

Clifford Circuits on Qudits of Mixed Dimension

Milo Moses^{1,2,*}, Jacek Horecki^{2,3}, Konrad Deka^{2,3} and Jan Tułowiecki^{2,4,5}

¹ Department of Mathematics, UC Santa Barbara, 552 University Rd, Isla Vista, CA 93117, USA

² BEIT Inc., Mogilska 43, 31-545 Kraków, Poland

³ Institute of Mathematics, Jagiellonian University, ul. Łojasiewicza 6, 30-348 Kraków, Poland

⁴ Department of Theoretical Computer Science, Jagiellonian University, ul. Łojasiewicza 6, 30-348 Kraków, Poland

⁵ Doctoral School of Exact and Natural Sciences, Jagiellonian University, ul. Prof. Łojasiewicza 11, I piętro, pok. H-1-02, 30-348 Kraków, Poland

* Corresponding author: milo@tacocat.com

Received date: 29 September 2025; Accepted date: 21 February 2026; Published online: 28 February 2026

Abstract: Associated to every finite abelian group G , there is a generalization of qubit Clifford group associated to G . We demonstrate that every G -Clifford gate can be decomposed into some distinguished elementary types: Fourier transforms, quadratic phase gates, and automorphism gates. Combined with earlier results on classical simulation of normalizer circuits, this implies a generalized Gottesman-Knill-type result. We additionally provide circuits for a universal quantum computing scheme based on local two-qudit G -Clifford gates and magic states.

Keywords: Gottesman-Knill; Clifford circuits; qudits

1. Introduction

Creating a fault-tolerant application-scale quantum computer is the goal of many scientists. One of the steps towards the realization of this goal is the development of low-overhead error correcting codes on which a universal set of logical gates can be applied fault-tolerantly. These error correcting codes are typically stabilizer codes, and the fault-tolerant gates are typically made from constant-depth local unitary circuits.

A fundamental challenge within error correction is that constant-depth local unitary circuits on two dimensional stabilizer codes can only act on the codespace by Clifford gates. This is known as the Bravyi-Koenig bound [1], and along with related no-go theorems like the Eastin-Knill theorem [2], it sets out a clear difficulty. Not only is the Clifford gate set a proper subset of all possible quantum gates, but the Gottesman-Knill theorem asserts that the result of any quantum computation using only Clifford gates can be efficiently simulated on a classical computer [3]. Hence, any approach to quantum computing based on two-dimensional local stabilizer codes will need to confront these no-go results, and as such will need to deal with the structure of the space of Clifford operations.

In this paper we discuss a generalized version of the qubit Clifford group, based on qudits with an algebra specified by a finite abelian group G with cyclic factors of mixed dimension. This is the relevant group of logical operations when considering generalized stabilizer codes over a finite group G , such as Kitaev's quantum double model associated to G [4]. These G -Pauli groups were already known to quantum information researchers a few years before Kitaev's model [5,6]. We recall this group and its basic properties in Sections 2 and 3. Our analysis of the G -Clifford group is based on three elementary classes of gates - Fourier transforms, automorphism gates, and quadratic phase gates. These gates were introduced in Refs. [7,8], where it was conjectured that they efficiently generate all G -Clifford group. Our main result is the proof of this conjecture. It was shown in Refs. [7,8] that any circuit consisting of elementary Clifford gates can be efficiently classically simulated, and thus our results imply that every G -Clifford circuit can be efficiently classically simulated, a generalization of the Gottesman-Knill theorem. Our technique uses a group-theoretic generalization of the qudit linear algebra performed in Ref. [9].

We additionally provide several constructions related to Fourier transforms, automorphism gates, and quadratic phase gates which we believe will be of utility to the community. We show that every G -Clifford on multiple qudits can be decomposed into one-qudit and two-qudit gates (Section 3), we decompose the CX gate using 2-qudit G -Pauli

measurements and elementary one-qudit Clifford gates (Section 4), we give an algorithm to implement non- G -Clifford gates using magic state injection (Section 5), and we simplify the primitive gate set by demonstrating that the global Fourier transform on any finite abelian group G can be used to obtain Fourier transforms on split subgroups of G (Section 6).

2. The G -Pauli Group

Let G be a finite abelian group. Let $\widehat{G} = \text{Hom}(G, \mathbb{C}^\times)$ be the character group and let $\mathbb{C}[G] = \text{span}\{|g\rangle, g \in G\}$ be the group algebra. The G -Pauli group is

$$\text{Pauli}(G) = \left\{ \omega X_g Z_\chi, (g, \chi) \in G \times \widehat{G}, \omega \in U(1) \right\}, \quad (1)$$

where the gates X_g and Z_χ are defined by

$$\begin{aligned} X_g : \mathbb{C}[G] &\rightarrow \mathbb{C}[G], g \in G \\ |h\rangle &\mapsto |gh\rangle \end{aligned} \quad (2)$$

$$\begin{aligned} Z_\chi : \mathbb{C}[G] &\rightarrow \mathbb{C}[G], \chi \in \widehat{G} \\ |g\rangle &\mapsto \chi(g)|g\rangle \end{aligned} \quad (3)$$

The G -Pauli group on n qudits is the space of operators on $\mathbb{C}[G]^n$ which are the tensor products of G -Pauli matrices on each component. Alternatively, one can identify this group with $\text{Pauli}(G^n)$ via the canonical isomorphism $\mathbb{C}[G^n] \cong \mathbb{C}[G]^n$. The Pauli group on the product of groups decomposes as a product of $U(1)$ -modules, $\text{Pauli}(G \times H) \cong \text{Pauli}(G) \times_{U(1)} \text{Pauli}(H)$. Proposition 1 summarizes some known properties of the G -Pauli group.

