Generalizations of Various Results in Quantum Computation Theory to Mixed-Dimensional Quantum Systems

by

Randall S. Gay

A dissertation submitted to the Graduate Faculty of
Auburn University
in partial fulfillment of the
requirements for the Degree of
Doctor of Philosophy

Auburn, Alabama
May 1, 2021

Keywords: quantum system, generalization, abelian group, mixed-dimensional

Approved by

Randall R. Holmes, Professor Emeritus of Mathematics
Michel Smith, Professor of Mathematics
Huajun Huang, Associate Professor of Mathematics
Hans-Werner van Wyk, Assistant Professor of Mathematics

Abstract

The majority of the research in quantum computation theory is based on quantum mechanical systems consisting of quantum subsystems that are all of the same dimension. Following and expanding on the research conducted by Randall R. Holmes and Frédéric Texier in their paper "A Generalization of the Deutsch-Jozsa Quantum Algorithm", we generalize several results in quantum computation theory to quantum systems consisting of quantum subsystems of varying dimensions, which amounts to a generalization to arbitrary finite abelian groups. These results include the Bernstein-Vazirani algorithm, Simon's algorithm, the Pauli group and algebra, the Clifford group, and stabilizer codes. We also further generalize the Deutsch-Jozsa algorithm to arbitrary finite groups. Additionally, we expand on the topic of orthogonal complements of subgroups of finite abelian groups as introduced by Holmes and Texier, and we define the symplectic complement of a subgroup of a group $G \oplus G$, where G is a finite abelian group. Lastly, we define pseudo-unitarity and find results relating this definition to quantum computation theory, where the prefix 'pseudo' comes from the Moore-Penrose pseudo-inverse.

Acknowledgments

I would like to thank God for the wonders of the physical universe and the universe of the mind through which I can humbly explore. I would also like to thank my loving wife for her patience and understanding while I worked on a PhD and worked full-time on active duty in the US Navy while she took charge in raising our daughter to become the lovely and loquacious little girl she is. I would also like to thank my parents for raising me and loving me the way they did and for their guidance and encouragement throughout my life.

Table of Contents

Chapter 1

Introduction

The idea for quantum computing began to materialize in the last few decades of the 20^{th} century when scientists sought to combine information theory and quantum mechanics. In the 1990s, researchers devised the first algorithms that were entirely based on quantum mechanics, and they proved that these so-called quantum algorithms could, in theory, outperform any classical algorithm that used deterministic methods and give the correct answer with certainty [RP11, p. 1-3]. For example, the *Deutsch-Jozsa algorithm* (1992), the *Bernstein-Vazirani algorithm* (1992), and *Simon's algorithm* (1994) offer exponential speedup over their classical analogues [RP11, p. 141-144]. In 1994, inspired by Simon's algorithm, Peter Shor developed a polynomial-time quantum algorithm for factoring integers called *Shor's algorithm* [RP11, p. 163], and this discovery prompted widespread interest in quantum computing [RP11, p. 163]. However, due to the sheer number of unavoidable environmental interactions a quantum computer would suffer, Shor's algorithm was thought, at the time of its discovery, to not be of any practical use. Also, at the time no one had any ideas as to how one could perform error correction on a quantum computer since a straightforward application of classical methods to the quantum case was impossible. However, thanks to a surprising and clever use of classical techniques to quantum errors, researchers have been able to develop sophisticated quantum error correction techniques. One such technique for quantum error correction is the class of so-called *stabilizer codes* [RP11, p. 245].

Currently, most of the research in quantum computation is based on quantum systems that are entanglements of smaller quantum systems all of the same dimension. There is also the case where the smaller quantum systems are of differing, or *mixed*, dimensions. For example, there

is currently a considerable amount of research being conducted in the dynamics of a qubit-qutrit system, which is a quantum system in which a two-dimensional quantum system (qubit) is combined or entangled with a three-dimensional quantum system (qutrit).

The advantages of a quantum computer over a classical computer depend on the existence of a sufficiently large-scale quantum computer, which is only theoretical at this point. Companies like IBM, Honeywell, and others are making tremendous headway into the construction of the first quantum computer large enough to be of practical use. As of the year 2020, IBM's largest quantum computer contains 65 qubits, and the company promises to build a 1000-qubit quantum computer by 2023 [Cho20].

This paper has been inspired mainly by the work done by Randall R. Holmes and Frédéric Texier in their paper "A Generalization of the Deutsch-Jozsa Quantum Algorithm", as well as the work done by Daniel Gottesman in his paper "Fault-Tolerant Quantum Computation with Higher-Dimensional Systems". In this paper, we generalize the Deutsch-Jozsa problem and algorithm even further to arbitrary finite groups in Subsection 2.3, we apply the generalization of the Deutsch-Jozsa problem and algorithm to finite abelian groups by Holmes and Texier to generalize the Bernstein-Vazirani problem and algorithm in Subsection 2.4 and Simon's problem and algorithm in Subsection 2.5. We also generalize the so-called Pauli group in Subsection 4.2 and stabilizer codes in Subsection 4.6 to arbitrary finite abelian groups. We attempt to generalize the so-called Clifford group in Subsection 4.8, but we only get close and leave the reader with two open problems in this topic, namely Open Problems 4.8.1 and 4.8.2.

Chapter 2

Generalizations of Some Quantum Algorithms

2.1 Dirac Notation and Qudits

Since our goal is to make a generalization about quantum error correction, we will henceforth use notation from quantum mechanics, the so-called $Dirac$ notation, also known as *bra-ket* notation, where the words "bra" and "ket" come from splitting the word "braket", or "bracket", in two. A *bra* is a row vector represented by $\langle\psi|$ and a *ket* is a column vector represented by $|\varphi\rangle$, with $\langle\psi| = |\psi\rangle^T$, and $|\psi\rangle$ and $|\varphi\rangle$ belong to a vector space over $\mathbb{C}$ with their inner product being $\langle\psi|\varphi\rangle$. Using this notation, it follows that the outer product of $|\psi\rangle$ and $|\varphi\rangle$ is given by $|\varphi\rangle\langle\psi|$.

2.1.1 Definition. Let $n \in \mathbb{N}$. Set $H_n = \mathbb{C}^n$. We call the space H_n an *n-dimensional qudit* (or just *qudit* if there is no need to refer to the dimension). A 2-dimensional qudit is referred to as a *qubit* (a portmanteau of the words "quantum" and "bit"), and a 3-dimensional qudit is referred to as a *qutrit*.

2.1.2 Definition. Let $(G, \cdot)$ be a finite group and K be a field. We define the *group algebra* KG as the K-vector space with basis G together with the product defined for vectors $|v\rangle = \sum_{g\in G} a_g|g\rangle$ and $|w\rangle = \sum_{g'\in G} b_{g'}|g'\rangle$ in KG by the formula

$$|v\rangle \star |w\rangle = \left(\sum_{g\in G} a_g|g\rangle\right) \star \left(\sum_{g'\in G} b_{g'}|g'\rangle\right) = \sum_{g\in G}\sum_{g'\in G} a_g b_{g'}|g\cdot g'\rangle.$$

In addition, it is important to note that G can be taken to be abelian or non-abelian, where in the latter case, one has to be careful with the products $|g\rangle \star |g'\rangle$ and $|g'\rangle \star |g\rangle$ since they need not be equal in general.

2.1.3 Example. Let $G = \mathbb{Z}_4$ and $K = \mathbb{C}$. Let $|v\rangle = \mathbf{i}|0\rangle + (3 - 2\,\mathbf{i})|2\rangle$ and $|w\rangle = 3|0\rangle - 2\,\mathbf{i}|3\rangle$. Then $|v\rangle, |w\rangle \in KG$ and

$$\begin{aligned}
|v\rangle \star |w\rangle &= (\mathbf{i}|0\rangle + (3 - 2\,\mathbf{i})|2\rangle) \star (3|0\rangle - 2\,\mathbf{i}|3\rangle) \\
&= 3\,\mathbf{i}|0+0\rangle - 2\mathbf{i}^2|0+3\rangle + (9 - 6\mathbf{i})|2+0\rangle - (6\,\mathbf{i} - 4\,\mathbf{i}^2)|2+3\rangle \\
&= 3\,\mathbf{i}|0\rangle + 2|3\rangle + (9 - 6\,\mathbf{i})|2\rangle - (4 + 6\,\mathbf{i})|1\rangle \\
&= 3\,\mathbf{i}|0\rangle - (4 + 6\,\mathbf{i})|1\rangle + (9 - 6\,\mathbf{i})|2\rangle + 2|3\rangle.
\end{aligned}$$

2.2 The Holmes-Texier Generalization of the Deutsch-Jozsa Algorithm

Let $G = \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_n}$ for some positive integers m_i $(1 \leq i \leq n)$, and let m be the least common multiple of $m_1, m_2, \ldots, m_n$. For each integer i with $1 \leq i \leq n$, let H_{m_i} be an m_i-dimensional qudit. If m_i is even, then as an example, H_{m_i} could be taken to be the z-spin state space of a fermion, and if m_i is odd, then H_{m_i} could be taken to be the z-spin state space of a boson [HT03, p. 2].

Put $H' = H_{m_1} \otimes H_{m_2} \otimes \cdots \otimes H_{m_n}$, where the product $\otimes$ is the tensor product. We require an additional m-dimensional qudit H_m for the storage of images $f(a)$, where $f : G \to \mathbb{Z}_m$ is a function. The vector space $H := H' \otimes H_m$ has basis $\{|a\rangle|z\rangle \mid a \in G, z \in \mathbb{Z}_m\}$, where $|a\rangle|z\rangle : |a_1\rangle \otimes \cdots \otimes |a_n\rangle \otimes |z\rangle$ [HT03, p. 2].

2.2.1 Note. For the rest of the paper, we view H_{m_i} as the vector space of m_i-dimensional column vectors over $\mathbb{C}$ by identifying $|j\rangle$ for each $j \in \mathbb{Z}_{m_i}$ with the column vector having a one in the $(j+1)$st position and zeros elsewhere. Thus we view the set $\{|j\rangle \mid j \in \mathbb{Z}_{m_i}\}$ as the standard basis for H_{m_i}.

2.2.2 Definition. For a function $f : G \to \mathbb{Z}_m$, define $U_f : H \to H$ by

$$U_f(|a\rangle|z\rangle) = |a\rangle|z + f(a)\rangle,$$

for $a \in G$ and $z \in \mathbb{Z}_m$.

Under the assumption that $G = \mathbb{Z}_2^n$, the classical Deutsch-Jozsa Problem is stated as follows [RP11, p. 140]:

A function $f : G \to \mathbb{Z}_2$ is balanced if an equal number of input values to the function return 0 and 1. Given a function $f : G \to \mathbb{Z}_2$ that is known to be either constant or balanced, determine whether the function f is constant or balanced.

A traditional, deterministic algorithm must evaluate the function f at least $2^{n-1} + 1$ times to solve the problem with certainty. On the other hand, Deutsch and Jozsa discovered a quantum algorithm that uses the properties of quantum mechanics to solve the problem with a single evaluation of U_f [RP11, p. 141].

Instead of presenting the Deutsch-Jozsa Algorithm, we present the generalization of Holmes and Texier. Before we state the generalization of the problem, we must first state definitions integral to the problem statement.

Let $\mathcal{F}$ denote the additive group of functions $G \to \mathbb{Z}_m$, where m is the least common multiple of the m_i. For $f, g \in \mathcal{F}$, the sum $f + g$ is defined by $(f + g)(a) = f(a) + g(a)$, where the addition is modulo m. For $a \in G$, define $\iota_a \in \mathcal{F}$ by

$$\iota_a(b) = a \circ b = \sum_{i=1}^{n} a_i b_i \left(\frac{m}{m_i}\right) \cdot 1,$$

where $\sum_{i=1}^{n} a_i b_i \left(\frac{m}{m_i}\right) \in \mathbb{Z}$ and $1 \in \mathbb{Z}_m$. Since $\mathbb{Z}_m$ is a $\mathbb{Z}$-module, we have $\iota_a(b) \in \mathbb{Z}_m$ and thus ι_a is well-defined in that it maps to the indicated codomain.

Note that when $m_1 = m_2 = \cdots = m_n = m$, $a \circ b$ is the usual inner (dot) product of a and b. Also, observe that for fixed a and b, $\iota_a(b) = a \circ b = b \circ a = \iota_b(a)$.

Let $\epsilon \in \mathbb{C}$ be a primitive m^{th} root of unity, that is, $\epsilon^m = 1$ and $\epsilon^j \neq 1$ for all $0 < j < m$. A common example is $\epsilon = e^{2\pi i/m}$, where $i = \sqrt{-1}$, for instance.

2.2.3 Definition. For $f \in \mathcal{F}$, define

$$\varphi(f) = \sum_{a \in G} \epsilon^{f(a)} \in \mathbb{C}.$$

2.2.4 Definition. Given a subset P of G, we shall say that $f \in \mathcal{F}$ is *P-based* if $\varphi(\iota_a - f) = 0$ for all $a \in G \backslash P$.

The Holmes-Texier generalization of the Deutsch-Jozsa Problem is stated as follows:

Let $\{P_1, \ldots, P_t\}$ be a partition of G so that $G = P_1 \cup \cdots \cup P_t$ and $P_i \cap P_j = \emptyset$ for $i \neq j$. Let f be an element of $\mathcal{F}$ and suppose that f is P_k-based for some k. Then this k is uniquely determined (see Remark 1 below); we present a quantum algorithm for its determination. The Deutsch-Jozsa algorithm is recovered as a special case (see Remark 2).

The Algorithm. Recall that H_{m_i} is an m_i-dimensional qudit $(1 \leq i \leq n)$, $H' = H_{m_1} \otimes H_{m_2} \otimes \cdots \otimes H_{m_n}$, and $H = H' \otimes H_m$, where H_m is an m-dimensional qudit. Recall that $U_f : H \to H$ is defined by

$$U_f(|a\rangle|z\rangle) = |a\rangle|z + f(a)\rangle$$

for $a \in G$ and $z \in \mathbb{Z}_m$.

Now, define $W : H' \to H'$ and $\sigma : H_m \to H_m$ by

$$W(|b\rangle) = |A|^{-1/2} \sum_{a \in A} \epsilon^{b \circ a} |a\rangle,$$

for $b \in G$, and

$$\sigma(|z\rangle) = \epsilon^z |z\rangle,$$

for $z \in \mathbb{Z}_m$, respectively.

It is straightforward to prove that U_f, W, and σ are unitary. We initialize our system to the state $|0\rangle|0\rangle$ and then apply unitary operators as follows :

$$\begin{aligned}
|0\rangle|0\rangle &\overset{W\otimes 1}{\longmapsto} |G|^{-1/2} \sum_{a\in G} |a\rangle|0\rangle \\
&\overset{U_{-f}}{\longmapsto} |G|^{-1/2} \sum_{a\in G} |a\rangle|-f(a)\rangle \\
&\overset{1\otimes\sigma}{\longmapsto} |G|^{-1/2} \sum_{a\in G} |a\rangle\epsilon^{-f(a)}|-f(a)\rangle \\
&\overset{U_f}{\longmapsto} |G|^{-1/2} \sum_{a\in G} |a\rangle\epsilon^{-f(a)}|0\rangle \\
&\overset{W\otimes 1}{\longmapsto} |G|^{-1} \sum_{b\in G} |b\rangle|0\rangle \sum_{a\in G} \epsilon^{a\circ b}\epsilon^{-f(a)}.
\end{aligned}$$

Since $\sum_{a\in G} \epsilon^{a\circ b}\epsilon^{-f(a)} = \sum_{a\in G} \epsilon^{\iota_b(a)}\epsilon^{-f(a)} = \varphi(\iota_b - f)$, and since $\varphi(\iota_b - f) = 0$ for each $b \in A\backslash P_k$, due to f being P_k-based, this last expression equals

$$|G|^{-1} \sum_{b\in P_k} |b\rangle|0\rangle\varphi(\iota_b - f).$$

It follows that a measurement at this point will produce a state $|b\rangle$ for some $b \in P_k$, and as a result, k will be determined with certainty.

Remark 1. If $f \in \mathcal{F}$ is P_k-based, then it follows from the algorithm that f is not P_j-based for any $j \neq k$.

2.2.5 Theorem. *For a subset P of G and an element a of G, the function $\iota_a \in \mathcal{F}$ is $P - based$ if and only if $a \in P$.*

Let $f \in \mathcal{F}$ and let $B \subseteq G$. We say that f is $balanced$ on B if $f(B)$ is a coset C of a nontrivial subgroup of $\mathbb{Z}_m$ and the cardinality $\left|f|_B^{-1}(c)\right|$, where $c \in C$, does not depend on the choice of c. In other words, $f|_B$ takes on each element of C the same number of times. Note that if f is balanced on B, then, due to the nontriviality of the subgroup in the definition, f is not constant on B.

2.2.6 Theorem. *Let H be a subgroup of G. A homomorphism $f : G \to \mathbb{Z}_m$ is either constant on each coset of H or balanced on each coset of H.*

2.2.7 Lemma. *If B is a subset of G and f is a function in $\mathcal{F}$ that is balanced on B, then* $\sum_{b \in B} \epsilon^{f(b)} = 0$.

Let H be a subgroup of G. Let $\mathcal{F}_H$ denote the set of all functions in $\mathcal{F}$ that are either constant on every coset of H or balanced on every coset of H. Denote by $H^\perp$ the orthogonal complement relative to $\circ$ of H in G:

$$H^\perp = \{g \in G \mid g \circ h = 0 \text{ for all } h \in H\}.$$

2.2.8 Theorem. *Let H be a subgroup of G and let f be a function in $\mathcal{F}_H$.*

(1) f is constant on each coset of H if and only if f is $H^\perp$-based.

(2) f is balanced on each coset of H if and only if f is $G \backslash H^\perp$-based.

Remark 2. In the notation of the theorem, $\{H^\perp, G \backslash H^\perp\}$ is a partition of G, so the algorithm can be applied to distinguish between a function that is constant on each coset of H and one that is balanced on each coset of H. In particular, this applies to the choice $H = G$. Considering the special case $m_1 = m_2 = \cdots = m_n$, we see that the algorithm can be used to distinguish between a function that is constant on G and a function that takes on each of the values $0, 1, 2, \ldots, m-1$ an equal number of times. When $m = 2$, this is precisely the situation for the Deutsch-Jozsa algorithm.

2.3 A Generalization of the Deutsch-Jozsa Algorithm to Arbitrary Finite Groups

The Deutsch-Jozsa Algorithm takes a function $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ that is known to be either constant or balanced on the domain, that is, f either maps all of the domain to one value (constant) or it maps half to 0 and half to 1 (balanced), and it determines whether f is constant or balanced. This algorithm was generalized by Holmes and Texier to a function $f : G \to \mathbb{Z}_m$, where $G = \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_n}$ and where m is the least common multiple of $m_1, m_2, \ldots, m_n$. Now, we wish to generalize the problem further by replacing G with an arbitrary finite group (not necessarily abelian). Before we state the problem, we define the notion of a function being balanced on a subset of its domain.

2.3.1 Definition. Let G and G^* be groups. A function $f : G \to G^*$ is said to be *balanced* on a subset B of G if $f(B)$ is a coset C of a nontrivial subgroup of G^* and the cardinality $|f|_B^{-1}(c)|$, where $c \in C$, does not depend on the choice of c.

Note that if f is balanced on B, then, due to the nontriviality of the subgroup in the definition, f is not constant on B.

Problem: Let G be a finite group, let H be a subgroup of G, and let $f : G \to \mathbb{Z}_m$ be a function that is constant on the cosets of the commutator subgroup G' of G in G. Assuming it is known that f is either constant on every coset of H or is balanced on every coset of H, determine which is the case.

