S_{e_1 \cdots e_k})$, or equivalently the subgroups $S_{e_1 \cdots e_k}$, provide a resolution of the identity, and elements (errors) in $HW_N$ simply permute these subspaces (under conjugation).

Given a $[m,m-k]$ stabilizer code, it is possible to perform encoded quantum computation in any of the subspaces $V(S_{e_1 \cdots e_k})$ by synthesizing appropriate logical Clifford operators (see [42] 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 [58] and references therein).

A stabilizer group $S$ defined by $k = m$ generators is called a maximal commutative subgroup of $HW_N$ and $\gamma(S)$ is called a maximal isotropic subspace of $F_{2^m}^2$. The generator matrix $G_S$ has rank $m$ and can be row-reduced to $[0 | I_m]$ if $S = Z_N \triangleq \{ E(0, b) : b \in F_{2^m}^2 \}$, or to the form $[I_m | P]$ if $S$ is disjoint from $Z_N$. We will denote these subgroups as $E([0 | I_m])$ and $E([I_m | P])$, respectively. The condition $G_S G_T^T = 0$ implies $P = P^T$, and any element of $\gamma(S)$ can be expressed in the form $[a, aP]$ for some $a \in F_{2^m}^2$. Note that $E([I_m | 0]) = X_N \triangleq \{ E(a,0) : a \in F_{2^m}^2 \}$. Since $\dim V(S) = 2^{m-m} = 1$, the subgroup $S$ fixes exactly one vector. The $N$ eigenvectors in an orthonormal eigenbasis for $S$ are defined up to an overall phase and called stabilizer states [28], [29]. The number of non-zero entries in a stabilizer state is determined by the intersection of $S$ with $Z_N$ [59].

IV. Weight Distributions of Kerdock Codes
Kerdock codes were first constructed as non-linear binary codes [45], as was the Goethals code [47] and the Delsarte-Goethals codes [49]. In this section, we describe the Kerdock and Delsarte-Goethals codes as linear codes over $Z_4$, the ring of integers modulo 4. These $Z_4$-linear codes were constructed by Hammons et al. [25] as Hensel lifts of binary cyclic codes, and this description requires Galois rings. The description given in Section IV-A requires finite field arithmetic, but is entirely binary and follows [27]. Our construction of unitary 2-designs in Section VI uses the matrices that are defined in Section IV-A. In Section IV-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 [27]
The finite field $F_{2^m}$ is obtained from the binary field $F_2$ by adjoining a root $\alpha$ of a primitive irreducible polynomial $p(x)$ of degree $m$ [60]. The elements of $F_{2^m}$ are polynomials in $\alpha$ of degree at most $m-1$, with coefficients in $F_2$, 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 $f : F_{2^m} \rightarrow F_{2^m}$ is defined by $f(x) \triangleq x^2$, and the trace map $Tr : F_{2^m} \rightarrow F_2$ is defined by
\[
Tr(x) \triangleq x + x^2 + \ldots + x^{2^m-1}.
\]  
(16)
Since $(x+y)^2 = x^2 + y^2$ for all $x, y \in F_{2^m}$, the trace is linear over $F_2$. The trace inner product $\langle x; y \rangle = Tr(xy)$ defines a symmetric bilinear form, so there exists a binary symmetric matrix $W$ for which $Tr(xy) = xWy^T$. In fact
\[
W_{ij} = Tr(\alpha^i \alpha^j), \quad i,j = 0,1,\ldots,m-1.
\]  
(17)
The matrix $W$ is non-singular since the trace inner product is non-degenerate (if $Tr(zx) = 0$ for all $x \in F_{2^m}$, then $x = 0$). Observe that $W$ is a Hankel matrix, since if $i+j = k$, then $Tr(\alpha^i \alpha^j) = Tr(\alpha^k)$). The matrix $W$ can be interpreted as the primal-to-dual-basis conversion matrix for $F_{2^m}$, with the primal basis being $\{1, \alpha, \alpha^2, \ldots, \alpha^{m-1}\}$ (see [17]).

The Frobenius map $f(x) = x^2$ is linear over $F_2$, so there exists a binary matrix $R$ for which $f(x) \equiv xR$. Since
\[
f(x_0 + x_1 \alpha + \ldots + x_{m-1} \alpha^{m-1}) = x_0 + x_1 \alpha^2 + \ldots + x_{m-1} \alpha^{2(m-1)}
\]  
(18)
the rows of $R$ are the vectors representing the field elements $\alpha^2i, i = 0, \ldots, m-1$. Note that square roots exist for all elements of $F_{2^m}$ since $R$ is invertible.

We write multiplication by $z \in F_{2^m}$ 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 $\alpha$. The matrix $A$ is the companion matrix of the primitive irreducible polynomial $p(x) = p_0 + p_1 x + \ldots + p_{m-1} x^{m-1} + x^m$ over the binary field. Thus
\[
A \triangleq \\
\begin{bmatrix}
0 & 1 & 0 & \cdots & 0 \\
0 & 0 & 1 & \cdots & 0 \\
\vdots & \ddots & \ddots & \ddots & \vdots \\
0 & 0 & 0 & \cdots & 1 \\
p_0 & p_1 & p_2 & \cdots & p_{m-1}
\end{bmatrix},
\]  
(19)
and we have chosen $A$ rather than $A^T$ as the companion matrix since we are representing field elements in $F_{2^m}$ by row vectors (rather than column vectors).

**Lemma 4**: The matrices $A_z, W, \text{ and } R^i$, for $i \in [m]$, satisfy:
(a) $A_z A_z = A_z A_{z^2}$;
(b) $A_z A_z = A_{z+z^2}$;
(c) $A_z W = W A_z^2$;
(d) $R^i A^2 z^i = A_z R^i$, $R^i A^2 z = A_z R^i$, and $R^{-i} A^{-2} = A^{-i} R^{-i}$;
(e) $R^i W = W R^{-i}$ and $W^{-1} R^{-i} W = (R^i)^T$. 

For stabilizer states of matrices, and demonstrate that exponentiating these matrices produces stabilizer states. The Delsarte-Goethals set consists of all matrices of all binary matrices. For the remainder of this paper we represent a binary symmetric matrix $A_{\mathbb{Z}_2}$ as $A_{\mathbb{Z}_2} = A_{\mathbb{Z}_2} W + \sum_{i=1}^{r} [A_{\mathbb{Z}_2} W (R_i^T) + R_i W A_{\mathbb{Z}_2}^T]$. 