Proposition 1. *Let G be a finite abelian group. The following statements about $\text{Pauli}(G)$ are all true:*

1. *Every element of $\text{Pauli}(G)$ is unitary.*
2. *We have that $X_{g_0} X_{g_1} = X_{g_1} X_{g_0} = X_{g_0 g_1}$ and $Z_{\chi_0} Z_{\chi_1} = Z_{\chi_1} Z_{\chi_0} = Z_{\chi_0 \chi_1}$ for all $g_0, g_1 \in G, \chi_0, \chi_1 \in \widehat{G}$.*
3. *We have that $Z_\chi X_g = \chi(g) X_g Z_\chi$ for all $g \in G, \chi \in \widehat{G}$.*
4. *If a unitary operator $U : \mathbb{C}[G] \rightarrow \mathbb{C}[G]$ commutes with all elements of $\text{Pauli}(G)$ it must be a scalar multiple of the identity.*
5. *If a unitary operator $U : \mathbb{C}[G] \rightarrow \mathbb{C}[G]$ commutes with all elements of $\text{Pauli}(G)$ up to phase it must be a Pauli operator.*

Proof. Points (1)-(3) are straightforward. For point (4), suppose that

$$U|1\rangle = \sum_{g \in G} c_g |g\rangle. \quad (4)$$

We have that

$$Z_\chi U|1\rangle = U Z_\chi |1\rangle = U|1\rangle \quad \forall \chi \in \widehat{G} \quad (5)$$

and hence $\chi(g)c_g = c_g$ for all $\chi \in \widehat{G}$ so $c_g = 0$ for all $g \neq 1$. Thus, $U|1\rangle = c_1|1\rangle$. We conclude that $U = c_1 I$, since

$$U|g\rangle = U X_g |1\rangle = X_g U|1\rangle = c_1 X_g |1\rangle = c_1 |g\rangle. \quad (6)$$

We now move on to point (5). By assumption, $Z_\chi U$ equals $U Z_\chi$ up to a phase for every $\chi \in \widehat{G}$. The map $\widehat{G} \rightarrow \mathbb{C}^\times$ sending χ to this phase is clearly a homomorphism. Since every character on $\widehat{G}$ is induced by application on a group element, there exists $g \in G$ such that $Z_\chi U = \chi(g) U Z_\chi$ for all $\chi \in \widehat{G}$. If $U|1\rangle = \sum_{h \in G} c_h |h\rangle$ as before, then we have $\chi(h)c_h = \chi(g)c_h$. Thus, $U|1\rangle = c_g |g\rangle$.

Now, we know by assumption that UX_h equals X_hU up to a phase. The map $G \rightarrow \mathbb{C}^\times$ sending a group element to the phase it induces is a homomorphism, and thus there exists a character χ such that $UX_h = \chi(h)X_hU$. Hence,

$$U|h\rangle = UX_h|1\rangle = \chi(h)X_hU|1\rangle = c_g\chi(h)X_h|g\rangle = c_g\chi(h)|hg\rangle. \quad (7)$$

Thus, $U = c_g X_g Z_\chi$ so U is a Pauli operator as desired. $\square$

3. The G -Clifford Group

Given a finite abelian group G , the G -Clifford group is

$$\text{Cliff}(G) = \{U : \mathbb{C}[G] \rightarrow \mathbb{C}[G] \text{ s.t. } UMU^\dagger \in \text{Pauli}(G), \forall M \in \text{Pauli}(G)\}. \quad (8)$$

The qubit Clifford group can be generated by the Hadamard gate, S gate, and controlled- X gate as shown in Ref. [3]. We now describe the generalizations of these gates to the G -Clifford group, as introduced in Ref. [7]. We will see in Theorem 1 that these families are enough to generate all of $\text{Cliff}(G)$.

The automorphism gates A_τ are parameterized by automorphisms $\tau : G \rightarrow G$. They act by

$$\begin{aligned} A_\tau : \mathbb{C}[G] &\rightarrow \mathbb{C}[G]. \\ |g\rangle &\mapsto |\tau(g)\rangle \end{aligned} \quad (9)$$

For example, if $G = \mathbb{Z}_2 \times \mathbb{Z}_2$ the automorphism $\tau((a, b)) = (a, a + b)$ induces the usual qubit CX gate.

The quadratic phase gates S_ξ are parameterized by quadratic forms $\xi : G \rightarrow \mathbb{C}^\times$. That is, maps ξ such that the assignment

$$g, h \mapsto \frac{\xi(gh)}{\xi(g)\xi(h)} \quad (10)$$

is a character in each component individually. They act by

$$\begin{aligned} S_\xi : \mathbb{C}[G] &\rightarrow \mathbb{C}[G]. \\ |g\rangle &\mapsto \xi(g)|g\rangle \end{aligned} \quad (11)$$

We do not require our quadratic forms to be homogeneous, that is, it can be the case that $\xi(g^{-1}) \neq \xi(g)$. This implies that $\xi(g^n) = \xi(g)^{\frac{(n+1)n}{2}} \xi(g^{-1})^{\frac{(n-1)n}{2}}$.

The G -Fourier transform is the map

$$\begin{aligned} \mathcal{F} : \mathbb{C}[G] &\rightarrow \mathbb{C}[\widehat{G}] \\ |g\rangle &\mapsto \frac{1}{\sqrt{|G|}} \sum_{\chi \in \widehat{G}} \overline{\chi(g)} |\chi\rangle \end{aligned} \quad (12)$$

Naively, the G -Fourier transform is not a Clifford gate because its codomain is $\mathbb{C}[\widehat{G}]$, not $\mathbb{C}[G]$. For this reason one must parameterize the Fourier transform by some isomorphism $i : \widehat{G} \xrightarrow{\sim} G$, defining

$$\begin{aligned} \mathcal{F}_i : \mathbb{C}[G] &\rightarrow \mathbb{C}[G]. \\ |g\rangle &\mapsto \frac{1}{\sqrt{|G|}} \sum_{\chi \in \widehat{G}} \overline{\chi(g)} |i(\chi)\rangle. \end{aligned} \quad (13)$$

The formula for the inverse Fourier transform is

$$\mathcal{F}_i^\dagger : \mathbb{C}[G] \rightarrow \mathbb{C}[G], \quad (14)$$

$$|g\rangle \mapsto \frac{1}{\sqrt{|G|}} \sum_{\chi \in \widehat{G}} \chi(g) |\chi \circ i\rangle.$$

where we identify $\chi \circ i$ with a group element via the double dual isomorphism. We observe that $\chi \circ i = i(\chi)$ if and only if for all $\chi' \in \widehat{G}$ the equation $\chi'(i(\chi)) = \chi(i(\chi'))$ holds, which in general it does not.