2.3.2 Note. When referring to the cosets of a subgroup of a (general) finite group G, we will not be specific as to whether we are referring to left or right cosets, since the results will be true regardless.

2.3.3 Theorem. *Let G and G^* be groups, let $\varphi : G \to G^*$ be a homomorphism, and let H be a subgroup of G. The function φ is either constant or balanced on each coset of H. More specifically, φ is constant on each coset of H if H is contained in the kernel of φ, and it is balanced on each coset of H otherwise.*

Proof. Suppose $H \subseteq \ker \varphi$. Thus $\varphi(h) = e^*$ for all $h \in H$, where e^* is the identity in G^*. Let $a \in G$. Consider the coset aH of H in G. We have $\varphi(ah) = \varphi(a) \cdot \varphi(h) = \varphi(a) \cdot e^* = \varphi(a)$ for all $h \in H$, and φ is therefore constant on aH. Since $a \in G$ was arbitrary, it follows that φ is constant on each coset of H.

Now, suppose $H \not\subseteq \ker \varphi$. Set $\overline{H} := H \cap \ker \varphi$. Then $\overline{H} \subseteq \ker \varphi$, so φ is constant on each coset of $\overline{H}$. We see that $\overline{H} = \ker \varphi|_H$, so by the First Isomorphism Theorem, $H/\overline{H} = H/\ker \varphi|_H \cong \operatorname{im} \varphi|_H = \varphi(H)$, which shows there is a one-to-one correspondence between the cosets of $\overline{H}$ in H and the elements of $\varphi(H)$. Moreover, since the cosets of $\overline{H}$ in H have the same cardinality, it follows that $\varphi|_H$ takes on each element of $\varphi(H)$ the same number of times; in fact, $\varphi|_H$ is a $|\overline{H}|$-to-one map onto $\varphi(H)$. Also, since φ is a homomorphism, $\varphi(H)$ is a subgroup of G^*, which is the same as the coset $e^* \cdot \varphi(H) = \varphi(H)$, which is nontrivial since $H \not\subseteq \ker \varphi$. Thus φ is balanced on H. Now, observe that since $\overline{H} \subseteq H$, aH is the union of a collection of cosets of $\overline{H}$ (in G) in one-to-one correspondence with the collection of cosets of $\overline{H}$ in H. In fact, if $b\overline{H}$ is a coset of $\overline{H}$ in H, then the corresponding coset of $\overline{H}$ lying in aH is $a(b\overline{H}) = (ab)\overline{H}$. Now φ is constant on $a(b\overline{H})$ for all $b \in H$, and since the cosets of $\overline{H}$ in H have the same cardinality, it follows that φ takes on each element of $\varphi(aH)$ the same number of times. Additionally, since $\varphi(aH) = \varphi(a)\varphi(H)$ and $\varphi(H)$ is nontrivial, $\varphi(aH)$ is a coset of the nontrivial subgroup $\varphi(H)$ in G^*. Thus φ is balanced on aH. Hence φ is balanced on each coset of H.

□

2.3.4 Corollary. *Let G be a group and H be a subgroup of G. A homomorphism $f : G \to \mathbb{Z}_m$ is either constant on each coset of H or balanced on each coset of H.*

Proof. (1) Corollary of Theorem 2.3.3.

□

2.3.5 Theorem (Fundamental Homomorphism Theorem [Hun80, p. 43])**.** *Let G and G^* be groups, and let $f : G \to G^*$ be a homomorphism. If H is a normal subgroup of G such that $H \subseteq \ker f$, then there exists a unique homomorphism $\bar{f} : G/H \to G^*$ such that $\bar{f}\pi = f$, where $\pi : G \to G/H$ is the canonical epimorphism. The function $\bar{f}$ is given by $\bar{f}(gH) = f(g)$.*

2.3.6 Definition. For a group G, put $G^{\mathrm{ab}} = G/G'$, where $G' = [G, G]$ is the commutator subgroup of G, which is the subgroup of G generated by the set $\{[a, b] = a^{-1}b^{-1}ab : a, b \in G\}$. The group G^{ab} is the *abelianization* of the group G.

Fix a finite group G. We have $G^{\mathrm{ab}} \cong \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_n}$ for some $n, m_i \in \mathbb{Z}^+$. Put $m = \mathrm{lcm}(m_1, m_2, \ldots, m_n)$. Let $f : G \to \mathbb{Z}_m$ be a function that is constant on the cosets of G', and let $\bar{f} : G^{\mathrm{ab}} \to \mathbb{Z}_m$ be the function defined by $\bar{f}(gG') = f(g)$ for each $g \in G$. Given $\pi : G \to G^{\mathrm{ab}}$ is the canonical epimorphism, we have

$$\bar{f}\pi(g) = \bar{f}(gG') = f(g).$$

Therefore, $\bar{f}\pi = f$ and we get the following commutative diagram:

$$\begin{array}{ccc} G & \xrightarrow{\ f\ } & \mathbb{Z}_m \\ {\scriptstyle\pi}\downarrow & \nearrow_{\bar{f}} & \\ G^{\mathrm{ab}} & & \end{array}$$

2.3.7 Lemma (R. Holmes)**.** *For each $a \in G$ and $x \in f(aH)$, we have $\left|f|_{aH}^{-1}(x)\right| = |H \cap G'|\left|\bar{f}|_{\pi(aH)}^{-1}(x)\right|$.*

Proof. Let $a \in G$ and let $x \in f(aH)$. Put

$$B = f|_{aH}^{-1}(x) = \{b \in aH \mid f(b) = x\}$$

and

$$C = \bar{f}|^{-1}_{\pi(aH)}(x) = \{c \in \pi(aH) \mid \bar{f}(c) = x\}.$$

Let R be a set of representatives of the (left) cosets of $H \cap G'$ in H. For $b \in aH$, let $r(b) \in R$ denote the coset representative for which $a^{-1}b \in r(b)(H \cap G')$. Define $\iota : aH \to H \cap G'$ by $\iota(b) = r(b)^{-1}a^{-1}b$. It is straightforward to check that ι is a function that maps to the indicated codomain. Thus for $b \in aH$, we have $a^{-1}b = r(b)\iota(b)$, and it follows that the elements $r(b) \in R$ and $\iota(b) \in H \cap G'$ are uniquely determined. Define $F : B \to (H \cap G') \times C$ by $F(b) = (\iota(b), \pi(b))$. It suffices to show that F is a well-defined bijection.

Claim: F is well-defined. To prove the claim, it suffices to check that F is a function that maps to the indicated codomain. Since both ι and π are functions, it follows that F is a function. Since ι maps B to $H \cap G'$, it suffices to prove that π maps B to C. Let $z \in \pi(B)$, and let $b \in B$ satisfy $z = \pi(b)$. Since $b \in aH$ and $f(b) = x$, we have $z = \pi(b) \in \pi(aH)$ and $\bar{f}(z) = \bar{f}(\pi(b)) = \bar{f}\pi(b) = f(b) = x$. Thus $z \in C$, and we have $\pi(B) \subseteq C$. Now, let $c \in C$. Then we have $c \in \pi(aH)$ and $\bar{f}(c) = x$. Let $h \in H$ satisfy $c = \pi(ah)$. Then we have $f(ah) = \bar{f}\pi(ah) = \bar{f}(\pi(ah)) = \bar{f}(c) = x$. Since $ah \in aH$, it follows that $ah \in B$, and thus $c = \pi(ah) \in \pi(B)$. Therefore, $\pi(B) \supseteq C$, so $\pi(B) = C$. Thus F maps B to $(H \cap G') \times C$, and we have that F is well-defined, as claimed.

Claim: F is injective. Let $b_1, b_2 \in B$. Suppose $F(b_1) = F(b_2)$. Then we have $(\iota(b_1), \pi(b_1)) = (\iota(b_2), \pi(b_2))$ so that $\iota(b_1) = \iota(b_2)$ and $\pi(b_1) = \pi(b_2)$. Thus $b_1G' = \pi(b_1) = \pi(b_2) = b_2G'$, so $b_1^{-1}b_2 \in G'$. Since $b_1, b_2 \in aH$, $b_1 = ah_1$ and $b_2 = ah_2$ for some $h_1, h_2 \in H$. Thus $h_1^{-1}h_2 = h_1^{-1}a^{-1}ah_2 = (ah_1)^{-1}(ah_2) = b_1^{-1}b_2 \in G'$. Therefore, $h_1^{-1}h_2 \in H \cap G'$, which implies $h_1(H \cap G') = h_2(H \cap G')$. Thus

$$\begin{aligned} r(b_1)(H \cap G') &= r(b_1)\iota(b_1)(H \cap G') \\ &= a^{-1}b_1(H \cap G') \end{aligned}$$

$$
\begin{aligned}
&= h_1(H \cap G') \\
&= h_2(H \cap G') \\
&= a^{-1}b_2(H \cap G') \\
&= r(b_2)\iota(b_2)(H \cap G') \\
&= r(b_2)(H \cap G').
\end{aligned}
$$

Since $r(b_1)$ and $r(b_2)$ are coset representatives of the (left) cosets of $H \cap G'$ in H, it follows that $r(b_1) = r(b_2)$. Therefore, $b_1 = a(a^{-1}b_1) = a(r(b_1)\iota(b_1)) = a(r(b_2)\iota(b_2)) = a(a^{-1}b_2) = b_2$. This proves the claim.

Claim: F is surjective. Let $(g, c) \in (H \cap G') \times C$. Thus $c \in \pi(B)$. Let $b \in B$ satisfy $c = \pi(b)$. Then we have

$$\pi(a)^{-1}c = \pi(a^{-1})\pi(b) = \pi(a^{-1}b) = \pi(r(b)\iota(b)) = \pi(r(b))\pi(\iota(b)) = \pi(r(b)) \cdot \iota(b)G',$$

for uniquely determined $r(b) \in R$ and $\iota(b) \in H \cap G'$. Thus

$$\pi(a)^{-1}c = \pi(r(b)) \cdot \iota(b)G' = \pi(r(b)) \cdot G' = \pi(r(b)) \cdot gG' = \pi(r(b))\pi(g) = \pi(r(b)g),$$

and hence $c = \pi(ar(b)g)$. Put $y = ar(b)g$. Observe that since $g \in H \cap G'$ and $r(b) \in R$, $y \in aH$. Since $c \in C$, we have $f(y) = \bar{f}\pi(y) = \bar{f}(\pi(y)) = \bar{f}(c) = x$, and thus $y \in B$. Then we also have $r(b)g = a^{-1}(ar(b)g) = a^{-1}y = r(y)\iota(y)$, which shows $r(b)g \in r(y)(H \cap G')$. Since $r(b)g \in r(b)(H \cap G')$ as well, we must have that $r(b) = r(y)$. Therefore, $g = r(b)^{-1}r(b)g = r(y)^{-1}(r(b)g) = r(y)^{-1}(r(y)\iota(y)) = \iota(y)$. It follows that $F(y) = (\iota(y), \pi(y)) = (g, c)$, and thus F is surjective.

Therefore, F is bijective, which implies

$$\left|f|_{aH}^{-1}(x)\right| = |B| = |(H \cap G') \times C| = |H \cap G'||C| = |H \cap G'| \left|\bar{f}|_{\pi(aH)}^{-1}(x)\right|.$$

The claim follows.

□

2.3.8 Corollary. *Let the notation be as above and let H be a subgroup of G. Then f is constant (resp. balanced) on each coset of H if and only if $\bar{f}$ is constant (resp. balanced) on each coset of $\pi(H)$.*

Proof. First, we claim that an arbitrary coset of $\pi(H)$ in G^{ab} can be written as $\pi(aH)$ for some $a \in G$. To that end, let C be a coset of $\pi(H)$. Then we have $C = x \cdot \pi(H)$ for some $x \in G^{\mathrm{ab}}$. Since π is a surjection, $x = \pi(a)$ for some $a \in G$. Therefore, $C = x \cdot \pi(H) = \pi(a) \cdot \pi(H) = \pi(aH)$ for some $a \in G$, and the claim is proved. For the rest of the proof, we fix an $a \in G$ that satisfies $C = \pi(aH)$.

($\Rightarrow$) Assume f is constant on each coset of H (*). Let $x, y \in C$. Thus $x, y \in \pi(aH)$, so $x = \pi(ah)$ and $y = \pi(ah')$ for some $h, h' \in H$. Thus

$$\bar{f}(x) = \bar{f}\pi(ah) = f(ah) \overset{*}{=} f(ah') = \bar{f}\pi(ah') = \bar{f}(y),$$

for some $h, h' \in H$, proving $\bar{f}$ is constant on C. Thus $\bar{f}$ is constant on each coset of $\pi(H)$.

Now, assume f is balanced on each coset of H (**). Since $\bar{f}(C) = \bar{f}\pi(aH) = f(aH)$ and $f(aH)$ is a coset of a nontrivial subgroup of $\mathbb{Z}_m$ by assumption, we see that $\bar{f}(C)$ is a coset of a nontrivial subgroup of $\mathbb{Z}_m$.

Let $x, y \in \bar{f}(C)$. Thus $x, y \in f(aH)$, so we have $\left|f|_{aH}^{-1}(x)\right| \overset{**}{=} \left|f|_{aH}^{-1}(y)\right|$, and by Lemma 2.3.7,

$$\left|\bar{f}|_{\pi(aH)}^{-1}(x)\right| = \frac{\left|f|_{aH}^{-1}(x)\right|}{|H \cap G'|} = \frac{\left|f|_{aH}^{-1}(y)\right|}{|H \cap G'|} = \left|\bar{f}|_{\pi(aH)}^{-1}(y)\right|.$$

It follows that $\bar{f}$ is balanced on each coset of $\pi(H)$.

($\Leftarrow$) Assume $\bar{f}$ is constant on each coset of $\pi(H)$ (*). Let $a \in G$, and let $x, y \in aH$. Then $x = ah$ and $y = ah'$ for some $h, h' \in H$. Thus

$$f(x) = f(ah) = \bar{f}\pi(ah) = \bar{f}(\pi(a)\pi(h)) \overset{*}{=} \bar{f}(\pi(a)\pi(h')) = \bar{f}\pi(ah') = f(ah') = f(y),$$

for some $h, h' \in H$, which proves f is constant on aH. Thus f is constant on each coset of H.

Now, suppose $\bar{f}$ is balanced on each coset of $\pi(H)$ (**). Let $a \in G$, and let $x, y \in aH$. Since $f(aH) = \bar{f}\pi(aH) = \bar{f}(\pi(aH)) = \bar{f}(\pi(a)\pi(H))$ and $\bar{f}(\pi(a)\pi(H))$ is a coset of a nontrivial subgroup of $\mathbb{Z}_m$ by assumption, $f(aH)$ is a coset of a nontrivial subgroup of $\mathbb{Z}_m$.

Additionally, by Lemma 2.3.7

$$\left|f|_{aH}^{-1}(x)\right| = |H \cap G'| \left|\bar{f}|_{\pi(aH)}^{-1}(x)\right| \overset{**}{=} |H \cap G'| \left|\bar{f}|_{\pi(aH)}^{-1}(y)\right| = \left|f|_{aH}^{-1}(y)\right|.$$

It follows that f is balanced on each coset of H.

□

We can see that the previous corollary, together with the results in the paper by Holmes and Texier, solves the problem described at the beginning of the section, which we recall was stated as:

Problem: Let G be a finite group, let H be a subgroup of G, and let $f : G \to \mathbb{Z}_m$ be a function that is constant on the cosets of the commutator subgroup G' of G in G. Assuming it is known that f is either constant on every coset of H or is balanced on every coset of H, determine which is the case.

The generalized Deutsch-Jozsa algorithm of Holmes and Texier solves the previous problem under the additional assumption that G is abelian. In this case, we observe that $G' = \{e\}$ and thus $G^{\text{ab}} = G/G' \cong G$, so the condition on f stating it needs to be constant on the cosets of G' can be dropped.

As a special case by setting $H = G$, if we are given a function $f : G \to \mathbb{Z}_m$ that is known to be constant on the cosets of G' in G and is known to be either constant or balanced on G, then $\bar{f}$ defined above must be either constant or balanced on $\pi(G) = G^{\text{ab}}$. Since G^{ab} is abelian, the results in the Holmes-Texier paper give a determination on whether $\bar{f}$ is constant or balanced on G^{ab}, at which point we apply Corollary 2.3.8 to determine whether f is constant or balanced on G.

2.4 A Generalization of the Bernstein-Vazirani Algorithm

Let $G = \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_n}$ with $n, m_i \in \mathbb{Z}^+$, and let m be the least common multiple of $m_1, m_2, \ldots, m_n$. The Bernstein-Vazirani problem is stated as follows:

For some unknown $u \in G$, determine u where one is only allowed queries of the form $q \circ u$ for some known $q \in G$.

Assume $m_i = 2$ for all i. Thus $m = 2$, and we obtain the classical Bernstein-Vazirani problem. The best non-quantum algorithm uses $O(n)$ calls to the function $f_u : G \to \mathbb{Z}_m$ given by $f_u(q) = q \cdot u$. On the other hand, the problem is solved by applying the Deutsch-Jozsa quantum algorithm to some initial state in one call to U_{f_u}, where U_{f_u} was defined in Definition 2.2.2 [RP11, p. 141]. We make extensive use of the paper written by Holmes and Texier which generalizes the Deutsch-Jozsa algorithm, including notation used in that paper, for ease of transferability of the ideas presented there.

The Algorithm. Define $f_u : G \to \mathbb{Z}_m$ by

$$f_u(a) = a \circ u.$$

From the Deutsch-Jozsa quantum algorithm, beginning with the initial state $|0\rangle|0\rangle$, we obtain the following (recall the Deutsch-Jozsa quantum algorithm from Section 2.2):

$$\begin{aligned}
|0\rangle|0\rangle &\mapsto |G|^{-1} \sum_{b \in G} |b\rangle|0\rangle \sum_{a \in G} \epsilon_m^{a \circ b} \epsilon_m^{-f_u(a)} \\
&= |G|^{-1} \sum_{b \in G} |b\rangle|0\rangle \sum_{a \in G} \epsilon_m^{a \circ b - f_u(a)} \\
&= |G|^{-1} \sum_{b \in G} |b\rangle|0\rangle \sum_{a \in G} \epsilon_m^{a \circ b - a \circ u} \\
&= |G|^{-1} \sum_{b \in G} |b\rangle|0\rangle \sum_{a \in G} \epsilon_m^{(\iota_b - \iota_u)(a)}
\end{aligned}$$

$$= |G|^{-1} \sum_{b \in G} |b\rangle|0\rangle\varphi(\iota_b - \iota_u)$$

Set $P = \{u\}$ and $a = u$. Applying Theorem 2.2.5, we find that ι_u is $\{u\} - based$, that is, $\varphi(\iota_b - \iota_u) = 0$ for all $b \in G \backslash \{u\}$ by Definition 2.2.4. Thus

$$\begin{aligned} |G|^{-1} \sum_{b \in G} |b\rangle|0\rangle\varphi(\iota_b - \iota_u) &= |G|^{-1}|u\rangle|0\rangle\varphi(0) \\ &= |G|^{-1}|u\rangle|0\rangle \sum_{a \in G} \epsilon_m^{0(a)} \\ &= |G|^{-1}|u\rangle|0\rangle|G| \\ &= |u\rangle|0\rangle. \end{aligned}$$

Thus u is determined with certainty.

2.5 A Generalization of Simon's Algorithm

Recall that $G = \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_n}$ with $n, m_i \in \mathbb{Z}^+$ and that m is the least common multiple of $m_1, m_2, \ldots, m_n$. Let p be a prime number, and assume that $m_i = p$ for all i. Thus $m = p$ and $\mathbb{Z}_m$ is a field.