**Definition 5:** For $0 \leq r \leq (m-1)/2$ and for $z = (z_0, z_1, \ldots, z_r) \in \mathbb{F}_{2^{m+1}}$, define the bilinear form $\beta_{z,r}(x,y) \triangleq \text{Tr}[z_0 xy + z_1 (x^2 y + xy^2) + \ldots + z_r (x^{2r} y + xy^{2r})]$. Note that $\beta_{z,r}(x,y)$ is represented by the binary symmetric matrix $P_{z,r} \triangleq A_{\mathbb{Z}_2} W + \sum_{i=1}^{r} [A_{\mathbb{Z}_2} W (R_i^T) + R_i W A_{\mathbb{Z}_2}^T]$. 

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

**Lemma 6:** The Delsarte-Goethals set $P_{DG}(m,r)$ is an $(m+r+1)$-dimensional vector space of symmetric matrices. If $z \neq 0$ then rank$(P_{z,r}) \geq m-2r$. Matrices in the Kerdock set $P_{DG}(m,0)$ are non-singular.

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

$$0 = \text{Tr}[z_0 xy + z_1 (x^2 y + xy^2) + \ldots + z_r (x^{2r} y + xy^{2r})] = \text{Tr}[(z_0 x)^{2r} y^{2r} + (z_1 x^{2r+1}) y^{2r} + (z_1 x)^{2r-1} y^{2r}] + \ldots + (z_r x^{2r} y^{2r} + (z_r x) y^{2r})] = \text{Tr}[y^{2r} ((z_0 x)^{2r} + (z_1 x^{2r+1} + (z_1 x)^{2r-1}) + \ldots + (z_r x^{2r} + x z_r)]].$$

This holds for all $y$, so $(z_0 x)^{2r} + (z_1 x^{2r+1} + (z_1 x)^{2r-1}) + \ldots + (z_r x^{2r} + x z_r)$ must be identically 0, i.e., $x$ is a root of the polynomial. Since the polynomial has at most $2^r$ roots, the nullspace of $P_{z,r}$ has dimension at most $2r$, which implies that rank$(P_{z,r}) \geq m-2r$.

**Remark 7:** Note that since the dimension of the vector space of all binary $m \times m$ symmetric matrices is $m(m+1)/2$, the set $P_{DG}(m,(m-1)/2)$ contains all possible symmetric matrices. For the remainder of this paper we represent a general symmetric matrix as simply $P$, thereby dropping the subscripts $z,r$ unless necessary. We will continue to represent Kerdock matrices as $P_z$.

### B. Delsarte-Goethals Codes and Weight Distributions

Hammons et al. [25] showed that the classical nonlinear Kerdock and Delsarte-Goethals codes, defined by quadratic forms in $[45, 48]$, 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 $i$ produces stabilizer states. For stabilizer states of $E([I_m | P_{z,i,r}])$ and $E([I_m | P_{z,i,r}])$, we calculate their Hermitian inner products using the trace of certain projection operators, and show that the distribution of inner products depends only on rank$(P_{z,i,r} + P_{z,i,r})$. Then, since rank$(P_Z) \in \{0, m\}$ for all $P_z \in P_{DG}(m)$, 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-Goethals sets $P_{DG}(m,r)$. While this question is straightforward for $P_k(m)$, it remains open for general $P_{DG}(m,r)$ and will be investigated in future work.

**Definition 8:** The $\mathbb{Z}_4$-linear Delsarte-Goethals code is given by $DG(m,r) \triangleq \{ [xP_rT + 2wXT + \kappa]_{x \in \mathbb{F}_{2^m}} : P \in P_{DG}(m,r), w \in \mathbb{F}_{2^m}, \kappa \in \mathbb{Z}_4 \}$. (21)

This code has size $2^{m(r+1)+m+2}$ and is of type $4^{m+1}2^{mr}$ [50, Section 12.1]. The Kerdock code $K(m) \triangleq DG(m,0)$. Here the notation $[xP_rT + 2wXT + \kappa]_{x \in \mathbb{F}_{2^m}}$ represents a $\mathbb{Z}_4$-valued column vector with each entry $xP_rT + 2wXT + \kappa$ (mod 4) indexed by the vector $x \in \mathbb{F}_{2^m}$.

**Definition 9:** For $u, v \in \mathbb{Z}_4^N$, the Lee weight of $u$ is defined as $w_L(u) \triangleq n_L(u) + 2u_2(u) + u_3(u)$, where $n_L(u)$ denotes the number of entries of $u$ with value $u$, 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) to binary pairs (see Remark 2 for details). 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 2). The shortest distance around the circle defines the Lee metric on $\mathbb{Z}_4^N$ and Gray encoding is an isometry from $(\mathbb{Z}_4^N, \text{Lee metric})$ to $(\mathbb{Z}_2^{2N}, \text{Hamming metric})$. However, since $g(1+3) \neq g(1)+g(3)$, the Gray map is non-linear. Hence the binary Kerdock and Delsarte-Goethals codes obtained by Gray-mapping the codewords in $K(m)$ and $DG(m,r)$, respectively, are non-linear (see [50, Chapter 12]).

![Fig. 1. The Gray map assigning integers modulo 4 or quaternary phases to binary pairs (that are length-2 row vectors).](image_url)
Lemma 10: Let \( u, v \in \mathbb{C}^N \) be two length-\( N \) vectors of quaternary phases. Then
\[
\langle u - v, u - v \rangle = 2d_H(g(u), g(v)),
\]
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 \( E([I_m | P]) \) determined by a binary symmetric matrix \( P \) (see Remark 1). Note that we denote the maximal commutative subgroup determined by the rows of \([I_m | P]\) as \( E([I_m | P]) \), and that we do not normalize eigenvectors (stabilizer states) in this section, since the Gray map needs to be applied to quaternary phases.

Lemma 11: Given a binary symmetric matrix \( P \), the (column) vectors \([x^{P}x^{T}+2wx^{T}]_{x \in \mathbb{F}_2^m}\) are common eigenvectors of the maximal commutative subgroup \( E([I_m | P]) \). 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 \( E(a, aP) \cdot [x^{P}x^{T}+2wx^{T}]_{x \in \mathbb{F}_2^m} \) for some \( a \in \mathbb{F}_2^m \), but the following argument uses the mathematical framework described in Section III. Note that
\[
[x^{P}x^{T}+2wx^{T}]_{x \in \mathbb{F}_2^m} = \sum_{x \in \mathbb{F}_2^m} t^P \cdot [x^{P}x^{T}+2wx^{T}]_{x \in \mathbb{F}_2^m},
\]
where \( e_x \) denotes the standard basis vector in \( \mathbb{C}^N \) with a 1 in the position \( x \) and 0 elsewhere.