Proposition 2. *Let G be a finite abelian group. For all $g \in G$, $\chi \in \widehat{G}$ we have that*

1. A_τ is a Clifford gate, for all automorphisms $\tau : G \xrightarrow{\sim} G$. Namely,

$$A_\tau X_g A_\tau^\dagger = X_{\tau(g)}, \quad (15)$$

$$A_\tau Z_\chi A_\tau^\dagger = Z_{\chi \circ \tau^{-1}}. \quad (16)$$

2. S_ξ is a Clifford gate, for quadratic forms $\xi : G \rightarrow \mathbb{C}^\times$. Namely,

$$S_\xi X_g S_\xi^\dagger = \xi(g) X_g Z_{b_\xi(g, -)}, \quad (17)$$

$$S_\xi Z_\chi S_\xi^\dagger = Z_\chi. \quad (18)$$

where $b_\xi(g, h) = \xi(gh) / (\xi(g)\xi(h))$

3. $\mathcal{F}_i$ is a Clifford gate, for isomorphisms $i : \widehat{G} \xrightarrow{\sim} G$. Namely,

$$\mathcal{F}_i X_g \mathcal{F}_i^\dagger = Z_{g \circ i^{-1}}, \quad (19)$$

$$\mathcal{F}_i Z_\chi \mathcal{F}_i^\dagger = X_{i(\chi)}, \quad (20)$$

where $\chi \circ i \in \widehat{G}$ is identified with an element of G via the double dual isomorphism.

Proof. These follow from direct calculations. $\square$

In Section 7 we prove the converse:

Theorem 1. *Let G be a finite abelian group. Every Clifford gate on G can be constructed from $\leq 5 \log_2 |G|$ gates of the form A_τ , S_ξ , and $\mathcal{F}_i$.*

It was demonstrated in Ref. [8] for every finite group G that circuits consisting of automorphism gates, quadratic phase gates, and Fourier gates can be efficiently simulated by classical computers. This result was extended in Ref. [7], which allowed the quantum computer to perform mid-circuit G -Pauli measurements. Thus, from Theorem 1 one concludes that the results of Refs. [7,8] apply to all G -Clifford circuits.

We now discuss $\text{Cliff}(G^n)$, which we refer to as the group of n -qudit G -Clifford gates.

Proposition 3. *Every G -Clifford operation can be decomposed into one-qudit G -Clifford gates and two-qudit automorphism gates.*

Proof. In light of Theorem 1, we only need to demonstrate the result for the A_τ , S_ξ , and $\mathcal{F}_i$ gates. Choosing an appropriate isomorphism i , the Fourier transform on $\mathbb{C}[G^n]$ is the tensor product of the Fourier transform on components. Thus, the global Fourier transform decomposes into one-qudit Clifford gates because the Fourier transform on each component is itself Clifford.

We now move on to the case of quadratic phase gates. Let ξ be a quadratic form on G^n . We can decompose

$$\xi(g_1, g_2, \dots, g_n) = \prod_{k=1}^n \xi_k(g_k) \cdot \prod_{1 \leq j < k \leq n} b_{jk}(g_j, g_k) \quad (21)$$

where $\xi_k(g) = \xi(1, \dots, g, \dots, 1)$ is ξ with a non-identity entry only at the k index, $b_{jk}(h, k) = b((1, \dots, h, \dots, 1), (1, \dots, g, \dots, 1))$ with non-identity entries only at indices j, k , and $b(g, h) = \xi(gh) / (\xi(g)\xi(h))$.

To implement S_ξ , we implement gates which act by each of the constituent phases within equation (21). The terms $\xi_k(g_k)$ are one-qudit G -Clifford gates since each ξ_k is itself a quadratic form on G . To realize the b_{jk} phases, for any symmetric bilinear map $b : G \times G \rightarrow \mathbb{C}^\times$ we construct a decomposition of the two-qudit G -Clifford gate $|(g_1, g_2)\rangle \mapsto b(g_1, g_2) |(g_1, g_2)\rangle$ into one-qudit G -Cliffords and two-qudit automorphism gates.

We decompose G in terms of cyclic groups, $G \cong \prod_{j=1}^\ell \mathbb{Z}_{r_j}$ for some $\ell \geq 0, r_j \geq 2$. Using the bilinearity of b , we find that

$$b((s_1, \dots, s_\ell), (s'_1, \dots, s'_\ell)) = \prod_{1 \leq j < k \leq \ell} c_{jk}^{s_j s'_k} \quad (22)$$

where $c_{jk} = b((0, \dots, 1, \dots, 0), (0, \dots, 1, \dots, 0))$ with non-zero entries only indices j, k . It thus suffices to construct a gate which realizes the phases $c_{jk}^{s_j s'_k}$. To do this, we first apply the two-qudit automorphism gate parameterized by the automorphism $\tau : G \times G \rightarrow G \times G$, $\tau((s_1, \dots, s_\ell), (s'_1, \dots, s'_\ell)) = ((s_1, \dots, s_j s'_k, \dots, s_\ell), (s'_1, \dots, s'_\ell))$. Then, we apply the one-qudit phase gate S_χ associated to the character $\chi((s_1, \dots, s_\ell)) = c_{jk}^{s_j}$. We then apply the two-qudit automorphism gate parameterized by the automorphism τ^{-1} .

