Un-Weyl-ing the Clifford Hierarchy

Tefjol Pllaha[1], Narayanan Rengaswamy[2], Olav Tirkkonen[1], and Robert Calderbank[3]

[1]Department of Communications and Networking, Aalto University, Finland
[2]Department of Electrical and Computer Engineering, University of Arizona, Tucson, AZ, USA
[3]Department of Electrical and Computer Engineering, Duke University, NC, USA

The teleportation model of quantum computation introduced by Gottesman and Chuang (1999) motivated the development of the Clifford hierarchy. Despite its intrinsic value for quantum computing, the widespread use of magic state distillation, which is closely related to this model, emphasizes the importance of comprehending the hierarchy. There is currently a limited understanding of the structure of this hierarchy, apart from the case of diagonal unitaries (Cui et al., 2017; Rengaswamy et al. 2019). We explore the structure of the second and third levels of the hierarchy, the first level being the ubiquitous Pauli group, via the Weyl (i.e., Pauli) expansion of unitaries at these levels. In particular, we characterize the support of the standard Clifford operations on the Pauli group. Since conjugation of a Pauli by a third level unitary produces traceless Hermitian Cliffords, we characterize their Pauli support as well. Semi-Clifford unitaries are known to have ancilla savings in the teleportation model, and we explore their Pauli support via symplectic transvections. Finally, we show that, up to multiplication by a Clifford, every third level unitary commutes with at least one Pauli matrix. This can be used inductively to show that, up to a multiplication by a Clifford, every third level unitary is supported on a maximal commutative subgroup of the Pauli group. Additionally, it can be easily seen that the latter implies the generalized semi-Clifford conjecture, proven by Beigi and Shor (2010). We discuss potential applications in quantum error correction and the design of flag gadgets.

1 Introduction

Quantum computing provides a fundamentally new approach to computation by exploiting the laws of quantum mechanics that govern our universe. In this computational model, a quantum circuit consists of a sequence of operations each of which is either a *quantum gate*, characterized by a unitary matrix, or a *quantum measurement*, characterized by a Hermitian matrix (i.e., an *observable*) [23]. So, a *universal* quantum computer must be capable of implementing *arbitrary* unitary operations and measuring any Hermitian operator on a given set of m qubits. In 1999, Gottesman and Chuang demonstrated that such universal quantum computing can be performed just by using the quantum teleportation protocol if one has access to certain standard resources — Bell-state preparation, Bell-basis measurements, and arbitrary single-qubit rotations [17]. They defined the *Clifford hierarchy* as part of their proof, and this has proven to be a useful characterization of a large set of unitary operations, both in theory and practice. In fact, in their teleportation model of computation, the level of a unitary in the hierarchy can be interpreted as a measure of complexity of implementing it. Furthermore, this model is closely related to the currently widespread scheme of distilling "magic" states and injecting them via teleportation-like methods in order to fault-tolerantly execute unitary operations on qubits encoded in a quantum error-correcting code [3, 4]. Hence, it is very important to understand the structure of this hierarchy since it has important implications for fault-tolerant quantum computing.

The first level of the hierarchy is the *Pauli* (or *Heisenberg-Weyl*) group and the second level is the *Clifford* group, which is defined as the *normalizer* of the Pauli group in the unitary group. Subsequent levels $\mathcal{C}^{(k)}$ of the hierarchy, for $k \geq 2$, are defined recursively as those unitaries that map Pauli matrices to $\mathcal{C}^{(k-1)}$ under conjugation [17] (see (23) for the precise definition). While the first two levels form groups, it is known that the higher levels are only finite sets of unitary matrices (up to overall phases) and that even when $k \to \infty$, the hierarchy does not encompass all unitary matrices (see Example 2). Furthermore, each level is closed under left or right multiplication by Cliffords [35].

It is well-known that the Pauli matrices form an orthonormal basis for all square matrices under the Hilbert-Schmidt inner product [16]. Therefore, a natural question to consider is to determine the Pauli

Tefjol Pllaha: tefjol.pllaha@aalto.fi
Narayanan Rengaswamy: narayananr@arizona.edu, Most of this work was conducted when N.R. was with the Department of Electrical and Computer Engineering, Duke University, NC, USA
Olav Tirkkonen: olav.tirkkonen@aalto.fi
Robert Calderbank: robert.calderbank@duke.edu

(i.e., Weyl) expansion of all unitaries in the Clifford hierarchy. It is reasonable to expect that the Pauli expansion of elements at a level provides insight into the structure of the hierarchy. Indeed, a subset of the current authors recently identified a special set of diagonal unitary matrices in the hierarchy, called *Quadratic Form Diagonal (QFD)* gates, and produced formulae for their action on Pauli matrices [28]. In subsequent work, they considered QFD gates constructed as tensor products of integer powers of the "$\mathbf{T}$" gate, $\mathbf{T} := \mathrm{diag}\left(1, \exp\left(\frac{i\pi}{4}\right)\right)$. There they examined the result of conjugating Pauli matrices by such gates, and fully characterized the Pauli expansion of the (Clifford) result. Then they used this characterization to understand when such a physical operation preserves the code subspace of a *stabilizer* quantum error-correcting code [27, 29]. This is fundamental because such codes are necessary to make the quantum computer tolerate noise, and all operations on the encoded information have to be performed by such codespace-preserving physical fault-tolerant operations. Furthermore, for universal quantum computation we need to implement at least one non-Clifford gate, and the $\mathbf{T}$ gate is one of the easiest non-Clifford gates to engineer. As a general recipe, one could replace this (tensor product) gate with any high fidelity lab operation and attempt to repeat this process to understand required code structure.

The Heisenberg-Weyl expansion considered in this paper is intimately connected with the Wigner functions [32] via the Fourier transform. The discrete counterparts are explored in [15, 18, 33]. These insights have played an important role in the simulation and general understanding of magic states, as well as with non-stabilizer resources [31].

In this paper, we make contributions towards a few related questions about the hierarchy. First, surprisingly, the Pauli support (i.e., the Pauli matrices with non-zero coefficients in the Pauli expansion) of even the well-known Clifford group operations remains unknown. (Note that conjugating a Pauli matrix by the transversal $\mathbf{T}$ gate produces a Clifford gate, so the aforementioned result already calculates the Pauli expansion of certain types of Cliffords.) Hence, we study the support of the "standard" Clifford operations that correspond to the standard Clifford gate-set consisting of Hadamard, Phase, Controlled-NOT (CNOT), and Controlled-Z (CZ) gates.

Second, Zeng et al. [35] considered certain operations called *semi-Clifford* unitaries in the hierarchy [19], which have the advantage that they require fewer ancillae than general unitaries in the teleportation model of Gottesman and Chuang [36]. They also showed that any semi-Clifford $\mathbf{U}$ can be expressed as $\mathbf{U} = \mathbf{G}_1\mathbf{D}\mathbf{G}_2$, where $\mathbf{D}$ is diagonal and $\mathbf{G}_1, \mathbf{G}_2$ are Clifford operators. Cui et al. [14] have recently characterized the diagonal unitaries in the Clifford hierarchy. We prove a general result that provides an exact decomposition of any semi-Clifford operation in terms of diagonal gates and physical permutation operators composed of CNOTs and Pauli X's. Thus, when combined with [14] and our contribution of characterizing the Pauli support of standard Cliffords, this essentially produces the Weyl expansion of semi-Cliffords.

Third, Zeng et al. conjectured in the above paper that all unitaries in $\mathcal{C}^{(3)}$ are semi-Clifford and all unitaries in $\mathcal{C}^{(k)}$ are *generalized* semi-Clifford for any k. While a semi-Clifford operation maps, by conjugation, a maximal commutative subgroup (MCS) of the Pauli group to another MCS of the Paulis, a generalized semi-Clifford operation maps the *span* (i.e., complex linear combination) of a MCS to the span of another MCS. It is well-known that for $m = 1, 2$ qubits all unitaries are semi-Clifford, and for $m = 3$ qubits the third level is semi-Clifford, so these conjectures are for $k = 3$ for all $m > 3$ and for $k \geq 4$ for all $m \geq 3$, respectively. Gottesman and Mochon have provided a counterexample for $\mathcal{C}^{(3)}$ that disproves the semi-Clifford conjecture [34][1]. Subsequently, Beigi and Shor [1] proved that all unitaries in $\mathcal{C}^{(3)}$ are generalized semi-Clifford operations, thereby settling the conjecture for $k = 3$. In this paper, we prove the stronger result that for any unitary $\mathbf{C}$ from $\mathcal{C}^{(3)}$, there exists a Clifford $\mathbf{G}$ such that $\mathbf{GC}$ is supported on a MCS of the Pauli group. Our proof uses a much simpler induction argument based on the fact that any third level unitary must map (under conjugation) at least one Pauli to some other Pauli.

Finally, the third level of the hierarchy is of particular interest since any third level gate enables universal quantum computation when combined with the Clifford group [2, 17]. When a $\mathcal{C}^{(3)}$ gate acts by conjugation on a Pauli matrix, the result is a Hermitian Clifford, one example being the aforementioned case of choosing a $\mathcal{C}^{(3)}$ operation that is a tensor product of integer powers of $\mathbf{T}$. It is well-known that Clifford transvections (that is, square roots of Hermitian Pauli matrices; see (28)) form a different generating set for all Cliffords, compared to the standard Clifford gate set mentioned earlier [9, 20, 24]. We prove a necessary and sufficient condition for the Paulis involved in the transvection decomposition of an arbitrary Hermitian Clifford operator. Since expanding the product of transvections provides the Pauli expansion of these Hermitian Cliffords, this can potentially be applied to extend the aforementioned result on characterizing stabilizer codes that support transversal $\mathbf{T}$ gates to other gates from $\mathcal{C}^{(3)}$.

As a different application, *flag gadgets* have recently become popular as a near-term method to detect correlated faults in circuits [10–13, 30]. The idea is to introduce a multi-qubit Pauli measurement before and after the circuit, using one or more ancilla qubits, such that the extra gadget acts trivially in the case of no

[1] The authors of [28] were unaware of this result, and they regret reporting that this conjecture remained open.

errors but catches catastrophic errors otherwise. A key requirement to construct flag gadgets for a specific application circuit is to determine the best Pauli measurement to apply before the circuit and identify the result of "propagating" the Pauli through the circuit, i.e., determine the result of conjugating the Pauli by the circuit. The simplest case is to use a Pauli operator that commutes with the circuit. For this purpose, any Pauli in the centralizer/dual of the support (of the circuit/unitary) would suffice. Hence, our aforesaid results on characterizing Pauli supports can be applied to determine the Paulis that commute with the corresponding circuit. In particular, since flag gadgets are generally applied only to Clifford circuits, our result that any $\mathcal{C}^{(3)}$ element is supported on a MCS of the Paulis, up to multiplication by a Clifford, provides a way to determine a Pauli that commutes with a non-Clifford element. Therefore, this insight could be used to design flag gadgets beyond Clifford (subsections of) circuits.

2 Preliminaries

2.1 The Binary Symplectic Group

We will denote by $\mathrm{GL}(n)$ and $\mathrm{Sym}(n)$ the groups of $n \times n$ invertible and symmetric matrices over the binary field $\mathbb{F}_2$, respectively. Addition in $\mathbb{F}_2$ will be denoted by $\oplus$. The *binary symplectic group* $\mathrm{Sp}(2m) \subset \mathrm{GL}(2m)$ is the set of $2m \times 2m$ binary matrices that preserve the *symplectic inner product* in $\mathbb{F}_2^{2m}$:

$$\langle\, (\mathbf{a},\mathbf{b}) \,|\, (\mathbf{c},\mathbf{d}) \,\rangle_{\mathrm{s}} = \mathbf{a}\mathbf{d}^{\mathrm{t}} \oplus \mathbf{b}\mathbf{c}^{\mathrm{t}} = (\mathbf{a},\mathbf{b})\Omega(\mathbf{c},\mathbf{d})^{\mathrm{t}}, \quad (1)$$

where

$$\Omega = \begin{bmatrix} \mathbf{0}_m & \mathbf{I}_m \\ \mathbf{I}_m & \mathbf{0}_m \end{bmatrix}, \quad (2)$$

A matrix $\mathbf{F} = \begin{bmatrix} \mathbf{A} & \mathbf{B} \\ \mathbf{C} & \mathbf{D} \end{bmatrix} \in \mathrm{Sp}(2m)$ satisfies $\mathbf{F}\Omega\mathbf{F}^{\mathrm{t}} = \Omega$, which in turn is equivalent with $\mathbf{A}\mathbf{B}^{\mathrm{t}}, \mathbf{C}\mathbf{D}^{\mathrm{t}} \in \mathrm{Sym}(m)$ and $\mathbf{A}\mathbf{D}^{\mathrm{t}} \oplus \mathbf{B}\mathbf{C}^{\mathrm{t}} = \mathbf{I}_m$.