The columns \([x^{P}x^{T}+2wx^{T}]_{x \in \mathbb{F}_2^m} = [(−1)wx^{T}]_{x \in \mathbb{F}_2^m}\) 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 \( X_N = E([I_m | 0]) \). The Clifford operator \( t_{P} = \text{diag}(x^{P}x^{T}) \) (see Table I). Hence conjugation by \( t_{P} \) maps \( E([I_m | 0]) \) to \( E([I_m | P]) \), i.e., \( t_{P}E(a, 0)t_{P}^{-1} = E(a, aP) \), and so the common eigenvectors of \( E([I_m | P]) \) are
\[
t_{P} \cdot [x^{P}x^{T}+2wx^{T}]_{x \in \mathbb{F}_2^m} = [t^P \cdot [x^{P}x^{T}+2wx^{T}]_{x \in \mathbb{F}_2^m}.
\]

It is easily verified that for any \( a \in \mathbb{F}_2^m \),
\[
\left(t_{P}E(a, 0)t_{P}^{-1}\right) \cdot [x^{P}x^{T}+2wx^{T}]_{x \in \mathbb{F}_2^m} = \pm [x^{P}x^{T}+2wx^{T}]_{x \in \mathbb{F}_2^m}.
\]

Now we have the following important observation. Given \( v \in \mathbb{C}^N \), define
\[
S_v = \{ g \in \text{HW} : gv = \alpha v, \text{ where } \alpha \in \mathbb{C} \text{ and } |\alpha| = 1 \}.
\]

Lemma 12:

(a) \( S_v \) is commutative.

(b) There is a 1-1 correspondence between maximal commutative subgroups of \( \text{HW} \) and stabilizer states.

Proof:

(a) If \( E(a, b), E(a', b') \in S_v \) then
\[
E(a, b)E(a', b')v = \alpha \alpha' v = \alpha' \alpha v = E(a', b')E(a, b)v.
\]

(b) If \( v \) is a stabilizer state then \( S_v \) is a maximal commutative subgroup of \( \text{HW} \).

Remark 13: Any stabilizer state of a maximal commutative subgroup of \( \text{HW} \) disjoint from \( Z_N \) can be obtained by exponentiating Delsarte-Goethals codewords, and multiplying the quaternary phase vector by \( N^{-\frac{1}{2}} \). The maximal commutative subgroups \( E([I_m | P]) \) determined by the Kerdock matrices \( P_{k} \) intersect trivially. Together with \( Z_N = E([0 | I_m]) \), they partition all \((N^2 - 1)\) non-identity Hermitian Pauli matrices. Hence, 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 \( P_{k} \in P_{k}(m) \) and \( Z_N \).

Therefore, stabilizer states connect the classical world of Kerdock and Delsarte-Goethals codes and the quantum world of maximal commutative subgroups of \( \text{HW} \). This synergy has proven successful in several applications \([27, 31–33, 35, 51]\) and our construction of a unitary 2-design here, from stabilizer states, is yet another instance.

Remark 14: Note that in Lemma 11 we only considered \( \kappa = 0 \) while exponentiating codewords \( c_{u} \in \text{DG}(m, r) \). This is to ensure that the resulting eigenvector corresponds to a \( \pm 1 \) eigenvalue (and not a value in \{\pm 1, \pm i\}). However, Theorem 7 considers all \( \kappa \in \mathbb{Z}_4 \) while calculating the weight distribution.

Given \( P \in P_{\text{DG}}(m, r) \), we scale the common eigenvectors of \( E([I_m | P]) \) 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 III and observe that here we consider all eigenvectors, albeit unnormalized, and not just the \( \pm 1 \) eigenspace.) Therefore, if we can compute the Hermitian inner products between these unnormalized stabilizer states then we can use Lemma 10 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 \([24\text{ Chapter 15}]\) which follows from \( Z_4 \)-linearity and Gray isometry.

Lemma 15: Let \( P_{1}, P_{2} \in P_{\text{DG}}(m, r) \) be distinct. Fix \( v \in V(P_{1}) \) and let \( u \) run through \( V(P_{1}) \). If \( \text{rank}(P_{1} + P_{2}) = k \) then
\[
|\langle u, v \rangle|^2 = \begin{cases} 2^{m-k} & \text{for } 2^k \text{ eigenvectors } u, \\ 0 & \text{for } 2^m - 2^k \text{ eigenvectors } u. \end{cases}
\]

Proof: Let \( Q = [I_m | P_{1}] \cap [I_m | P_{2}] \) represent a basis for the subspace formed by intersecting the spaces generated by \([I_m | P_{1}] \) and \([I_m | P_{2}] \). Then \( \text{dim}(Q) = m - k \). 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 \([e_{j}, d_{j}], j = m - k + 1, \ldots, m \) and \([e_{j}^{'}, d_{j}^{'}, j = m - k + 1, \ldots, m \) respectively. Since \( v \) is fixed, using \([14]\), there are fixed \( i_{j} \in \{\pm 1\} \) such that
\[
\left(\frac{1}{\sqrt{N}}\right)^{v} \left(\frac{1}{\sqrt{N}}\right)^{u} = \prod_{i=1}^{m-k} (I_{N} + f_{i}E(a_{i}, b_{i})) \prod_{j=m-k+1}^{m} (I_{N} + t_{j}E(e_{j}^{'}, d_{j}^{'})) / 2,
\]
and since the only constraint on \( u \) is to be from \( V(P_{1}) \),
\[
\left(\frac{1}{\sqrt{N}}\right)^{v} \left(\frac{1}{\sqrt{N}}\right)^{u} \]
where \( e_i, s_i \in \{ \pm 1 \} \) are variable. Since \( \langle (u, v) \rangle^2 = \text{Tr}(uu^\dagger vv^\dagger) \) it only remains to calculate \( \text{Tr}(uu^\dagger vv^\dagger) \). If \( e_i = f_i \forall i \), then
\[
\langle I_N + e_iE(a_i, b_i) | I_N + f_iE(a_i, b_i) \rangle = 2(I_N + e_iE(a_i, b_i))
\]
so that
\[
\text{Tr}(uu^\dagger vv^\dagger) = 2^{m-k}\text{Tr}\left( \prod_{i=1}^{m-k} (I_N + e_iE(a_i, b_i)) \right)
\]
\[
\times \prod_{j=m-k+1}^{m} (I_N + s_jE(c_j, d_j))
\]
\[
\times \prod_{j=m-k+1}^{m} (I_N + t_jE(c'_j, d'_j)).
\]

Expanding the right hand side, the only term with nonzero trace is the identity with trace \( 2^m \). Hence in this case \( \text{Tr}(uu^\dagger vv^\dagger) = 2^{m-k} \). 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
\[
\langle I_N + e_iE(a_i, b_i) | I_N + f_iE(a_i, b_i) \rangle = 0
\]
and \( \text{Tr}(uu^\dagger vv^\dagger) = 0 \). There are \( 2^m - 2^k \) such eigenvectors.