The last case is automorphism gates. This amounts to asking whether every automorphisms of G^n can be written as a composition of automorphisms which affect only two of the components. To demonstrate this we appeal to the matrix theory of automorphisms, described in detail in Ref. [10] and used in Section 7 to prove Theorem 1. Every automorphism can be embedded into a matrix group with modular entries. Gaussian elimination shows that every invertible matrix can be row-reduced to the identity matrix. Each step in row reduction touches at most two rows, and hence can be implemented by an automorphism which touches at most two components. Hence, every automorphism can be decomposed as an iterated composition of automorphisms which touch at most two components. $\square$

We observe that Proposition 3 does not imply that every G -Clifford operation can be turned into one-qudit gates and CX gates. In particular, there are automorphism gates which cannot be decomposed into one-qudit automorphisms and CX automorphisms. This is in contrast to the case when $G = \mathbb{Z}_d$ is cyclic, where every Clifford can be generated by one-qudit gates and CX only. The generalized CX gate is defined as follows:

$$\begin{aligned} CX : \mathbb{C}[G \times G] &\rightarrow \mathbb{C}[G \times G]. \\ |g\rangle |h\rangle &\mapsto |g\rangle |gh\rangle \end{aligned} \quad (23)$$

This gate is visualized as a circuit via

$$\begin{array}{c} \bullet \\ | \\ \boxed{X} \end{array} \quad (24)$$

The following proposition characterizes the behavior of the CX gate:

Proposition 4. *Let G be a finite abelian group. The CX gate is Clifford. Explicitly,*

$$\begin{array}{c} \bullet \\ | \\ \boxed{X} \end{array} \boxed{X_g} = \begin{array}{c} \boxed{X_g} \bullet \\ | \\ \boxed{X_g^{-1}} \boxed{X} \end{array} \quad (25)$$

$$\begin{array}{c} \bullet \\ | \\ \boxed{X} \end{array} \boxed{Z_\chi} = \begin{array}{c} \boxed{Z_\chi} \bullet \\ | \\ \boxed{X} \end{array} \quad (26)$$

$$\begin{array}{c} \bullet \\ | \\ \boxed{X} \end{array} \boxed{X_g} = \begin{array}{c} \bullet \\ | \\ \boxed{X_g} \end{array} \boxed{X} \quad (27)$$

$$\begin{array}{c} \bullet \\ | \\ \boxed{X} \end{array} \boxed{Z_\chi} = \begin{array}{c} \boxed{Z_\chi} \bullet \\ | \\ \boxed{Z_\chi} \boxed{X} \end{array} \quad (28)$$

$$\frac{1}{\sqrt{|G|}} \sum_{g \in G} \xi(g) |g\rangle \begin{array}{c} \bullet \\ | \\ \text{---} \end{array} \begin{array}{c} \boxed{S_{b_{\xi}(k,-)}} \\ \text{---} \end{array} = \begin{array}{c} \boxed{S_{\xi}} \\ \text{---} \end{array} \quad (32)$$

where k is the result of the measurement on the $\mathbf{Z}$ measurement, and $b_{\xi}(k, g) = \xi(kg) / (\xi(k)\xi(g))$.

Proof. We apply the circuit to the state $|g\rangle$. After applying $CX^{\dagger}$, the state is

$$\frac{1}{\sqrt{|G|}} \sum_{h \in G} \xi(h) |g\rangle |g^{-1}h\rangle. \quad (33)$$

Measuring $k = g^{-1}h$ results in the state $\xi(gk) |g\rangle |k\rangle$. Applying $S_{b_{\xi}(k,-)}$ yields $\xi(g)\xi(k) |g\rangle |k\rangle$. Since $\xi(k)$ is a global phase, the result is as desired. $\square$

Wherever $\xi : G \rightarrow U(1)$ is a function such that $b_{\xi}(k, -)$ is a quadratic form for every $k \in G$, Proposition 7 gives an algorithm for performing the gate S_{ξ} using only G -Cliffords and an ancillary state of the form $|G|^{-1/2} \sum_{g \in G} \xi(g) |g\rangle$. Choosing suitable ξ , the G -Clifford gates along with S_{ξ} can be used to perform universal quantum computing, following the techniques from for cyclic qudits presented in Ref. [11].

6. Fourier Transform on Split Subgroups

Whenever there is an equality of finite abelian groups $G = H \times K$, the Fourier transform on H times the identity gate on K is a Clifford gate on $G = H \times K$. In this section we show this H -Fourier transform gate can be decomposed into elementary G -Cliffords, namely, in terms of the Fourier transform on G . This is a necessary step in our proof of Theorem 1, which allows us to decompose every G -Clifford into elementary G -Cliffords.

Theorem 2. Let $\xi : G \rightarrow \mathbb{C}^{\times}$ be a non-degenerate quadratic form. Given $\chi \in \hat{G}$ let $i_{\xi}(\chi)$ be the unique element of G such that

$$\frac{\xi(g)\xi(i_{\xi}(\chi))}{\xi(gi_{\xi}(\chi))} = \chi(g), \quad \forall g \in G. \quad (34)$$

1. $(F_{i_{\xi}} S_{\xi})^3 = I$ up to global phase
2. $F_{i_{\xi}}^2 = A_{(-)^{-1}}$, where $A_{(-)^{-1}}$ is the automorphism gate associated to the inversion automorphism, $g \mapsto g^{-1}$.
3. Let H be another finite group, and let $i : \hat{H} \xrightarrow{\sim} H$ be any isomorphism. Letting the top qudit denote the Hilbert space $\mathbb{C}[G]$ and letting the bottom qudit denote $\mathbb{C}[H]$, we have that

$$\begin{array}{c} \boxed{F_{i_{\xi}}} \\ \text{---} \end{array} = \begin{array}{c} \boxed{S_{\xi}} \\ \text{---} \end{array} \begin{array}{c} \boxed{\mathcal{F}_{i_{\xi} \times i}} \\ \text{---} \end{array} \begin{array}{c} \boxed{S_{\xi}} \\ \text{---} \end{array} \begin{array}{c} \boxed{\mathcal{F}_{i_{\xi} \times i}} \\ \text{---} \end{array} \begin{array}{c} \boxed{S_{\xi}} \\ \text{---} \end{array} \begin{array}{c} \boxed{A_{(-)^{-1}}} \\ \text{---} \end{array} \quad (35)$$