In $\mathrm{Sp}(2m)$ we distinguish two subgroups:

$$S_D := \left\{ \mathbf{F}_D(\mathbf{P}) = \begin{bmatrix} \mathbf{P} & \mathbf{0}_m \\ \mathbf{0}_m & \mathbf{P}^{-\mathrm{t}} \end{bmatrix} \;\middle|\; \mathbf{P} \in \mathrm{GL}(m) \right\} \quad (3)$$
$$\cong \mathrm{GL}(m),$$
$$S_U := \left\{ \mathbf{F}_U(\mathbf{S}) = \begin{bmatrix} \mathbf{I}_m & \mathbf{S} \\ \mathbf{0}_m & \mathbf{I}_m \end{bmatrix} \;\middle|\; \mathbf{S} \in \mathrm{Sym}(m) \right\} \quad (4)$$
$$\cong \mathrm{Sym}(m).$$

Then every $\mathbf{F} \in \mathrm{Sp}(2m)$ can be *Bruhat-decomposed* [22, 25] as

$$\mathbf{F} = \mathbf{F}_D(\mathbf{P}_1)\mathbf{F}_U(\mathbf{S}_1)\mathbf{F}_\Omega(r)\mathbf{F}_U(\mathbf{S}_2)\mathbf{F}_D(\mathbf{P}_2), \quad (5)$$

where

$$\mathbf{F}_\Omega(r) = \begin{bmatrix} \mathbf{I}_{m|-r} & \mathbf{I}_{m|r} \\ \mathbf{I}_{m|r} & \mathbf{I}_{m|-r} \end{bmatrix}, \quad (6)$$

with $\mathbf{I}_{m|r}$ being the block matrix with $\mathbf{I}_r$ in upper left corner and 0 elsewhere, and $\mathbf{I}_{m|-r} = \mathbf{I}_m - \mathbf{I}_{m|r}$. Here $r = \mathrm{rank}\,(\mathbf{C})$. The semidirect product S of S_D and S_U corresponds to $r = 0$, that is, symplectic matrices with $\mathbf{C} = \mathbf{0}$. Let $\widetilde{S}$ be the subgroup of S consisting of matrices $\mathbf{F}_D(\mathbf{P})\mathbf{F}_U(\mathbf{S})$ with $\mathbf{P}$ upper triangular. Then $\widetilde{S}$ has size $2^{m(m-1)/2} \cdot 2^{m(m+1)/2} = 2^{m^2}$ and is a 2-Sylow subgroup of $\mathrm{Sp}(2m)$ that contains S_U.

Another type of decomposition of $\mathrm{Sp}(2m)$ can be achieved via *symplectic transvections* $\mathbf{T}_{\mathbf{v}} := \mathbf{I}_{2m} + \Omega\mathbf{v}^{\mathrm{t}}\mathbf{v}$, $\mathbf{v} \in \mathbb{F}_2^{2m}$. Such matrix acts on $\mathbb{F}_2^{2m}$ as $\mathbf{x} \longmapsto \mathbf{x} + \langle\, \mathbf{v} \,|\, \mathbf{x} \,\rangle_{\mathrm{s}}\mathbf{v}$, and thus $\mathbf{T}_{\mathbf{v}}^2 = \mathbf{I}_{2m}$. In general, $\mathbf{F} \in \mathrm{Sp}(2m)$ is said to be an *involution* if $\mathbf{F}^2 = \mathbf{I}_{2m}$ and is said to be *hyperbolic* if $\langle\, \mathbf{v} \,|\, \mathbf{v}\mathbf{F} \,\rangle_{\mathrm{s}} = 0$ for all $\mathbf{v} \in \mathbb{F}_2^{2m}$. It is well-known that symplectic transvections generate $\mathrm{Sp}(2m)$ [9, 20, 24]. It is shown there that a non-hyperbolic involution can be written as product of r transvections $\mathbf{T}_{\mathbf{v}_1}, \ldots, \mathbf{T}_{\mathbf{v}_r}$, where $r = 2m - \dim(\mathrm{Fix}(\mathbf{F})) = \dim(\mathrm{Res}(\mathbf{F}))$ and

$$\mathrm{Fix}(\mathbf{F}) := \ker(\mathbf{I} \oplus \mathbf{F}) := \{\mathbf{v} \in \mathbb{F}_2^{2m} \mid \mathbf{v} = \mathbf{v}\mathbf{F}\}, \quad (7)$$
$$\mathrm{Res}(\mathbf{F}) := \mathrm{rs}\,(\mathbf{I} \oplus \mathbf{F}) := \{\mathbf{v} \oplus \mathbf{v}\mathbf{F} \mid \mathbf{v} \in \mathbb{F}_2^{2m}\}. \quad (8)$$

Throughout the paper $\mathrm{rs}\,(\bullet)$ will denote the row space of a matrix. Note here that, by definition, $\mathrm{Fix}(\mathbf{F})$ and $\mathrm{Res}(\mathbf{F})$ are dual of each other. The vectors $\mathbf{v}_1, \ldots, \mathbf{v}_r \in \mathrm{Res}(\mathbf{F})$ must be independent, in which case we say that corresponding transvections are independent. On the other hand, a hyperbolic involution can be written as a product of $r+1$ transvections (r as above), r of which are independent and the additional one is dependent of the others. We will see that the *residue* space $\mathrm{Res}(\mathbf{F})$ of a symplectic $\mathbf{F}$ is intimately connected with the support (33) of the corresponding Clifford $\mathbf{G}$. On the other hand, the *fixed* space $\mathrm{Fix}(\mathbf{F})$ being the dual of $\mathrm{Res}(\mathbf{F})$ is intimately connected with the Paulis that commute with $\mathbf{G}$. Transvections are the simplest form of involutions in $\mathrm{Sp}(2m)$ and will play a central role throughout the paper for the simple reason that they correspond to square roots of Hermitian Paulis; see (28) and (29).

2.2 Quantum Computation

Fix $N = 2^m$. The standard basis vectors of $\mathbb{C}^N$ will be indexed by binary vectors and denoted as kets, that is, $\mathbf{e}_{\mathbf{v}} = |\mathbf{v}\rangle, \mathbf{v} \in \mathbb{F}_2^m$, will have 1 in the position indexed by $\mathbf{v}$ and 0 else. The *Heisenberg-Weyl* group is defined as

$$\mathcal{HW}_N := \{i^k\mathbf{D}(\mathbf{a},\mathbf{b}) \mid \mathbf{a},\mathbf{b} \in \mathbb{F}_2^m, k \in \mathbb{Z}_4\} \subset \mathbb{U}(N), \quad (9)$$

where

$$\mathbf{D}(\mathbf{a},\mathbf{b}) : |\mathbf{v}\rangle \longrightarrow (-1)^{\mathbf{b}\mathbf{v}^{\mathrm{t}}}|\mathbf{v} \oplus \mathbf{a}\rangle. \quad (10)$$

We will denote by $\mathcal{PHW}_N := \mathcal{HW}_N/\{\pm\mathbf{I}_N, \pm i\mathbf{I}_N\}$ the *projective* Heisenberg-Weyl group. Directly by definition, we have

$$\mathbf{D}(\mathbf{a},\mathbf{b})\mathbf{D}(\mathbf{c},\mathbf{d}) = (-1)^{\mathbf{b}\mathbf{c}^{\mathrm{t}}}\mathbf{D}(\mathbf{a} \oplus \mathbf{c}, \mathbf{b} \oplus \mathbf{d}). \quad (11)$$

We will also define $\mathbf{E}(\mathbf{a},\mathbf{b}) := i^{\mathbf{a}\mathbf{b}^{\mathrm{t}}}\mathbf{D}(\mathbf{a},\mathbf{b})$, which constitute the Hermitian matrices in $\mathcal{HW}_N$. If follows by (11) that such matrices satisfy

$$\mathbf{E}(\mathbf{a},\mathbf{b})\mathbf{E}(\mathbf{c},\mathbf{d}) = i^{\mathbf{b}\mathbf{c}^{\mathrm{t}}-\mathbf{a}\mathbf{d}^{\mathrm{t}}}\mathbf{E}(\mathbf{a}+\mathbf{c},\mathbf{b}+\mathbf{d}), \tag{12}$$

where we view all binary vectors as integer vectors and operations are done modulo 4; see [28, Rem. 1] for the meaning of $\mathbf{E}(\mathbf{a},\mathbf{b})$ with $(\mathbf{a},\mathbf{b}) \in \mathbb{Z}_4^{2m}$. If the arithmetic of the arguments of operators $\mathbf{E}(\mathbf{a},\mathbf{b})$ were to be done modulo 2 one would have

$$\begin{aligned}
&\mathbf{E}(\mathbf{a},\mathbf{b})\mathbf{E}(\mathbf{c},\mathbf{d}) \\
&= (-1)^{\langle\,(\mathbf{a},\mathbf{b})\,|\,(\mathbf{c},\mathbf{d})\,\rangle_{\mathrm{s}}}\mathbf{E}(\mathbf{c},\mathbf{d})\mathbf{E}(\mathbf{a},\mathbf{b}) && (13)\\
&= i^{\mathbf{b}\mathbf{c}^{\mathrm{t}}-\mathbf{a}\mathbf{d}^{\mathrm{t}}}\mathbf{E}(\mathbf{a}+\mathbf{c},\mathbf{b}+\mathbf{d}) && (14)\\
&= i^{\mathbf{b}\mathbf{c}^{\mathrm{t}}-\mathbf{a}\mathbf{d}^{\mathrm{t}}}\mathbf{E}(\mathbf{a}+\mathbf{c},(\mathbf{b}\oplus\mathbf{d})+2(\mathbf{b}*\mathbf{d})) && (15)\\
&= i^{\mathbf{b}\mathbf{c}^{\mathrm{t}}-\mathbf{a}\mathbf{d}^{\mathrm{t}}}(-1)^{(\mathbf{a}+\mathbf{c})(\mathbf{b}*\mathbf{d})^{\mathrm{t}}}\mathbf{E}((\mathbf{a}\oplus\mathbf{c})+2(\mathbf{a}*\mathbf{c}),\mathbf{b}\oplus\mathbf{d}) && (16)\\
&= i^{\mathbf{b}\mathbf{c}^{\mathrm{t}}-\mathbf{a}\mathbf{d}^{\mathrm{t}}}(-1)^{(\mathbf{a}\oplus\mathbf{c})(\mathbf{b}*\mathbf{d})^{\mathrm{t}}+(\mathbf{b}\oplus\mathbf{d})(\mathbf{a}*\mathbf{c})^{\mathrm{t}}}\mathbf{E}(\mathbf{a}\oplus\mathbf{c},\mathbf{b}\oplus\mathbf{d}). && (17)
\end{aligned}$$

Above, the asterisk stands for the coordinate-wise product. We see that binary arithmetic only ever introduces an additional sign. Thus when the sign is not relevant (e.g., (25)) we will stick to binary arithmetic.

Remark 1. From (11) we have that $\mathbf{D}(\mathbf{a},\mathbf{b})$ and $\mathbf{D}(\mathbf{c},\mathbf{d})$ commute iff $\langle\,(\mathbf{a},\mathbf{b})\,|\,(\mathbf{c},\mathbf{d})\,\rangle_{\mathrm{s}} = 0$, and otherwise they anticommute. Similarly, (12) implies $\mathbf{E}(\mathbf{a},\mathbf{b})\mathbf{E}(\mathbf{c},\mathbf{d}) = \pm\mathbf{E}(\mathbf{a}+\mathbf{c},\mathbf{b}+\mathbf{d})$ if $\langle\,(\mathbf{a},\mathbf{b})\,|\,(\mathbf{c},\mathbf{d})\,\rangle_{\mathrm{s}} = 0$ and $\mathbf{E}(\mathbf{a},\mathbf{b})\mathbf{E}(\mathbf{c},\mathbf{d}) = \pm i\mathbf{E}(\mathbf{a}+\mathbf{c},\mathbf{b}+\mathbf{d})$ otherwise.

A *stabilizer* is a commutative subgroup of $\mathcal{HW}_N$ generated by Hermitian matrices of form $\pm\mathbf{E}(\mathbf{a},\mathbf{b})$ that does not contain $-\mathbf{I}_N$. Thus either $\mathbf{E}$ or $-\mathbf{E}$ belong to a stabilizer, but not both. We will write $S = \mathbf{E}(\mathbf{A},\mathbf{B})$ if the stabilizer S is generated by $\mathbf{E}(\mathbf{a}_1,\mathbf{b}_1),\dots\mathbf{E}(\mathbf{a}_k,\mathbf{b}_k)$, where $\mathbf{A}$ and $\mathbf{B}$ are $k\times m$ matrices obtained by stacking $\mathbf{a}_i$'s and $\mathbf{b}_i$'s. Since S is abelian, the matrix $\mathbf{C} = (\mathbf{A}\ \mathbf{B})$ satisfies $\mathbf{C}\Omega\mathbf{C}^{\mathrm{t}} = \mathbf{0}$, and thus the row space of $\mathbf{C}$ is a self-orthogonal (isotropic) subspace of $\mathbb{F}_2^{2m}$, with respect to the symplectic inner product. A *maximal stabilizer*, or a *maximal commutative subgroup* (MCS) is a stabilizer of size 2^m. Of particular interest are MCSs

$$X_N = \mathbf{E}(\mathbf{I}_m,\mathbf{0}_m) = \{\mathbf{E}(\mathbf{a},\mathbf{0}) \mid \mathbf{a}\in\mathbb{F}_2^m\}, \tag{18}$$
$$Z_N = \mathbf{E}(\mathbf{0}_m,\mathbf{I}_m) = \{\mathbf{E}(\mathbf{0},\mathbf{b}) \mid \mathbf{b}\in\mathbb{F}_2^m\}. \tag{19}$$

We will refer to their elements as X *stabilizers* and Z *stabilizers*, respectively. Naturally, we identify X stabilizers with vectors $(\mathbf{a},\mathbf{0})\in\mathbb{F}_2^{2m}$ and Z stabilizers with vectors $(\mathbf{0},\mathbf{b})\in\mathbb{F}_2^{2m}$.