Finally, if \( k = m \) then \( \text{Tr}(uu^\dagger vv^\dagger) = \text{Tr}(I_N) = 2^m \forall u, v \). 

**Corollary 16:** For \( P_1, P_2 \in P_k(m) \), since \( \text{rank}(P_1 + P_2) \in \{0, m\} \) the inner products are
\[
\langle (u, v) \rangle^2 = \begin{cases} 0 & \text{if } P_1 = P_2 \text{ and } u \neq v \\ 2^m & \text{if } P_1 \neq P_2, \\ 2^{2m} & \text{if } (P_1 = P_2 \text{ and } u = v). \end{cases}
\]

This result is the primary tool that allowed us to simplify the derivation of the weight distribution of Kerdock codes in Theorem 1. Note that Theorem 1 is the only result in this section that is restricted to Kerdock codes but not general Delarte-Goethals codes (and requires \( m \) to be odd).

**V. MUTUALLY UNBIASED BASES FROM \( P_k(m) \)**

In this section, we will organize the columns of \( I_N \) (i.e., the common eigenbasis of \( Z_N \)) and all stabilizer states determined by \( P_z \in P_k(m) \) 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 Delarte-Goethals sets.

**Definition 17:** Given a collection \( M \) of unit vectors in \( \mathbb{C}^N \) (Grassmannian lines) the chordal distance \( \text{chord}(S) \) is given by
\[
\text{chord}(M) \triangleq \min_{(u,v) \in M} \sqrt{1 - \langle (u,v) \rangle^2}.
\]

It follows from Lemma 15 that the Delarte-Goethals set \( \text{PGD}(m, r) \) determines \( 2^{m(r+2)} \) complex lines (stabilizer states) in \( \mathbb{C}^N \) with chordal distance \( \sqrt{1 - 2^{-2(m-2r)}} \) (cf. [61]).

**Definition 18:** Two \( N \times N \) unitary matrices \( U \) and \( V \) are said to be mutually unbiased if \( \langle (u, v) \rangle = N^{-\frac{1}{2}} \) 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 16** when applied to normalized eigenvectors, shows that the \( N \) eigenbases determined by the Kerdock set \( P_k(m) \) are mutually unbiased (also see Remark 13). Let \( B_k(m) \) denote the collection of these \( N \) eigenbases (of \( E([I_m \mid P]) \) for all \( P \in P_k(m) \)) along with the eigenbasis \( I_N \) of \( E([0 \mid I_m]) \). This is a set of \( N+m \) mutually unbiased bases and they determine an ensemble of \( N(N+1) \) complex lines (stabilizer states) that is extremal [34]. In this section, we provide an elementary description of their group of Clifford symmetries.

A. The Kerdock MUBs

Recall from Section [IV-A] that the Kerdock matrices are \( P_z = A_zW \), where \( W \) is a symmetric Hankel matrix with binary entries that satisfies \( \text{Tr}(xy) = xWy^T \) and \( A_z \) represents multiplication by \( z \), both in \( \mathbb{F}_{2^m} \). Using the result of Lemma 11 define \( N \) mutually unbiased bases
\[
M_z \triangleq t_P H_N = \text{diag}(i^{xP_x} x^T) H_N, \quad z \in \mathbb{F}_{2^m},
\]
where \( [H_N]_{x,y} \triangleq \frac{1}{\sqrt{N}}(-1)^{xy} \), for \( x, y \in \mathbb{F}^{2^m}_{2} \), 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 \( M_{M \infty} \triangleq I_N \). 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
\[
B_k(m) \triangleq \{ I_N, M_z : z \in \mathbb{F}_{2^m} \}
\]
is a maximal collection of mutually unbiased bases [34].

B. Symmetries of Kerdock MUBs

Let \( M \) be the \( N \times N(N+1) \) matrix given by
\[
M \triangleq [ M_{M \infty} \mid M_0 \mid \cdots \mid M_z \mid \cdots ],
\]
Note that \( M_{M \infty} = I_N \) 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 \( \Pi \) 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 16 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 \( \text{Cliff}_N \).
Proof: A Pauli matrix $E(a, b) \in E([I_m \mid P_2])$ that fixes $M_z$ can be written as $E(a, b) = \sum_{v \in M_z} e_v v^T$, where $e_v = \pm 1$ for all $v$. Since $U$ permutes the eigenbases $M_z$, it follows that $Uv \in M_z$, for some $z' \in F_{2m} \cup \{\infty\}$, is fixed by $UE(a, b)U^T$ which must again be a Pauli matrix. Hence $U$ is a Clifford element.

We first observe the symmetries induced by elements of $HN$.

1) Pauli Matrices $E(a, 0)$ and $E(0, b)$: 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 $E(0, b)$ 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 $PSL(2, 2^m)$ is the group of all transformations

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

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

$$f: \begin{pmatrix} z \\ 1 \end{pmatrix} \rightarrow \begin{pmatrix} az + b \\ cz + d \end{pmatrix} \equiv \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ or } \begin{pmatrix} az + b \\ cz + d \end{pmatrix}. \tag{31}$$

The projective linear group $PL(2, 2^m)$ is the group of all transformations

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

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

$$|PSL(2, 2^m)| = (N + 1)N(N - 1) = 2^{2m} - 2^m,$$

$$|PL(2, 2^m)| = (N + 1)N(N - 1)m. \tag{32}$$

Now we analyze the symmetries induced by elements of the binary symplectic group $Sp(2m, F_2)$.

2) Clifford Symmetries of $M$: The group $PSL(2, 2^m)$ is generated by the transformations $z \mapsto z + x$, $z \mapsto xz$, and $z \mapsto 1/z$. The group $PTL(2, 2^m)$ is $PSL(2, 2^m)$ enlarged by the Frobenius automorphisms $z \mapsto z^{2^{-i}} \equiv zR_i$ discussed in Section [V.A] We realize each of these transformations as a symmetry of $M$. We recall that $A_zW^TA_z^T = A_z^2W$ from part (c) of Lemma [4] and for convenience we work with maximal commutative subgroups $E([I_m \mid A_z^2W])$, i.e., the Kerckoff matrices are $P_z = A_z^2W$. Note that every field element $\beta \in F_{2^m}$ is a square, so this is equivalent to $P_z = A_z^2W$.