Proof. We begin by proving part (1). Choose $g \in G$. We compute

$$(\mathcal{F}_{i_{\xi}} S_{\xi})^3 |g\rangle = \frac{\mathcal{F}_{i_{\xi}} S_{\xi} \mathcal{F}_{i_{\xi}}}{\sqrt{|G|}} \sum_{\chi \in \hat{G}} \xi(i_{\xi}(\chi)) \xi(g) \overline{\chi(g)} |i_{\xi}(\chi)\rangle. \quad (36)$$

By the defining formula of $i_{\xi}(\chi)$ we get that $\xi(i_{\xi}(\chi)) \xi(g) \overline{\chi(g)} = \xi(gi_{\xi}(\chi))$. Hence, changing variables via $h = gi_{\xi}(\chi)$ we arrive at

$$(\mathcal{F}_{i_{\xi}} S_{\xi})^3 |g\rangle = \frac{\mathcal{F}_{i_{\xi}} S_{\xi} \mathcal{F}_{i_{\xi}}}{\sqrt{|G|}} \sum_{h \in G} \xi(h) |g^{-1}h\rangle. \quad (37)$$

Expanding further, we obtain

$$(\mathcal{F}_{i_{\xi}} S_{\xi})^3 |g\rangle = \frac{\mathcal{F}_{i_{\xi}}}{|G|} \sum_{\chi \in \hat{G}} \sum_{h \in G} \xi(h) \xi(i_{\xi}(\chi)) \overline{\chi(h)} \chi(g) |i_{\xi}(\chi)\rangle. \quad (38)$$

Applying the defining relation $\xi(h) \xi(i_{\xi}(\chi)) \overline{\chi(h)} = \xi(hi_{\xi}(\chi))$ and changing variables via $h \mapsto h \cdot \overline{i_{\xi}(\chi)}$ gives

$$(\mathcal{F}_{i_\xi} S_\xi)^3 |g\rangle = \left(\frac{1}{\sqrt{|G|}} \sum_{h \in G} \xi(h) \right) \cdot \frac{\mathcal{F}_{i_\xi}}{\sqrt{|G|}} \sum_{\chi \in \widehat{G}} \chi(g) |i_\xi(\chi)\rangle \quad (39)$$

$$= \left(\frac{1}{\sqrt{|G|}} \sum_{h \in G} \xi(h) \right) |g\rangle. \quad (40)$$

Since $|g\rangle$ was chosen arbitrarily and the phase has no dependence on g , we conclude the result. Part (2) follows from direct calculation, and part (3) follows from the first two. $\square$

7. The Generating Set of Clifford Gates

In this section we prove Theorem 1, which asserts that every G -Clifford gate can be efficiently decomposed into Fourier, quadratic phase, and automorphism gates. Our proof is in terms of the algebra of the symplectic group, which we recall now. Every Clifford operator U induces a map $\text{Pauli}(G)/U(1) \rightarrow \text{Pauli}(G)/U(1)$ by sending P to $UPU^\dagger$. Seeing as $\text{Pauli}(G)/U(1) \cong G \times \widehat{G}$, we get a natural map $\text{Cliff}(G) \rightarrow \text{Aut}(G \times \widehat{G})$. To understand $\text{Cliff}(G)$ we study the properties of this map. Define the symplectic group on G to be

$$\text{Sp}(G) = \{\sigma \in \text{Aut}(G \times \widehat{G}) \text{ s.t. } \beta(\sigma(x), \sigma(y)) = \beta(x, y)\}, \quad (41)$$

where β is the bilinear form

$$\begin{aligned} \beta : (G \times \widehat{G}) \times (G \times \widehat{G}) &\rightarrow \mathbb{C}^\times \\ (g_0, \chi_0) \times (g_1, \chi_1) &\mapsto \chi_0(g_1) \overline{\chi_1(g_0)}. \end{aligned} \quad (42)$$

Proposition 8. *The image of the natural map $\text{Cliff}(G) \rightarrow \text{Aut}(G \times \widehat{G})$ is contained in $\text{Sp}(G)$, and the sequence*

$$0 \rightarrow \text{Pauli}(G) \rightarrow \text{Cliff}(G) \rightarrow \text{Sp}(G) \quad (43)$$

is exact.

Proof. To begin, we observe that for every pair of pairs $(g_0, \chi_0), (g_1, \chi_1) \in G \times \widehat{G}$ we have that

$$(X_{g_0} Z_{\chi_0})(X_{g_1} Z_{\chi_1}) = \chi_0(g_1) \overline{\chi_1(g_0)} (X_{g_1} Z_{\chi_1})(X_{g_0} Z_{\chi_0}). \quad (44)$$

Thus, we can re-cast $\beta((g_0, \chi_0), (g_1, \chi_1))$ as the relative phase that appears upon commuting $X_{g_0} Z_{\chi_0}$ and $X_{g_1} Z_{\chi_1}$. Conjugating by $U \in \text{Cliff}(G)$ must preserve this relative phase. Thus, the image of U in $\text{Aut}(G \times \widehat{G})$ must preserve $\beta(x, y)$, and thus the image of U must lie in $\text{Sp}(G)$.