Let $d \in \mathbb{Z}^+$. Let $f : G \to G$ be a d-to-1 function such that for all $x \in G$, we have

$$f(x) = f(x + s_1) = \cdots = f(x + s_{d-1}),$$

where $s_1, \ldots, s_{d-1} \in G$ are distinct nonzero unknowns. Our goal is to find $s_1, \ldots, s_{d-1}$.

2.5.1 Note. In the case where $m_i = 2$ for all i and $d = 2$, we have $m = 2$, and we obtain the classical version of Simon's problem. In the aforementioned case, Simon's algorithm can find s_1 in only $O(n)$ calls to U_f, followed by $O(n^2)$ additional steps, whereas the best non-quantum algorithm requires $O(2^{n/2})$ calls to f [RP11, p. 144].

Set $S = \{0, s_1, \ldots, s_{d-1}\}$.

2.5.2 Theorem. *S is a subgroup of G.*

Proof. First, observe that $0 \in S$ so that S contains the identity. Put $s_0 = 0$. Let $0 \leq j, k \leq d-1$.

The assumption on f with $x = s_j$ yields $f(s_j) = f(s_j + s_1) = \cdots = f(s_j + s_k) = \cdots = f(s_j + s_{d-1})$. Since f is d-to-1, $f(S) = f(s_j)$, and $|S| = d$, we conclude that $f^{-1}(f(s_j)) = S$. Thus $f(s_j) = f(s_j + s_k)$ implies $s_j + s_k \in f^{-1}(f(s_j)) = S$. Therefore, S is closed under addition.

Now, observe that $f(-s_j) = f(-s_j + s_1) = \cdots = f(-s_j + s_j) = \cdots = f(-s_j + s_{d-1})$, which becomes $f(-s_j) = f(-s_j + s_1) = \cdots = f(0) = \cdots = f(-s_j + s_{d-1})$. From the reasoning above, we have $f^{-1}(f(0)) = f^{-1}(f(s_0)) = S$. Thus $f(-s_j) = f(0)$ implies $-s_j \in f^{-1}(f(0)) = S$, so S is closed under inversion.

Therefore, S is a subgroup of G.

□

Letting S be the subgroup H in the language of Theorem 2.2.8, and observing that f is constant on each coset of S, we see that f is $S^{\perp}$-*based*. Thus $\varphi(\iota_b - f) = 0$ for all $b \in G \backslash S^{\perp}$, and $\varphi(\iota_b - f) \neq 0$ for all $b \in S^{\perp}$ by Definition 2.2.4.

The Algorithm.

Beginning in the same manner as the Bernstein-Vazirani Algorithm but with f replacing ι_u, we initialize our system to $|0\rangle|0\rangle$ and apply unitary operators to get the following:

$$\begin{aligned} |0\rangle|0\rangle &\mapsto |G|^{-1} \sum_{b \in G} |b\rangle|0\rangle\varphi(\iota_b - f) \\ &= |G|^{-1} \sum_{b \in S^{\perp}} |b\rangle|0\rangle\varphi(\iota_b - f). \end{aligned}$$

Measuring the left register gives a random element $|b\rangle$ such that $b \in S^{\perp}$, that is, such that $b \circ s_j = 0$ for all $s_j \in S$. Thus, for each $s_j \in S$, we get a linear equation

$$\sum_{i=1}^{n} b_i s_{ji} \left(\frac{m}{m_i} \right) = b \circ s_j = 0.$$

We need to repeat the algorithm until we have n linearly independent equations in the unknowns $s_{j1}, s_{j2}, \ldots, s_{jn}$ for each j. From this, we may compute the unknowns $s_{j1}, s_{j2}, \ldots, s_{jn}$

and thus s_j for each j, and thus we may compute each element of S.

We have the following special case (pointed out by R. Holmes) of our generalization of Simon's algorithm that solves for only one unknown, like in the original formulation of Simon's problem:

Let p be a prime number, and assume that $m_i = p$ for every i so that $m = p$. Let a be a nonzero element of G, and let $f : G \to G$ be a p-to-1 function such that $f(x) = f(x + ka)$ for every $x \in G$ and every $0 < k < p$. The task then is to find a.

solution. Since $f(x) = f(x + ka)$ for every $x \in G$ and every $0 < k < p$, we have that $f(x) = f(x+a) = \cdots = f(x+(p-1)a)$. Claim: $a, 2a, \ldots, (p-1)a$ are distinct and nonzero. Let $0 < j, k < p$. Assume $ja = ka$. Thus $(j-k)a = 0$, and since G is a $\mathbb{Z}_m$-vector space, we must have that $j-k = 0$, so $j = k$. Thus $a, 2a, \ldots, (p-1)a$ are distinct. Since $1, 2, \ldots, (p-1)$ are nonzero elements of $\mathbb{Z}_m$ and G is a $\mathbb{Z}_m$-vector space, it follows that each of the elements $a, 2a, \ldots, (p-1)a$ are nonzero. This proves the claim. We may then apply the generalization of the algorithm in this section to compute the elements of the subgroup $S = \{0, a, \ldots, (p-1)a\}$ of G. In particular, we can find a.

□

Chapter 3

Bilinear Forms and Complements

3.1 General definitions and results

Let R be a ring with $1_R \neq 0$ and let I be a two-sided ideal of R. The set R/I of cosets of I in R is a ring (called the quotient ring R mod I). Let M be an R-module that is annihilated by I. For $r \in R$ and $m \in M$ define $(r+I)\cdot m = r\cdot m$. This action gives M the structure of R/I-module.

Now, let R also be commutative, and let M and N be R-modules. Define $\mathrm{Hom}_R(M,N) := \{\varphi : M \to N \mid \varphi \text{ is an } R\text{-module homomorphism}\}$. Put $M^* = \mathrm{Hom}_R(M,R)$. We have that M^* is an R-module with action on M given by $(r\varphi)(m) = \varphi(rm)$ $(\varphi \in M^*, r \in R, m \in M)$.

For the rest of the section, we let R be a commutative ring with unity and M be an R-module.

3.1.1 Definition. An *R-bilinear form* (or simply *bilinear form* if the ring R is understood) on M is a function $f : M \oplus M \to R$ such that, for each $m \in M$, $f_1(m) : M \to R$ and $f_2(m) : M \to R$ given by $f_1(m)(n) = f(m,n)$ and $f_2(m)(n) = f(n,m)$ are R-module homomorphisms. The bilinear form f on M is said to be *symmetric, alternating, or skew-symmetric* if, for all $m, n \in M$, $f(m,n) = f(n,m)$, $f(m,m) = 0$, or $f(m,n) = -f(n,m)$, respectively. Additionally, the bilinear form f is said to be *left non-degenerate* if $f(m,n) = 0$ for all $n \in M$ if and only if $m = 0$ and *right non-degenerate* if $f(m,n) = 0$ for all $m \in M$ if and only if

$n = 0$. A bilinear form that is both left and right non-degenerate is called *non-degenerate*.

3.1.2 Definition. A symplectic bilinear form on M is a bilinear form that is alternating and non-degenerate.

For the following, let N be a submodule of M, and let f be a bilinear form on M. Put $N_L^f := \{m \in M \mid f(m,n) = 0 \text{ for all } n \in N\}$ and $N_R^f := \{m \in M \mid f(n,m) = 0 \text{ for all } n \in N\}$.

3.1.3 Theorem. *We have that N_L^f and N_R^f are submodules of M.*

Proof. Claim: N_L^f is a submodule of M. Let $x, y \in N_L^f$ and $r, s \in R$. Then for all $n \in N$ we have

$$f(rx+sy, n) = f_2(n)(rx+sy) = rf_2(n)(x)+sf_2(n)(y) = rf(x,n)+sf(y,n) = r\cdot 0+s\cdot 0 = 0,$$

and thus $rx + sy \in N_L^f$. This proves the claim. By a similar argument, N_R^f is a submodule of M.

□

3.1.4 Theorem. *If f is symmetric or skew-symmetric, then $N_L^f = N_R^f$.*

Proof. Assume f is symmetric. Thus $f(m,n) = f(n,m)$ for all $m, n \in M$, and we have

$$N_L^f = \{m \in M \mid f(m,n) = 0 \text{ for all } n \in N\} = \{m \in M \mid f(n,m) = 0 \text{ for all } n \in N\} = N_R^f.$$

Now, assume f is skew-symmetric. Thus $f(m,n) = -f(n,m)$ for all $m, n \in N$, and we have

$$\begin{aligned} N_L^f &= \{m \in M \mid f(m,n) = 0 \text{ for all } n \in N\} \\ &= \{m \in M \mid -f(n,m) = 0 \text{ for all } n \in N\} \\ &= \{m \in M \mid f(n,m) = 0 \text{ for all } n \in N\} \end{aligned}$$

$$= N_R^f.$$

The claim follows.

□

3.1.5 Note. When $N_L^f = N_R^f$, we will simply write $N^f = \{m \in M \mid f(m,n) = 0 \text{ for all } n \in N\}$.

For the following, define $f_i : M \to M^*$ $(i = 1, 2)$ such that $f_1(m)(n) = f(m,n)$ and $f_2(m)(n) = f(n,m)$.

3.1.6 Theorem. *The maps $f_i : M \to M^*$ $(i = 1, 2)$ are R-module homomorphisms.*

Proof. It is straightforward to prove that each f_i maps to the indicated codomain, so each f_i is well-defined. Now, let $m, n \in M$ and $r, s \in R$. Then we have

$$\begin{aligned} f_1(rm+sn)(x) &= f(rm+sn, x) \\ &= f_2(x)(rm+sn) \\ &= rf_2(x)(m) + sf_2(x)(n) \\ &= rf(m,x) + sf(n,x) \\ &= rf_1(m)(x) + sf_1(n)(x) \\ &= (rf_1(m) + sf_1(n))(x) \end{aligned}$$

for each $x \in M$. Thus $f_1(rm+sn) = rf_1(m) + sf_1(n)$, so f_1 is an R-module homomorphism. By a similar argument, f_2 is a R-module homomorphism.

□

3.1.7 Theorem. *The bilinear form f is non-degenerate if and only if f_1 and f_2 are injections.*

Proof. Assume f is non-degenerate. Let $m, n \in M$. Suppose $f_1(m) = f_1(n)$. Thus for all $p \in M$ we have

$$f_2(p)(m) = f_1(m)(p) = f_1(n)(p) = f_2(p)(n).$$

Therefore, $f(m-n, p) = f_2(p)(m-n) = 0$ for all $p \in M$. Since f is non-degenerate, we have $m - n = 0$, and thus $m = n$. Hence f_1 is an injection. By a similar argument, f_2 is an injection.

For the other direction, assume f_1 and f_2 are injections. Let $m \in M$. Suppose $f(m, n) = 0$ for all $n \in M$. Thus

$$f_1(m)(n) = f(m, n) = 0 = f_2(n)(0) = f_1(0)(n)$$

for all $n \in M$, so $f_1(m) = f_1(0)$. Since f_1 is an injection, we have $m = 0$. Suppose $f(n, m) = 0$ for all $n \in M$. Thus

$$f_2(m)(n) = f(n, m) = 0 = f_1(n)(0) = f_2(0)(n)$$

for all $n \in M$, so $f_2(m) = f_2(0)$. Since f_2 is an injection, we have $m = 0$. Thus f is non-degenerate.

□

3.1.8 Theorem. *If f is skew-symmetric, then $f_1 = -f_2$.*

Proof. Assume f is skew-symmetric. Let $m \in M$. For all $p \in M$, we have

$$f_1(m)(p) = f(m, p) = -f(p, m) = -f_2(m)(p).$$

Thus $f_1(m) = -f_2(m)$. Since m was arbitrary, it follows that $f_1 = -f_2$.

□

3.1.9 Theorem. *If f is alternating, then f is skew-symmetric.*

Proof. Suppose f is alternating. Since f_1 and f_2 are R-module homomorphisms, we have

$$\begin{aligned}
0 &= f(m+n, m+n) \\
&= f_1(m+n)(m+n) \\
&= f_1(m+n)(m) + f_1(m+n)(n) \\
&= f(m+n, m) + f(m+n, n) \\
&= f_2(m)(m+n) + f_2(n)(m+n) \\
&= f_2(m)(m) + f_2(m)(n) + f_2(n)(m) + f_2(n)(n) \\
&= f(m, m) + f(n, m) + f(m, n) + f(n, n) \\
&= f(n, m) + f(m, n).
\end{aligned}$$

Therefore, $f(m, n) = -f(n, m)$, so f is skew-symmetric.

□

For the following results, set $M_N^* := \{\varphi \in M^* \mid N \subseteq \ker \varphi\}$.

3.1.10 Theorem. *M_N^* is a submodule of M^*.*

Proof. First, it is immediate that $M_N^* \subset M^*$. Let $\varphi, \rho \in M_N^*$ and $r, s \in R$. Let $n \in N$. Then we have

$$\begin{aligned}
(r\varphi + s\rho)(n) &= r\varphi(n) + s\rho(n) \\
&= r \cdot 0 + s \cdot 0 \\
&= 0.
\end{aligned}$$

Thus $N \subseteq \ker(r\varphi + s\rho)$, so $r\varphi + s\rho \in M_N^*$. Therefore, M_N^* is a submodule of M^*.

□

3.2 The Finite Abelian Group G and its Dual

Recall (Section 2.2) that $G = \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_n}$ with $m_i, n \in \mathbb{Z}^+$. In the paper by Holmes and Texier, m was defined to be the least common multiple of $m_1, m_2, \ldots, m_n$. For our purposes in the rest of this paper, we relax this condition on m and let it be a common multiple of $m_1, m_2, \ldots, m_n$.

Now, the set $I = m\mathbb{Z}$ is a two-sided ideal of $\mathbb{Z}$ and $m\mathbb{Z}$ annihilates G, since, for any $a \in G$, we have

$$m \cdot a = m \cdot (a_1, a_2, \ldots, a_n) = (m \cdot a_1, m \cdot a_2, \ldots, m \cdot a_n) = (0, 0, \ldots, 0).$$

Hence $\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}_m$ induces a $\mathbb{Z}_m$-module structure on G by Section 3.1.

Recall (Section 2.2) that $\iota_a \in \mathcal{F}$, for $a \in G$, is defined by

$$\iota_a(b) = a \circ b = \sum_{i=1}^{n} a_i b_i \left(\frac{m}{m_i}\right) \cdot 1 \in \mathbb{Z}_m,$$

where $\displaystyle\sum_{i=1}^{n} a_i b_i \left(\frac{m}{m_i}\right) \in \mathbb{Z}$ and $1 \in \mathbb{Z}_m$.

We identify $\mathbb{Z}_{m_i}$ and $\mathbb{Z}_m$ with the quotient groups $\mathbb{Z}/m_i\mathbb{Z}$ and $\mathbb{Z}/m\mathbb{Z}$, respectively, and for an integer x we denote by $\overline{x}$ the coset $x + m_i\mathbb{Z}$ or $x + m\mathbb{Z}$, respectively, with context making the meaning clear.

While the $\circ$ product was defined in the paper by Holmes and Texier and was therein assumed to be well-defined, we provide a proof that it is indeed well-defined.

3.2.1 Proposition. *The product $\circ$ is well-defined.*

Proof. Let $a, b \in G$. Then we have $a = (a_i)_{i=1}^n$ and $b = (b_i)_{i=1}^n$, where $a_i, b_i \in \mathbb{Z}_{m_i}$. For each i let a_i' and b_i' be integers such that $\overline{a_i} = \overline{a_i'}$ and $\overline{b_i} = \overline{b_i'}$, and denote $a' = (a_i')_{i=1}^n$ and $b' = (b_i')_{i=1}^n$. Thus $a_i = a_i' + mj$ and $b_i = b_i' + mk$, for some $j, k \in \mathbb{Z}$, and we have

$$\begin{aligned}
a \circ b &= \sum_{i=1}^{n} \left(\frac{m}{m_i}\right)(a_i b_i) \\
&= \sum_{i=1}^{n} \left(\frac{m}{m_i}\right)(a_i' + mj)(b_i' + mk) \\
&= \sum_{i=1}^{n} \left(\frac{m}{m_i}\right)(a_i' b_i' + m(a_i' k + b_i' j + mjk)) \\
&= \sum_{i=1}^{n} \left(\frac{m}{m_i}\right)(a_i' b_i') + \sum_{i=1}^{n} \left(\frac{m}{m_i}\right)(m(a_i' k + b_i' j + mjk)) \\
&= \sum_{i=1}^{n} \left(\frac{m}{m_i}\right)(a_i' b_i') + m \sum_{i=1}^{n} \left(\frac{m}{m_i}\right)(a_i' k + b_i' j + mjk) \\
&= \sum_{i=1}^{n} \left(\frac{m}{m_i}\right)(a_i' b_i') \\
&= a' \circ b'.
\end{aligned}$$

The claim follows.

□

Define $\iota : G \oplus G \to \mathbb{Z}_m$ by $\iota(a, b) := a \circ b$. Then we have $\iota_a(b) = a \circ b = \iota(a, b)$ and $\iota_b(a) = b \circ a = a \circ b = \iota(a, b)$. It is straightforward to check that ι is a symmetric $\mathbb{Z}_m$-bilinear form, and thus for each $a \in G$ the map $\iota_a : G \to \mathbb{Z}_m$ given by $\iota_a(b) = a \circ b$ is a $\mathbb{Z}_m$-homomorphism so that for each $a \in G$, $\iota_a \in G^*$. It is also true that ι is non-degenerate, but we postpone the proof of this to the next section (see Lemma 3.3.3).

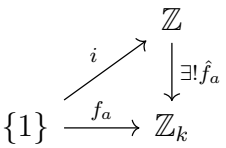
Define $\varphi : G \to G^*$ by $\varphi(a) = \iota_a$. Since $\iota_a \in G^*$ for every $a \in G$, the function φ is well-defined in the sense that it maps into the indicated codomain. Moreover, since ι is $\mathbb{Z}_m$-bilinear, it follows that $\iota_{a+b} = \iota_a + \iota_b$ and $\iota_{ra} = r\iota_a$ for every $a, b \in \mathbb{Z}_m$ and $r \in \mathbb{Z}_m$, which implies in turn that φ is a $\mathbb{Z}_m$-homomorphism.

In fact, every element of G^* can be written in the form ι_a, for some $a \in G$, as we now show.

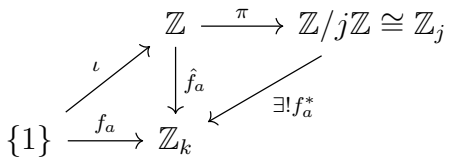
For a finite group G, let $o(x)$ denote the order of the element $x \in G$.