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

$$[I_m \mid A_z^2W] \begin{bmatrix} I_m & A_z^{-1} \\ 0 & A_z \end{bmatrix} = [I_m \mid (A_z^{-1} + A_z^2)W] \equiv [I_m \mid (A_z^{z+x})W]. \tag{33}$$

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

$$[I_m \mid A_z^2W] \begin{bmatrix} A_z^{-1} & 0 \\ 0 & A_z \end{bmatrix} = [A_x^{-1} \mid A_x^2W^T] = [A_x^{-1} \mid A_xA_z^2W]. \tag{34}$$

(iii) $z \mapsto 1/z$ becomes $[I_m \mid A_z^2W] \mapsto [I_m \mid A_z^2W^T]$:

$$[I_m \mid A_z^2W] \begin{bmatrix} 0 & I_m \\ I_m & 0 \end{bmatrix} \begin{bmatrix} W^{-1} & 0 \\ 0 & WT \end{bmatrix} = [A_z^2W \mid I_m] \begin{bmatrix} W^{-1} & 0 \\ 0 & W \end{bmatrix} = [A_z^2 \mid W] \equiv [I_m \mid A_z^{2^{-1}}W]. \tag{35}$$

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

$$[I_m \mid A_z^2W] \begin{bmatrix} R^{-i} & 0 \\ 0 & (R^iT)^T \end{bmatrix} = [R^{-i} \mid A_z^2W(R^iT)^T] = [R^{-i} \mid A_z^2W^{-i}W] \equiv [I_m \mid A_z^2W]. \tag{36}$$

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

$$\mathcal{P}_{k,m} \equiv (T_{A_z^2W}, L_{A_z^{-1}}, \Omega_{L_{W^{-1}}}; x \in F_{2^m}) \cong PSL(2, 2^m), \tag{37}$$

$$\mathcal{P}_{k,m}^* \equiv (T_{A_z^2W}, L_{R^{-i}A_z^{-1}}, \Omega_{L_{W^{-1}}}; x \in F_{2^m}) \cong PTL(2, 2^m). \tag{38}$$

Although $T_{A_z}^2 = I_{2^m}$ in the unitary group we have $t_{A_z}^2 = E(0, dW)$. Therefore the corresponding Clifford elements will generate a group larger than $PSL(2, 2^m)$ and $PTL(2, 2^m)$. 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 [42 Section II]).

Remark 22: Note that $\Omega \notin \mathcal{P}_{k,m}$ but $\Omega L_{W^{-1}} \notin \mathcal{P}_{k,m}$, which means $HN$ does not permute columns of $M$ but $HN_L W_{-1}$ does. Hence, for example, to map $[0, a]$ to $[a, 0]$ one sequence would be $(\Omega L_{W^{-1}}) \cdot L_{A_z^{-1}}$, where $b$ satisfies $aW^{-1}A_z^{-1} = a$. This does not force $A_z^{-1} = W$.

Lemma 23: Any element of $\mathcal{P}_{k,m}$ can be described as a product of at most 4 basis symplectic matrices given in Section [V.B2].

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

$$[I_m \mid A_z^2W] \begin{bmatrix} A_z^{-2} & 0 \\ 0 & (A_z^2)^T \end{bmatrix} \begin{bmatrix} W^{-1} & 0 \\ 0 & WT \end{bmatrix} = \begin{bmatrix} 0 & A_z^2W \\ W^{-1}A_z^2W & 0 \end{bmatrix}. \tag{39}$$

It can be verified that the above is a valid symplectic matrix and satisfies all conditions in (10). We now show that this matrix can be decomposed as a product of 4 basis matrices.

We use the results in Lemma 4 and observe the following:

$$\begin{bmatrix} A_z^{-2} & 0 \\ 0 & (A_z^2)^T \end{bmatrix} \begin{bmatrix} W^{-1} & 0 \\ 0 & WT \end{bmatrix} = \begin{bmatrix} 0 & A_z^2W \\ W^{-1}A_z^2W & 0 \end{bmatrix}.$$
\[
\begin{bmatrix}
I_m & A_{2}^2 W \\
0 & I_m
\end{bmatrix}
\begin{bmatrix}
0 & A_{2}^2 W \\
W^{-1} A_{2}^2 & 0
\end{bmatrix} =
\begin{bmatrix}
A_{2}^2 y & A_{2}^2 W \\
W^{-1} A_{2}^2 & 0
\end{bmatrix}.
\]

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

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

\[
\tau \left( \begin{bmatrix}
a & b \\
c & d
\end{bmatrix} \right) \triangleq T_{A_{2}^2 W} \cdot L_{A_{2}^2} \cdot \Omega L^{-1} W \cdot T_{A_{2}^2} W.
\]

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

\[
F_{\alpha,\beta,\delta} \triangleq T_{A_{2}^2 W} \cdot L_{A_{2}^2} \cdot \Omega L^{-1} W \cdot T_{A_{2}^2 W}.
\]

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 ensures 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 [PV-A].

**Lemma 25:** An arbitrary element from \( \mathcal{P}_{K,m} \), specified by \( a, b, c, d \in \mathbb{F}_m \) and \( e \in \{0, \ldots, m-1\} \) takes the form

\[
F = \begin{bmatrix}
R^{-1} A_{2}^2 & R^{-1} A_{2}^2 W \\
W^{-1} R^{-1} A_{2}^2 & (R^i)^T (A_{2}^2)^T
\end{bmatrix},
\]

with \( ad + bc = 1 \), and realizes the block permutation

\[
[I_m \mid A_{2}^2 W] \mapsto [I_m \mid A_{2}^2 z^{-1}] W ,
\]

\( z' \triangleq z^{-2} \).

**Proof:** See Appendix [\ref{Appendix}].

**VI. UNITARY 2-DESIGNS FROM THE KERDOCK MUBS**

In this section, we show that the unitary transformations determined by \( \mathcal{P}_{K,m} \), along with Pauli matrices \( D(a, b) \in \text{HW}_N \), 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 \([a, b] \rightarrow [c, d] \) to represent an edge between two vertices.

**Remark 27:** Elements of the Clifford group act by conjugation on \( \text{HW}_N \), 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 \( E([I_m \mid P_z]), z \in \mathbb{F}_m \), or from \( E([0 \mid I_m]) \). Type 2 edges connect vertices from different maximal commutative subgroups.

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

**Definition 28 ([62] Def. 2.4):** A strongly regular graph with parameters \((n, t, \lambda, \mu)\) 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 \( \lambda \) or \( \mu \) according as \( x, y \) are joined or not joined respectively.