Let S be a stabilizer group of size 2^k. For $\varepsilon\in\{1,-1\}$, the complex vector space

$$\mathcal{F}_\varepsilon(S) := \{v\in\mathbb{C}^N \mid \mathbf{E}v = \varepsilon v \text{ for all } \mathbf{E}\in S\} \tag{20}$$

has dimension 2^{m-k}. In literature, $\mathcal{F}_+(S)$ is known as the $[\![m, m-k]\!]$ *stabilizer code associated to* S [23], which encodes $m-k$ *logical* qubits to m *physical* qubits. It follows that a MCS S defines a $[\![m,0]\!]$ stabilizer code, that is, $\dim(\mathcal{F}_\varepsilon(S)) = 1$. For this reason $|\psi_\varepsilon\rangle := \mathcal{F}_\varepsilon(S)$ is called a *stabilizer state*. Let $S = \langle\mathbf{E}_1,\dots,\mathbf{E}_k\rangle$ be the stabilizer group generated by the commuting Hermitian Paulis $\{\mathbf{E}_1,\dots,\mathbf{E}_k\}$. For $\mathbf{d}\in\mathbb{F}_2^k$, we will denote $S_{\mathbf{d}} := \langle(-1)^{d_1}\mathbf{E}_1,\dots,(-1)^{d_k}\mathbf{E}_k\rangle$. Then

$$\Pi_{\mathbf{d}} := \prod_{n=1}^{k}\frac{\mathbf{I}_N+(-1)^{d_n}\mathbf{E}_n}{2} = \frac{1}{2^k}\sum_{\mathbf{E}\in S_{\mathbf{d}}}\mathbf{E} \tag{21}$$

is a projection onto $\mathcal{F}_+(S_{\mathbf{d}})$, which in turn gives a *resolution* of the identity [23, Sec. 10.5]:

$$\sum_{\mathbf{d}\in\mathbb{F}_2^k}\Pi_{\mathbf{d}} = \mathbf{I}_N. \tag{22}$$

2.3 The Clifford Hierarchy

The *Clifford hierarchy* $\{\mathcal{C}^{(k)}, k\geq 1\}$ is defined recursively, where the first level is the Heisenberg-Weyl group, and higher levels are defined by

$$\mathcal{C}^{(k)} = \{\mathbf{U}\in\mathbb{U}(N) \mid \mathbf{U}\mathcal{HW}_N\mathbf{U}^\dagger\subset\mathcal{C}^{(k-1)}\}. \tag{23}$$

By definition, the *Clifford group* Cliff_N is the second level of the hierarchy up to overall phases, that is $\mathrm{Cliff}_N := \mathcal{C}^{(2)}/\mathbb{U}(1)$. The following example shows that the Clifford hierarchy does not exhaust $\mathbb{U}(N)$ and also motivates the Weyl expansion.

Example 2. Set $\mathbf{E}_1 = \mathbf{E}(010,010), \mathbf{E}_2 = \mathbf{E}(011,001), \mathbf{E}_3 = \mathbf{E}(001,111), \mathbf{E}_4 = \mathbf{E}(101,011)$. Then $\mathbf{W} = (\mathbf{E}_1+\mathbf{E}_2+\mathbf{E}_3+\mathbf{E}_4)/2$ is easily seen to be outside of Cliff_N. Further, set $\mathbf{E} = \mathbf{E}(100,000)$. We have $\mathbf{W}\mathbf{E}\mathbf{W}^\dagger = \mathbf{E}_3\mathbf{W}\mathbf{E}$ and $(\mathbf{E}_3\mathbf{W}\mathbf{E})\mathbf{E}(\mathbf{E}_3\mathbf{W}\mathbf{E})^\dagger = -\mathbf{E}\mathbf{E}_3\mathbf{W}$. Thus, since multiplication by Paulis (or even Cliffords) preserves the level, iterative conjugation cannot bring $\mathbf{E}$ up to the same level as $\mathbf{W}$.

Let $\{\mathbf{e}_1,\dots,\mathbf{e}_{2m}\}$ be the standard basis of $\mathbb{F}_2^{2m}$, and consider $\mathbf{G}\in\mathrm{Cliff}_N$. Let $\mathbf{c}_i\in\mathbb{F}_2^{2m}$ be such that

$$\mathbf{G}\mathbf{E}(\mathbf{e}_i)\mathbf{G}^\dagger = \pm\mathbf{E}(\mathbf{c}_i). \tag{24}$$

Then the matrix $\mathbf{F}_{\mathbf{G}}$ whose ith row is $\mathbf{c}_i$ is a symplectic matrix such that

$$\mathbf{G}\mathbf{E}(\mathbf{c})\mathbf{G}^\dagger = \pm\mathbf{E}(\mathbf{c}\mathbf{F}_{\mathbf{G}}) \tag{25}$$

for all $\mathbf{c}\in\mathbb{F}_2^{2m}$. We thus have a group homomorphism

$$\Phi : \mathrm{Cliff}_N \longrightarrow \mathrm{Sp}(2m),\ \mathbf{G}\longmapsto\mathbf{F}_{\mathbf{G}}. \tag{26}$$

In addition, Φ is surjective with kernel $\ker\Phi = \mathcal{PHW}_N$ [26], and thus $\mathrm{Cliff}_N/\mathcal{PHW}_N\cong\mathrm{Sp}(2m)$.

Given the decomposition (5), one is naturally interested on preimages of respective symplectic matrices via Φ. Namely, the unitary matrices

$$\begin{aligned}\mathbf{G}_D(\mathbf{P}) &:= |\mathbf{v}\rangle \longmapsto |\mathbf{v}\mathbf{P}\rangle,\\ \mathbf{G}_U(\mathbf{S}) &:= \operatorname{diag}\left(i^{\mathbf{v}\mathbf{S}\mathbf{v}^{\mathrm{t}} \mod 4}\right)_{\mathbf{v}\in\mathbb{F}_2^m},\\ \mathbf{G}_\Omega(r) &:= (\mathbf{H}_2)^{\otimes r}\otimes \mathbf{I}_{2^{m-r}},\end{aligned} \tag{27}$$

where $\mathbf{H}_2$ is the 2×2 Hadamard matrix, correspond to $\mathbf{F}_D(\mathbf{P}), \mathbf{F}_U(\mathbf{S})$, and $\mathbf{F}_\Omega(r)$, respectively [6]. Strictly speaking, a preimage $\Phi^{-1}(\mathbf{F})$ is meant up to $\mathcal{HW}_N$ (and up to a eighth root of unity which we have disregarded throughout [7]).

Remark 3. Since Φ is a homomorphism we have that $\Phi(\mathbf{G}^\dagger) = \mathbf{F}_{\mathbf{G}}^{-1}$. It follows that if $\mathbf{G}\in \mathrm{Cliff}_N$ is Hermitian then $\mathbf{F}_{\mathbf{G}}$ is a symplectic involution. Conversely, if $\mathbf{F}$ is a symplectic involution then $\mathbf{G} = \Phi^{-1}(\mathbf{F})$ satisfies $\mathbf{G}^2 \in \mathcal{HW}_N$.

We will call $\mathbf{G}\in\mathrm{Cliff}_N$ a *Clifford transvection* if $\Phi(\mathbf{G})$ is a symplectic transvection. For $\mathbf{v}\in\mathbb{F}_2^{2m}$ define[2]

$$\mathbf{G}_{\mathbf{v}} := \frac{\mathbf{I}_N \pm i\mathbf{E}(\mathbf{v})}{\sqrt{2}}. \tag{28}$$

For $\mathbf{W}\in\mathcal{HW}_N$ we have

$$\mathbf{G}_{\mathbf{v}}\mathbf{W}\mathbf{G}_{\mathbf{v}}^\dagger = \begin{cases}\mathbf{W}, & \text{if } \mathbf{W}\mathbf{E}(\mathbf{v}) = \mathbf{E}(\mathbf{v})\mathbf{W},\\ \mp i\mathbf{W}\mathbf{E}(\mathbf{v}), & \text{if } \mathbf{W}\mathbf{E}(\mathbf{v}) = -\mathbf{E}(\mathbf{v})\mathbf{W}.\end{cases} \tag{29}$$

It follows that $\Phi(\mathbf{G}_{\mathbf{v}}) = \mathbf{T}_{\mathbf{v}}$, and any Clifford transvection is of this form (up to $\mathcal{HW}_N$).

In addition, we mentioned that $\mathrm{Sp}(2m)$ is generated by transvections, thus $\mathbf{G}\in\mathrm{Cliff}_N$ is a product of Clifford transvections. We have proved the following.

Proposition 4. *Any Clifford matrix $\mathbf{G}\in\mathrm{Cliff}_N$ can be written as*

$$\mathbf{G} = \mathbf{E}_0\prod_{n=1}^{k}\frac{\mathbf{I}_N + i\mathbf{E}_n}{\sqrt{2}} = \frac{\mathbf{E}_0}{\sqrt{|S|}}\sum_{\mathbf{E}\in S}\alpha_{\mathbf{E}}\mathbf{E}, \tag{30}$$

where $\mathbf{E}_0\in\mathcal{HW}_N$, $S = \langle \mathbf{E}_1,\dots,\mathbf{E}_k\rangle$, and $\alpha_{\mathbf{E}}\in\mathbb{C}$.

One of the goals of this paper is to determine the $\alpha_{\mathbf{E}}$'s produced by Clifford matrices. In particular we will see that if $\mathbf{E}_1,\dots,\mathbf{E}_k$ are independent then $\alpha_{\mathbf{E}}\in\{\pm 1,\pm i\}$; see (63)-(64). If $\mathbf{G}$ is Hermitian then $\mathbf{F}_{\mathbf{G}}$ is an involution, and thus $k\in\{r, r+1\}$ where $r = 2m - \dim(\mathrm{Fix}(\mathbf{F}_{\mathbf{G}}))$ with at least r transvections being independent.

[2]Note that $(\mathbf{I}_N + i^\lambda\mathbf{E}(\mathbf{v}))/\sqrt{2}$ is unitary iff $\lambda = 1, 3$, and otherwise it is a projection.

3 Support of the Clifford Group

The set $\mathcal{E}_N = \{\mathbf{E}(\mathbf{c}) \mid \mathbf{c}\in\mathbb{F}_2^{2m}\}$ is an orthonormal basis for the vector space $\mathcal{M}_N(\mathbb{C})$ of $N\times N$ complex matrices with respect to the Hermitian inner product

$$\langle \mathbf{M} \,|\, \mathbf{N}\rangle := \frac{1}{N}\mathrm{Tr}(\mathbf{M}^\dagger\mathbf{N}). \tag{31}$$

Thus any matrix $\mathbf{M}\in\mathcal{M}_N(\mathbb{C})$ is a linear combination

$$\mathbf{M} = \sum_{\mathbf{c}\in\mathbb{F}_2^{2m}}\alpha_{\mathbf{c}}\mathbf{E}(\mathbf{c}), \quad \alpha_{\mathbf{c}} = \langle \mathbf{E}(\mathbf{c}) \,|\, \mathbf{M}\rangle \in\mathbb{C}. \tag{32}$$

We are interested in sums of Pauli matrices that yield Clifford matrices. The *support* of $\mathbf{M}\in\mathcal{M}_N(\mathbb{C})$ as in (32) with respect to $\mathcal{E}_N$ is defined as

$$\begin{aligned}\mathrm{supp}(\mathbf{M}) &:= \{\mathbf{E}(\mathbf{c})\in\mathcal{HW}_N \mid \alpha_{\mathbf{c}}\neq 0\} &(33)\\ &\cong \{\mathbf{c}\in\mathbb{F}_2^{2m} \mid \alpha_{\mathbf{c}}\neq 0\}. &(34)\end{aligned}$$

When dealing with the support, we will conveniently switch between the two equivalent definitions. Thus $\mathbf{E}(\mathbf{c})\in\mathrm{supp}(\mathbf{M})$ iff $\mathrm{Tr}(\mathbf{M}^\dagger\mathbf{E}(\mathbf{c}))\neq 0$. We say in this case that $\mathbf{M}$ is *supported* on $\mathrm{supp}(\mathbf{M})$.

Remark 5. (1) Since $\mathbf{E}(\mathbf{c})$ differs from $\mathbf{D}(\mathbf{c})$ only by a factor i^k we see that $\mathrm{Tr}(\mathbf{M}^\dagger\mathbf{E}(\mathbf{c}))\neq 0$ iff $\mathrm{Tr}(\mathbf{M}^\dagger\mathbf{D}(\mathbf{c}))\neq 0$. Thus, to avoid the additional scaling factor, we will use matrices $\mathbf{D}(\mathbf{c})$ when computing supports/traces.

(2) It follows directly by the definition of support and (11) that the support of $\mathbf{M}\mathbf{D}(\mathbf{x})$ (or $\mathbf{D}(\mathbf{x})\mathbf{M}$) is just the translate $\{\mathbf{x}\} + \mathrm{supp}(\mathbf{M})$ for all $\mathbf{x}\in\mathbb{F}_2^{2m}$.

It is clear that $\mathcal{HW}_N$ is supported on singletons. It follows that a unitary $\mathbf{M}$ is a Clifford matrix iff $\mathbf{M}\mathbf{E}\mathbf{M}^\dagger$ is supported on a singleton for all $\mathbf{E}\in\mathcal{HW}_N$. On the other hand, for $\mathbf{G}\in\mathrm{Cliff}_N$, we have $|\mathrm{supp}(\mathbf{M})| = 2$ iff $\mathbf{G}$ is a Clifford transvection (up to $\mathcal{HW}_N$). In general, we have the following immediate consequence of Proposition 4.