3.2.2 Lemma. *Let $j, k \in \mathbb{Z}^+$, and set $d = \gcd(j, k)$. For each $0 \leq a \leq d-1$ there exists a homomorphism $\gamma_a : \mathbb{Z}_j \to \mathbb{Z}_k$ such that $\gamma_a(1) = (k/d)a \cdot 1$. Moreover, the homomorphisms γ_a $(0 \leq a \leq d-1)$ are distinct and for every homomorphism $f : \mathbb{Z}_j \to \mathbb{Z}_k$ we have $f = \gamma_a$ for some a.*

Proof. Set $D = \{0, \ldots, d-1\}$. Let $a \in D$. Define the function $f_a : \{1\} \to \mathbb{Z}_k$ by $f_a(1) = (k/d)a \cdot 1$. Here, we view $(k/d)a$ as an integer and $\mathbb{Z}_k$ as a $\mathbb{Z}$-module so that $(k/d)a \cdot 1$ is an element of $\mathbb{Z}_k$, where we take $1 \in \mathbb{Z}_k$. Now, since $\mathbb{Z}$ is free on the set $\{1\}$, the universal property of free groups guarantees a unique homomorphism $\hat{f}_a : \mathbb{Z} \to \mathbb{Z}_k$ such that the following diagram commutes ($i : \{1\} \to \mathbb{Z}$ is the inclusion map):



Thus $\hat{f}_a(1) = \hat{f}_a i(1) = f_a(1) = (k/d)a \cdot 1$, so $\hat{f}_a(j) = j \cdot \hat{f}_a(1) = j \cdot ((k/d)a \cdot 1) = k \cdot ((j/d)a \cdot 1) = 0$. Thus $j\mathbb{Z} \subset \ker \hat{f}_a$. By the fundamental homomorphism theorem, there is a homomorphism $f_a^* : \mathbb{Z}_j \to \mathbb{Z}_k$ such that the following diagram commutes (here, we identify $\mathbb{Z}/j\mathbb{Z}$ with $\mathbb{Z}_j$ in the statement of the FHT and replace $\mathbb{Z}/j\mathbb{Z}$ with $\mathbb{Z}_j$ in the codomain of the canonical epimorphism π):



Observe that $f_a^*(1) = f_a^*\pi(1) = \hat{f}_a(1) = (k/d)a \cdot 1$. Setting $\gamma_a := f_a^*$ for each $a \in G$, we have $\gamma_a(1) = f_a^*(1) = (k/d)a \cdot 1$. This completes the first statement of the lemma.

Claim: each $a \in D$ yields a distinct γ_a. To that end, let $a, b \in D$, and suppose $\gamma_a = \gamma_b$. Thus, in particular, we have $(k/d)a \cdot 1 = \gamma_a(1) = \gamma_b(1) = (k/d)b \cdot 1$, which implies $(k/d)(a-b) \cdot 1 = 0$. Hence $k = o(1) \mid (k/d)(a-b)$, so $(k/d)(a-b) = pk$, for some $p \in \mathbb{Z}$. Therefore, for some $p \in \mathbb{Z}$, we have $a - b = pd$, or $a = b + pd$, so $a \equiv b \pmod{d}$. Hence $a = b$ in D. The claim follows.

Let $f : \mathbb{Z}_j \to \mathbb{Z}_k$ be an arbitrary homomorphism. We claim that $f = \gamma_a$ for some $a \in D$. Since $j \cdot f(1) = f(j) = f(0) = 0$, it follows that $o(f(1))$ is a divisor of j. In addition, $o(f(1)) = |\text{im } f| \mid |\mathbb{Z}_k| = k$, so $o(f(1))$ is a divisor of k as well. Therefore, $o(f(1))$ must be a common divisor of j and k. Thus $o(f(1)) \mid d$. Since $f(1) \in \mathbb{Z}_k$ we have $f(1) = x \cdot 1$ for some integer x with $0 \leq x < k$. Now $dx \cdot 1 = d \cdot (x \cdot 1) = d \cdot f(1) = 0$, so $k \mid dx$ and hence we have $dx = ka$ for some integer a. Thus $ka = xd < kd$, which implies $a < d$. Hence $a \in D$, and we have $f(\ell) = \ell f(1) = \ell(x \cdot 1) = \ell((k/d)a \cdot 1) = \ell\gamma_a(1) = \gamma_a(\ell)$ for all $\ell \in \mathbb{Z}_j$. This proves the claim and completes the proof.

□

3.2.3 Corollary. *Let $j, k \in \mathbb{Z}^+$ such that $j \mid k$. For each $0 \leq a \leq j-1$ there exists a homomorphism $\gamma_a : \mathbb{Z}_j \to \mathbb{Z}_k$ such that $\gamma_a(1) = (k/j)a \cdot 1$. Moreover, the homomorphisms γ_a $(0 \leq a \leq j-1)$ are distinct and for every homomorphism $f : \mathbb{Z}_j \to \mathbb{Z}_k$ we have $f = \gamma_a$ for some a.*

Proof. Observe that $j = \gcd(j, k)$, so by invoking the previous lemma with $d = j$, we obtain the result.

□

For the following result, recall that $G = \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_n}$ for $n, m_i \in \mathbb{Z}^+$ and m is a multiple of $m_1, m_2, \ldots, m_n$.

3.2.4 Lemma. *The function $\mathbb{Z}_{m_i} \to \mathrm{Hom}_{\mathbb{Z}_m}(\mathbb{Z}_{m_i}, \mathbb{Z}_m)$ given by $a_i \mapsto \gamma_{a_i}$ is an isomorphism.*

Proof. Fix $1 \leq i \leq n$. Since $m_i \mid m$, we can apply Corollary 3.2.3, which implies there are exactly $m_i = \gcd(m_i, m)$ homomorphisms from $\mathbb{Z}_{m_i}$ to $\mathbb{Z}_m$, all given by $\gamma_{a_i} : \mathbb{Z}_{m_i} \to \mathbb{Z}_m$, where $0 \leq a_i \leq m_i - 1$, such that $\gamma_{a_i}(1) = (m/m_i)a_i \cdot 1$. Thus the function $\mathbb{Z}_{m_i} \to \mathrm{Hom}_{\mathbb{Z}_m}(\mathbb{Z}_{m_i}, \mathbb{Z}_m)$ given by $a_i \mapsto \gamma_{a_i}$ is a bijection. Observe that, for $x_i \in \mathbb{Z}_{m_i}$, we have

$$\gamma_{a_i}(x_i) = x_i\gamma_{a_i}(1) = x_i((m/m_i)a_i \cdot 1) = (m/m_i)a_i \cdot x_i.$$

Let $a_i, b_i \in \mathbb{Z}_{m_i}$. Then we have

$$\gamma_{a_i+b_i}(x_i) = \left(\frac{m}{m_i}\right)(a_i+b_i)\cdot x_i = \left(\frac{m}{m_i}\right)a_i\cdot x_i + \left(\frac{m}{m_i}\right)b_i\cdot x_i = \gamma_{a_i}(x_i)+\gamma_{b_i}(x_i) = (\gamma_{a_i}+\gamma_{b_i})(x_i).$$

Thus the function $\mathbb{Z}_{m_i} \to \mathrm{Hom}_{\mathbb{Z}_m}(\mathbb{Z}_{m_i}, \mathbb{Z}_m)$ given by $a_i \mapsto \gamma_{a_i}$ is a homomorphism and is therefore an isomorphism. The claim follows.

□

3.2.5 Lemma. *Let $f_i : \mathbb{Z}_{m_i} \to \mathbb{Z}_m$ $(i = 1, \ldots, n)$ be homomorphisms. The function $f : G \to \mathbb{Z}_m$ given by $f(a) = \sum_{i=1}^{n} f_i(a_i)$ is a homomorphism.*

Proof. First, observe that $\{\mathbb{Z}_{m_i}\}_{i=1}^n$ is a family of $\mathbb{Z}_m$-modules. It is straightforward to check that $G = \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_n}$ with the natural injections $\varphi_i : \mathbb{Z}_{m_i} \to G$ given by $\varphi_i(x)_j = \delta_{ij}(x)$ is a coproduct of the family $\{\mathbb{Z}_{m_i}\}_{i=1}^n$ in the category ${}_{\mathbb{Z}_m}\mathbf{Mod}$, where $\delta_{ij} : \mathbb{Z}_{m_i} \to \mathbb{Z}_{m_j}$ is the identity map if $i = j$ and the zero map otherwise.

In the usual proof that (G, φ_i) is a coproduct, the function $f : G \to \mathbb{Z}_m$ given by $f(a) = \sum_{i=1}^{n} f_i(a_i)$ is a homomorphism with the property that $f_i = f\varphi_i$ for each i.

□

For the following result, recall the definition of $\iota_a : G \to \mathbb{Z}_m$, for $a \in G$:

$$\iota_a(b) := \sum_{i=1}^{n} \left(\frac{m}{m_i}\right)(a_i b_i) \cdot 1,$$

where $\left(\frac{m}{m_i}\right)(a_i b_i) \in \mathbb{Z}$ for all i and $1 \in \mathbb{Z}_m$.

3.2.6 Lemma. *Every element of G^* is of the form ι_a for some $a \in G$.*

Proof. Applying Corollary 3.2.3 and Lemma 3.2.5 and observing that $m_i = \gcd(m_i, m)$ for all i, the claim follows.

□

3.2.7 Theorem. *The map $\varphi : G \to G^*$ given by $\varphi(a) = \iota_a$ is an isomorphism.*

Proof. Recall from the remarks preceding Lemma 3.2.2 that φ is a homomorphism, and the previous result gives us the needed bijectivity to make φ an isomorphism.

□

3.2.8 Note. While the previous theorem implies that G is isomorphic to G^*, we now state a more general result that proves $G \cong G^*$ irrespective of a particular isomorphism from G to G^*. We keep the previous result since it will prove useful in the next section.

3.2.9 Lemma. *We have $G \cong G^*$.*

Proof. By Lemma 3.2.4, we have $\mathbb{Z}_{m_i} \cong \mathrm{Hom}_{\mathbb{Z}_m}(\mathbb{Z}_{m_i}, \mathbb{Z}_m)$ for each i, and thus $G = \bigoplus_{i=1}^{n} \mathbb{Z}_{m_i} \cong \bigoplus_{i=1}^{n} \mathrm{Hom}_{\mathbb{Z}_m}(\mathbb{Z}_{m_i}, \mathbb{Z}_m)$. Now, we have $\bigoplus_{i=1}^{n} \mathrm{Hom}_{\mathbb{Z}_m}(\mathbb{Z}_{m_i}, \mathbb{Z}_m) \cong \mathrm{Hom}_{\mathbb{Z}_m}(\bigoplus_{i=1}^{n} \mathbb{Z}_{m_i}, \mathbb{Z}_m)$, which is a special case of [Hun80, Theorem 4.7, p. 202]. Therefore, we obtain

$$G = \bigoplus_{i=1}^{n} \mathbb{Z}_{m_i} \cong \bigoplus_{i=1}^{n} \mathrm{Hom}_{\mathbb{Z}_m}(\mathbb{Z}_{m_i}, \mathbb{Z}_m) \cong \mathrm{Hom}_{\mathbb{Z}_m}\left(\bigoplus_{i=1}^{n} \mathbb{Z}_{m_i}, \mathbb{Z}_m\right) = \mathrm{Hom}_{\mathbb{Z}_m}(G, \mathbb{Z}_m) = G^*.$$

□

3.2.10 Theorem. *Let $\beta : G \oplus G \to \mathbb{Z}_m$ be a non-degenerate bilinear form on G. Then $\beta_i : G \to G^*$ $(i = 1, 2)$ given by $\beta_1(g)(h) = \beta(g, h)$ and $\beta_2(g)(h) = \beta(h, g)$ are isomorphisms.*

Proof. By Theorems 3.1.6 and 3.1.7, the maps $\beta_i : G \to G^*$ $(i = 1, 2)$ defined such that $\beta_1(g)(h) = \beta(g, h)$ and $\beta_2(g)(h) = \beta(h, g)$ are monomorphisms. The previous lemma then implies $|G| = |G^*|$, so surjectivity of β_1 and β_2 follows. Thus β_i $(i = 1, 2)$ are isomorphisms.

□

3.3 Orthogonal Complements of Subgroups of G

Let H be a subgroup of the fixed group $G = \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_n}$. It follows that H is a $\mathbb{Z}_m$-submodule of G. Let $\beta : G \oplus G \to \mathbb{Z}_m$ be a $\mathbb{Z}_m$-bilinear form on G. Recall from Section 3.1 the sets $H_L^\beta = \{g \in G \mid \beta(g,h) = 0 \text{ for all } h \in H\}$ and $H_R^\beta = \{g \in G \mid \beta(h,g) = 0 \text{ for all } h \in H\}$. By Theorem 3.1.3, H_L^β and H_R^β are submodules, and thus subgroups, of G.

For the following results, set $G_H^* := \{f \in G^* \mid H \subseteq \ker f\}$. By Theorem 3.1.10, we have that G_H^* is a subgroup of G^*.

3.3.1 Lemma. *If β is non-degenerate, then $H_L^\beta \cong G_H^*$ and $H_R^\beta \cong G_H^*$.*

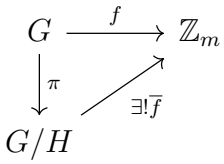
Proof. Assume β is non-degenerate. Then Theorem 3.2.10 implies $\beta_1 : G \to G^*$ is an isomorphism. Observe that $H_L^\beta = \{g \in G \mid \beta_1(g)(h) = 0 \text{ for all } h \in H\}$. Thus the restriction $\beta_1|_{H_L^\beta} : H_L^\beta \to G_H^*$ of β_1 to H_L^β is well-defined since $H \subseteq \ker \beta_1(g)$ for all $g \in H_L^\beta$. Since β_1 is an isomorphism, β_1 is a surjection, so for every $f \in G_H^* \subseteq G^*$ there exists a $g \in G$ such that $f = \beta_1(g)$, and thus $H \subseteq \ker f = \ker \beta_1(g)$, whence $g \in H_L^\beta$. Thus $\beta_1|_{H_L^\beta}$ is a surjection. It follows that G_H^* is the isomorphic image of H_L^β. In other words, $H_L^\beta \cong G_H^*$.

Replacing β_1 with β_2 and H_L^β with H_R^β in the preceding argument, we see that $H_R^\beta \cong G_H^*$.

□

3.3.2 Theorem. *Let $\beta : G \oplus G \to \mathbb{Z}_m$ be a non-degenerate bilinear form on G. Then we have that $H_L^\beta \cong G/H$ and $H_R^\beta \cong G/H$.*

Proof. Let $f \in G_H^*$. Then we have that $H \subseteq \ker f$, so by the Fundamental Homomorphism Theorem, there is a unique homomorphism $\bar{f} : G/H \to \mathbb{Z}_m$ such that $\bar{f}\pi = f$, where $\pi : G \to G/H$ is the canonical epimorphism. We have the following diagram:



Since G is a $\mathbb{Z}_m$-module and H is a $\mathbb{Z}_m$-submodule of G, it follows that G/H has a natural structure of $\mathbb{Z}_m$-module, so we may write $(G/H)^* = \mathrm{Hom}_{\mathbb{Z}_m}(G/H, \mathbb{Z}_m)$. It follows that $\bar{f} \in (G/H)^*$.

Now, define $\rho : G_H^* \to (G/H)^*$ by $\rho(f) = \overline{f}$, where $\overline{f}$ is as in the Fundamental Homomorphism Theorem above. The argument above shows that ρ is well-defined in that it maps to the indicated codomain. Let $\alpha, \varphi \in G_H^*$. Then we have that

$$\begin{aligned}
\overline{(\alpha+\varphi)}(gH) &= \overline{(\alpha+\varphi)}\pi(g) \\
&= (\alpha+\varphi)(g) \\
&= \alpha(g) + \varphi(g) \\
&= \overline{\alpha}\pi(g) + \overline{\varphi}\pi(g) \\
&= \overline{\alpha}(gH) + \overline{\varphi}(gH) \\
&= (\overline{\alpha}+\overline{\varphi})(gH),
\end{aligned}$$

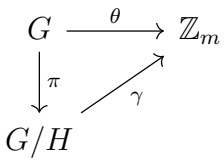
i.e., $\overline{\alpha+\varphi} = \overline{\alpha} + \overline{\varphi}$, so we have

$$\rho(\alpha+\varphi) = \overline{\alpha+\varphi} = \overline{\alpha} + \overline{\varphi} = \rho(\alpha) + \rho(\varphi),$$

showing ρ is a homomorphism.

Claim: ρ is surjective. Let $\gamma \in (G/H)^*$. Then $\gamma : G/H \to \mathbb{Z}_m$ is a homomorphism. Given the canonical projection map $\pi : G \to G/H$, we see that $\theta := \gamma\pi : G \to \mathbb{Z}_m$ is a composition of homomorphisms and is thus a homomorphism. Additionally, for all $h \in H$, we have $\theta(h) =$

$\gamma\pi(h) = \gamma(hH) = \gamma(H) = 0$, so $H \subseteq \ker\theta$, and thus $\theta \in G_H^*$. Moreover, by the FHT, γ is the unique homomorphism from G/H to $\mathbb{Z}_m$ for which $\theta = \gamma\pi$. Therefore, $\rho(\theta) = \overline{\theta} = \gamma$.



This proves the claim.

Claim: ρ is injective. Let $\alpha, \varphi \in G_H^*$. Suppose $\overline{\alpha} = \rho(\alpha) = \rho(\varphi) = \overline{\varphi}$. For $g \in G$, we have

$$\alpha(g) = \overline{\alpha}\pi(g) = \overline{\alpha}(gH) = \overline{\varphi}(gH) = \overline{\varphi}\pi(g) = \varphi(g).$$

Hence $\alpha = \varphi$, and this proves the claim.

Therefore ρ is an isomorphism, so $G_H^* \cong (G/H)^*$. By the previous lemma, $H_L^\beta \cong G_H^*$ and $H_R^\beta \cong G_H^*$. Since $(G/H)^* \cong G/H$ by Theorem 3.2.9, it follows that $H_L^\beta \cong G_H^* \cong (G/H)^* \cong G/H$ and $H_R^\beta \cong G_H^* \cong (G/H)^* \cong G/H$, as claimed.

□

Recall that the map $\iota : G \oplus G \to \mathbb{Z}_m$ defined by $\iota(a, b) = a \circ b$ is a bilinear form, and recall the map $\varphi : G \to G^*$ defined by $\varphi(a) = \iota_a$.

3.3.3 Lemma. *The bilinear form ι is non-degenerate.*

Proof. By Theorem 3.1.7, it suffices to prove that ι_1 and ι_2 are injections. Since ι is symmetric, it follows that we need to prove that ι_1 is an injection. Let $g, h \in G$. Suppose $\iota_1(g) = \iota_1(h)$. Thus $\varphi(g) = \iota_g = \iota_1(g) = \iota_1(h) = \iota_h = \varphi(h)$. By Theorem 3.2.7, φ is an isomorphism. Thus φ is an injection, so $g = h$. Therefore, ι_1 is an injection. The claim follows.

□

3.3.4 Note. Since ι is symmetric, Theorem 3.1.4 gives $H_L^\iota = H_R^\iota$. By Note 3.1.5 we may write $H^\iota = \{g \in G \mid \iota(g,h) = 0 \text{ for all } h \in H\}$. From Section 2.2, we observe that H^ι is in fact the orthogonal complement of H in G, which we will henceforth denote by $H^\perp$.

3.3.5 Theorem. *We have* $H^\perp \cong G/H$.

Proof. Since ι is non-degenerate by Lemma 3.3.3, Theorem 3.3.2 and the previous note give the result.

□

3.3.6 Theorem. *We have* $(H^\perp)^\perp = H$.

Proof. Since $(H^\perp)^\perp = \{g \in G \mid \iota_g(a) = 0 \quad \forall a \in H^\perp\}$, and $\iota_g(a) = g \circ a = a \circ g = \iota_a(g)$ for all $a, g \in G$, it follows that $H \subseteq (H^\perp)^\perp$. By Lagrange's Theorem and Theorem 3.3.5, we have

$$|(H^\perp)^\perp| = \frac{|G|}{|H^\perp|} = \frac{|G|}{|G|/|H|} = |H|.$$

Thus $(H^\perp)^\perp = H$. □

3.3.7 Corollary. *We have* $G/H^\perp \cong H$.

Proof. By the previous theorem, $(H^\perp)^\perp = H$, and Theorem 3.3.5 gives $G/H^\perp \cong (H^\perp)^\perp = H$.