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

\[
n = N^2 - 1 ,
t = \frac{N^2}{2} - 2 ,
\lambda = \frac{N^2}{4} - 3 ,
\mu = \frac{N^2}{4} - 1.
\]

**Proof:** A vertex \([c, d] \) joined to a given vertex \([a, b] \) is a solution to \([a, b] [c, d] \) \( \Omega \) \( [c, d] \) \( \Omega \) \( [a, b] \). 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 \( \text{Sp}(2m, \mathbb{F}_2) \) acts transitively on vertices, on edges, and on non-edges of \( \mathbb{H}_N \).

(b) The groups \( \mathcal{P}_{K,m} \) and \( \mathcal{P}_{K,m}^* \) 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 \( \mathcal{P}_{K,m} \) acts transitively on maximal commutative subgroups \( E([0 \mid I_m]), E([I_m \mid P_z]), z \in \mathbb{F}_m \) (see (34) and (36), we need only show that \( \mathcal{P}_{K,m} \) is transitive on a particular subgroup, say \( E([I_m \mid 0]) \). If \([a, b] \in \mathbb{F}_m \) then there exists \( c \in \mathbb{F}_m \) such that \( b = ac \), and it follows from (35) that the symplectic matrix \( A_{c, e} \) maps \([a, 0] \) to \([b, 0] \).

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

**Definition 33 ([12] [63] Chap. 7):** Let \( k \) be a positive integer. An ensemble \( \mathcal{E} = \{p_i, U_i\}_{i=1}^m \), 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 \( X \in (\mathbb{C}^N)^{\otimes k} \)

\[
\sum_{(p,U) \in \mathcal{E}} p U^{\otimes k} X (U^\dagger)^{\otimes k} = \int_{U_N} d\eta(U) U^{\otimes k} X (U^\dagger)^{\otimes k},
\]

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

We define the \textit{Kerdock twirl} to be the linear transformation of \((\mathbb{C}^N)^{\otimes 2}\) determined by the uniformly weighted ensemble consisting of \(\phi^{-1}(\mathcal{P}_{K,m})\) along with Pauli matrices \(D(a,b)\), where \(\phi: \text{Cliff}_N/\text{HW}_N \to \text{Sp}(2m, \mathbb{F}_2)\) (from Section \ref{sectionIII}). Similarly, we define the 2-fold action (in \cite{43}) of the ensemble determined by \(\mathcal{P}_{K,m}\) as the \textit{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 \(D(a,b) \in \text{HW}_N\), 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 \cite{12} or \cite{17} 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 \(\mathcal{P}_{K,m}, \mathcal{P}_{K,m}\) followed by a random Pauli matrix \(D(a,b)\) gives unitary 2-designs.

Puchała and Miszczak have developed a useful Mathematica\textsuperscript{\textregistered} package IntU \cite{63} for symbolic integration with respect to the Haar measure on unitaries. For small \(m\), we used this utility to verify the equality in \cite{45} explicitly for the Kerdock 2-design.

Sampling uniformly from the groups \(\mathcal{P}_{K,m}\) can be achieved using the \textit{systematic} procedure shown in \cite{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 II (see \cite{42} Section II). Although our unitary 2-design is equivalent to that discovered by Cleve et al. \cite{17}, 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 \textit{tailored} for the design, our algorithm from \cite{36} (whose details are discussed in \cite{42} Appendix II) is a \textit{general purpose} procedure that can be used to translate \textit{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 \textit{near-linear} when compared to the \(O(m^2)\) gate-complexity for general Clifford elements. Our open-source implementation\footnote{Implementations online: \url{https://github.com/nrenga/symplectic-arxiv18a}} allows one to construct the design for a specified number of qubits, and we use this utility to calculate \textit{worst-case} gate complexities on up to 16 qubits.

In our sampling procedure \cite{41} we have three elementary forms \(T_{A_w}, L_{A_z}\), and \(\Omega\), which translate to phase and controlled-Z gates, permutations and controlled-NOT gates, and Hadamard gates on all qubits, respectively (see \cite{42} Appendix I). Note that \(L_{W^{-1}}\) has the same elementary form as \(L_{A_z}\), although \(W\) is fixed for a given \(m\). The Hadamard gates add only \(O(m)\) complexity. Figures 2, 3 and 4 plot the \textit{worst-case} complexities of the gates \(T_{A_w}, L_{A_z}\), and \(L_{W^{-1}}\) obtained using our procedure. The only form that seems to grow faster than \(O(m \log m \log \log m)\) is \(L_{A_z}\), and we are currently investigating methods to calculate this gate complexity via analytical arguments that leverage results in the classical computation literature. 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 \cite{41} involves a \textit{constant} number of factors, the overall complexity is that of the factor with largest order term. We will also investigate 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 \textit{quantum} unitary 2-design discovered by Cleve et al. by establishing a connection to \textit{classical} Kerdock codes, and simplified the description of the design as well as its translation to circuits. Since we also appear to achieve competitive Clifford-gate-complexities, and provide implementations for our methods, we believe this paves the way for employing this 2-design in several applications, specifically in randomized benchmarking \cite{10, 52}.\footnote{Implementations online: \url{https://github.com/nrenga/symplectic-arxiv18a}}

**VII. LOGICAL UNITARY 2-DESIGNS**

In this section, we apply our synthesis algorithm \cite{42} to logical randomized benchmarking, which was recently proposed by Combes et al. \cite{11} as a more precise protocol to reliably
The logical Pauli operators are

\begin{align*}
\bar{X}_1 &\triangleq E(110000, 000000) & \bar{Z}_1 &\triangleq E(000000, 010001) \\
\bar{X}_2 &\triangleq E(101000, 000000) & \bar{Z}_2 &\triangleq E(000000, 001001) \\
\bar{X}_3 &\triangleq E(100100, 000000) & \bar{Z}_3 &\triangleq E(000000, 000101) \\
\bar{X}_4 &\triangleq E(100010, 000000) & \bar{Z}_4 &\triangleq E(000000, 000011)
\end{align*}

Consider \( \mathbb{F}_{16} \) constructed by adjoining to \( \mathbb{F}_2 \) a root \( \alpha \) of the primitive polynomial \( p(x) = x^2 + x + 1 \). Consider the element \( F_{abcd} \) in \( \mathcal{P}_{K,4} \) identified by the tuple \( (a = \alpha^3, b = \alpha^8, c = \alpha^7, d = 0) \), or equivalently \((a, b, c, d) = 0)\) in \( \mathcal{P}_{K,4} \). In this case the matrices defined in Section [IV-A] are

\[ W = \begin{bmatrix}
0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 \\
1 & 0 & 0 & 1 \\
0 & 1 & 0 & 0
\end{bmatrix}, \quad W^{-1} = \begin{bmatrix}
1 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 \\
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0
\end{bmatrix}. \]