Corollary 6. *Any Clifford matrix $\mathbf{G}$ is supported either on a group S or on a coset $\mathbf{E}_0 S$ depending on whether $\mathbf{G}$ has trace or not.*

Proof. Observe that $\mathbf{E}\in\mathcal{HW}_N$ is traceless unless $\mathbf{E} = \mathbf{I}_N$. Thus, for $\mathbf{G}$ as in (30) we have that $\mathrm{Tr}(\mathbf{G})\neq 0$ iff $\mathbf{E}_0\in S$. It also follows that $\mathrm{supp}(\mathbf{G}) = \mathbf{E}_0 S$. □

Remark 7. One can easily construct non-Clifford matrices supported on a subgroup. For instance, it follows easily from Proposition 13 that $\mathbf{T}^{\otimes m}$ is supported on the subspace $\{\mathbf{0}\}\times\mathbb{F}_2^m$, or alternatively, on the subgroup Z_N of diagonal Paulis. Thus, Corollary 6 does not completely characterize Cliff_N. In fact, for any $\mathbf{G}\in\mathrm{Cliff}_N$, we have

$$\begin{aligned}\mathbf{E}(\mathbf{c})\in\mathrm{supp}(\mathbf{G}) &\iff \mathrm{Tr}\big((\mathbf{G}\mathbf{E}(\mathbf{c})\mathbf{G}^\dagger)\mathbf{G}\big)\neq 0 &(35)\\ &\iff \mathrm{Tr}\big(\mathbf{E}(\mathbf{c}\mathbf{F}_{\mathbf{G}})\mathbf{G}\big)\neq 0 &(36)\\ &\iff \mathbf{E}(\mathbf{c}\mathbf{F}_{\mathbf{G}})\in\mathrm{supp}(\mathbf{G}), &(37)\end{aligned}$$

which implies that the support of $\mathbf{G}$ is an *invariant* subspace of $\mathbf{F}_{\mathbf{G}}$.

By definition, in order to understand $\mathbf{G} \in \mathrm{Cliff}_N$ it is sufficient to understand its action on $\mathcal{HW}_N$, which thanks to (26) can be understood via the action of the corresponding symplectic matrix $\mathbf{F}_{\mathbf{G}}$ on $\mathbb{F}_2^{2m}$. Consider the fixed space $\mathrm{Fix}(\mathbf{F}_{\mathbf{G}})$ from (7). Then $\mathbf{c} \in \mathrm{Fix}(\mathbf{F}_{\mathbf{G}})$ iff

$$\mathbf{GE}(\mathbf{c})\mathbf{G}^\dagger = \pm\mathbf{E}(\mathbf{c}\mathbf{F}_{\mathbf{G}}) = \pm\mathbf{E}(\mathbf{c}), \tag{38}$$

that is, iff $\mathbf{E}(\mathbf{c})$ either commutes or anticommutes with $\mathbf{G}$. Let us now consider the Pauli matrices that commute with $\mathbf{G}$, that is

$$C_{\mathbf{G}} = \{\mathbf{c} \in \mathrm{Fix}(\mathbf{F}_{\mathbf{G}}) \mid \mathbf{GE}(\mathbf{c})\mathbf{G}^\dagger = \mathbf{E}(\mathbf{c})\}. \tag{39}$$

It is then clear that the quotient $\mathrm{Fix}(\mathbf{F}_{\mathbf{G}})/C_{\mathbf{G}}$ captures the Pauli matrices that anticommute with $\mathbf{G}$. We will denote by $(\bullet)^{\perp_{\mathrm{s}}}$ the dual w.r.t. the symplectic inner product (1). With this notation we have the following.

Proposition 8. $\mathrm{supp}(\mathbf{G}) \subseteq C_{\mathbf{G}}^{\perp_{\mathrm{s}}}$.

Proof. We will show the reverse inclusion of the complements. Indeed, let $\mathbf{c} \in \mathbb{F}_2^{2m}$ be such that $\mathbf{c} \notin C_{\mathbf{G}}^{\perp_{\mathrm{s}}}$. Then, there exists $\mathbf{v} \in C_{\mathbf{G}}$ such that $\langle \mathbf{c} \,|\, \mathbf{v} \rangle_{\mathrm{s}} = 1$. It follows that $\mathbf{E}(\mathbf{v})$ commutes with $\mathbf{G}$ and anticommutes with $\mathbf{E}(\mathbf{c})$. Thus

$$\begin{aligned}
\mathrm{Tr}\big(\mathbf{GE}(\mathbf{c})\big) &= \mathrm{Tr}\Big(\mathbf{E}(\mathbf{v})^\dagger\mathbf{E}(\mathbf{v})\mathbf{GE}(\mathbf{c})\Big) && (40)\\
&= \mathrm{Tr}\Big(\mathbf{E}(\mathbf{v})^\dagger\mathbf{GE}(\mathbf{v})\mathbf{E}(\mathbf{c})\Big) && (41)\\
&= -\mathrm{Tr}\Big(\mathbf{E}(\mathbf{v})^\dagger\mathbf{GE}(\mathbf{c})\mathbf{E}(\mathbf{v})\Big) && (42)\\
&= -\mathrm{Tr}\big(\mathbf{GE}(\mathbf{c})\big), && (43)
\end{aligned}$$

which in turn implies $\mathrm{Tr}(\mathbf{GE}(\mathbf{c})) = 0$, and hence $\mathbf{c} \notin \mathrm{supp}(\mathbf{G})$. □

Next, we completely characterize the supports of standard Clifford matrices (27) in terms of the invariants (7)-(8) of the defining symplectic matrices.

Proposition 9. *The support of standard Clifford matrices introduced in (27) satisfies the following:*

(1) $\mathrm{supp}(\mathbf{G}_D(\mathbf{P})) = \mathrm{Res}(\mathbf{P}^{-1}) \times \mathrm{Fix}(\mathbf{P})^\perp = \mathrm{Res}(\mathbf{P}^{-1}) \times \mathrm{Res}(\mathbf{P})$.

(2) Let $\mathbf{S} \in \mathrm{Sym}(m)$ *and* $W = \ker(\mathbf{S}) = \{\mathbf{w} \in \mathbb{F}_2^m \mid \mathbf{wS} = \mathbf{0}\}$. *If* $\mathrm{Tr}(\mathbf{G}_U(\mathbf{S})) \neq 0$ *then* $\mathrm{supp}(\mathbf{G}_U(\mathbf{S})) = \{\mathbf{0}\} \times W^\perp$. *Otherwise* $\mathbf{G}_U(\mathbf{S})$ *is supported on a coset of* $\{\mathbf{0}\} \times W^\perp$. *As a consequence, the support of diagonal Cliffords is completely characterized by the row/column space of the associated symmetric* $\mathbf{S}$.

(3) Let $D_r = \{(\mathbf{x}, \mathbf{0}_{m-r}, \mathbf{x}, \mathbf{0}_{m-r}) \mid \mathbf{x} \in \mathbb{F}_2^r\} \subset \mathbb{F}_2^{2m}$. *Then* $\mathrm{supp}(\mathbf{G}_\Omega(r)) = (\mathbf{1}_r, \mathbf{0}_{2m-r}) \oplus D_r$, *where* $\mathbf{1}_r$ *denotes the all ones vector of size* r. *As a consequence, partial Hadamard matrices* $\mathbf{G}_\Omega(r)$ *are supported on a coset of* $\mathrm{Res}(\mathbf{F}_\Omega(r))$.

Proof. (1) By definition we have $\mathbf{G}_D(\mathbf{P}) = \sum_{\mathbf{v}\in\mathbb{F}_2^m} |\mathbf{vP}\rangle\langle\mathbf{v}|$. Thus, for $\mathbf{G} = \mathbf{G}_D(\mathbf{P})$ we have

$$\begin{aligned}
\mathbf{GD}(\mathbf{a},\mathbf{b}) &= \sum_{\mathbf{v}\in\mathbb{F}_2^m} |\mathbf{vP}\rangle\langle\mathbf{v}| \sum_{\mathbf{w}\in\mathbb{F}_2^m} (-1)^{\mathbf{wb}^{\mathrm{t}}} |\mathbf{w}\oplus\mathbf{a}\rangle\langle\mathbf{w}| && (44)\\
&= \sum_{\mathbf{v}\in\mathbb{F}_2^m} (-1)^{\mathbf{vb}^{\mathrm{t}}} |(\mathbf{v}\oplus\mathbf{a})\mathbf{P}\rangle\langle\mathbf{v}|. && (45)
\end{aligned}$$

For $\mathbf{a} \in \mathbb{F}_2^m$ we will denote $\mathrm{Fix}_{\mathbf{a}}(\mathbf{P}) = \{\mathbf{v} \in \mathbb{F}_2^m \mid \mathbf{v} \oplus \mathbf{vP} = \mathbf{aP}\}$. With this notation we have

$$\mathrm{Tr}\big(\mathbf{GD}(\mathbf{a},\mathbf{b})\big) = \sum_{\mathbf{v}\in\mathrm{Fix}_{\mathbf{a}}(\mathbf{P})} (-1)^{\mathbf{vb}^{\mathrm{t}}}. \tag{46}$$

Since $\mathrm{Fix}(\mathbf{P})$ is a subspace of $\mathbb{F}_2^m$ we have that $\mathbf{D}(\mathbf{0},\mathbf{b}) \in \mathrm{supp}(\mathbf{G})$ iff $\mathbf{b} \in \mathrm{Fix}(\mathbf{P})^\perp$. On the other hand, for $\mathbf{x} \in \mathrm{Fix}_{\mathbf{a}}(\mathbf{P})$ we have $\mathbf{x} \oplus \mathrm{Fix}(\mathbf{P}) = \mathrm{Fix}_{\mathbf{a}}(\mathbf{P})$. Indeed, the forward containment is trivial and equality follows due to equal cardinalities. Thus, if $\mathrm{Fix}_{\mathbf{a}}(\mathbf{P}) \neq \emptyset$, we have that $\mathbf{D}(\mathbf{a},\mathbf{b}) \in \mathrm{supp}(\mathbf{G})$ iff $\mathbf{b} \in \mathrm{Fix}(\mathbf{P})^\perp$. Next, recall the subspace $\mathrm{Res}(\mathbf{P})$ from (8). We have that $\mathrm{Fix}_{\mathbf{a}}(\mathbf{P}) \neq \emptyset$ iff $\mathbf{a} \in \mathrm{Res}(\mathbf{P}^{-1})$. We conclude that $\mathbf{G}_D(\mathbf{P})$ is supported on $\mathrm{Res}(\mathbf{P}^{-1}) \times \mathrm{Fix}(\mathbf{P})^\perp \subset \mathbb{F}_2^{2m}$. Then by definition $\mathrm{Fix}(\mathbf{P})^\perp = \mathrm{Res}(\mathbf{P})$.

(2) Let $\mathbf{G} := \mathbf{G}_U(\mathbf{S})$. Then

$$\mathrm{Tr}\big(\mathbf{GD}(\mathbf{a},\mathbf{b})\big) = \sum_{\mathbf{v}\in\mathbb{F}_2^m} i^{(\mathbf{v}\oplus\mathbf{a})\mathbf{S}(\mathbf{v}\oplus\mathbf{a})^{\mathrm{t}} + 2\mathbf{vb}^{\mathrm{t}}} \langle\mathbf{v}|\mathbf{v}\oplus\mathbf{a}\rangle. \tag{47}$$

It follows that $\mathbf{D}(\mathbf{a},\mathbf{b}) \in \mathrm{supp}(\mathbf{G})$ only if $\mathbf{a} = \mathbf{0}$. So from now on we fix $\mathbf{a} = \mathbf{0}$. It is shown in [8, Appendix A] that the sum in (47) is nonzero iff

$$\sum_{\mathbf{w}\in W} i^{\mathbf{wSw}^{\mathrm{t}} + 2\mathbf{wb}^{\mathrm{t}}} \neq 0. \tag{48}$$

Consider the maps $\chi_{\mathbf{S}} : \mathbf{w} \longmapsto \mathbf{wSw}^{\mathrm{t}}$ and $\chi_{\mathbf{b}} : \mathbf{w} \longmapsto +2\mathbf{wb}^{\mathrm{t}}$, and put $\chi_{\mathbf{S},\mathbf{b}} := \chi_{\mathbf{S}} + \chi_{\mathbf{b}}$. For $\mathbf{v}, \mathbf{w} \in W$ we have

$$\begin{aligned}
\chi_{\mathbf{S},\mathbf{b}}(\mathbf{v}\oplus\mathbf{w}) &= (\mathbf{v}\oplus\mathbf{w})\mathbf{S}(\mathbf{v}\oplus\mathbf{w})^{\mathrm{t}} + 2(\mathbf{v}\oplus\mathbf{w})\mathbf{b}^{\mathrm{t}} && (49)\\
&= (\mathbf{v}+\mathbf{w})\mathbf{S}(\mathbf{v}+\mathbf{w})^{\mathrm{t}} + 2(\mathbf{v}+\mathbf{w})\mathbf{b}^{\mathrm{t}} \bmod 4 && (50)\\
&= \chi_{\mathbf{S},\mathbf{b}}(\mathbf{v}) + \chi_{\mathbf{S},\mathbf{b}}(\mathbf{w}) + 2\mathbf{wSv}^{\mathrm{t}} && (51)\\
&= \chi_{\mathbf{S},\mathbf{b}}(\mathbf{v}) + \chi_{\mathbf{S},\mathbf{b}}(\mathbf{w}) \mod 4, && (52)
\end{aligned}$$

where the last equality follows by the fact that $\mathbf{wS} = \mathbf{0} \bmod 2$. Thus the map $\mathbf{w} \longmapsto i^{\chi_{\mathbf{S},\mathbf{b}}(\mathbf{w})}$ is a character of W. It follows that $\mathbf{D}(\mathbf{0},\mathbf{b}) \in \mathrm{supp}(\mathbf{G})$ iff $\chi_{\mathbf{S},\mathbf{b}}(\mathbf{w}) = 0$ for all $\mathbf{w} \in W$.