□

3.3.8 Definition. A *self-orthogonal* subgroup of G is a subgroup O of G such that $O = O^\perp$.

3.3.9 Theorem. *Let* O *be a subgroup of* G*. If* O *is self-orthogonal, then* $|O| = \sqrt{|G|}$.

Proof. By Theorem 3.3.5 and Lagrange's Theorem, we have

$$O \text{ is self-orthogonal} \Rightarrow O = O^\perp$$

$$\Rightarrow O = O^{\perp} \cong G/O$$

$$\Rightarrow |O|^2 = |G|$$

$$\Rightarrow |O| = \sqrt{|G|}.$$

□

3.3.10 Note. Observe that the contrapositive of the previous theorem states that *if* $|O| \neq \sqrt{|G|}$, *then* O *is not self-orthogonal*. Thus it follows that, if $|G|$ is not a perfect square, then G contains no self-orthogonal subgroups.

3.3.11 Theorem. *Let* H *and* K *be subgroups of* G. *We have* $K \subseteq H$ *if and only if* $H^{\perp} \subseteq K^{\perp}$.

Proof. For the forward direction, suppose $K \subseteq H$. Let $a \in H^{\perp}$. Then $a \circ h = 0$ for all $h \in H$, and thus $a \circ k = 0$ for all $k \in K$. Hence $a \in K^{\perp}$, and therefore, $H^{\perp} \subseteq K^{\perp}$. For the other direction, assume that $H^{\perp} \subseteq K^{\perp}$. By Theorem 3.3.6 and what we have just shown, we have $K = (K^{\perp})^{\perp} \subseteq (H^{\perp})^{\perp} = H$. The claim follows.

□

3.3.12 Definition. By an *orthomorphism* of G we mean a permutation f of G with $f(a) \circ f(b) = a \circ b$ for all $a, b \in G$.

3.3.13 Theorem. *If* f *is an orthomorphism of* G, *then* f *is an automorphism of* G.

Proof. Let f be an orthomorphism on G. Let $x, y \in G$. Since f is by definition a permutation of G, it suffices to show only that f is a homomorphism. Thus for any $a \in G$, we have

$$\begin{aligned} \iota_{f(x+y)}(a) &= f(x+y) \circ a \\ &= f(x+y) \circ f(f^{-1}(a)) \\ &= (x+y) \circ f^{-1}(a) \end{aligned}$$

$$
\begin{aligned}
&= x \circ f^{-1}(a) + y \circ f^{-1}(a) \\
&= f(x) \circ f(f^{-1}(a)) + f(y) \circ f(f^{-1}(a)) \\
&= f(x) \circ a + f(y) \circ a \\
&= (f(x) + f(y)) \circ a \\
&= \iota_{f(x)+f(y)}(a),
\end{aligned}
$$

which implies $\iota_{f(x+y)} = \iota_{f(x)+f(y)}$. Since $\varphi : G \to G^*$ given by $\varphi(g) = \iota_g$ is an isomorphism and

$$\varphi(f(x+y)) = \iota_{f(x+y)} = \iota_{f(x)+f(y)} = \varphi(f(x) + f(y)),$$

we obtain $f(x+y) = f(x) + f(y)$. Hence f is an automorphism of G.

□

3.3.14 Theorem. *For every orthomorphism f of G and subgroup H of G, we have $f(H^\perp) = f(H)^\perp$.*

Proof. Let f be a orthomorphism of G, and let $H \leq G$. Let $g \in G$. Then

$$
\begin{aligned}
g \in f(H^\perp) &\iff f^{-1}(g) \in H^\perp \\
&\iff f^{-1}(g) \circ h = 0, \quad \forall h \in H \\
&\iff f(f^{-1}(g)) \circ f(h) = 0, \quad \forall h \in H \\
&\iff g \circ f(h) = 0, \quad \forall h \in H \\
&\iff g \in f(H)^\perp.
\end{aligned}
$$

The claim follows.

□

3.3.15 Corollary. *Orthomorphic images of self-orthogonal subgroups of G are self-orthogonal subgroups of G.*

Proof. Let f be an orthomorphism of G, and let O be a self-orthogonal subgroup of G. Observe that $f(H^{\perp}) = f(H)^{\perp}$ for all $H \leq G$ from the previous theorem and $O = O^{\perp}$, respectively. Therefore, we get $f(O) = f(O^{\perp}) = f(O)^{\perp}$. The claim follows.

□

3.4 Symplectic Complements of Subgroups of G

Set $\overline{G} = G \oplus G$. We have

$$\overline{G} = G \oplus G = (\mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_n}) \oplus (\mathbb{Z}_{m_{n+1}} \oplus \mathbb{Z}_{m_{n+2}} \oplus \cdots \oplus \mathbb{Z}_{m_{2n}}),$$

where $m_{n+j} = m_j$, since $G = \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_n}$. Thus observe that an element $x \in \overline{G}$ can be expressed as $x = (a, b)$, for some $a, b \in G$; hence, $x = (x_1, x_2, \ldots, x_n, x_{n+1}, \ldots, x_{2n}) = (a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_n)$, where $x_i = a_i, x_{n+i} = b_i \in \mathbb{Z}_{m_i}$ $(1 \leq i \leq n)$.

For the following, let K be a subgroup of $\overline{G}$.

3.4.1 Definition. The symplectic product of two elements $(a, b), (c, d) \in \overline{G}$ is defined by $(a, b) * (c, d) := b \circ c - a \circ d$, where the product $\circ$ is defined as it is in Section 3.2.

3.4.2 Definition. Define $\psi : \overline{G} \oplus \overline{G} \to \mathbb{Z}_m$ by

$$\psi((a, b), (c, d)) = (a, b) * (c, d).$$

For $x \in \overline{G}$, define $\psi_x : \overline{G} \to \mathbb{Z}_m$ by $\psi_x(y) = \psi(x, y)$.

3.4.3 Note. It is straightforward to check that ψ is a bilinear form. Moreover, ψ is alternating since $\psi((a, b), (a, b)) = 0$ for all $(a, b) \in \overline{G}$. Thus by Theorem 3.1.9, ψ is skew-symmetric, so by Theorem 3.1.4 and the note following it, $K^\psi = \{x \in \overline{G} \mid \psi(x, y) = 0 \text{ for all } y \in K\}$.

3.4.4 Definition. Define the *symplectic complement* K^Δ of K by $K^\Delta = \{x \in \overline{G} \mid x * y = 0 \text{ for all } y \in K\}$.

3.4.5 Note. Observe from the previous definition that indeed, $K^{\Delta} = K^{\psi}$. By Theorem 3.1.3 it follows from the fact that ψ is bilinear that K^{Δ} is a subgroup of $\overline{G}$.

3.4.6 Note. Substituting G for $\overline{G}$ in the definition of $\circ$, we obtain a bilinear form $(x, y) \mapsto x \circ y$ on $\overline{G}$ having the property that for every $(a, b), (c, d) \in \overline{G}$ we have $(a, b) \circ (c, d) = a \circ c + b \circ d$, with each $\circ$ on the right being the operator defined on G.

3.4.7 Corollary. *Let* $(a, b), (c, d) \in \overline{G}$. *Then we have* $(a, b) * (c, d) = (a, b) \circ (-d, c)$ *and also* $(a, b) * (c, d) = (b, -a) \circ (c, d)$.

Proof. This fact follows immediately from the definition of $(a, b) * (c, d)$ and the previous note. □

3.4.8 Note. Recall that since ψ is a bilinear form, we have that ψ_x is a $\mathbb{Z}_m$-module homomorphism, and thus $\psi_x \in \overline{G}^*$ for each $x \in \overline{G}$. Define $\rho : \overline{G} \to \overline{G}^*$ by $\rho(x) = \psi_x$. Recall from Theorem 3.2.7 the isomorphism $\varphi : \overline{G} \to \overline{G}^*$ defined by $\varphi(x) = \iota_x$. Then the previous corollary implies

$$\psi_{(a,b)}\big((c, d)\big) = (a, b) * (c, d) = (b, -a) \circ (c, d) = \iota_{(b,-a)}\big((c, d)\big)$$

for all $(c, d) \in \overline{G}$. Thus $\rho(a, b) = \psi_{(a,b)} = \iota_{(b,-a)} = \varphi(b, -a)$ for $(a, b) \in \overline{G}$. Since $\varphi : \overline{G} \to \overline{G}^*$ is an isomorphism by Theorem 3.2.7, it follows that $\rho : \overline{G} \to \overline{G}^*$ is an isomorphism.

3.4.9 Lemma. *The bilinear form* ψ *is non-degenerate.*

Proof. By Theorem 3.1.7, it suffices to prove that ψ_1 and ψ_2 are injections. Since ψ is skew-symmetric, Theorem 3.1.8 implies $\psi_1 = -\psi_2$, and it follows that we only need to prove that ψ_1 is an injection. Let $x, y \in \overline{G}$. Suppose $\psi_1(x) = \psi_1(y)$. Thus $\rho(x) = \psi_x = \psi_1(x) = \psi_1(y) = \psi_y = \rho(y)$. By Note 3.4.8, ρ is an isomorphism. Thus ρ is an injection, so $x = y$. Therefore,

ψ_1 is an injection. The claim follows.

□

3.4.10 Note. Since ψ is alternating and non-degenerate, we have that ψ is a symplectic bilinear form by Definition 3.1.2.

3.4.11 Theorem. *We have* $K^{\perp} \cong \overline{G}/K$ *and* $K^{\Delta} \cong \overline{G}/K$.

Proof. Since both $\iota : \overline{G} \oplus \overline{G} \to \mathbb{Z}_m$ and $\psi : \overline{G} \oplus \overline{G} \to \mathbb{Z}_m$ are non-degenerate by Lemmas 3.3.3 and 3.4.9, respectively, Theorem 3.3.2 implies $K^{\perp} \cong \overline{G}/K$ and $K^{\Delta} \cong \overline{G}/K$.

□

3.4.12 Corollary. *We have* $(K^{\Delta})^{\Delta} = K$.

Proof. Since $(K^{\Delta})^{\Delta} = \{x \in \overline{G} \mid \psi_x(y) = 0 \ \forall y \in K^{\Delta}\}$ and $\psi_x(y) = x*y = -y*x = -\psi_y(x)$ for all $x, y \in \overline{G}$, it follows that $K \subseteq (K^{\Delta})^{\Delta}$. The previous corollary implies $(K^{\Delta})^{\Delta} \cong \overline{G}/K^{\Delta}$. By Lagrange's Theorem, we have

$$|(K^{\Delta})^{\Delta}| = \frac{|\overline{G}|}{|K^{\Delta}|} = \frac{|\overline{G}|}{|\overline{G}|/|K|} = |K|.$$

Thus $(K^{\Delta})^{\Delta} = K$.

□

3.4.13 Corollary. *Let* H *and* K *be subgroups of* $\overline{G}$. *Then* $K \subseteq H$ *if and only if* $H^{\Delta} \subseteq K^{\Delta}$.

Proof. The proof of Theorem 3.3.11 applies with $\perp$ replaced by Δ and $\circ$ replaced by $*$.

□

3.4.14 Definition. A *Lagrangian* subgroup of $\overline{G}$ is a subgroup L of $\overline{G}$ such that $L = L^{\Delta}$.

3.4.15 Theorem. *Let* L *be a subgroup of* $\overline{G}$. *If* L *is Lagrangian, then* $|L| = |G|$.

Proof. By Theorem 3.4.11 and Lagrange's Theorem, we have

$$\begin{aligned} L \text{ is Lagragian} &\Rightarrow L = L^{\Delta} \\ &\Rightarrow \overline{G}/L \cong L^{\Delta} = L \\ &\Rightarrow |G|^2 = |G \oplus G| = |\overline{G}| = |L|^2 \\ &\Rightarrow |G| = |L|. \end{aligned}$$

□

3.4.16 Definition. By a *symplectomorphism* of $\overline{G}$ we mean a permutation f of $\overline{G}$ with $f(x) * f(y) = x * y$ for all $x, y \in \overline{G}$.

3.4.17 Theorem. *If f is a symplectomorphism of $\overline{G}$, then f is an automorphism of $\overline{G}$.*

Proof. Let f be a symplectomorphism on $\overline{G}$. Let $(a, b), (c, d) \in \overline{G}$. Since f is by definition a permutation of G, it suffices to show simply that f is a homomorphism. Let $(g, h) \in \overline{G}$. Thus $(g, h) = f(g', h')$ for some $(g', h') \in \overline{G}$. Then

$$\begin{aligned} \psi_{f((a,b)+(c,d))}(g, h) &= f(a + c, b + d) * (g, h) \\ &= f(a + c, b + d) * f(g', h') \\ &= (a + c, b + d) * (g', h') \\ &= (b + d) \circ g' - (a + c) \circ h' \\ &= b \circ g' - a \circ h' + d \circ g' - c \circ h' \\ &= (a, b) * (g', h') + (c, d) * (g', h') \\ &= f(a, b) * f(g', h') + f(c, d) * f(g', h') \\ &= (f(a, b) + f(c, d)) * (g, h) \\ &= \psi_{f(a,b)+f(c,d)}(g, h), \end{aligned}$$

which implies $\psi_{f((a,b)+(c,d))} = \psi_{f(a,b)+f(c,d)}$. Since $\rho : \overline{G} \to \overline{G}^*$ given by $\rho(a,b) = \psi_{(a,b)}$ is an isomorphism, we obtain $f((a,b)+(c,d)) = f(a,b) + f(c,d)$. Hence f is an automorphism of $\overline{G}$.

□

Let $\mathrm{Sp}(\overline{G})$ denote the collection of symplectomorphisms of $\overline{G}$. It is straightforward to prove that $\mathrm{Sp}(\overline{G})$ is a subgroup of the group $Aut(\overline{G})$ of automorphisms of $\overline{G}$.

The next theorem says that symplectomorphisms preserve symplectic complements.

3.4.18 Theorem. *For every symplectomorphism f of $\overline{G}$ and subgroup H of $\overline{G}$, we have $f(H^\Delta) = f(H)^\Delta$.*

Proof. Let f be a symplectomorphism of $\overline{G}$, and let $H \leq \overline{G}$. Let $(a,b) \in \overline{G}$. Then

$$\begin{aligned}
(a,b) \in f(H^\Delta) &\iff f^{-1}(a,b) \in H^\Delta \\
&\iff f^{-1}(a,b) * (h,k) = 0, \quad \forall (h,k) \in H \\
&\iff f(f^{-1}(a,b)) * f(h,k) = 0, \quad \forall (h,k) \in H \\
&\iff (a,b) * f(h,k) = 0, \quad \forall (h,k) \in H \\
&\iff (a,b) \in f(H)^\Delta.
\end{aligned}$$

The claim follows.

□

3.4.19 Corollary. *Symplectomorphic images of Lagrangian subgroups of $\overline{G}$ are Lagrangian subgroups of $\overline{G}$.*

Proof. Let f be a symplectomorphism of $\overline{G}$, and let L be a Lagrangian subgroup of $\overline{G}$. Observe that $f(H^\Delta) = f(H)^\Delta$ for all $H \leq \overline{G}$ from Theorem 3.4.18 and $L = L^\Delta$, respectively.

Therefore, we get $f(L) = f(L^{\Delta}) = f(L)^{\Delta}$. The claim follows.

□

Chapter 4

Generalizations of the Pauli Group, the Pauli Algebra, and the Clifford Group

4.1 Pauli Maps

Recall that $G = \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_n}$ with $n, m_i \in \mathbb{Z}^+$. Henceforth, we let m be a fixed common multiple of the set $\{2m_i \mid 1 \leq i \leq n\}$. Put $m' = m/2$. It is straightforward to prove that m' is a common multiple of the set $\{m_i \mid 1 \leq i \leq n\}$. Thus we may apply the results from Section 3.2 to G with $m' = m/2$. Recall again the definition of $a \circ b$ for $a, b \in G$:

$$a \circ b = \sum_{i=1}^{n} a_i b_i \left(\frac{m}{m_i}\right) \cdot 1.$$

where we take $a_i b_i \left(\frac{m}{m_i}\right) \in \mathbb{Z}$ and $1 \in \mathbb{Z}_m$. Thus

$$a \circ b = 2 \sum_{i=1}^{n} a_i b_i \left(\frac{m'}{m_i}\right) \cdot 1,$$

where $1 \in \mathbb{Z}_m$. Since $m'/m_i \in \mathbb{Z}$ for all i, we have that $\sum_{i=1}^{n} a_i b_i \left(\frac{m'}{m_i}\right) \in \mathbb{Z}$, and thus $\sum_{i=1}^{n} a_i b_i \left(\frac{m'}{m_i}\right) \cdot 1 \in \mathbb{Z}_m$. Therefore, for $a, b \in G$, we have $a \circ b = 2 \sum_{i=1}^{n} a_i b_i \left(\frac{m'}{m_i}\right) \cdot 1 \in 2\mathbb{Z}_m$.

Recall that the group algebra $\mathbb{C}G$ of G over $\mathbb{C}$ is the algebra over $\mathbb{C}$ having as its underlying vector space the vector space with basis G and having as its product the product in the group G extended linearly. Let $\langle \cdot \mid \cdot \rangle$ be the inner product on $\mathbb{C}G$ uniquely determined by the assignment $\langle g \mid h \rangle = \delta_{gh}$, where δ_{gh} is the Kronecker delta function.

For each $g \in G$, let X^g denote the linear operator on $\mathbb{C}G$ uniquely determined by $X^g|h\rangle := X^g(|h\rangle) = |h+g\rangle$, for $h \in G$. Written explicitly, we see that $X^g = \sum_{h \in G} |h+g\rangle\langle h|$ and hence

$$X^g \left(\sum_{h \in G} \alpha_h |h\rangle \right) = \sum_{h \in G} \alpha_h |h+g\rangle.$$

Similarly, for each $g \in G$, let Z^g denote the linear operator on $\mathbb{C}G$ uniquely determined by $Z^g|h\rangle := Z^g(|h\rangle) = \epsilon_m^{g \circ h}|h\rangle$, for $h \in G$, where $\epsilon_m = e^{2\pi i/m}$, where $i = \sqrt{-1}$. Written explicitly, we see that $Z^g = \sum_{h \in G} \epsilon_m^{g \circ h} |h\rangle\langle h|$ and hence

$$Z^g \left(\sum_{h \in G} \alpha_h |h\rangle \right) = \sum_{h \in G} \alpha_h \epsilon_m^{g \circ h} |h\rangle.$$

For general $k \in \mathbb{Z}^+$, define $\epsilon_k \in \mathbb{C}$ by $\epsilon_k := e^{2\pi i/k}$, where $i = \sqrt{-1}$.

Define $X, Z : G \to \mathrm{GL}(\mathbb{C}G)$ by $X(g) = X^g$ and $Z(g) = Z^g$.

4.1.1 Theorem. *The maps X and Z are monomorphisms. In particular, $X^{g+h} = X^g X^h$ and $Z^{g+h} = Z^g Z^h$ for any $g, h \in G$.*

Proof. Let $g, h \in G$. For any $a \in G$, we have

$$X(g+h)|a\rangle = X^{g+h}|a\rangle = |a+g+h\rangle = X^g|a+h\rangle = X^g X^h|a\rangle = X(g)X(h)|a\rangle.$$

Thus $X(g+h) = X(g)X(h)$, so X is a homomorphism. It is straightforward to prove that X is injective. Thus X is a monomorphism. In particular, we have $X^{g+h} = X(g+h) = X(g)X(h) = X^g X^h$.

Similarly, for any $a \in G$, we have

$$Z(g+h)|a\rangle = \epsilon_m^{(h+g)\circ a}|a\rangle = \epsilon_m^{h\circ a}\epsilon_m^{g\circ a}|a\rangle = \epsilon_m^{h\circ a}Z^g|a\rangle = Z^g(\epsilon_m^{h\circ a}|a\rangle) = Z^g Z^h|a\rangle = Z(g)Z(h)|a\rangle.$$

Thus $Z(g+h) = Z(g)Z(h)$, so Z is a homomorphism. It is also straightforward to prove that Z is injective. Thus Z is a monomorphism. In particular, we have $Z^{g+h} = Z(g+h) = Z(g)Z(h) = Z^g Z^h$.