Then, using the isomorphism in Corollary [24] and the direct form in Lemma [23], we can express the element in \( \mathcal{P}_{K,4} \) as

\[ F_{abcd} = T_{A^2} \cdot L_{A^{-2}} \cdot \Omega L_{W^{-1}} \cdot T_{A^{11}} \cdot W \\
= I_8 \cdot L_{(A^7)^{-2}} \cdot \Omega L_{W^{-1}} \cdot T_{(A^{11})^2} \cdot W \\
= \begin{bmatrix}
0 & A^2 W \\
W^{-1} A^2 & (A^2)^T
\end{bmatrix}
\]

Using the explicit decomposition in [49], we map the elementary symplectic matrices to standard Clifford gates (as discussed in [42]) and get the following circuit (CKT1)\(^2\)

\begin{align*}
\text{‘Permute’} &\quad [4,1,2,3] \\
\text{‘CNOT’} &\quad [1,2] \\
\text{‘Permute’} &\quad [4,3,2,1] \\
\text{‘CNOT’} &\quad [1,4] \\
\text{‘H’} &\quad [1,2,3,4] \\
\text{‘P’} &\quad [1,2,3,4] \\
\text{‘CZ’} &\quad [1,3] \\
\text{‘CZ’} &\quad [2,4] \\
\text{‘CZ’} &\quad [3,4]
\end{align*}

Here the indices corresponding to ‘Permute’ imply the cycle permutation (1432), i.e., the first qubit has been replaced by

\[ S \triangleq \langle X^{\otimes 6}, Z^{\otimes 6} \rangle \]
the fourth, the fourth by the third, 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 \( F \) to the symplectic decomposition algorithm in [36] (also see [42, Section II]), yielding the following circuit (\( \text{CKT}_3 \)).

\textbf{REFERENCES}

[1] T. Can, N. Rengaswamy, R. Calderbank, and H. D. Pfister, “Kerdock codes determine unitary 2-designs,” in Proc. IEEE Int. Symp. Inform. Theory, pp. 2908–2912, 2019.

[2] S. Bravyi, D. Gosset, and R. König, “Quantum advantage with shallow circuits,” Science, vol. 362, no. 6412, pp. 308–311, 2018.

[3] E. Conover, “Quantum computers are about to get real,” Science News, vol. 191, no. 13, p. 28, 2017. https://www.sciencenews.org/article/quantum-computers-are-about-get-real.

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

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

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

A. Calderbank, P. Cameron, W. Kantor, and J. Seidel, “Z4-Kerdock Codes, Orthogonal Spreads, and Extremal Euclidean Line-Sets,” Proc. London Math. Soc., vol. 75, pp. 436–480, Sep 1997.

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.

T. Can, “The Heisenberg-Weyl group, finite symplectic geometry, and their applications,” Senior Thesis, Duke University, May 2018.

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.

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.

R. Koenig and J. A. Smolin, “How to efficiently select an arbitrary Clifford group element,” J. Math. Phys., vol. 55, p. 122202, Dec 2014.

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

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.

N. Rengaswamy, R. Calderbank, S. Kadhe, and H. D. Pfister, “Synthesis of Logical Clifford Operators via Symplectic Geometry,” in Proc. IEEE Int. Symp. Inform. Theory, pp. 791–795, Jun 2018.

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

A. W. Nordstrom and J. P. Robinson, “An optimum nonlinear code,” Inform. and Control, vol. 11, no. 5-6, pp. 613–616, 1967.

A. Kendock, “A class of low-rate nonlinear binary codes,” Inform. and Control, vol. 20, pp. 182–187, Mar 1972.

F. P. Preparata, “A class of optimum nonlinear double-error-correcting codes,” Inform. and Control, vol. 13, no. 13, pp. 378–400, 1968.

J. Goethals, “Two dual families of nonlinear binary codes,” Electronic Letters, vol. 10, no. 23, p. 471, 1974.

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

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.

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

A. Thompson and R. Calderbank, “Sparse near-equiquantal tight frames with an implementation in full duplex wireless communication,” in IEEE Glob. Conf. Signal Inf. Process., pp. 868–872, Nov 2017.

J. Helsen, J. J. Wallman, S. T. Flammia, and S. Wehner, “Multiquit randomized benchmarking using few samples,” Phys. Rev. A, vol. 100, no. 5, p. 052304, 2019.

D. Gottesman, “An Introduction to Quantum Error Correction and Fault-Tolerant Quantum Computation,” arXiv preprint arXiv:0904.2577 [quant-ph], 2009.

M. M. Wilde, Quantum Information Theory. Cambridge University Press, 2013.

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

M. A. De Groos, Symplectic Geometry and Quantum Mechanics, vol. 166. Springer Science & Business Media, 2006.

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.

R. Calderbank, S. Howard, S. Jafarpour, and J. Kent, “Sparse approximation and compressed sensing using the Reed-Muller sieve,” Tech. Rep. TR-888-10, Department of Computer Science, Princeton University, 2010.

R. J. McEliece, Finite Fields for Computer Scientists and Engineers. Kluwer Academic Publishers, 1987.

A. Calderbank, R. Hardin, E. Rains, P. Shor, and N. Sloane, “A Group-Theoretic Framework for the Construction of Packings in Grassmannian Spaces,” J. Algebra Comb. Inform., vol. 9, no. 2, pp. 129–140, 1999.

J. H. Cameron and J. H. VanLint, Designs, Graphs, Codes and their Links, vol. 3. Cambridge University Press, 1991.

J. Watrous, The Theory of Quantum Information. Cambridge University Press, 2018.
Appendix A

Proof of Lemma 22

We proceed as in the proof of Lemma 22 to derive the general form of an element in \( \mathcal{E}_{k,m} \). Introducing the new generators \( I_{R^{-i}} \), and using identities from Lemma 23 we calculate

\[
\left[ R^{-i} A_x^{-2} \right] = \left[ \begin{array}{cc} 0 & W^{-1} \\ (R)^T \end{array} \right] A_x^{-2} W
\]

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

\[
w + (y) z^{-2} x^{-2} = a + \left( z + \left( \frac{d}{c} \right)^2 \right)^2 - \frac{1}{c^2}
\]

Hence we have proved that \( F \) performs the permutation

\[
\left[ I_m \mid A_x^2 W \right] \mapsto \left[ I_m \mid A_x^{2(2i)} W \right], \quad z' \triangleq z^{2i}
\]

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 22. We now substitute these back in \( F \) and observe the following simplifications.

\[
(A_y^{-1} R)^{-1} A_x^2 = R^{-i} A_y^{-1} A_x^2 = R^{-i} A_y^{-1} A_x^2 = R^{-i} A_y^{-1} A_x^2
\]

\[
W^{-1} R^{-i} A_x^2 = W^{-1} R^{-i} A_x^2 = (R)^T W^{-1} A_x^2
\]

These imply that the general form of an element in \( \mathcal{E}_{k,m} \) is

\[
F = \left[ I_m \mid A_x^2 W \right] \mapsto \left[ I_m \mid A_x^{2(2i)} W \right]
\]

Applying this back we get

\[
\left[ I_m \mid A_x^2 W \right] = \left[ I_m \mid A_x^{-2} W \right] \mapsto \left[ I_m \mid A_x^{2(2i)} W \right]
\]

References

[64] Z. Puchala 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.