By the above argument, it also follows that $\mathrm{Tr}(\mathbf{G}) \neq 0$ iff $\chi_{\mathbf{S}}(\mathbf{w}) = 0$ for all $\mathbf{w} \in W$. In this case, (48) reduces to $\sum_{\mathbf{w}\in W}(-1)^{\mathbf{wb}^{\mathrm{t}}} \neq 0$, which holds iff $\mathbf{b} \in W^\perp$. Similarly, $\mathrm{Tr}(\mathbf{G}) = 0$ iff $\chi_{\mathbf{S}}$ is not the trivial map. Since $\chi_{\mathbf{S}}$ is an even-valued linear map

(mod 4) then there exists $\mathbf{c}$ (depending on $\mathbf{S}$) such that $\chi_{\mathbf{S}}(\mathbf{w}) = 2\mathbf{w}\mathbf{c}^{\mathrm{t}}$. But then it is clear that $\chi_{\mathbf{S},\mathbf{b}}$ is the zero map iff $\mathbf{c} \oplus \mathbf{b} \in W^{\perp}$ iff $\mathbf{b} \in \mathbf{c} \oplus W^{\perp}$. It follows that $\mathrm{supp}(\mathbf{G}) = \{\mathbf{0}\} \times (\mathbf{c} \oplus W^{\perp})$ for any such $\mathbf{c}$ as above.

(3) Consider $\mathbf{G} = \mathbf{G}_{\Omega}(r)$ for $0 \leq r \leq m$, and let us first handle $r = m$, which corresponds to the fully occupied Hadamard matrix in $N = 2^m$ dimensions. In this case, we have

$$\begin{aligned}&\mathbf{GD}(\mathbf{a},\mathbf{b})\\ &= \frac{1}{\sqrt{N}} \sum_{\mathbf{v},\mathbf{w}} (-1)^{\mathbf{v}\mathbf{w}^{\mathrm{t}}} |\mathbf{v}\rangle\langle\mathbf{w}| \sum_{\mathbf{x}\in\mathbb{F}_2^m} (-1)^{\mathbf{x}\mathbf{b}^{\mathrm{t}}} |\mathbf{x}\oplus\mathbf{a}\rangle\langle\mathbf{x}| \qquad (53)\\ &= \frac{1}{\sqrt{N}} \sum_{\mathbf{v},\mathbf{x}\in\mathbb{F}_2^m} (-1)^{\mathbf{v}(\mathbf{x}\oplus\mathbf{a})^{\mathrm{t}} + \mathbf{x}\mathbf{b}^{\mathrm{t}}} |\mathbf{v}\rangle\langle\mathbf{x}|. \qquad (54)\end{aligned}$$

The above yields

$$\mathrm{Tr}\big(\mathbf{GD}(\mathbf{a},\mathbf{b})\big) = \frac{1}{\sqrt{N}} \sum_{\mathbf{v}\in\mathbb{F}_2^m} (-1)^{\mathbf{v}(\mathbf{v}\oplus\mathbf{a}\oplus\mathbf{b})^{\mathrm{t}}}. \qquad (55)$$

Then map $\mathbf{v} \longmapsto \mathbf{v}(\mathbf{v}\oplus\mathbf{a}\oplus\mathbf{b})^{\mathrm{t}}$ is additive, and it is the trivial map iff $\mathbf{a} \oplus \mathbf{b} = \mathbf{1}_m$. Thus $\mathbf{D}(\mathbf{a},\mathbf{b}) \in \mathrm{supp}(\mathbf{G})$ iff $\mathbf{a}+\mathbf{b} = \mathbf{1}_m$. It follows that $\mathrm{supp}(\mathbf{G}) = (\mathbf{1}_m, \mathbf{0}_m) \oplus D_m$. Then, for $r < m$, a similar argument implies that $\mathbf{D}(\mathbf{a},\mathbf{b}) \in \mathrm{supp}(\mathbf{G})$ iff $\mathbf{a}_{1:r} + \mathbf{b}_{1:r} = \mathbf{1}_r$ and $\mathbf{a}_{r+1:m} = \mathbf{b}_{r+1:m} = \mathbf{0}_{m-r}$. The proof is concluded with the observation that $D_r = \mathrm{Res}(\mathbf{F}_{\Omega}(r))$. □

Remark 10. Let $\mathbf{P} \in \mathrm{GL}(m)$ and $\mathbf{S} \in \mathrm{Sym}(m)$, and put $\mathbf{G} = \mathbf{G}_D(\mathbf{P})\mathbf{G}_U(\mathbf{S})$. Then $\mathbf{G} = \sum_{\mathbf{v}\in\mathbb{F}_2^m} i^{\mathbf{v}\mathbf{S}\mathbf{v}^{\mathrm{t}}} |\mathbf{v}\mathbf{P}\rangle\langle\mathbf{v}|$, which in turn yields,

$$\begin{aligned}\mathrm{Tr}\big(\mathbf{GD}(\mathbf{a},\mathbf{b})\big) &= \mathrm{Tr}\left(\sum_{\mathbf{v}\in\mathbb{F}_2^m} i^{\mathbf{v}\mathbf{S}\mathbf{v}^{\mathrm{t}} + 2\mathbf{v}\mathbf{b}^{\mathrm{t}}} |(\mathbf{v}\oplus\mathbf{a})\mathbf{P}\rangle\langle\mathbf{v}|\right) \qquad (56)\\ &= \sum_{\mathbf{v}\in\mathrm{Fix}_{\mathbf{a}}(\mathbf{P})} i^{\mathbf{v}\mathbf{S}\mathbf{v}^{\mathrm{t}} + 2\mathbf{v}\mathbf{b}^{\mathrm{t}}}. \qquad (57)\end{aligned}$$

Now the analysis continues as in Proposition 9(2); see also [5, Lem. 6] for further details.

Example 11. We saw from Proposition 9 that matrices $\mathbf{G}_D(\mathbf{P})$ are supported on a subspace/subgroup. This is of course consistent with Corollary 6 since these matrices always have trace. Indeed, entry (1,1) is always 1 since $\mathbf{0}\mathbf{P} = \mathbf{0}$. The CNOT gate is of form $\mathbf{G}_D(\mathbf{P})$ where

$$\mathbf{P} = \mathbf{P}^{-1} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}. \qquad (58)$$

We have $\mathrm{Res}(\mathbf{P}^{-1}) = \{00, 01\}$ and $\mathrm{Fix}(\mathbf{P})^{\perp} = \{00, 10\}$. Thus, $\mathrm{supp}(\mathrm{CNOT}) = \{0000, 0010, 0100, 0110\}$, as one can directly verify. Here we have $m = 2$ and CNOT corresponds to the symplectic $\mathbf{F}_{\mathrm{CNOT}} = \mathbf{F}_D(\mathbf{P})$, which is a hyperbolic involution with $\mathrm{Fix}(\mathbf{F}_{\mathrm{CNOT}}) = \mathrm{supp}(\mathrm{CNOT})$. Note also that $\mathrm{Fix}(\mathbf{F}_{\mathrm{CNOT}}) = C_{\mathrm{CNOT}}$, and thus equality in Proposition 8 can be achieved. In addition $\mathbf{F}_{\mathrm{CNOT}} = \mathbf{T}_{0010}\mathbf{T}_{0100}\mathbf{T}_{0110}$. On the complex domain we have

$$\begin{aligned}\mathrm{CNOT} &= \frac{1-i}{\sqrt{2}} \cdot \frac{(\mathbf{I}+i\mathbf{E}_1)(\mathbf{I}+i\mathbf{E}_2)(\mathbf{I}-i\mathbf{E}_1\mathbf{E}_2)}{\sqrt{8}} \qquad (59)\\ &= \frac{1}{2}(\mathbf{I}+\mathbf{E}_1+\mathbf{E}_2-\mathbf{E}_1\mathbf{E}_2), \qquad (60)\end{aligned}$$

where $\mathbf{E}_1 = \mathbf{E}(00,10), \mathbf{E}_2 = \mathbf{E}(01,00)$. It follows that CNOT is supported on the MCS generated by $\mathbf{E}_1$ and $\mathbf{E}_2$.

Example 12. (1) Let $\mathbf{b} \in \mathbb{F}_2^m$ and consider the symmetric matrix $\mathbf{S}_{\mathbf{b}} := \mathbf{b}^{\mathrm{t}}\mathbf{b}$. In this case $[\ker(\mathbf{S}_{\mathbf{b}})]^{\perp} = \{\mathbf{0}, \mathbf{b}\}$. In addition $\mathbf{G}_U(\mathbf{S}_{\mathbf{b}}) = (\mathbf{I}_N \pm i\mathbf{E}(\mathbf{0},\mathbf{b}))/\sqrt{2}$.

(2) Let $\mathbf{S}$ be a diagonal matrix with diagonal $d_{\mathbf{S}}$. Let $r = \mathrm{wt}_{\mathrm{H}}(d_{\mathbf{S}})$ be the number of non-zero elements in $d_{\mathbf{S}}$. In this case $\mathbf{F}_U(\mathbf{S})$ is a product of transvections $\mathbf{T}_{\mathbf{v}_n}$ where $\mathbf{v}_n = (\mathbf{0}, \mathbf{b}_n)$ where $\mathbf{b}_n$ is the nth nonzero row of $\mathbf{S}$. Then

$$\mathbf{G}_U(\mathbf{S}) = \prod_{n=1}^{r} \frac{\mathbf{I}_N + i\mathbf{E}(\mathbf{v}_n)}{\sqrt{2}}, \qquad (61)$$

from which we may also conclude that $\mathrm{Tr}(\mathbf{G}_U(\mathbf{S})) \neq 0$.

We end this section by computing the supports of the *local* Clifford group $(\mathrm{Cliff}_2)^{\otimes m} \subset \mathrm{Cliff}_N$.

Proposition 13 (Support of local Cliffords)**.** *Let $\mathbf{G} = \mathbf{G}_1 \otimes \cdots \otimes \mathbf{G}_m \in (\mathrm{Cliff}_2)^{\otimes m}$, and let S_i be the support of $\mathbf{G}_i$ in $\mathbb{F}_2^2$. Then* $\mathrm{supp}(\mathbf{G}) = \sigma(S_1 \times \cdots \times S_m)$*, where σ is the permutation $(a_1, b_1, \ldots, a_m, b_m) \longmapsto (a_1, \ldots, a_m, b_1, \ldots, b_m)$.*

Proof. The result follows immediately by the fact that the trace function is multiplicative on pure tensors. □

4 On Hermitian Clifford matrices

Hermitian Clifford matrices, on top of being interesting on their own right, they also play a prominent role on understanding the third level of the Clifford hierarchy $\mathcal{C}^{(3)}$. Indeed, by definition, $\mathbf{C}\mathcal{HW}_N\mathbf{C}^{\dagger} \subset \mathrm{Cliff}_N$ for all $\mathbf{C} \in \mathcal{C}^{(3)}$. The conjugate action preserves traces and the Hermitian property. Thus, other than the identity, only traceless Clifford matrices can emerge from conjugate action with a third level matrix. With the same notation as in Proposition 4, we see that $\mathbf{G}$ is traceless iff $\mathbf{E}_0 \notin S$. Further, $\mathbf{CEC}^{\dagger}$ must also be a Hermitian Clifford matrix for any Hermitian

Pauli matrix $\mathbf{E}$. The corresponding symplectic matrix $\Phi(\mathbf{CEC}^\dagger)$ is an involution, and symplectic matrices emerging in this way ($\mathbf{C}$ fixed, $\mathbf{E}$ varies) must commute. This fact, although elementary, is crucial because any group of commuting involutions is conjugate[3] with some subgroup of S_U from (4). This means that, for instance, the CNOT gate (or any Clifford matrix of form $\mathbf{G}_D(\mathbf{P})$) cannot emerge from a third level action, despite $\mathbf{F}_{\text{CNOT}}$ being a symplectic involution; see also Example 11.

We have mentioned that any Clifford matrix, is, up to a multiplication by a Pauli, a product of transvections. We have the following structural results if the transvections involved are independent.

Theorem 14. *Let $\mathbf{E}_n = \mathbf{E}(\mathbf{c}_n), n = 1, \ldots, k$, be a set of k* independent *Hermitian Pauli matrices. Let also $\mathbf{E}_0 = \mathbf{E}(\mathbf{c}_0)$ be a Hermitian Pauli matrix. Then, the Clifford matrix*

$$\mathbf{G} = \mathbf{E}_0 \prod_{n=1}^{k} \frac{1}{\sqrt{2}}(\mathbf{I} + i\mathbf{E}_n), \tag{62}$$

is Hermitian iff $\mathbf{E}_0$ anticommutes with all $\mathbf{E}_n$ and all $\mathbf{E}_n$ commute with each other. As a consequence, if $\mathbf{G}$ is Hermitian then it is also traceless.