□

4.1.2 Definition. The *generalized Walsh-Hadamard transform* of $\mathbb{C}G$ is the linear operator W on $\mathbb{C}G$ given by

$$W = |G|^{-1/2} \sum_{b\in G} \sum_{a\in G} \epsilon_m^{a\circ b}|a\rangle\langle b|.$$

4.1.3 Theorem. *For all $g \in G$, $WX^g = Z^g W$.*

Proof. Let $g, h \in G$. Then

$$\begin{aligned}
WX^g|h\rangle &= W|h+g\rangle \\
&= \left(|G|^{-1/2} \sum_{b\in G} \sum_{a\in G} \epsilon_m^{a\circ b}|a\rangle\langle b|\right)|h+g\rangle \\
&= |G|^{-1/2} \sum_{a\in G} \epsilon_m^{a\circ(h+g)}|a\rangle \\
&= |G|^{-1/2} \sum_{a\in G} \epsilon_m^{a\circ h}\epsilon_m^{a\circ g}|a\rangle \\
&= |G|^{-1/2} \sum_{a\in G} \epsilon_m^{a\circ h} Z^g|a\rangle
\end{aligned}$$

$$
\begin{aligned}
&= Z^g \left(|G|^{-1/2} \sum_{a \in G} \epsilon_m^{a \circ h} |a\rangle \right) \\
&= Z^g W |h\rangle.
\end{aligned}
$$

Since $h \in G$ was arbitrary, the claim follows.

□

4.1.4 Note. It is routine to check that W is invertible. Therefore, since W^{-1} exists, we have $WX^gW^{-1} = Z^g$.

4.1.5 Note. The above linear operators on $\mathbb{C}G$ generalize the notion of the $bit\ flip$ and $phase\ flip$ operations in the case $G = \mathbb{Z}_2 \oplus \cdots \oplus \mathbb{Z}_2$.

The following theorem describes the commutation relationship between X^g and Z^h under multiplication for $g, h \in G$.

4.1.6 Theorem. *Let $g, h \in G$. Then $Z^h X^g = \epsilon_m^{h \circ g} \cdot X^g Z^h$.*

Proof. Let $b \in G$. Then

$$
Z^h X^g |b\rangle = Z^h |b + g\rangle = \epsilon_m^{h \circ (g+b)} |b + g\rangle = \epsilon_m^{h \circ g} \epsilon_m^{h \circ b} X^g |b\rangle = \epsilon_m^{h \circ g} X^g (\epsilon_m^{h \circ b} |b\rangle) = \epsilon_m^{h \circ g} \cdot X^g Z^h |b\rangle.
$$

The claim follows.

□

4.2 Pauli Group

Again recall that $G = \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_n}$ with $n, m_i \in \mathbb{Z}^+$, and m is a fixed common multiple of the set $\{2m_i \mid 1 \leq i \leq n\}$.

4.2.1 Definition. Define the *(General) Pauli group $\mathcal{P}_G$ of G* to be the subgroup of $\mathrm{GL}(\mathbb{C}G)$ generated by the set $\{\epsilon_m^k I, X^g, Z^h \mid k \in \mathbb{Z}_m,\ g, h \in G\}$.

4.2.2 Theorem. *The (General) Pauli group is equal to the set $\{\epsilon_m^k X^g Z^h \mid k \in \mathbb{Z}_m,\ g, h \in G\}$.*

Proof. Since $\mathcal{P}_G$ is defined as the subgroup of $\mathrm{GL}(\mathbb{C}G)$ generated by the set $\{\epsilon_m^k I, X^g, Z^h \mid k \in \mathbb{Z}_m,\ g, h \in G\}$, we have that $\mathcal{P}_G$ is the collection of all products of elements from the set $\{\epsilon_m^k I, X^g, Z^h \mid k \in \mathbb{Z}_m,\ g, h \in G\}$. By Theorems 4.1 and 4.1.6, it follows that $\mathcal{P}_G \subseteq \{\epsilon_m^k X^g Z^h \mid k \in \mathbb{Z}_m,\ g, h \in G\}$. Since the other inclusion is immediate as each element of $\{\epsilon_m^k X^g Z^h \mid k \in \mathbb{Z}_m,\ g, h \in G\}$ is a product of elements from $\{\epsilon_m^k I, X^g, Z^h \mid k \in \mathbb{Z}_m,\ g, h \in G\}$, we obtain $\mathcal{P}_G = \{\epsilon_m^k X^g Z^h \mid k \in \mathbb{Z}_m,\ g, h \in G\}$. The claim follows.

□

A basis for $\mathbb{C}G$ is $\{|g_1 g_2 \cdots g_n\rangle \mid g_i \in \mathbb{Z}_{m_i}\}$. For $g_i \in \mathbb{Z}_{m_i}$, an equivalent way to express $|g_1 g_2 \cdots g_n\rangle$ is by $|g_1\rangle|g_2\rangle \cdots |g_n\rangle$, which is itself shorthand for $|g_1\rangle \otimes |g_2\rangle \otimes \cdots \otimes |g_n\rangle$, and this is due to the identification of the spaces $\mathbb{C}G$ and $\mathbb{C}\mathbb{Z}_{m_1} \otimes \mathbb{C}\mathbb{Z}_{m_2} \otimes \cdots \otimes \mathbb{C}\mathbb{Z}_{m_n}$.

4.2.3 Theorem. *Let $g \in G$. We have $X^g = X^{g_1} \otimes X^{g_2} \otimes \cdots \otimes X^{g_n}$ and $Z^g = Z^{g_1} \otimes Z^{g_2} \otimes \cdots \otimes Z^{g_n}$.*

Proof. Let $h \in G$. Then $h = (h_1, h_2, \ldots, h_n)$ for some $h_i \in \mathbb{Z}_{m_i}$. Thus

$$\begin{aligned} X^g|h\rangle &= |g + h\rangle \\ &= |g_1 + h_1\rangle|g_2 + h_2\rangle \cdots |g_n + h_n\rangle \end{aligned}$$

$$
\begin{aligned}
&= X^{g_1}|h_1\rangle X^{g_2}|h_2\rangle \cdots X^{g_n}|h_n\rangle \\
&= (X^{g_1} \otimes X^{g_2} \otimes \cdots \otimes X^{g_n})(|h_1\rangle|h_2\rangle \cdots |h_n\rangle) \\
&= (X^{g_1} \otimes X^{g_2} \otimes \cdots \otimes X^{g_n})|h\rangle.
\end{aligned}
$$

Also, we have

$$
\begin{aligned}
Z^g|h\rangle &= \epsilon_m^{g\circ h}|h\rangle \\
&= \epsilon_m^{\sum_{i=1}^n (m/m_i)g_ih_i}(|h_1\rangle|h_2\rangle \cdots |h_n\rangle) \\
&= \prod_{i=1}^n \epsilon_m^{(m/m_i)g_ih_i}(|h_1\rangle|h_2\rangle \cdots |h_n\rangle) \\
&= (\epsilon_m^{(m/m_1)g_1h_1}|h_1\rangle)(\epsilon_m^{(m/m_2)g_2h_2}|h_2\rangle) \cdots (\epsilon_m^{(m/m_n)g_nh_n}|h_n\rangle) \\
&= ((e^{2\pi\sqrt{-1}/m})^{(m/m_1)g_1h_1}|h_1\rangle)((e^{2\pi\sqrt{-1}/m})^{(m/m_2)g_2h_2}|h_2\rangle) \cdots ((e^{2\pi\sqrt{-1}/m})^{(m/m_n)g_nh_n}|h_n\rangle) \\
&= ((e^{2\pi\sqrt{-1}/m_1})^{g_1h_1}|h_1\rangle)((e^{2\pi\sqrt{-1}/m_2})^{g_2h_2}|h_2\rangle) \cdots ((e^{2\pi\sqrt{-1}/m_n})^{g_nh_n}|h_n\rangle) \\
&= (\epsilon_{m_1}^{g_1h_1}|h_1\rangle)(\epsilon_{m_2}^{g_2h_2}|h_2\rangle) \cdots (\epsilon_{m_n}^{g_nh_n}|h_n\rangle) \\
&= Z^{g_1}|h_1\rangle Z^{g_2}|h_2\rangle \cdots Z^{g_n}|h_n\rangle. \\
&= (Z^{g_1} \otimes Z^{g_2} \otimes \cdots \otimes Z^{g_n})|h_1\rangle|h_2\rangle \cdots |h_n\rangle \\
&= (Z^{g_1} \otimes Z^{g_2} \otimes \cdots \otimes Z^{g_n})|h\rangle.
\end{aligned}
$$

The claims follow.

□

4.2.4 Lemma. *Let $g, g' \in G$. The following statements are equivalent:*

(a) $g \circ g' = 0$

(b) $g \in \langle g' \rangle^\perp$

(c) $g' \in \langle g \rangle^\perp$

Proof. $(a) \Rightarrow (b)$: Suppose $g \circ g' = 0$. Let $x \in \langle g' \rangle$. We have $x = kg'$ for some $k \in \mathbb{Z}$. Then

$$g \circ x = g \circ kg' = g \circ (\underbrace{g' + g' + \cdots + g'}_{k \text{ times}}) = \underbrace{g \circ g' + g \circ g' + \cdots + g \circ g'}_{k \text{ times}} = 0,$$

implying $g \in \langle g' \rangle^{\perp}$.

$(b) \Rightarrow (a)$: Trivial.

$(a) \Leftrightarrow (c)$: This follows from $(a) \Leftrightarrow (b)$ and the fact that the form $\circ$ is symmetric.

The claim follows.

□

4.2.5 Definition. Let $g, h \in G$. We say X^g and Z^h are *compatible* if $X^g Z^h = Z^h X^g$.

4.2.6 Theorem. *Let $g, h \in G$. Then X^g and Z^h are compatible if and only if $g \in \langle h \rangle^{\perp}$ (equivalently $h \in \langle g \rangle^{\perp}$).*

Proof. By Theorem 4.1.6, $Z^h X^g = \epsilon_m^{h \circ g} X^g Z^h$. We have

$$\begin{aligned} X^g \text{ and } Z^h \text{ are compatible} &\iff X^g Z^h = Z^h X^g \\ &\iff X^g Z^h = \epsilon_m^{h \circ g} X^g Z^h \\ &\iff 1 = \epsilon_m^{h \circ g} \\ &\iff h \circ g = 0 \\ &\iff g \in \langle h \rangle^{\perp}. \end{aligned}$$

The implications $(b) \Leftrightarrow (c)$ in the preceding lemma complete the proof. □

4.2.7 Theorem. *Let $a, b, c, d \in G$. Then $(X^a Z^b)(X^c Z^d) = \epsilon_m^{b \circ c - a \circ d} (X^c Z^d)(X^a Z^b)$.*

Proof. We have

$$\begin{aligned} X^a(Z^bX^c)Z^d &= X^a(\epsilon_m^{b\circ c}X^cZ^b)Z^d \\ &= \epsilon_m^{b\circ c}X^{a+c}Z^{b+d} \\ &= \epsilon_m^{b\circ c}X^c(X^aZ^d)Z^b \\ &= \epsilon_m^{b\circ c}X^c(\epsilon_m^{-a\circ d}Z^dX^a)Z^b \\ &= \epsilon_m^{b\circ c-a\circ d}(X^cZ^d)(X^aZ^b). \end{aligned}$$

□

4.2.8 Note. Utilizing the notation for the symplectic product on $\overline{G}$, the previous result could be expressed as

$$(X^aZ^b)(X^cZ^d) = \epsilon_m^{(a,b)*(c,d)}(X^cZ^d)(X^aZ^b) \text{ for all } a,b,c,d \in G.$$

4.2.9 Theorem. *Let $g, h \in G$. For any $k \in \mathbb{Z}$, $(X^gZ^h)^k = \epsilon_m^{\frac{k(k-1)}{2}\cdot(g\circ h)}X^{kg}Z^{kh}$.*

Proof. We first prove by induction that the equality holds for all $k \geq 0$. The case for $k = 0$ is trivial. Now let $k > 0$. By induction, $(X^gZ^h)^{k-1} = \epsilon_m^{\frac{(k-1)(k-2)}{2}\cdot(g\circ h)}X^{(k-1)g}Z^{(k-1)h}$. Then we have

$$\begin{aligned} (X^gZ^h)^k &= (X^gZ^h)^{k-1}(X^gZ^h) \\ &= \epsilon_m^{\frac{(k-1)(k-2)}{2}\cdot(g\circ h)}X^{(k-1)g}(Z^{(k-1)h}X^g)Z^h \\ &= \epsilon_m^{\frac{(k-1)(k-2)}{2}\cdot(g\circ h)}X^{(k-1)g}(\epsilon_m^{(k-1)g\circ h}X^gZ^{(k-1)h})Z^h \\ &= \epsilon_m^{\frac{(k-1)(k-2)+2(k-1)}{2}\cdot(g\circ h)}X^{kg}Z^{kh} \\ &= \epsilon_m^{\frac{k^2-k}{2}\cdot(g\circ h)}X^{kg}Z^{kh} \\ &= \epsilon_m^{\frac{k(k-1)}{2}\cdot(g\circ h)}X^{kg}Z^{kh}. \end{aligned}$$

Now, observe that inverting both sides of the equation $(X^g Z^h)^k = \epsilon_m^{\frac{k(k-1)}{2}\cdot(g\circ h)} X^{kg} Z^{kh}$ gives

$$\begin{aligned}
(X^g Z^h)^{-k} &= \epsilon_m^{-\frac{k(k-1)}{2}\cdot(g\circ h)} Z^{-kh} X^{-kg} \\
&= \epsilon_m^{-\frac{k(k-1)}{2}\cdot(g\circ h)} \left(\epsilon_m^{(-kh)\circ(-kg)} X^{-kg} Z^{-kh}\right) \\
&= \epsilon_m^{\frac{-k^2+k}{2}\cdot(g\circ h)} \left(\epsilon_m^{k^2(g\circ h)} X^{-kg} Z^{-kh}\right) \\
&= \epsilon_m^{\frac{-k^2+k+2k^2}{2}\cdot(g\circ h)} X^{-kg} Z^{-kh} \\
&= \epsilon_m^{\frac{k^2+k}{2}\cdot(g\circ h)} X^{-kg} Z^{-kh} \\
&= \epsilon_m^{\frac{-k(-k-1)}{2}\cdot(g\circ h)} X^{-kg} Z^{-kh}.
\end{aligned}$$

Thus, for $k > 0$ and $j = -k$, we obtain $(X^g Z^h)^j = \epsilon_m^{\frac{j(j-1)}{2} g\circ h} X^{jg} Z^{jh}$. Thus the formula holds for $j = -k < 0$.

□

Recall that $o(x)$ denotes the order of the element $x \in G$. By Theorem 4.1, $X : G \to \mathrm{GL}(\mathbb{C}G)$ and $Z : G \to \mathrm{GL}(\mathbb{C}G)$ given by $X(g) = X^g$ and $Z(h) = Z^h$, respectively, are monomorphisms. Thus for all $g, h \in G$, we have $o(g) = o(X^g)$ and $o(h) = o(Z^h)$.

4.2.10 Theorem. *Let $g, h \in G$, and set $\ell := \mathrm{lcm}(o(g), o(h)) = \mathrm{lcm}(o(X^g), o(Z^h))$. If ℓ is odd, then $o(X^g Z^h)$ has order ℓ, and if ℓ is even, then $X^g Z^h$ has order ℓ when $o(g \circ h)$ divides $\ell/2$, and $X^g Z^h$ has order 2ℓ otherwise.*

Proof. Let $k \in \mathbb{Z}^+$, and assume that $(X^g Z^h)^k = I$. Thus $\epsilon_m^{\frac{k(k-1)}{2}\cdot(g\circ h)} X^{kg} Z^{kh} = I$ by the previous theorem. In particular, this implies $X^{kg} = I$ and $Z^{kh} = I$ so that k is a common multiple of $o(X^g)$ and $o(Z^h)$. Therefore, $\ell \mid k$.

Now, suppose ℓ is odd, i.e. $\ell = 2j + 1$ for some $j \in \mathbb{N}$. Thus

$$\begin{aligned}
(X^g Z^h)^\ell &= \epsilon_m^{\frac{\ell(\ell-1)}{2}\cdot(g\circ h)} X^{\ell g} Z^{\ell h} \\
&= \epsilon_m^{\frac{\ell(2j)}{2}\cdot(g\circ h)} (X^g)^\ell (Z^h)^\ell \\
&= \epsilon_m^{\ell j(g\circ h)} I
\end{aligned}$$

$$= \epsilon_m^{j((\ell g)\circ h)} I$$
$$= \epsilon_m^{0} I$$
$$= I.$$

If ℓ is even, i.e. $\ell = 2j$ for some $j \in \mathbb{N}$, then

$$\begin{aligned}(X^g Z^h)^\ell &= \epsilon_m^{\frac{\ell(\ell-1)}{2}\cdot(g\circ h)} X^{\ell g} Z^{\ell h} \\ &= \epsilon_m^{\frac{2j(\ell-1)}{2}\cdot(g\circ h)} I \\ &= \epsilon_m^{j(\ell-1)(g\circ h)} I \\ &= \epsilon_m^{\ell j(g\circ h) - j(g\circ h)} I \\ &= \epsilon_m^{j((\ell g)\circ h) - j(g\circ h)} I \\ &= \epsilon_m^{-j(g\circ h)} I.\end{aligned}$$

Therefore, if $\ell = 2j$ for some $j \in \mathbb{N}$, then

$$\begin{aligned} & (X^g Z^h)^\ell = I \\ \iff \quad & \epsilon_m^{-j(g\circ h)} I = I \\ \iff \quad & \epsilon_m^{-j(g\circ h)} = 1 \\ \iff \quad & -j(g\circ h) = 0 \\ \iff \quad & o(g\circ h) \mid j = \ell/2.\end{aligned}$$

In particular, if $o(g \circ h) \mid \ell/2$, then $X^g Z^h$ has order ℓ. On the other hand, if $o(g \circ h) \nmid \ell/2$, and thus $(X^g Z^h)^\ell = \epsilon_m^{-j(g\circ h)} I \neq I$, then the equations $(X^g Z^h)^{2\ell} = \epsilon_m^{-2j(g\circ h)} I = \epsilon_m^{-((\ell g)\circ h)} I = I$ and $(X^g Z^h)^\ell \neq I$, together with the fact established earlier that the order of $X^g Z^h$ is a multiple of ℓ, yield the conclusion that $X^g Z^h$ has order 2ℓ. The claim follows.

□

For the following, recall from the opening statements in Section 4.1 that for $a, b \in G$, $a \circ b \in 2\mathbb{Z}_m$. It follows that, for $a, b \in G$, we have $a \circ b = 2k$ for some $k \in \mathbb{Z}_m$, and thus $(a \circ b)/2$ can be taken to mean k.

4.2.11 Corollary. *Let $g, h \in G$. If $\ell = \operatorname{lcm}(o(X^g), o(Z^h))$ is even, then $\epsilon_m^{(g\circ h)/2} X^g Z^h$ has order ℓ.*

Proof. From the previous proof, we observe that for $\ell = 2j$, with $j \in \mathbb{N}$, the equation $(X^g Z^h)^\ell = \epsilon_m^{-j(g\circ h)} I$ implies $\epsilon_m^{j(g\circ h)} (X^g Z^h)^\ell = I$, which implies

$$(\epsilon_m^{(g\circ h)/2} X^g Z^h)^\ell = \epsilon_m^{\frac{\ell}{2}(g\circ h)} (X^g Z^h)^\ell = \epsilon_m^{j(g\circ h)} (X^g Z^h)^\ell = I.$$

The claim follows.