The kernel of the map $\text{Cliff}(G) \rightarrow \text{Sp}(G)$ consists of all matrices which act trivially on $\text{Pauli}(G)/U(1)$. That is, matrices which commute with $\text{Pauli}(G)$ up to phase. By Proposition 2, these are exactly the Pauli matrices. $\square$

We will make use of the group of symmetric bilinear forms:

$$\text{SymBil}(G) = \{b : G \times G \rightarrow \mathbb{C}^\times \text{ s.t. } b(x, y) = b(y, x)\}. \quad (45)$$

Every symmetric bilinear form b induces a map $\tilde{b} : G \rightarrow \widehat{G}$ sending g to $b(g, -)$. This map satisfies $\tilde{b}(x)(y) = \tilde{b}(y)(x)$. Similarly, every symmetric homomorphism $G \rightarrow \widehat{G}$ induces a symmetric bilinear form. We will conflate symmetric bilinear forms and their induced homomorphisms $G \rightarrow \widehat{G}$. Letting $\text{Quad}(G)$ denote the group of quadratic forms, we have a map $\text{Quad}(G) \rightarrow \text{SymBil}(G)$ defined by sending $\xi : G \rightarrow \mathbb{C}^\times$ to $b(g, h) = \xi(gh)/(\xi(g)\xi(h))$.

Lemma 1. *For any finite group G , we have a short exact sequence*

$$0 \rightarrow \widehat{G} \rightarrow \text{Quad}(G) \rightarrow \text{SymBil}(G) \rightarrow 0. \quad (46)$$

Proof. A modern exposition of this result is given in Theorem 2.1 of Ref. [12]. $\square$

We now describe the matrix theory of automorphisms (c.f., for instance, Ref. [10]). In this theory, group elements correspond to vectors and endomorphisms correspond to matrices. Matrix-vector products and matrix-matrix products correspond to application of endomorphisms of composition of endomorphisms respectively. The fundamental theorem of finite abelian groups tells us that

$$G \cong \mathbb{Z}_{q_0} \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \dots \times \mathbb{Z}_{q_d} \quad (47)$$

with $q_j | q_{j-1}$. We write elements of $G \times \widehat{G}$ as vectors

$$\begin{pmatrix} \mathbb{Z}_{q_0} \\ \dots \\ \mathbb{Z}_{q_d} \\ \widehat{\mathbb{Z}}_{q_0} \\ \dots \\ \widehat{\mathbb{Z}}_{q_d} \end{pmatrix} \begin{pmatrix} \dots \\ \dots \\ \dots \\ \dots \\ \dots \end{pmatrix} \quad (48)$$

We write elements of the endomorphism group $\text{End}(G \times \widehat{G})$ as matrices. To compare cyclic groups of different orders, we view each $\mathbb{Z}_{q_j}$ as the subgroup of $\mathbb{Z}_{q_0}$ consisting of multiples of q_0/q_j . For convenience with comparison between group elements and characters we canonically identify $\widehat{\mathbb{Z}}_{q_j}$ with $\mathbb{Z}_{q_j}$ by working with the distinguished generator $n \mapsto e^{2\pi i n / q_j}$.

Every homomorphism between cyclic groups is a scalar multiplication, and as such we write the entries of the matrix as integers. For example, if $G = \mathbb{Z}_4 \times \mathbb{Z}_2$ we have the matrix equation

$$\begin{array}{cc} \mathbb{Z}_4 & \mathbb{Z}_2 \\ \mathbb{Z}_4 & \mathbb{Z}_2 \end{array} \begin{pmatrix} 2 & 1 \\ 2 & 0 \\ 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 3 & 0 \\ 2 & 0 \\ 0 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 3 \\ 2 \end{pmatrix} = \begin{pmatrix} 2 \cdot 1 + 1 \cdot 0 + 3 \cdot 3 + 0 \cdot 2 \\ 2 \cdot 1 + 0 \cdot 0 + 2 \cdot 3 + 0 \cdot 2 \\ 1 \cdot 1 + 0 \cdot 0 + 0 \cdot 3 + 1 \cdot 2 \\ 0 \cdot 1 + 1 \cdot 0 + 0 \cdot 3 + 1 \cdot 2 \end{pmatrix} = \begin{pmatrix} 3 \\ 0 \\ 3 \\ 2 \end{pmatrix} \quad (49)$$

Our strategy for proving Theorem 1 is as follows. Representing automorphisms as matrices, we will use row-reduction operations to show that every matrix in $\text{Sp}(G)$ can be decomposed into products of the matrices associated to A_τ , S_ξ , $\mathcal{F}_i$. This shows that the subgroup generated by the A_τ , S_ξ , $\mathcal{F}_i$ surjects onto $\text{Sp}(G)$. Combining with Proposition 8 we can conclude the result.

Proof of Theorem 1. We begin with a generic automorphism of $G \times \widehat{G}$ in $\text{Sp}(G)$ and reduce to the identity matrix using automorphisms of the form A_τ , S_ξ , and $\mathcal{F}_i$. We proceed by induction on the number of cyclic factors in the canonical decomposition of G . Suppose that we can always reduce elements of $\text{Sp}(G)$ to matrices with 0s and 1s in the following configuration, and arbitrarily elements elsewhere

$$\begin{array}{cc} \mathbb{Z}_{q_0} & \dots & \mathbb{Z}_{q_d} & \widehat{\mathbb{Z}}_{q_0} & \dots & \widehat{\mathbb{Z}}_{q_d} \\ \mathbb{Z}_{q_0} & \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 0 & 0 & 0 \end{array} \right) \\ \dots & \left(\begin{array}{ccc|ccc} 0 & \dots & \dots & 0 & \dots & \dots \end{array} \right) \\ \mathbb{Z}_{q_d} & \left(\begin{array}{ccc|ccc} 0 & \dots & \dots & 0 & \dots & \dots \end{array} \right) \\ \widehat{\mathbb{Z}}_{q_0} & \left(\begin{array}{ccc|ccc} 0 & 0 & 0 & 1 & 0 & 0 \end{array} \right) \\ \dots & \left(\begin{array}{ccc|ccc} 0 & \dots & \dots & 0 & \dots & \dots \end{array} \right) \\ \widehat{\mathbb{Z}}_{q_d} & \left(\begin{array}{ccc|ccc} 0 & \dots & \dots & 0 & \dots & \dots \end{array} \right) \end{array} \quad (50)$$