Proof. Let $\mathbf{C} := (\mathbf{A}\ \mathbf{B})$ be the $k \times 2m$ binary matrix whose nth row is $\mathbf{c}_n = (\mathbf{a}_n, \mathbf{b}_n)$. Since all the $\mathbf{E}_n$ are independent we have that $\operatorname{rank}(\mathbf{C}) = k$. Using (12) we have that

$$\begin{aligned}\mathbf{G} &= \frac{\mathbf{E}_0}{\sqrt{2^k}} \sum_{\mathbf{d}\in\mathbb{F}_2^k} i^{\mathbf{d}(\mathbf{I}_k + \widetilde{\mathbf{C}})\mathbf{d}^{\mathrm{t}}} \mathbf{E}(\mathbf{dC} \bmod 4) \\ &= \frac{1}{\sqrt{2^k}} \sum_{\mathbf{d}\in\mathbb{F}_2^k} i^{\mathbf{d}(\mathbf{I}_k + \widetilde{\mathbf{C}})\mathbf{d}^{\mathrm{t}}} \mathbf{E}_0\mathbf{E}(\mathbf{dC} \bmod 4),\end{aligned} \tag{63}$$

where $\widetilde{\mathbf{C}}$ is the $k\times k$ matrix whose (i,j) entry is $\mathbf{a}_j\mathbf{b}_i^{\mathrm{t}} - \mathbf{a}_i\mathbf{b}_j^{\mathrm{t}} \bmod 4$ if $i < j$ and 0 else. If we write $\mathbf{c}_0 = (\mathbf{a}_0, \mathbf{b}_0)$, then (63) can be further rewritten as

$$\mathbf{G} = \frac{1}{\sqrt{2^k}} \sum_{\mathbf{d}\in\mathbb{F}_2^k} i^{\mathbf{d}(\mathbf{I}_k + \widetilde{\mathbf{C}})\mathbf{d}^{\mathrm{t}}} i^{\mathbf{d}\mathbf{A}\mathbf{b}_0^{\mathrm{t}} - \mathbf{a}_0\mathbf{B}^{\mathrm{t}}\mathbf{d}^{\mathrm{t}}} \mathbf{E}(\mathbf{dC} + \mathbf{c}_0) \tag{64}$$

It follows immediately that $\mathbf{G}$ is Hermitian iff all coefficients in (64) are ± 1.

By looking at the standard basis of $\mathbb{F}_2^k$, i.e., $\mathbf{d} = \mathbf{e}_n$, and corresponding coefficients, we see that $\mathbf{a}_n\mathbf{b}_0^{\mathrm{t}} \oplus \mathbf{a}_0\mathbf{b}_n^{\mathrm{t}} = 1$ for $n = 1, \ldots, k$, which in turn means that $\mathbf{E}_0$ anticommutes with $\mathbf{E}_n$. To show that $\mathbf{E}_j, \mathbf{E}_n$ commute, consider $\mathbf{d}$ of weight two with ones in positions j, n. This corresponds to looking at the coefficient of $\mathbf{E}_0\mathbf{E}_j\mathbf{E}_n$. Because $\mathbf{E}_0$ anticommutes with both $\mathbf{E}_j, \mathbf{E}_n$, the term $i^{\mathbf{d}\mathbf{A}\mathbf{b}_0^{\mathrm{t}} - \mathbf{a}_0\mathbf{B}^{\mathrm{t}}\mathbf{d}^{\mathrm{t}}}$ contributes ± 1 and the term $i^{\mathbf{d}\mathbf{I}_k\mathbf{d}^{\mathrm{t}}} = i^{\mathrm{wt}(\mathbf{d})}$ contributes -1. Thus, the overall coefficient will be ± 1 only if $\mathbf{E}_j, \mathbf{E}_n$ commute.

[3] Two groups S and S' are called conjugate if there exists g such that $S' = gSg^\dagger$.

For the converse, one could argue similarly to show that the coefficients in (64) are ± 1. However, we point out here that the statement follows immediately from (62).

Finally, for Hermitian $\mathbf{G}$ as in (62) we argued that $\mathbf{E}_0$ anticommutes with all $\mathbf{E}_n$. Thus $\mathbf{E}_0$ cannot be contained on the commutative group generated by all $\mathbf{E}_n$. As we have mentioned earlier, this implies that $\mathbf{G}$ is traceless. □

Remark 15. Recall Proposition 4 where a Clifford matrix $\mathbf{G}$ is written as a generic sum of Hermitian matrices $\mathbf{E}$. In (64) we have explicitly computed the coefficients $\alpha_{\mathbf{E}}$, and evidently, they are of form $i^{Q(\mathbf{v})}, \mathbf{v} \in \mathbb{F}_2^m$ where Q is a quadratic form mod 4. This generalizes a result of [6] (see also [8]) where the authors showed that the coefficients of *diagonal* Clifford matrices are determined by a quadratic form. Indeed, diagonal Clifford matrices are of form $\mathbf{G}_U(\mathbf{S}), \mathbf{S} \in \mathrm{Sym}(m)$, and we see the aforementioned quadratic form in (47)-(48).

Remark 16. If $\mathbf{G} \in \mathrm{Cliff}_N$ is Hermitian, we mentioned that the corresponding symplectic matrix $\mathbf{F}_{\mathbf{G}}$ must be an involution, which we also mentioned can be written as a product of $k \in \{r, r+1\}$ transvections, $r = 2m - \dim(\mathrm{Fix}(\mathbf{F}_{\mathbf{G}}))$, where at least r are independent. Theorem 14 settles the scenario when $\mathbf{F}_{\mathbf{G}}$ is a product of only independent transvections. When the additional transvection $\mathbf{T}_{r+1}$ is dependent of the other r transvections, then multiplying $\mathbf{G} = \mathbf{T}_1 \cdots \mathbf{T}_r$ with $\mathbf{T}_{r+1}$ may preserve the support of $\mathbf{G}$ (see Example 11) or reduce the support of $\mathbf{G}$. In the latter instance the supported is reduced by half. Keeping track of the support of $\mathbf{G}\mathbf{T}_{r+1}$ becomes tedious and involves sign chasing that depends on the commutativity relation of $\mathbf{T}_1, \ldots, \mathbf{T}_r$.

5 On (Generalized) Semi-Clifford Matrices

For $k \geq 3$ the levels $\mathcal{C}^{(k)}$ of the Clifford hierarchy do not form a group, and thus a complete characterization becomes challenging. In [35] the authors use the notion of semi-Clifford matrices to achieve partial results. A unitary matrix $\mathbf{U} \in \mathbb{U}(N)$ is called *semi-Clifford* if there exists a MCS $S_1 \subset \mathcal{HW}_N$ such that $S_2 = \mathbf{U}S_1\mathbf{U}^\dagger$ is also MCS. Since the Clifford group Cliff_N permutes stabilizers of a given dimension, a Clifford matrix is trivially semi-Clifford. It is shown in [35] that for $m = 1, 2$ qubits the Clifford hierarchy is comprised of semi-Clifford matrices, and for $m = 3$ qubits the third level $\mathcal{C}^{(3)}$ is comprised of semi-Clifford matrices. Moreover, they show that for $m > 2$ qubits that there exist non semi-Clifford matrices in each level $\mathcal{C}^{(k)}, k > 3$, and conjecture that the third level $\mathcal{C}^{(3)}$ is comprised of semi-Cliffords for any number of qubits. The conjecture was disproved by

Gottesman and Mochon via a counterexample with $m = 7$ qubits; see [1]. On the other hand, the diagonal elements of each level, denoted $\mathcal{C}_d^{(k)}$ do form a group [35, Prop. 4], and are completely characterized in [14]. The QFD gates of [28] represent all 1- and 2-local diagonal gates in the hierarchy, and thus forming a particularly nice subclass of diagonal gates.

Remark 17. Multiplying by Clifford matrix preserves the levels of the hierarchy. Thus, without loss of generality, we will consider semi-Clifford matrices (and any matrix in the hierarchy) up to multiplication by Clifford matrices. This enables us to adjust any semi-Clifford $\mathbf{U}$ matrix so that it fixes any given given MCS S. Indeed, assume $\mathbf{U}S_1\mathbf{U}^\dagger = S_2$. Let $\mathbf{G}_1, \mathbf{G}_2 \in \mathrm{Cliff}_N$ be such that $\mathbf{G}_1 S \mathbf{G}_1^\dagger = S_1$ and $\mathbf{G}_2 S_2 \mathbf{G}_2^\dagger = S$. Then $\mathbf{G}_2\mathbf{U}\mathbf{G}_1$ is a semi-Clifford matrix that fixes S. As mentioned earlier, by [26, Alg. 1], there exists $\mathbf{G}_3 \in \mathrm{Cliff}_N$ such that $\mathbf{G}_3\mathbf{G}_2\mathbf{U}\mathbf{G}_1$ fixes S pointwise.

Theorem 18. *Let $\mathbf{C} \in \mathcal{C}^{(k)}$ be a unitary matrix that fixes the group of diagonal Paulis $Z_N = \mathbf{E}(\mathbf{0}_m, \mathbf{I}_m)$. Then $\mathbf{C} = \mathbf{D}\mathbf{E}(\mathbf{a}, \mathbf{0})\mathbf{G}_D(\mathbf{P})$, for some diagonal $\mathbf{D} \in \mathcal{C}_d^{(k)}, \mathbf{P} \in \mathrm{GL}(m)$, and $\mathbf{a} \in \mathbb{F}_2^m$.*

We will make use of the structure of first order Reed-Muller codes to prove Theorem 18. Let $C = \{(\mathbf{v}\mathbf{b}^{\mathrm{t}} \bmod 2)_{\mathbf{v}\in\mathbb{F}_2^m} \mid \mathbf{b} \in \mathbb{F}_2^m\}$. Then, the *first-order Reed-Muller* code is the linear $[2^m, m+1, 2^{m-1}]_2$-code

$$\mathrm{RM}(1, m) = C \cup \{\mathbf{c} \oplus \mathbf{1} \mid \mathbf{c} \in C\}. \tag{65}$$

The automorphism group of $\mathrm{RM}(1, m)$ is the general affine group $\mathrm{GA}(m)$ of maps $\mathbf{v} \longmapsto \mathbf{v}\mathbf{P} \oplus \mathbf{a}, \mathbf{P} \in \mathrm{GL}(m), \mathbf{a} \in \mathbb{F}_2^m$; see [21, Chapter 13] for instance.

Proof of Theorem 18. Assume that $\mathbf{C} \in \mathcal{C}^{(k)}$ fixes Z_N, and let $v \in \mathbb{C}^N$ be a common eigenvector of all $\mathbf{D}(\mathbf{0}, \mathbf{b}) \in Z_N$. Then, by assumption, we have

$$\mathbf{E}(\mathbf{0}, \mathbf{b})\mathbf{C}v = \mathbf{C}\mathbf{E}(\mathbf{0}, \mathbf{b}')v = \pm\mathbf{C}v, \tag{66}$$

which in turn implies that $\mathbf{C}v$ is also a common eigenvector of Z_N. Thus $\mathbf{C}$ maps the common eigenvector $|\mathbf{v}\rangle$ to another common eigenvector which is of the form $\alpha_{\mathbf{v}}|\pi(\mathbf{v})\rangle$ for some $\pi(\mathbf{v}) \in \mathbb{F}_2^m$ and $\alpha_{\mathbf{v}} \in \mathbb{C}$. In other words, $\mathbf{C}$ is a monomial map, that is $\mathbf{C} = \mathbf{D}\Pi$, where $\mathbf{D}$ is the diagonal matrix with entry $\alpha_{\mathbf{v}}$ in position $\pi(\mathbf{v})$ and Π is the permutation $\mathbf{v} \longmapsto \pi(\mathbf{v})$. The assumption $\mathbf{C} \in \mathcal{C}^{(k)}$ implies $\mathbf{D} \in \mathcal{C}_d^{(k)}$. By construction, the diagonals of Paulis in Z_N are of form $\pm((-1)^{\mathbf{v}\mathbf{b}^{\mathrm{t}}})_{\mathbf{v}\in\mathbb{F}_2^m}$, and we point out that the exponents of such diagonals are precisely the elements of $\mathrm{RM}(1, m)$. Thus Π induces an isometry on $\mathrm{RM}(1, m)$, which as we mentioned must be an invertible affine map. That is, $\Pi = \mathbf{E}(\mathbf{a}, \mathbf{0})\mathbf{G}_D(\mathbf{P})$ for some diagonal $\mathbf{P} \in \mathrm{GL}(m)$, and $\mathbf{a} \in \mathbb{F}_2^m$. In particular we have $\Pi \in \mathrm{Cliff}_N$, which along with the assumption $\mathbf{C} \in \mathcal{C}^{(k)}$ implies $\mathbf{D} \in \mathcal{C}_d^{(k)}$. □

Remark 19. In [35] it was shown that a semi-Clifford $\mathbf{C} \in \mathcal{C}_d^{(k)}$ is of the form $\mathbf{C} = \mathbf{G}_1\mathbf{D}\mathbf{G}_2$ for some $\mathbf{G}_1, \mathbf{G}_2 \in \mathrm{Cliff}_N$ and $\mathbf{D} \in \mathcal{C}_d^{(k)}$. Theorem 18 further extends this result by characterizing the Clifford matrices that appear into decomposition of $\mathbf{C}$. Thus, we obtain a complete characterization of semi-Clifford elements in the Clifford hierarchy. We believe that this result, along with the notion of the support can be used in many applications, e.g., design of flag gadgets.