□

4.2.12 Theorem. *Let N and M be groups, and let $\rho, \varphi : N \to M$ be homomorphisms. The product $\rho \cdot \varphi : N \to M$ given by $(\rho \cdot \varphi)(n) = \rho(n)\varphi(n)$ is a homomorphism if and only if $\rho(b)\varphi(a) = \varphi(a)\rho(b)$ for all $a, b \in N$.*

Proof. Let $a, b \in N$. By direct computation, we have

$$\begin{aligned}
\rho \cdot \varphi \text{ is a homomorphism} &\iff (\rho \cdot \varphi)(ab) = (\rho \cdot \varphi)(a)(\rho \cdot \varphi)(b) \\
&\iff \rho(ab)\varphi(ab) = \rho(a)\varphi(a)\rho(b)\varphi(b) \\
&\iff \rho(a)\rho(b)\varphi(a)\varphi(b) = \rho(a)\varphi(a)\rho(b)\varphi(b) \\
&\iff \rho(b)\varphi(a) = \varphi(a)\rho(b).
\end{aligned}$$

□

4.2.13 Definition. Let N and M be groups, and let K be a subgroup of N. Let $\rho, \varphi : N \to M$ be homomorphisms. We say ρ and φ are *compatible* on K if $(\rho \cdot \varphi)|_K : K \to M$ is a homomorphism. Otherwise, we say they are *incompatible* on K.

4.2.14 Note. We make a few quick observations. First, if M is abelian, then ρ and φ are compatible on N. Second, ρ and φ are always compatible on the trivial subgroup of N. Lastly, if either ρ or φ is the trivial homomorphism that maps all of N to the identity of M, then ρ and φ are compatible on N.

Observe that we could apply the previous theorem to the maps $X : G \to \mathrm{GL}(\mathbb{C}G)$ and $Z : G \to \mathrm{GL}(\mathbb{C}G)$ given by $X(g) = X^g$ and $Z(g) = Z^g$, since these are homomorphisms.

4.2.15 Corollary. *Let α and β be endomorphisms of G, and let $X^\alpha, Z^\beta : G \to \mathcal{P}_G$ be maps defined by $X^\alpha(g) = X^{\alpha(g)}$ and $Z^\beta(g) = Z^{\beta(g)}$. The following are equivalent:*

(i) *The product $X^\alpha Z^\beta : G \to \mathcal{P}_G$ defined by $X^\alpha Z^\beta(g) = X^{\alpha(g)} Z^{\beta(g)}$ is a homomorphism.*

(ii) $\alpha(g) \circ \beta(h) = 0$ *for all pairs $g, h \in G$.*

(iii) $\alpha(G) \subseteq \beta(G)^\perp$ *(equivalently, $\beta(G) \subseteq \alpha(G)^\perp$ by Theorem 3.3.11.).*

Proof. First, it is straightforward to show that X^α and Z^β are homomorphisms.

(i $\Leftrightarrow$ ii): From the previous theorem, $X^\alpha Z^\beta : G \to \mathcal{P}_G$ is a homomorphism if and only if $X^{\alpha(g)} Z^{\beta(h)} = Z^{\beta(h)} X^{\alpha(g)}$ for all $g, h \in G$. Due to the commutation relations in $\mathcal{P}_G$, this is true if and only if $\epsilon_m^{\alpha(g) \circ \beta(h)} = 1$ for all $g, h \in G$, which is equivalent to $\alpha(g) \circ \beta(h) = 0$ for all $g, h \in G$.

(ii $\Leftrightarrow$ iii): Since the statement $\alpha(g) \circ \beta(h) = 0$ for all $g, h \in G$ is equivalent to $\alpha(G) \subseteq \beta(G)^{\perp}$ by definition of the orthogonal complement of a subgroup, the claim follows.

□

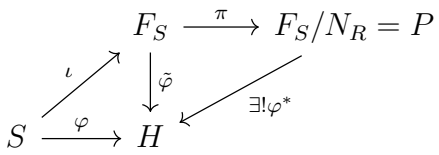
4.3 A Presentation of the Pauli Group

Let S be a set, let F_S be the free group on S, and let $R \subseteq F_S$ be a set of words on S. Let N_R be the normal closure of R in F_S (so N_R is the intersection of all normal subgroups of F_S containing R). Put

$$\langle S \mid R \rangle = F_S / N_R.$$

4.3.1 Theorem (Universal Property of Free Groups)**.** *[Hun80, p. 65] Let $\iota : S \to F_S$ be the inclusion map. If H is a group and $\varphi : S \to H$ is a map of sets, then there exists a unique homomorphism $\tilde{\varphi} : F_S \to H$ such that $\tilde{\varphi}\iota = \varphi$.*

4.3.2 Corollary. *Set $P = \langle S \mid R \rangle$, and suppose that $\varphi : S \to H$ is a function from a set S to a group H. Let $\tilde{\varphi} : F_S \to H$ be the homomorphism granted by the previous theorem that satisfies $\tilde{\varphi}\iota = \varphi$, where $\iota : S \to F_S$ is the inclusion map. Then φ extends to a homomorphism $\varphi^* : P \to H$ that satisfies $\varphi^*\pi = \tilde{\varphi}$ if and only if $\tilde{\varphi}(r) = e_H$ for all $r \in R$, where e_H is the identity in H.*



Proof. For the forward direction, assume there is a homomorphism $\varphi^* : P \to H$ that satisfies $\varphi^*\pi = \tilde{\varphi}$. Let $r \in R$. We have that $r \in N_R$, and thus $\tilde{\varphi}(r) = \varphi^*\pi(r) = \varphi^*(rN_R) = \varphi^*(N_R) = e_H$. Since r was arbitrary, the claim follows.

For the reverse direction, assume $\tilde{\varphi}(r) = e_H$ for all $r \in R$. Thus $R \subseteq \ker \tilde{\varphi}$, and since $\ker \tilde{\varphi}$ is a normal subgroup of F_S and N_R is the intersection of all normal subgroups of F_S containing R, it follows that $N_R \subseteq \ker \tilde{\varphi}$. By the FHT (Theorem 2.3.5), there is a (unique) homomorphism $f : F_S/N_R \to H$ such that $f\pi = \tilde{\varphi}$, where $\pi : F_S \to F_S/N_R$ is the canonical epimorphism. Setting $f = \varphi^*$ and observing that $P = F_S/N_R$, we obtain the desired result.

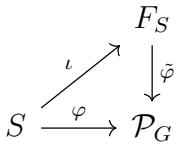
□

4.3.3 Definition. We say a group H has *presentation* $\langle S \mid R \rangle$ if $H \cong \langle S \mid R \rangle$.

4.3.4 Theorem. *$\mathcal{P}_G$ has presentation $\langle S \mid R \rangle$, where*

$$S = \{\epsilon_m^k I, X^g, Z^h \mid k \in \mathbb{Z}_m, g, h \in G\},$$
$$R = \{X^0, Z^0, \epsilon_m^0 I, X^{g+h}X^{-h}X^{-g}, Z^{g+h}Z^{-h}Z^{-g}, (\epsilon_m^{j+k}I)(\epsilon_m^{-k}I)(\epsilon_m^{-j}I),$$
$$(\epsilon_m^k I)X^g(\epsilon_m^{-k}I)X^{-g}, (\epsilon_m^k I)Z^g(\epsilon_m^{-k}I)Z^{-g}, (\epsilon_m^{g\circ h}I)X^gZ^hX^{-g}Z^{-h} \mid g, h \in G, j, k \in \mathbb{Z}_m\}.$$

Proof. Let S and R be defined as they are in the statement of the theorem. Since $S \subset \mathcal{P}_G$ and $S \subset F_S$, we have the inclusion maps $\varphi : S \to \mathcal{P}_G$ and $\iota : S \to F_S$, respectively. By Theorem 4.3.1, there is a homomorphism $\tilde{\varphi} : F_S \to \mathcal{P}_G$ such that $\tilde{\varphi}\iota = \varphi$. We then have the following diagram:



Claim: $\tilde{\varphi}(r) = I$ for all $r \in R$.

First, we have that $\tilde{\varphi}(X^0) = \tilde{\varphi}\iota(X^0) = \varphi(X^0) = X^0 = I$. Similarly, $\tilde{\varphi}(Z^0) = I$ and $\tilde{\varphi}(\epsilon_m^0 I) = I$. Let $g, h \in G$ and $j, k \in \mathbb{Z}_m$. Since $\tilde{\varphi}$ is a homomorphism and X^{g+h}, X^{-h}, and X^{-g} are all elements of S, we have

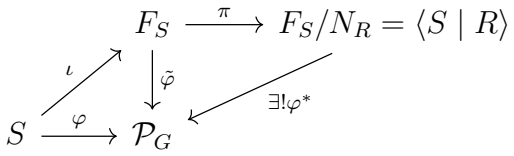
$$\begin{aligned}
\tilde{\varphi}(X^{g+h}X^{-h}X^{-g}) &= \tilde{\varphi}(X^{g+h})\tilde{\varphi}(X^{-h})\tilde{\varphi}(X^{-g}) \\
&= \tilde{\varphi}\iota(X^{g+h})\tilde{\varphi}\iota(X^{-h})\tilde{\varphi}\iota(X^{-g}) \\
&= \varphi(X^{g+h})\varphi(X^{-h})\varphi(X^{-g}) \\
&= X^{g+h}X^{-h}X^{-g} \\
&= X^{g+h-h-g} \\
&= X^0 \\
&= I.
\end{aligned}$$

Showing that $\tilde{\varphi}$ maps $Z^{g+h}Z^{-h}Z^{-g}$, $(\epsilon_m^{j+k}I)(\epsilon_m^{-k}I)(\epsilon_m^{-j}I)$, $(\epsilon_m^k I)X^g(\epsilon_m^{-k}I)X^{-g}$, and $(\epsilon_m^k I)Z^g(\epsilon_m^{-k}I)Z^{-g}$ to I are similar. Lastly, we have

$$\begin{aligned}
\tilde{\varphi}((\epsilon_m^{g\circ h}I)X^gZ^hX^{-g}Z^{-h}) &= \tilde{\varphi}(\epsilon_m^{g\circ h}I)\tilde{\varphi}(X^g)\tilde{\varphi}(Z^h)\tilde{\varphi}(X^{-g})\tilde{\varphi}(Z^{-h}) \\
&= \tilde{\varphi}\iota(\epsilon_m^{g\circ h}I)\tilde{\varphi}\iota(X^g)\tilde{\varphi}\iota(Z^h)\tilde{\varphi}\iota(X^{-g})\tilde{\varphi}\iota(Z^{-h}) \\
&= \varphi(\epsilon_m^{g\circ h}I)\varphi(X^g)\varphi(Z^h)\varphi(X^{-g})\varphi(Z^{-h}) \\
&= (\epsilon_m^{g\circ h}I)X^gZ^hX^{-g}Z^{-h} \\
&= (\epsilon_m^{g\circ h}I)X^g(\epsilon_m^{(-g)\circ h}X^{-g}Z^h)Z^{-h} \\
&= I.
\end{aligned}$$

The claim follows. Thus by Theorem 4.3.2, φ extends to a homomorphism $\varphi^* : \langle S \mid R \rangle \to \mathcal{P}_G$.

We have the following diagram:



By Definition 4.2.1, S generates $\mathcal{P}_G$, and thus it follows that $\tilde{\varphi}$ is a surjection. Also, it is straightforward to see that the elements of R are the reduced words in F_S that are mapped to I under $\tilde{\varphi}$. Therefore, we have by Theorems 4.1 and 4.1.6, and also by the commutativity of scalar multiples of I, that N_R contains all words in F_S that are mapped to I under $\tilde{\varphi}$. Thus $\ker \tilde{\varphi} = N_R$. Therefore, $\langle S \mid R \rangle = F_S/N_R = F_S/\ker \tilde{\varphi} \cong \operatorname{im} \tilde{\varphi} = \mathcal{P}_G$. The claim follows.

□

4.3.5 Note. Let the language be as in the previous theorem. Since $S \subset F_S$, we have $sN_R \in F_S/N_R$ for all $s \in S$. It follows that for all $s \in S$, $\varphi^*(sN_R) = \varphi^*\pi(s) = \tilde{\varphi}(s) = \tilde{\varphi}\iota(s) = \varphi(s) = s$.

4.4 Abelian Subgroups of the Pauli Group

Again recall that $G = \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_n}$ with $n, m_i \in \mathbb{Z}^+$, and m is a fixed common multiple of the set $\{2m_i \mid 1 \leq i \leq n\}$.

For a group H, recall that the commutator subgroup $[H, H]$ of H is the subgroup of H generated by the set $\{[a, b] = a^{-1}b^{-1}ab : a, b \in H\}$.

4.4.1 Lemma. *We have* $[\mathcal{P}_G, \mathcal{P}_G] \subseteq \{\epsilon_m^k I \mid k \in \mathbb{Z}_m\}$.

Proof. Let $a, b, c, d \in G$. Recall from Theorem 4.2.7 that $X^a Z^b X^c Z^d = \epsilon_m^{b \circ c - a \circ d} X^c Z^d X^a Z^b$. We have

$$\begin{aligned}
[X^a Z^b, X^c Z^d] &= (X^a Z^b)^{-1}(X^c Z^d)^{-1} X^a Z^b X^c Z^d \\
&= Z^{-b} X^{-a} Z^{-d} X^{-c} X^a Z^b X^c Z^d \\
&= Z^{-b} X^{-a} Z^{-d} X^{-c} (\epsilon_m^{b \circ c - a \circ d} X^c Z^d X^a Z^b) \\
&= \epsilon_m^{b \circ c - a \circ d} Z^{-b} X^{-a} Z^{-d} X^{-c} X^c Z^d X^a Z^b \\
&= \epsilon_m^{b \circ c - a \circ d} I.
\end{aligned}$$

It follows that $[\mathcal{P}_G, \mathcal{P}_G] \subseteq \{\epsilon_m^k I \mid k \in \mathbb{Z}_m\}$.

□

For the following, put $\mathcal{N} = \{\epsilon_m^k I \mid k \in \mathbb{Z}_m\}$. Observe that $\mathcal{N}$ is a normal subgroup of $\mathcal{P}_G$.

4.4.2 Theorem. *We have that* $\mathcal{P}_G/\mathcal{N}$ *is isomorphic to* $\overline{G}$.

Proof. Let $f : \mathcal{P}_G/\mathcal{N} \to \overline{G}$ be defined by $f\left(\overline{X^g Z^h}\right) = (g, h)$, where $\overline{X^g Z^h} = X^g Z^h \mathcal{N}$. It is straightforward to prove that f is well-defined. Let $a, b, c, d \in G$. Then we have

$$\begin{aligned} f\left(\overline{X^a Z^b}\ \overline{X^c Z^d}\right) &= f\left(X^a Z^b \mathcal{N}\ X^c Z^d \mathcal{N}\right) \\ &= f\left(X^a Z^b X^c Z^d \mathcal{N}\right) \\ &= f\left(X^{a+c} Z^{b+d} (\epsilon_m^{b \circ c} I) \mathcal{N})\right) \\ &= f\left(X^{a+c} Z^{b+d} \mathcal{N}\right) \\ &= f\left(\overline{X^{a+c} Z^{b+d}}\right) \\ &= (a + c, b + d) \\ &= (a, b) + (c, d) \\ &= f\left(\overline{X^a Z^b}\right) + f\left(\overline{X^c Z^d}\right). \end{aligned}$$

Thus f is a homomorphism.

Now, suppose $f\left(\overline{X^a Z^b}\right) = f\left(\overline{X^c Z^d}\right)$. Thus $(a, b) = (c, d)$, so $a = c$ and $b = d$. Therefore, $\overline{X^a Z^b} = \overline{X^c Z^d}$, so f is injective. It is straightforward to see that f is surjective. Thus f is an isomorphism. The claim follows.

□

Let $f : \mathcal{P}_G/\mathcal{N} \to \overline{G}$ be the isomorphism defined in the previous theorem and let $\pi : \mathcal{P}_G \to \mathcal{P}_G/\mathcal{N}$ be the canonical epimorphism. Set $\varphi := f\pi$. Thus $\varphi : \mathcal{P}_G \to \overline{G}$ is an epimorphism. Indeed, φ is an m-to-1 epimorphism, which is due to $\ker \varphi = \mathcal{N} = \{\epsilon_m^k I \mid k \in \mathbb{Z}_m\}$.

For the following, let $\mathcal{A}$ and $\mathcal{B}$ be subgroups of $\mathcal{P}_G$.

4.4.3 Lemma. *$\mathcal{A}$ and $\mathcal{B}$ commute element-wise if and only if $\varphi(\mathcal{A}) \subseteq \varphi(\mathcal{B})^{\Delta}$.*

Proof. Assume $\mathcal{A}$ and $\mathcal{B}$ commute element-wise. Let $x \in \varphi(\mathcal{A})$ and $y \in \varphi(\mathcal{B})$ so that $x = \varphi(a)$ and $y = \varphi(b)$ for some $a \in \mathcal{A}$, $b \in \mathcal{B}$. By Theorem 4.2.2 we have $a = \epsilon_m^k X^g Z^h$ and $b = \epsilon_m^l X^r Z^s$ for some $k, l \in \mathbb{Z}_m$ and $g, h, r, s \in G$. We then have $x = \varphi(\epsilon_m^k X^g Z^h) = (g, h)$ and $y = \varphi(\epsilon_m^l X^r Z^s) = (r, s)$. By assumption, $ab = ba$, so we have, by Note 4.2.8,

$$\epsilon_m^{k+l}(\epsilon_m^{(g,h)*(r,s)} X^r Z^s X^g Z^h) = \epsilon_m^{k+l} X^g Z^h X^r Z^s = ab = ba = \epsilon_m^{k+l} X^r Z^s X^g Z^h,$$

whence it follows that $\epsilon_m^{x*y} = \epsilon_m^{(g,h)*(r,s)} = 1$. Therefore, $x * y = 0$, so $x \in \varphi(\mathcal{B})^\Delta$, since $y \in \varphi(\mathcal{B})$ was arbitrary. Thus $\varphi(\mathcal{A}) \subseteq \varphi(\mathcal{B})^\Delta$.

Now assume that $\varphi(\mathcal{A}) \subseteq \varphi(\mathcal{B})^\Delta$. Let $a \in \mathcal{A}$ and $b \in \mathcal{B}$. By Theorem 4.2.2 we have $a = \epsilon_m^k X^g Z^h$ and $b = \epsilon_m^l X^r Z^s$ for some $k, l \in \mathbb{Z}_m$ and $g, h, r, s \in G$. Thus $\varphi(a) = (g, h)$ and $\varphi(b) = (r, s)$. By assumption, $(g, h) * (r, s) = \varphi(a) * \varphi(b) = 0$. Therefore,

$$ab = \epsilon_m^{k+l} X^g Z^h X^r Z^s = \epsilon_m^{k+l}(\epsilon_m^{(g,h)*(r,s)} X^r Z^s X^g Z^h) = \epsilon_m^{l+k} X^r Z^s X^g Z^h = ba,$$

and we have that $\mathcal{A}$ and $\mathcal{B}$ commute element-wise.

□

4.4.4 Lemma. *We have* $\varphi(C_{\mathcal{P}_G}(\mathcal{A})) = \varphi(\mathcal{A})^\Delta$.

Proof. Since $\mathcal{A}$ and $C_{\mathcal{P}_G}(\mathcal{A})$ commute element-wise, the previous lemma yields $\varphi(C_{\mathcal{P}_G}(\mathcal{A})) \subseteq \varphi(\mathcal{A})^\Delta$.