[65] R. Chao and B. W. Reichardt, “Fault-tolerant quantum computation with few qubits,” npj Quantum Inf., vol. 4, no. 1, p. 42, 2018.
Robert Calderbank (M’89–SM’97–F’98) received the B.S. degree in 1975 from Warwick University, England, the M.S. degree in 1976 from Oxford University, England, and the Ph.D. degree in 1980 from the California Institute of Technology, all in Mathematics. Dr. Calderbank is Professor of Electrical and Computer Engineering at Duke University where he directs the Rhodes Information Initiative at Duke (iiD). Prior to joining Duke in 2010, Dr. Calderbank was Professor of Electrical Engineering and Mathematics at Princeton University. Prior to joining Princeton in 2004, he was Vice President for Research at AT&T, responsible for directing the first industrial research lab in the world where the primary focus is data at scale. At the start of his career at Bell Labs, innovations by Dr. Calderbank were incorporated in a progression of voiceband modem standards that moved communications practice close to the Shannon limit. Together with Peter Shor and colleagues at AT&T Labs he developed the mathematical framework for quantum error correction. He is a co-inventor of space-time codes for wireless communication, where correlation of signals across different transmit antennas is the key to reliable transmission.

Dr. Calderbank served as Editor in Chief of the IEEE TRANSACTIONS ON INFORMATION THEORY from 1995 to 1998, and as Associate Editor for Coding Techniques from 1986 to 1989. He was a member of the Board of Governors of the IEEE Information Theory Society from 1991 to 1996 and from 2006 to 2008. Dr. Calderbank was honored by the IEEE Information Theory Prize Paper Award in 1995 for his work on the Z4 linearity of Kerdock and Preparata Codes (joint with A.R. Hammons Jr., P.V. Kumar, N.J.A. Sloane, and P. Sole), and again in 1999 for the invention of space-time codes (joint with V. Tarokh and N. Seshadri). He has received the 2006 IEEE Donald G. Fink Prize Paper Award, the IEEE Millennium Medal, the 2013 IEEE Richard W. Hamming Medal, and the 2015 Shannon Award. He was elected to the US National Academy of Engineering in 2005.

Narayanan Rengaswamy received his Ph.D. in Electrical Engineering from Duke University, USA, in May 2020 where he was supervised by Prof. Henry Pfister and Prof. Robert Calderbank. He is currently a research associate at Duke University continuing to work with his Ph.D. supervisors. His primary training is in classical information and coding theory, and compressed sensing. During his Ph.D. he actively learned about quantum computing and quantum error correction and this is now his primary area of research. Prior to this, he received his Master of Science (M.S.) degree, also in Electrical Engineering, from Texas A&M University, USA, in December 2015. Earlier he obtained his Bachelor of Technology (B. Tech.) degree in Electronics and Communication Engineering from Amrita University, Coimbatore, India in May 2013, where he ranked first in the college and third in the university.

He has studied the problem of realizing logical operations on quantum error correcting codes in a fault-tolerant manner and produced new insights via a perspective rooted in classical coding theory. His paper on developing conditions for a general stabilizer code to support transversal T gates was one among the 73 out of 283 submissions that were accepted as talks to the esteemed 2020 Quantum Information Processing (QIP) conference. His recent work on Joseph Renes’ belief propagation algorithm that passes quantum messages provides a potential near-term application with a quantum advantage for a special-purpose all-photic quantum processor. In general, he is excited about problems in the intersection of classical and quantum information processing and mathematical tools that help address problems of this sort. He has been a reviewer for IEEE Transactions on Information Theory, IEEE Transactions on Vehicular Technology, Quantum, Quantum Science and Technology, and Proceedings of the Royal Society A, besides the conferences IEEE International Symposium on Information Theory (2018, 2020) and IEEE Information Theory Workshop (2018). He also helped organize the 2016 North American School of Information Theory at Duke University.

Trung Can, a native of Ho Chi Minh City, Vietnam, received a B.A. in Math from Duke University in 2018 and is currently a Ph.D. student at the California Institute of Technology.

In high school, he received a Gold medal at the International Mathematical Olympiad, representing his home country, Vietnam. At Duke, he served as the vice-president of the Math Union. His undergraduate thesis on the applications of the Heisenberg-Weyl group and finite symplectic geometry received the highest distinction from the math department. He founded and currently serves as the president of PiMA, a nonprofit organization that organizes summer camps and seminars on math topics for high school students in Vietnam.

His current research interests are algebraic geometry and number theory; in particular, the Schottky problem and Shimura varieties.

Henry Pfister received his Ph.D. in Electrical Engineering in 2003 from the University of California, San Diego and is currently a professor in the Electrical and Computer Engineering Department of Duke University with a secondary appointment in Mathematics. Prior to that, he was an associate professor at Texas A&M University (2006-2014), a post-doctoral fellow at the École Polytechnique Fédérale de Lausanne (2005-2006), and a senior engineer at Qualcomm Corporate R&D in San Diego (2003-2004). His current research interests include information theory, error-correcting codes, quantum computing, and machine learning.

He received the NSF Career Award in 2008 and a Texas A&M ECE Department Outstanding Professor Award in 2010. He is a coauthor of the 2007 IEEE COMSOC best paper in Signal Processing and Coding for Data Storage and a coauthor of a 2016 Symposium on the Theory of Computing (STOC) best paper. He has served the IEEE Information Theory Society as a member of the Board of Governors (2019-2022), an Associate Editor for the IEEE Transactions on Information Theory (2013-2016), and a Distinguished Lecturer (2015-2016). He was also the General Chair of the 2016 North American School of Information Theory.

Rhoades Information Initiative at Duke University.