Then, further row reductions can be performed on the factors $\mathbb{Z}_{q_1} \dots \mathbb{Z}_{q_d}$ without affecting the $\mathbb{Z}_{q_0}$ -entries. This is true for A_τ and S_ξ gates because applying automorphisms and phases on one collection of cyclic factors does not affect the others, and it is true for $\mathcal{F}_i$ gates because we can apply partial Fourier transforms by Proposition 2. In particular, by induction we would arrive at a proof of the main result. Thus, the proof amounts to finding a series of reductions to arrive at a matrix of this form. We begin the process of finding such moves with a generic matrix, as below:

$$\begin{array}{c}
\mathbb{Z}_{q_0} \quad \dots \quad \mathbb{Z}_{q_d} \quad \widehat{\mathbb{Z}}_{q_0} \quad \dots \quad \widehat{\mathbb{Z}}_{q_d} \\
\begin{pmatrix}
r_0 & \dots & \dots & \dots & \dots & \dots \\
\dots & \dots & \dots & \dots & \dots & \dots \\
r_d & \dots & \dots & \dots & \dots & \dots \\
r'_0 & \dots & \dots & \dots & \dots & \dots \\
\dots & \dots & \dots & \dots & \dots & \dots \\
r'_d & \dots & \dots & \dots & \dots & \dots
\end{pmatrix}
\end{array} \tag{51}$$

We start by applying S_{ξ} operators. By Bézout's lemma, there exist integers k_i such that $r_i + k_i r'_i = \gcd(r_i, r'_i)$ in $\mathbb{Z}_{q_i}$. Let b be the map which acts as multiplication by k_i on the $\mathbb{Z}_{q_i}$ component. By the short exact sequence of Lemma 1, there exists some quadratic form ξ such that $b(g, -) = \xi(g \cdot -) / (\xi(g)\xi(-))$. Postcomposing with S_{ξ} and using the commutation relation in Proposition 2, we reduce our matrix to

$$\begin{array}{c}
\mathbb{Z}_{q_0} \quad \dots \quad \mathbb{Z}_{q_d} \quad \widehat{\mathbb{Z}}_{q_0} \quad \dots \quad \widehat{\mathbb{Z}}_{q_d} \\
\begin{pmatrix}
r_0 & \dots & \dots & \dots & \dots & \dots \\
\dots & \dots & \dots & \dots & \dots & \dots \\
r_d & \dots & \dots & \dots & \dots & \dots \\
\gcd(r_0, r'_0) & \dots & \dots & \dots & \dots & \dots \\
\dots & \dots & \dots & \dots & \dots & \dots \\
\gcd(r_d, r'_d) & \dots & \dots & \dots & \dots & \dots
\end{pmatrix}
\end{array} \tag{52}$$

Now, let $i : G \xrightarrow{\sim} \widehat{G}$ be the isomorphism induced by our identification $\mathbb{Z}_{q_i} \cong \widehat{\mathbb{Z}}_{q_i}$. Postcomposing with the Fourier transform $\mathcal{F}_i$ has the effect of swapping the $\mathbb{Z}_{q_i}$ and $\widehat{\mathbb{Z}}_{q_i}$ components by Proposition 2. Thus, we arrive at

$$\begin{array}{c}
\mathbb{Z}_{q_0} \quad \dots \quad \mathbb{Z}_{q_d} \quad \widehat{\mathbb{Z}}_{q_0} \quad \dots \quad \widehat{\mathbb{Z}}_{q_d} \\
\begin{pmatrix}
\gcd(r_0, r'_0) & \dots & \dots & \dots & \dots & \dots \\
\dots & \dots & \dots & \dots & \dots & \dots \\
\gcd(r_d, r'_d) & \dots & \dots & \dots & \dots & \dots \\
r_0 & \dots & \dots & \dots & \dots & \dots \\
\dots & \dots & \dots & \dots & \dots & \dots \\
r_d & \dots & \dots & \dots & \dots & \dots
\end{pmatrix}
\end{array} \tag{53}$$

Now, since the matrix is an automorphism the greatest common divisor of the first column must be 1. Hence, the greatest common divisor of $\gcd(r_0, r'_0) \dots \gcd(r_d, r'_d)$ is 1. Using the fact that q_0 is an element of maximal order in G , we know there exists an automorphism τ of G which maps $(\gcd(r_0, r'_0), \dots, \gcd(r_d, r'_d))$ to $(1, 0, \dots, 0)$. Applying A_{τ} and using the commutation relationship of Proposition 2, we reduce our matrix to

$$\begin{array}{c}
\mathbb{Z}_{q_0} \quad \dots \quad \mathbb{Z}_{q_d} \quad \widehat{\mathbb{Z}}_{q_0} \quad \dots \quad \widehat{\mathbb{Z}}_{q_d} \\
\begin{pmatrix}
1 & \dots & \dots & \dots & \dots & \dots \\
0 & \dots & \dots & \dots & \dots & \dots \\
0 & \dots & \dots & \dots & \dots & \dots \\
r''_0 & \dots & \dots & \dots & \dots & \dots \\
\dots & \dots & \dots & \dots & \dots & \dots \\
r''_d & \dots & \dots & \dots & \dots & \dots
\end{pmatrix}
\end{array} \tag{54}$$

Now, define the homomorphism $b : G \rightarrow \widehat{G}$ by sending $(1, 0, \dots, 0)$ to $(-r''_0, -r''_1, \dots, -r''_d)$ and acting by 0 on all other components. Using Lemma 1 we know that b is induced by a quadratic form ζ . Applying the corresponding S_{ζ} gate, we reduce without loss of generality to

$$\begin{array}{c}
\mathbb{Z}_{q_0} \quad \dots \quad \mathbb{Z}_{q_d} \quad \widehat{\mathbb{Z}}_{q_0} \quad \dots \quad \widehat{\mathbb{Z}}_{q_d} \\
\begin{pmatrix}
1 & \dots & \dots & \dots & \dots & \dots \\
0 & \dots & \dots & \dots & \dots & \dots \\
0 & \dots & \dots & \dots & \dots & \dots \\
0 & \dots & \dots & r & \dots & \dots \\
0 & \dots & \dots & \dots & \dots & \dots \\
0 & \dots & \dots & \dots & \dots & \dots
\end{pmatrix}
\end{array} \tag{55}$$