The argument of Theorem 18 holds in a slightly more general setting.

Remark 20. (1) Let $\mathbf{C}$ be any unitary matrix that fixes a MCS $S = \langle \mathbf{E}_1, \ldots, \mathbf{E}_m \rangle$. For $\mathbf{d} \in \mathbb{F}_2^m$ denote $S_{\mathbf{d}} := \langle (-1)^{d_1}\mathbf{E}_1, \ldots, (-1)^{d_m}\mathbf{E}_m \rangle$, and put $\mathcal{F}_+(S_{\mathbf{d}}) := |\psi_{\mathbf{d}}\rangle$. For any $\mathbf{E} \in S_{\mathbf{d}}$ we have

$$\mathbf{E}\mathbf{C}|\psi_{\mathbf{d}}\rangle = \mathbf{C}\mathbf{E}'|\psi_{\mathbf{d}}\rangle = \pm\mathbf{C}|\psi_{\mathbf{d}}\rangle, \tag{67}$$

and thus $\mathbf{C}|\psi_{\mathbf{d}}\rangle \in \mathcal{F}_+(S_{\mathbf{d}'})$ for some $\mathbf{d}' \in \mathbb{F}_2^m$. This means that $\mathbf{C}|\psi_{\mathbf{d}}\rangle = \lambda_{\mathbf{d}}|\psi_{\mathbf{d}'}\rangle$ for some eigenvalue $\lambda_{\mathbf{d}}$. In particular, $\mathbf{C}$ is a monomial matrix with respect to the eigenbasis $\mathcal{E}_S := \{|\psi_{\mathbf{d}}\rangle \mid \mathbf{d} \in \mathbb{F}_2^m\}$.

(2) Let $\mathbf{C}$ be a unitary matrix that fixes the *span* of Z_N, that is, $\mathbf{C}$ maps any diagonal to another diagonal. Then $\mathbf{C}$ is a monomial matrix. In particular, any semi-Clifford matrix is a monomial matrix up to some Clifford correction; see also [35, Prop. 2].

Let $\mathbf{C} \in \mathcal{C}^{(3)}$ be such that it fixes some subgroup $\widehat{S}$ (of $\mathcal{HW}_N$) under conjugation; see also Remark 17. Then, by [26, Alg. 1], there exists $\mathbf{G} \in \mathrm{Cliff}_N$, produced as a sequence of transvections, such that $\widehat{\mathbf{C}} := \mathbf{G}\mathbf{C}$ fixes $\widehat{S}$ *point-wise*. Let $\widehat{S}^{\perp_s}$ be all the Pauli matrices that commute with elements of $\widehat{S}$. Proceeding similarly as in the proof of Proposition 8 we have the following.

Proposition 21. $\mathrm{supp}(\widehat{\mathbf{C}}) \subset \widehat{S}^{\perp_s}$, *and thus* $\mathrm{supp}(\mathbf{C}) \subset S := \{\mathbf{E}\mathbf{E}' \mid \mathbf{E} \in \mathrm{supp}(\mathbf{G}^{-1}), \mathbf{E}' \in \widehat{S}^{\perp_s}\}$.

Corollary 22. *Let $\mathbf{C}$ be a unitary matrix and S be a MCS. If $\mathbf{C}$ fixes S pointwise then $\mathrm{supp}(\mathbf{C}) \subset S$. The converse is also true. This property characterizes semi-Clifford matrices up to multiplication by Clifford. In particular, as for Hermitian Clifford matrices, we have that $\mathbf{C}$ is supported on a* commutative *subgroup.*

In the reminder of this section we show that Corollary 22 holds for the entire third level $\mathcal{C}^{(3)}$ of the hierarchy (always up to Cliffords). Note that this is not a trivial step because, as mentioned before, there exist elements in $\mathcal{C}^{(3)}$ that are not semi-Cliffords [1].

Lemma 23. *For $\mathbf{C} \in \mathcal{C}^{(3)}$ there exists a Pauli $\widetilde{\mathbf{E}}$ such that $\mathbf{C}\widetilde{\mathbf{E}}\mathbf{C}^\dagger$ is also a Pauli. As a consequence, there exists a Clifford correction $\mathbf{G}$ such that $\mathbf{G}\mathbf{C}$ fixes (i.e., commutes with) some Pauli matrix.*

Proof. Let $\mathbf{C} \in \mathcal{C}^{(3)}$ and consider the map

$$\varphi_{\mathbf{C}} : \begin{cases} \mathcal{PHW}_N & \xrightarrow{\phi_{\mathbf{C}}} & \mathrm{Cliff}_N & \xrightarrow{\Phi} & \mathrm{Sp}(2m) \\ \mathbf{E} & \longmapsto & \mathbf{CEC}^\dagger & \longmapsto & \Phi(\mathbf{CEC}^\dagger) \end{cases}$$

where Φ is the map from (26) and $\mathcal{PHW}_N$ is the projective form of $\mathcal{HW}_N$ that ignores phases. Then $\ker \varphi_{\mathbf{C}} \subset \mathcal{PHW}_N$ has size 2^k for some $k \geq 0$. So, we see that $G := \operatorname{im} \varphi_{\mathbf{C}} \subset \mathrm{Sp}(2m)$ has size 2^{2m-k}.

Let G act on $\mathbb{F}_2^{2m} \setminus \{\mathbf{0}\}$. Since the size of an orbit must divide the size of the group G, each orbit has size a power of 2 as well. However, since the orbits partition a set of size $2^{2m}-1$ (odd), there must exist an orbit of odd size, and that size must be $2^0 = 1$. This means that there exists $\mathbf{0} \neq \mathbf{c} \in \mathbb{F}_2^{2m}$ that is fixed by all symplectic matrices $\Phi(\mathbf{CEC}^\dagger)$. The definition of Φ yields that the Hermitian Pauli $\widetilde{\mathbf{E}} := \mathbf{E}(\mathbf{c})$ either commutes or anticommutes with all $\mathbf{CEC}^\dagger$. In other words

$$\widetilde{\mathbf{E}}\mathbf{CEC}^\dagger = \alpha_{\mathbf{E}}\mathbf{CEC}^\dagger\widetilde{\mathbf{E}}, \quad \alpha_{\mathbf{E}} = \pm 1, \tag{68}$$

for all Paulis $\mathbf{E}$. Now put $\widetilde{\mathbf{C}} = \widetilde{\mathbf{E}}\mathbf{C}\widetilde{\mathbf{E}}$. Let also $\sigma_{\mathbf{E}} = \pm 1$ be such that $\widetilde{\mathbf{E}}\mathbf{E} = \sigma_{\mathbf{E}}\mathbf{E}\widetilde{\mathbf{E}}$. We have that

$$\widetilde{\mathbf{E}}\mathbf{C} = \widetilde{\mathbf{C}}\widetilde{\mathbf{E}} \quad \text{and} \quad \widetilde{\mathbf{E}}\mathbf{C}^\dagger = \widetilde{\mathbf{C}}^\dagger\widetilde{\mathbf{E}}, \tag{69}$$

which combined with (68) yields

$$\alpha_{\mathbf{E}}\mathbf{CEC}^\dagger = \sigma_{\mathbf{E}}\widetilde{\mathbf{C}}\mathbf{E}\widetilde{\mathbf{C}}^\dagger \tag{70}$$

for all Paulis $\mathbf{E}$. Now it is easy to see that $\mathbf{C}\widetilde{\mathbf{C}}^\dagger$ is a Pauli $\mathbf{E}'$, and thus (69) implies $\mathbf{C}\widetilde{\mathbf{E}}\mathbf{C}^\dagger = \mathbf{E}'\widetilde{\mathbf{E}}$. □

Remark 24. The proof of Lemma 23 could have been concluded using the language of stabilizer codes. With the same notation, let $\widetilde{\mathbf{E}}$ be such that it either commutes or anticommutes with all $\mathbf{CEC}^\dagger \in \mathrm{Cliff}_N$. Now consider the stabilizer group $S = \langle \widetilde{\mathbf{E}} \rangle$ and the corresponding stabilizer codes $\mathcal{F}_\varepsilon := \mathcal{F}_\varepsilon(S)$, for $\varepsilon = \pm 1$ (see (20)). We have that $\mathbf{CEC}^\dagger\mathcal{F}_\varepsilon = \pm\mathcal{F}_\varepsilon$ for all Paulis $\mathbf{E}$. In other words, for any $v \in \mathcal{F}_\varepsilon$, we have that

$$\varepsilon\widetilde{\mathbf{E}} \cdot \mathbf{CEC}^\dagger v = \pm\left(\mathbf{CEC}^\dagger \cdot \varepsilon\widetilde{\mathbf{E}}v\right) = \pm\mathbf{CEC}^\dagger v \tag{71}$$

holds for all $\mathbf{E}$. Next, express $\mathbf{C} = \sum_{\mathbf{E}} \alpha_{\mathbf{E}}\mathbf{E}$ and sum both sides in (71) to obtain

$$\varepsilon\widetilde{\mathbf{E}}\left(\sum_{\mathbf{E}} \alpha_{\mathbf{E}}\mathbf{E}\right)v = \varepsilon'\left(\sum_{\mathbf{E}} \alpha_{\mathbf{E}}\mathbf{E}\right)v. \tag{72}$$

In other words, $\varepsilon\widetilde{\mathbf{E}}\mathbf{C}v = \varepsilon'\mathbf{C}v$, and thus $\mathbf{C}$ permutes $\{\mathcal{F}_\varepsilon\}$. This is equivalent with $\mathbf{C}$ mapping $\widetilde{\mathbf{E}}$ to some other Pauli.

Next we prove the main result about the support of gates in $\mathcal{C}^{(3)}$, which can then be straightforwardly used to show that every gate in $\mathcal{C}^{(3)}$ is generalized semi-Clifford. Recall that a generalized semi-Clifford matrix is a unitary matrix that maps under conjugation the span of some MCS to the span of some other MCS.

Theorem 25. *Let* $\mathbf{C}$ *be a unitary matrix from* $\mathcal{C}^{(3)}$. *Then there exists a Clifford* $\mathbf{G}$ *such that* $\mathbf{GC}$ *is supported on a maximal commutative subgroup of* $\mathcal{HW}_N$.

Proof. From Lemma 23 we know that there exists some Clifford $\mathbf{H}$ such that $\mathbf{HC}$ commutes with some $\mathbf{E} \in \mathcal{HW}_N$. Now consider the group $S = \langle \mathbf{E} \rangle$ and its normalizer in $\mathcal{HW}_N$ which we denote by $S^{\perp_s}$. Then, since $\mathbf{HC}$ preserves S under conjugation, it is a valid logical operator for the $[\![m, m-1]\!]$ stabilizer code defined by S, i.e., it maps code states (+1 eigenvectors of $\mathbf{E}$) to code states. Denote this logical $(m-1)$-qubit operation realized by $\mathbf{HC}$ as $\overline{\mathbf{C}}_{\mathbf{H}}$. Since $\mathbf{HC} \in \mathcal{C}^{(3)}$, we know that $\mathbf{HC}$ must satisfy the necessary conjugation conditions on logical Paulis as determined by $\overline{\mathbf{C}}_{\mathbf{H}}$. These conditions can only correspond to physical realizations of logical Clifford gates (since physical Cliffords cannot realize anything above the second level $\mathrm{Cliff}_N = \mathcal{C}^{(2)}$). Hence, we conclude that $\overline{\mathbf{C}}_{\mathbf{H}} \in \mathcal{C}^{(3)}$ (in the logical space).

First, it has already been shown in [35] that operations in $\mathcal{C}^{(3)}$ are semi-Clifford for 1 and 2 qubits. Using Corollary 22, this automatically means that up to some Clifford correction such gates are supported on a MCS. Therefore, we consider the induction hypothesis that for $(m-1)$ qubits, any $\mathcal{C}^{(3)}$ element is supported on a MCS, up to multiplication by some Clifford. Applying this hypothesis for $\overline{\mathbf{C}}_{\mathbf{H}}$ above, we see that there exists some $(m-1)$-qubit logical Clifford $\overline{\mathbf{G}}'$ such that $\overline{\mathbf{G}}'\,\overline{\mathbf{C}}_{\mathbf{H}}$ is supported on a MCS (of size 2^{m-1}). Note that a logical Clifford operation is defined by its action on logical Paulis.

Let this MCS be generated by logical $(m-1)$-qubit Paulis $\overline{\mathbf{E}}_1, \overline{\mathbf{E}}_2, \ldots, \overline{\mathbf{E}}_{m-1}$, and let $\mathbf{E}_1, \mathbf{E}_2, \ldots, \mathbf{E}_{m-1} \in S^{\perp_s}$ form their respective physical m-qubit realizations in $\mathcal{HW}_N$. These realizations are automatically defined once $2(m-1)$ m-qubit Pauli operations are chosen to be the appropriate physical realizations of the logical X and Z on the $(m-1)$ logical qubits. As $\overline{\mathbf{G}}'\,\overline{\mathbf{C}}_{\mathbf{H}}$ is supported on $\overline{\mathbf{E}}_i$'s, it clearly commutes with each one of them. Hence, by taking $\mathbf{G}'$ to be an m-qubit Clifford that forms a physical realization of $\overline{\mathbf{G}}'$, we see that $\mathbf{G}'(\mathbf{HC})$ commutes with each $\mathbf{E}_i$. Note that, by definition of realizing a logical gate, such a $\mathbf{G}'$ must preserve the stabilizer S, i.e., commute with $\mathbf{E}$, and act on $\mathbf{E}_i$ as $\overline{\mathbf{G}}$ acts on $\overline{\mathbf{E}}_i$.