We now apply the symplectic condition of $\text{Sp}(G)$ to the pair of pairs $x = (g_0, 0)$ and $y = (0, \chi_1)$, where $g_0 = (1, 0, 0, \dots, 0)$, $\chi_1 = (1, 0, 0, \dots, 0)$. It gives us that $r = b(\sigma(x), \sigma(y)) = b(x, y) = 1$. We now repeat the same procedure as before but dualized, *postcomposing* with the appropriate A_τ and S_ξ gates. This reduces us to

$$\begin{array}{c}
\mathbb{Z}_{q_0} \quad \dots \quad \mathbb{Z}_{q_d} \quad \widehat{\mathbb{Z}}_{q_0} \quad \dots \quad \widehat{\mathbb{Z}}_{q_d} \\
\begin{pmatrix}
1 & \dots & \dots & 0 & \dots & \dots \\
0 & \dots & \dots & 0 & \dots & \dots \\
0 & \dots & \dots & 0 & \dots & \dots \\
0 & \dots & \dots & 1 & \dots & \dots \\
0 & \dots & \dots & 0 & \dots & \dots \\
0 & \dots & \dots & 0 & \dots & \dots
\end{pmatrix}
\end{array} \tag{56}$$

Importantly, such postcomposition does not affect the entries in the first column. We now apply the symplectic condition with the pair of pairs $x = (0, \chi_0)$ and $y = (g_1, \chi_1)$, where $\chi_0 = (1, 0, 0, \dots, 0)$. Varying g_1 and χ_1 , we conclude that the first row has all zeros after the 1st entry. Similarly, applying the symplectic condition with $x = (g_0, 0)$, $g_0 = (1, 0, 0, \dots, 0)$ we conclude that the $\widehat{\mathbb{Z}}_{q_0}$ row has all zeros outside of the $(\widehat{\mathbb{Z}}_{q_0}, \widehat{\mathbb{Z}}_{q_0})$ entry. Thus, we arrive at the reduction

$$\begin{array}{c}
\mathbb{Z}_{q_0} \quad \dots \quad \mathbb{Z}_{q_d} \quad \widehat{\mathbb{Z}}_{q_0} \quad \dots \quad \widehat{\mathbb{Z}}_{q_d} \\
\begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 \\
0 & \dots & \dots & 0 & \dots & \dots \\
0 & \dots & \dots & 0 & \dots & \dots \\
0 & 0 & 0 & 1 & 0 & 0 \\
0 & \dots & \dots & 0 & \dots & \dots \\
0 & \dots & \dots & 0 & \dots & \dots
\end{pmatrix}
\end{array} \tag{57}$$

By induction on the number of cyclic factors in G , we conclude the decomposition into elementary gates.

We now count how many gates were used in the decomposition. At every step in the induction, we used five gates. Namely, a quadratic phase gate, followed by a Fourier transform on a split subgroup, followed by an automorphism gate, followed by another quadratic phase gate, followed by another automorphism gate. The Fourier transform on a split subgroup is performed using the method in Proposition 2, which uses six elementary G -Clifford gates. So, the total number of gates is $10d$. Since $|G| \geq 2^d$, we get the desired bound. $\square$

Author Contributions

M.M. conceived the idea of the project, directed the research, and wrote the manuscript. M.M., J.H., K.D., and J.T. collaborated on the proof of Theorem 1. M.M. and J.T. collaborated on the revisions of the manuscript. All authors have read and agreed to the published version of the manuscript.

Funding

We thank BEIT.tech for hosting and funding this research in entirety.

Conflicts of Interest

The authors declare no conflicts of interest.

Data Availability Statement

No data was analyzed or generated during the study.

References

1. S. Bravyi and R. König (2013). “Classification of topologically protected gates for local stabilizer codes,” *Physical review letters*, vol. 110, no. 17, p. 170503.
2. B. Eastin and E. Knill (2009). “Restrictions on transversal encoded quantum gate sets,” *Physical review letters*, vol. 102, no. 11, p. 110502.
3. D. Gottesman (1998). “The heisenberg representation of quantum computers,” *arXiv preprint quant-ph/9807006*.
4. A. Y. Kitaev (2003). “Fault-tolerant quantum computation by anyons,” *Annals of physics*, vol. 303, no. 1, pp. 2–30.
5. E. Knill (1996). “Group representations, error bases and quantum codes,” *arXiv preprint quant-ph/9608049*.
6. E. Knill (1996). “Non-binary unitary error bases and quantum codes,” *arXiv preprint quant-ph/9608048*.
7. J. Bermejo-Vega and M. Van Den Nest (2014). “Classical simulations of abelian-group normalizer circuits with intermediate measurements,” *Quantum Information & Computation*, vol. 14, no. 3-4, pp. 181–216.
8. M. Van Den Nest (2013). “Efficient classical simulations of quantum fourier transforms and normalizer circuits over abelian groups,” *Quantum Information & Computation*, vol. 13, no. 11-12, pp. 1007–1037.
9. E. Hostens, J. Dehaene and B. De Moor (2005). “Stabilizer states and clifford operations for systems of arbitrary dimensions and modular arithmetic,” *Physical Review A*, vol. 71, no. 4, p. 042315.
10. C. J. Hillar and D. L. Rhea (2007). “Automorphisms of finite abelian groups,” *The American Mathematical Monthly*, vol. 114, no. 10, pp. 917–923.
11. Y. Wang, Z. Hu, B. C. Sanders and S. Kais (2020). “Qudits and high-dimensional quantum computing,” *Frontiers in Physics*, vol. 8, p. 589504.
12. T. Basak and R. Johnson (2015) “Indicators of tambara–yamagami categories and gauss sums,” *Algebra & Number Theory*, vol. 9, no. 8, pp. 1793–1823.