Finally, consider the group $\langle \mathbf{E}, \mathbf{E}_1, \mathbf{E}_2, \ldots, \mathbf{E}_{m-1} \rangle$. This is clearly a MCS and $(\mathbf{G}'\mathbf{H})\mathbf{C}$ fixes it pointwise. Therefore, by applying Corollary 22 we see that $\mathbf{GC} := (\mathbf{G}'\mathbf{H})\mathbf{C}$ is supported on this MCS. This completes the induction. □

Lemma 23 constitutes a crucial property of the third level $\mathcal{C}^{(3)}$ of the Clifford hierarchy. This property is of course exclusive to the third level because we highly rely on the fact that $\operatorname{im} \phi_{\mathbf{C}}$ is a subgroup of Cliff_N. This in turn enables an induction argument on the number of qubits, rather than the typical induction arguments on the levels of the Clifford hierarchy.

It is worth mentioning that the "up to Clifford" is indeed necessary throughout the paper. For instance, with regards to Lemma 23, the physical Clifford permutation

$$\mathbf{G} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} \tag{73}$$

does not fix (commute with) *any* Pauli matrix. Similarly, one can easily produce other instances of examples that require the "Clifford correction".

If $\mathbf{C} \in \mathcal{C}^{(3)}$ is supported on a MCS S then it trivially fixes the span of S, and therefore $\mathbf{C}$ is a generalized semi-Clifford matrix. The converse is not true since, for instance, even the CNOT gate fixes Z_4 but obviously is not supported on Z_4. In fact, any gate $\mathbf{G}_D(\mathbf{P})$ fixes Z_N by construction but is not supported on Z_N (see Proposition 9(1)).

Corollary 26 ([1, Thm. 1.1])**.** *Every* $\mathbf{C} \in \mathcal{C}^{(3)}$ *is a generalized semi-Clifford matrix.*

Proof. By Theorem 25, there exists a Clifford correction $\mathbf{G}$ such that $\mathbf{GC}$ is supported on a MCS S. Then $\mathbf{GC}$ fixes the span of S, and $\mathbf{C}$ maps the span of S to the span of $\mathbf{G}^\dagger S\mathbf{G}$. Thus $\mathbf{C}$ is generalized semi-Clifford. □

6 Conclusions and Future Research

In this paper we study the Clifford hierarchy via the Pauli/Weyl expansion/support. First, we consider the Clifford group, that is, the second level of the hierarchy. We show that every element of the group is supported on a subgroup of the Pauli group (or a coset, when traceless). Additionally, we give a closed form description of the support of standard group elements, and show that the coefficients are determined by a quadratic form modulo 4. We argue that the Hermitian elements of the group play a prominent role on understanding the third level of the hierarchy. For this reason, we treat them separately, and among other things, we show that they are supported on a *commutative* subgroup of the Pauli group (or a coset). Next, we consider the third level of the hierarchy. Our treatment is up to Clifford equivalence, which, at any rate, preservers the levels of the hierarchy. We show that, up to such equivalence, every third level matrix commutes with at least one Pauli matrix. This constitutes the main building block of a powerful induction argument on the number of qubits, which we use to prove that every third level matrix, up to Clifford equivalence, is supported on a maximal commutative subgroup of the Pauli group. We believe that such induction argument can be further exploited in various aspects of quantum computation and quantum error-correction.

In future research, we will consider the behaviour of the support under elementary transformations such as multiplication and conjugation (which, surprisingly, is unknown). This, among other things, would give a closed form description of the support of *any* Clifford group element. Next, with the ultimate goal of completely characterizing the third level of the hierarchy, we will consider the converse. That is, finding sufficient conditions under which a unitary $\mathbf{U}$, supported on some MCS, belongs to the third level. We expect the coefficients to be (scaled) eighth roots of unity that are perhaps determined by third-order Reed-Muller codes. Finally, we will use the structural results of this paper to develop flag gadgets for third level operators, as well as reduce circuit complexity for these operators.

Acknowledgements

The work of TP and OT was supported in part by the Academy of Finland under the grant 334539. The work of NR and RC was supported in part by NSF under the grant CCF1908730. TP and OT thank Robert Calderbank for his hospitality during visits to Duke University.

References

[1] Salman Beigi and Peter W. Shor. $\mathcal{C}_3$, semi-Clifford and generalized semi-Clifford operations. *Quantum Info. Comput.*, 10(1):41–59, January 2010. URL http://arxiv.org/abs/0810.5108.

[2] P. Oscar Boykin, Tal Mor, Matthew Pulver, Vwani Roychowdhury, and Farrokh Vatan. On universal and fault-tolerant quantum computing: A novel basis and a new constructive proof of universality for Shor's basis. page 486, USA, 1999. IEEE Computer Society. DOI: https://doi.org/10.1109/SFFCS.1999.814621.

[3] Sergey Bravyi and Jeongwan Haah. Magic-state distillation with low overhead. *Phys. Rev. A*, 86(5):052329, 2012. DOI: https://doi.org/10.1103/PhysRevA.86.052329.

[4] Sergey Bravyi and Alexei Kitaev. Universal quantum computation with ideal Clifford gates and noisy ancillas. *Phys. Rev. A*, 71:022316, Feb 2005. DOI: https://doi.org/10.1103/PhysRevA.71.022316.

[5] Robert A. Calderbank, Stephen Howard, Sina Jafarpour, and Jeremy Kent. Sparse approximation and compressed sensing using the Reed-Muller sieve. *Technical Report, Princeton University, TR-888-10, 2010.* URL https://www.cs.princeton.edu/research/techreps/TR-888-10.

[6] Robert A. Calderbank, Peter J. Cameron, William M. Kantor, and Jaap J. Seidel. $\mathbb{Z}_4$-Kerdock codes, orthogonal spreads, and extremal Euclidean line-sets. *Proceedings of the London*

Mathematical Society, 75(2):436–480, 1997. DOI: https://doi.org/10.1112/S0024611597000403.

[7] Robert A. Calderbank, Eric M. Rains, Peter W. Shor, and Neil J. A. Sloane. Quantum error correction via codes over GF(4). *IEEE Trans. Inform. Theory*, 44(4):1369–1387, 1998. DOI: https://doi.org/10.1109/18.681315.

[8] Robert A. Calderbank, Stephen Howard, and Sina Jafarpour. Construction of a large class of matrices satisfying a statistical isometry property. In *IEEE Journal of Selected Topics in Signal Processing, Special Issue on Compressive Sensing*, volume 4, pages 358–374, 2010. DOI: https://doi.org/10.1109/JSTSP.2010.2043161.

[9] David Callan. The generation of $\mathrm{Sp}(\mathbb{F}_2)$ by transvections. *J. Algebra*, 42(2):378–390, 1976. DOI: https://doi.org/10.1016/0021-8693(76)90105-8.

[10] Christopher Chamberland and Michael E. Beverland. Flag fault-tolerant error correction with arbitrary distance codes. *Quantum*, 2:53, 2018. DOI: https://doi.org/10.22331/q-2019-05-20-143.

[11] Rui Chao and Ben W Reichardt. Quantum Error Correction with Only Two Extra Qubits. *Phys. Rev. Lett.*, 121(5):050502, 2018. DOI: https://doi.org/10.1103/PhysRevLett.121.050502.

[12] Rui Chao and Ben W Reichardt. Fault-tolerant quantum computation with few qubits. *npj Quantum Inf.*, 4(1):42, 2018. DOI: https://doi.org/10.1038/s41534-018-0085-z.

[13] Rui Chao and Ben W. Reichardt. Flag fault-tolerant error correction for any stabilizer code. *PRX Quantum*, 1:010302, Sep 2020. DOI: https://doi.org/10.1103/PRXQuantum.1.010302.

[14] Shawn X. Cui, Daniel Gottesman, and Anirudh Krishna. Diagonal gates in the Clifford hierarchy. *Phys. Rev. A*, 95:012329, Jan 2017. DOI: https://doi.org/10.1103/PhysRevA.95.012329.

[15] Kathleen S. Gibbons, Matthew J. Hoffman, and William K. Wootters. Discrete phase space based on finite fields. *Phys. Rev. A*, 70:062101, Dec 2004. DOI: https://doi.org/10.1103/PhysRevA.70.062101.

[16] Daniel Gottesman. Stabilizer codes and quantum error correction. *PhD thesis, California Institute of Technology*, 1997. DOI: https://doi.org/10.7907/rzr7-dt72.

[17] Daniel Gottesman and Isaac L. Chuang. Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations. *Nature*, 402(6760):390–393, 1999. DOI: https://doi.org/10.1038/46503.

[18] David Gross. Hudson's theorem for finite-dimensional quantum systems. *Journal of Mathematical Physics*, 47(12):122107, 2006. DOI: https://doi.org/10.1063/1.2393152.

[19] David Gross and Maarten Van den Nest. The LU-LC conjecture, diagonal local operations and quadratic forms over GF(2). *Quantum Inf. Comput.*, 8(3-4):263–281, 2007. URL http://arxiv.org/abs/0707.4000.

[20] Robert Koenig and John A. Smolin. How to efficiently select an arbitrary Clifford group element. *J. Math. Phys.*, 55(12):122202, Dec 2014. DOI: https://doi.org/10.1063/1.4903507.

[21] Florence J. MacWilliams and Neil J. A. Sloane. *The theory of error-correcting codes*, volume 16. Elsevier, 1977.

[22] Dmitri Maslov and Martin Roetteler. Shorter stabilizer circuits via Bruhat decomposition and quantum circuit transformations. *IEEE Transactions on Information Theory*, 64(7):4729–4738, 2018. DOI: https://doi.org/10.1109/TIT.2018.2825602.

[23] Michael A. Nielsen and Isaac L. Chuang. *Quantum computation and quantum information*. Cambridge University Press, Cambridge, 2000.

[24] Onorato T. O'Meara. *Symplectic groups*, volume 16 of *Mathematical Surveys*. American Mathematical Society, Providence, R.I., 1978.

[25] Tefjol Pllaha, Olav Tirkkonen, and Robert A. Calderbank. Reconstruction of multi-user binary subspace chirps. In *2020 IEEE International Symposium on Information Theory (ISIT)*, pages 531–536, 2020. DOI: https://doi.org/10.1109/ISIT44484.2020.9174412.

[26] Narayanan Rengaswamy, Robert A. Calderbank, Henry D. Pfister, and Swanand Kadhe. Synthesis of logical Clifford operators via symplectic geometry. In *2018 IEEE International Symposium on Information Theory (ISIT)*, pages 791–795, 2018. DOI: https://doi.org/10.1109/ISIT.2018.8437652.

[27] Narayanan Rengaswamy, Robert Calderbank, Michael Newman, and Henry D. Pfister. On Optimality of CSS Codes for Transversal T. *arXiv preprint arXiv:1910.09333*, 2019. URL http://arxiv.org/abs/1910.09333.

[28] Narayanan Rengaswamy, Robert Calderbank, and Henry D. Pfister. Unifying the Clifford hierarchy via symmetric matrices over rings. *Phys. Rev. A*, 100(2):022304, 2019. DOI: https://doi.org/10.1103/PhysRevA.100.022304.

[29] Narayanan Rengaswamy, Robert Calderbank, Michael Newman, and Henry D. Pfister. Classical coding problem from transversal t gates. In *2020 IEEE International Symposium on Information Theory (ISIT)*, pages 1891–1896, 2020. DOI: https://doi.org/10.1109/ISIT44484.2020.9174408.

[30] Theerapat Tansuwannont, Christopher Chamberland, and Debbie Leung. Flag fault-tolerant error correction, measurement, and quantum computation for cyclic Calderbank-Shor-Steane codes. *Phys. Rev. A*, 101(1):012342, 2020. DOI: https://doi.org/10.1103/PhysRevA.101.012342.

[31] Victor Veitch, S A Hamed Mousavian, Daniel Gottesman, and Joseph Emerson. The resource theory of stabilizer quantum computation. *New Journal of Physics*, 16(1):013009, jan 2014. DOI: https://doi.org/10.1088/1367-2630/16/1/013009.

[32] Eugene Wigner. On the quantum correction for thermodynamic equilibrium. *Phys. Rev.*, 40:749–759, Jun 1932. DOI: https://doi.org/10.1103/PhysRev.40.749.

[33] William K. Wootters. Picturing qubits in phase space. *IBM Journal of Research and Development*, 48(1):99–110, 2004. DOI: https://doi.org/10.1147/rd.481.0099.

[34] Bei Zeng. Quantum operations and codes beyond the Stabilizer-Clifford framework. *PhD thesis, Massachusetts Institute of Technology*, 2009. URL `http://hdl.handle.net/1721.1/53235`.

[35] Bei Zeng, Xie Chen, and Isaac L. Chuang. Semi-Clifford operations, structure of $\mathcal{C}_k$ hierarchy, and gate complexity for fault-tolerant quantum computation. *Phys. Rev. A*, 77:042313, Apr 2008. DOI: https://doi.org/10.1103/PhysRevA.77.042313.

[36] Xinlan Zhou, Debbie W. Leung, and Isaac L. Chuang. Methodology for quantum logic gate construction. *Phys. Rev. A*, 62:052316, Oct 2000. DOI: 10.1103/PhysRevA.62.052316.