Claim: $\varphi(C_{\mathcal{P}_G}(\mathcal{A})) \supseteq \varphi(\mathcal{A})^\Delta$. Set $\mathcal{B} = \varphi^{-1}(\varphi(\mathcal{A})^\Delta)$. Since $\varphi : \mathcal{P}_G \to \overline{G}$ is a homomorphism, we have $\mathcal{B} \leq \mathcal{P}_G$. Moreover, since $\varphi(\mathcal{B}) = \varphi(\varphi^{-1}(\varphi(\mathcal{A})^\Delta)) = \varphi(\mathcal{A})^\Delta$, the previous theorem implies $\mathcal{B}$ and $\mathcal{A}$ commute element-wise. Since $C_{\mathcal{P}_G}(\mathcal{A})$ is the largest subgroup of $\mathcal{P}_G$ that commutes with $\mathcal{A}$ element-wise, it follows that $\mathcal{B} \subseteq C_{\mathcal{P}_G}(\mathcal{A})$. Thus

$$\varphi(\mathcal{A})^\Delta = \varphi(\mathcal{B}) \subseteq \varphi(C_{\mathcal{P}_G}(\mathcal{A})).$$

This proves the claim. Therefore, $\varphi(C_{\mathcal{P}_G}(\mathcal{A})) = \varphi(\mathcal{A})^{\Delta}$, and the claim follows.

□

4.4.5 Theorem. *If $\mathcal{A}$ is abelian, then $\varphi(\mathcal{A}) \subseteq \varphi(\mathcal{A})^{\Delta}$. Furthermore, if $\mathcal{A}$ is maximal among abelian subgroups, then $\varphi(\mathcal{A}) = \varphi(\mathcal{A})^{\Delta}$, i.e. $\varphi(\mathcal{A})$ is Lagrangian.*

Proof. If $\mathcal{A}$ is abelian, then $\varphi(\mathcal{A}) \subseteq \varphi(\mathcal{A})^{\Delta}$ follows immediately from Lemma 4.4.3. Now, suppose $\mathcal{A}$ is a maximal abelian subgroup of $\mathcal{P}_G$. Since $\mathcal{A}$ is abelian, $\mathcal{A} \subseteq C_{\mathcal{P}_G}(\mathcal{A})$. Claim: $\mathcal{A} = C_{\mathcal{P}_G}(\mathcal{A})$. Suppose the claim is false; i.e., suppose there exists an $M \in C_{\mathcal{P}_G}(\mathcal{A}) \backslash \mathcal{A}$. The subset $\langle \mathcal{A} \cup \{M\} \rangle$ is an abelian subgroup of $\mathcal{P}_G$, and it strictly contains $\mathcal{A}$. This contradicts the assumption that $\mathcal{A}$ is maximal among abelian subgroups. Hence, the claim is true. Therefore, $\varphi(\mathcal{A}) = \varphi(C_{\mathcal{P}_G}(\mathcal{A})) = \varphi(\mathcal{A})^{\Delta}$, where the last equality is from the previous lemma. Thus $\varphi(\mathcal{A})$ is Lagrangian.

□

4.4.6 Corollary. *If $\mathcal{A}$ is a maximal abelian subgroup of $\mathcal{P}_G$, then $|\varphi(\mathcal{A})| = |G|$.*

Proof. Suppose $\mathcal{A}$ is a maximal abelian subgroup of $\mathcal{P}_G$. By Theorem 4.4.5, $\varphi(\mathcal{A})$ is a Lagrangian subgroup of $\overline{G}$. By Theorem 3.4.15, we obtain $|\varphi(\mathcal{A})| = |G|$.

□

4.4.7 Lemma. *[Hun80, p. 45] Let $\rho : A \to A'$ be an epimorphism of groups. Put*

$$\mathbf{S} = \{B \mid \ker \rho \subseteq B \leq A\}.$$

For $B, C \in \mathbf{S}$, $\rho(B) \triangleleft \rho(C)$ if and only if $B \triangleleft C$, and $\rho(C)/\rho(B) \cong C/B$.

4.4.8 Theorem. *Let L be a Lagrangian subgroup of $\overline{G}$ and put $\mathcal{H} = \varphi^{-1}(L)$. The set $\mathcal{H}$ is an abelian subgroup of $\mathcal{P}_G$ containing $\mathcal{N} = \{\epsilon_m^k \mid k \in \mathbb{Z}_m\}$, and $\mathcal{H}/\mathcal{N} \cong L$.*

Proof. Since φ is a homomorphism, $\varphi^{-1}(L)$ is a subgroup of $\mathcal{P}_G$. Since L is Lagrangian, $L = L^{\Delta}$. Observe that $\varphi(\mathcal{H}) = L$, so it follows that $\varphi(\mathcal{H}) = \varphi(\mathcal{H})^{\Delta}$. Thus by Lemma 4.4.3,

$\mathcal{H}$ commutes element-wise with itself. In other words, $\mathcal{H}$ is abelian.

Now, set $\mathbf{S} = \{\mathcal{B} \mid \ker\varphi \subseteq \mathcal{B} \leq \mathcal{P}_G\}$. Observe that $\ker\varphi = \varphi^{-1}(\{\overline{0}\}) \subseteq \varphi^{-1}(L) = \mathcal{H}$, where $\overline{0}$ is the identity in $\overline{G}$, so $\mathcal{H} \in \mathbf{S}$. Also, since $\ker\varphi = \mathcal{N}$, we have that $\mathcal{N} \in \mathbf{S}$. Moreover, it follows that $\mathcal{N} \triangleleft \mathcal{H}$. Since $\varphi : \mathcal{P}_G \to \overline{G}$ is an epimorphism, we can apply Lemma 4.4.7 to see that $\varphi(\mathcal{N}) \triangleleft \varphi(\mathcal{H})$ and $\mathcal{H}/\mathcal{N} \cong \varphi(\mathcal{H})/\varphi(\mathcal{N}) = L/\{\overline{0}\} \cong L$.

□

4.4.9 Corollary. *If $\mathcal{A}$ is a maximal abelian subgroup of $\mathcal{P}_G$, then $|\mathcal{A}| = m|G|$.*

Proof. Suppose $\mathcal{A}$ is a maximal abelian subgroup of $\mathcal{P}_G$. By Theorem 4.4.5, $\varphi(\mathcal{A})$ is a Lagrangian subgroup of $\overline{G}$. Thus by Theorem 4.4.8, $\varphi^{-1}(\varphi(\mathcal{A}))$ is an abelian subgroup of $\mathcal{P}_G$ containing $\mathcal{N} = \{\epsilon_m^k I \mid k \in \mathbb{Z}_m\}$, and $\varphi^{-1}(\varphi(\mathcal{A}))/\mathcal{N} \cong \varphi(\mathcal{A})$. Observe that $\mathcal{A} \subseteq \varphi^{-1}(\varphi(\mathcal{A}))$, and due to maximality of $\mathcal{A}$, we have $\mathcal{A} = \varphi^{-1}(\varphi(\mathcal{A}))$. Therefore, $\mathcal{A}/\mathcal{N} \cong \varphi(\mathcal{A})$. By Corollary 4.4.6 and Lagrange's Theorem, we have $|\mathcal{A}| = |\mathcal{N}||\varphi(\mathcal{A})| = m|G|$. □

4.5 Pauli Algebra

Again recall that $G = \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_n}$ with $n, m_i \in \mathbb{Z}^+$, and m is a fixed common multiple of the set $\{2m_i \mid 1 \leq i \leq n\}$.

Identify the vector $|a\rangle$ ($a \in G$) with the $|G|$-dimensional column vector having 1 in the a-position (using a fixed ordering of the set G) and 0's elsewhere. For each $a, b \in G$ the linear map $|a\rangle\langle b| : \mathbb{C}G \to \mathbb{C}G$ identifies (using the basis G with the same ordering) with the element of $\mathrm{Mat}_{|G|}(\mathbb{C})$ having 1 in the (a, b)-position and 0's elsewhere. Since $\{|a\rangle \mid a \in G\}$ is the standard basis for $\mathbb{C}G$, it is straightforward to prove that $\{|a\rangle\langle b| \mid a, b \in G\}$ is the standard basis for the space $\mathrm{Mat}_{|G|}(\mathbb{C})$ of $|G| \times |G|$ matrices over $\mathbb{C}$.

4.5.1 Definition. Let A be a square complex matrix. We say A is unitary if $AA^* = I = A^*A$, where A^* is the conjugate transpose of A.

4.5.2 Note. Let $g \in G$. Since $X^g = \sum_{h \in G} |h + g\rangle\langle h|$ and $Z^g = \sum_{h \in G} \epsilon_m^{g \circ h} |h\rangle\langle h|$, we can view the Pauli group operators as elements of $\mathrm{Mat}_{|G|}(\mathbb{C})$ and thus identify $\mathcal{P}_G$ as a subset of $\mathrm{Mat}_{|G|}(\mathbb{C})$. Furthermore, by taking the conjugate transposes of X^g and Z^g, we have $(X^g)^* = \sum_{h \in G} |h\rangle\langle h+g|$ and $(Z^g)^* = \sum_{h \in G} \epsilon_m^{-g \circ h} |h\rangle\langle h|$, and noting that the identity matrix can be expressed as $I = \sum_{h \in G} |h\rangle\langle h|$, it follows that $X^g(X^g)^* = (X^g)^* X^g = I$ and $Z^g(Z^g)^* = (Z^g)^* Z^g = I$ so that X^g and Z^g are unitary.

4.5.3 Definition. Define the *Pauli algebra* $\overline{\mathcal{P}_G}$ to be the subalgebra of $\mathrm{Mat}_{|G|}(\mathbb{C})$ generated by $\mathcal{P}_G$ (identified as a subset of $\mathrm{Mat}_{|G|}(\mathbb{C})$). By definition, $\overline{\mathcal{P}_G}$ is the intersection of all subalgebras of $\mathrm{Mat}_{|G|}(\mathbb{C})$ containing $\mathcal{P}_G$.

4.5.4 Theorem. *The collection* $\left\{ X^a \left(\frac{1}{|G|} \sum_{g \in G} Z^g \right) X^{-b} \mid a, b \in G \right\}$ *is the standard basis for the space* $\mathrm{Mat}_{|G|}(\mathbb{C})$*, and hence* $\overline{\mathcal{P}_G} = \mathrm{Mat}_{|G|}(\mathbb{C})$.

Proof. It suffices to prove that for any $a, b \in G$, we have $X^a \left(\frac{1}{|G|} \sum_{g \in G} Z^g \right) X^{-b} = |a\rangle\langle b|$, since the collection $\{|a\rangle\langle b| \mid a, b \in G\}$ is the standard basis for $\mathrm{Mat}_{|G|}(\mathbb{C})$. To that end, for any $a, b \in G$, we have

$$\begin{aligned}
X^a \left(\frac{1}{|G|} \sum_{g \in G} Z^g \right) X^{-b} |b\rangle &= X^a \left(\frac{1}{|G|} \sum_{g \in G} Z^g \right) |0\rangle \\
&= X^a \left(\frac{1}{|G|} \sum_{g \in G} \epsilon_m^{g \circ 0} |0\rangle \right) \\
&= X^a \left(\frac{1}{|G|} \sum_{g \in G} 1 \right) |0\rangle \\
&= X^a \left(\frac{1}{|G|} |G| \right) |0\rangle \\
&= X^a |0\rangle \\
&= |a\rangle \\
&= |a\rangle \cdot 1 \\
&= |a\rangle\langle b|b\rangle \\
&= (|a\rangle\langle b|) \cdot |b\rangle,
\end{aligned}$$

and, for any $h \in G \backslash \{b\}$, we have

$$\begin{aligned}
X^a \left(\frac{1}{|G|} \sum_{g \in G} Z^g \right) X^{-b} |h\rangle &= X^a \left(\frac{1}{|G|} \sum_{g \in G} Z^g \right) | - b + h\rangle && (4.1) \\
&= X^a \left(\frac{1}{|G|} \sum_{g \in G} \epsilon_m^{g \circ (-b+h)} | - b + h\rangle \right) && (4.2) \\
&= X^a \left(\frac{1}{|G|} \sum_{g \in G} \epsilon_m^{\iota_{-b+h}(g)} | - b + h\rangle \right) && (4.3) \\
&= X^a \left(\frac{1}{|G|} \sum_{g \in G} \epsilon_m^{\iota_{-b+h}(g)} \right) | - b + h\rangle && (4.4)
\end{aligned}$$

$$= X^a \cdot 0 \cdot |-b+h\rangle \tag{4.5}$$

$$= \overline{0} \tag{4.6}$$

$$= |a\rangle \cdot 0 \tag{4.7}$$

$$= |a\rangle\langle b|h\rangle \tag{4.8}$$

$$= (|a\rangle\langle b|) \cdot |h\rangle, \tag{4.9}$$

where $\bar{0}$ is the zero vector in $\mathbb{C}G$. The connection from (4) to (5) above is due to $-b+h \notin \{0\} = G^{\perp}$, which implies the homomorphism ι_{-b+h} is not constant on G, which implies ι_{-b+h} is balanced on G by Theorem 2.2.6, and lastly, Lemma 2.2.7 gives $\sum_{g\in G} \epsilon_m^{\iota_{-b+h}(g)} = 0$. Therefore, $X^a \left(\frac{1}{|G|} \sum_{g\in G} Z^g \right) X^{-b} = |a\rangle\langle b|$. The claim follows.

□

Let $d \in \mathbb{Z}^+$ and K be an arbitrary field.

4.5.5 Theorem. *[GS17, p. 29] Every automorphism of the matrix ring* $\mathrm{Mat}_d(K)$ *is inner.*

The following corollary follows immediately from the previous two theorems.

4.5.6 Corollary. *Every automorphism of the Pauli algebra* $\overline{\mathcal{P}_G}$ *of* G *is inner.*

4.6 Stabilizer Codes

Again recall that $G = \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_n}$ with $n, m_i \in \mathbb{Z}^+$, and m is a fixed common multiple of the set $\{2m_i \mid 1 \leq i \leq n\}$.

For a subgroup $\mathcal{S}$ of $\mathcal{P}_G$, let $V_\mathcal{S}$ denote the subspace of $\mathbb{C}G$ that is stabilized pointwise by the members of $\mathcal{S}$ so that, for all $|\psi\rangle \in V_\mathcal{S}$, $s|\psi\rangle = |\psi\rangle$ for all $s \in \mathcal{S}$. Conversely, if W is a subspace of $\mathbb{C}G$, then we denote the *(pointwise) stabilizer* of W (in $\mathcal{P}_G$) by $\mathcal{S}_W$.

4.6.1 Definition. [RP11, (11.2.2), p. 257] Let V_1 and V_2 be complex vector spaces. A linear transformation $U : V_1 \to V_2$ is called an *encoding* (of V_1) if U is an injection. The *code* associated with an encoding $U : V_1 \to V_2$ is defined as the subspace of V_2 spanned by the image of U.

4.6.2 Theorem. *Let $\mathcal{S}$ be a subgroup of $\mathcal{P}_G$. For any $g \in G$, $|\mathcal{S}|^{-1/2} \sum_{s\in\mathcal{S}} s|g\rangle$ belongs to $V_\mathcal{S}$.*

Proof. Let $g \in G$. Put $|\tilde{g}\rangle = |\mathcal{S}|^{-1/2} \sum_{s\in\mathcal{S}} s|g\rangle$. Since $\mathcal{S}$ is a subgroup of $\mathcal{P}_G$, we have, for any $t \in \mathcal{S}$, $t|\tilde{g}\rangle = |\mathcal{S}|^{-1/2} \sum_{s\in\mathcal{S}} ts|g\rangle = |\mathcal{S}|^{-1/2} \sum_{s'\in\mathcal{S}} s'|g\rangle = |\tilde{g}\rangle$. Therefore, $|\tilde{g}\rangle \in V_\mathcal{S}$. □

4.6.3 Note. Using the language and notation of the previous theorem, once we have found the distinct elements of the set $\left\{ |\mathcal{S}|^{-1/2} \sum_{s\in\mathcal{S}} s|g\rangle \mid g \in G \right\}$, we can choose the largest subset H of G for which the map that sends $|h\rangle$ to $|\mathcal{S}|^{-1/2} \sum_{s\in\mathcal{S}} s|h\rangle$, for $h \in H$, is an injection. Such a map will be an injective linear transformation from $\mathbb{C}H$ to $\mathbb{C}G$ and thus an encoding of $\mathbb{C}H$. The subspace C of $\mathbb{C}G$ spanned by the set $\left\{ |\mathcal{S}|^{-1/2} \sum_{s\in\mathcal{S}} s|h\rangle \mid h \in H \right\}$ is stabilized by the members of $\mathcal{S}$, and thus C is contained in $V_\mathcal{S}$ [RP11, (11.4), p. 283]. We call the code C spanned by $\left\{ |\mathcal{S}|^{-1/2} \sum_{s\in\mathcal{S}} s|h\rangle \mid h \in H \right\}$ the *stabilizer code* afforded by $\mathcal{S}$.

4.6.4 Definition. A *principal ideal domain (PID)* is an integral domain in which every ideal can be generated by a single element.

4.6.5 Definition. [Wei94, p. 39] Let R be a PID. An R-module M is *divisible* if for each $a \in M$ and $r \neq 0 \in R$, there exists an $b \in M$ such that $a = br$.

4.6.6 Definition. [Hun80, p. 193-194] Let R be a ring. An R-module I is *injective* if given any diagram

$$\begin{array}{ccccc} 0 & \longrightarrow & M & \xrightarrow{f} & N \\ & & \downarrow{\scriptstyle \alpha} & & \\ & & I & & \end{array}$$

of R-modules and R-module homomorphisms with f an injective R-module homomorphism, there exists an R-module homomorphism $\beta : N \to I$ making the diagram commutative.

4.6.7 Lemma. *[Wei94, p. 39] Let R be a PID. An R-module M is injective if and only if it is divisible.*

For the following, put $\mathcal{N} = \{\epsilon_m^k \mid k \in \mathbb{Z}_m\}$, and observe that $\mathcal{N} \subset \mathcal{P}_G$.

4.6.8 Theorem. *Let $\mathcal{S}$ be a subgroup of $\mathcal{P}_G$. The space $V_\mathcal{S}$ is nontrivial if and only if the intersection $\mathcal{S} \cap \mathcal{N}$ is trivial.*

Proof. ($\Rightarrow$) Suppose $\mathcal{S} \cap \mathcal{N}$ is nontrivial. Fix a nonzero $k \in \mathbb{Z}_m$ such that $\epsilon_m^k I \in \mathcal{S}$. Let $|v\rangle \in V_\mathcal{S}$. It follows that $\epsilon_m^k |v\rangle = \epsilon_m^k I |v\rangle = |v\rangle$. Thus $(\epsilon_m^k - 1)|v\rangle = 0$. Since $k \neq 0$, it follows that $\epsilon_m^k - 1 \neq 0$, so we must have $|v\rangle = 0$. Hence $V_\mathcal{S} = \{0\}$, so $V_\mathcal{S}$ is trivial.

($\Leftarrow$ Proof due to R.R. Holmes) Assume that the intersection $\mathcal{S} \cap \mathcal{N}$ is trivial. For each $s \in \mathcal{S}$ we have $s = \epsilon_m^{k_s} X^{a_s} Z^{b_s}$ for some unique $k_s \in \mathbb{Z}_m$, $a_s, b_s \in G$. Put $\mathcal{S}_0 = \{s \in \mathcal{S} \mid s = \epsilon_m^{k_s} Z^{b_s}$ for some $k_s \in \mathbb{Z}_m, b_s \in G\} \subseteq \mathcal{S}$ and $B = \{b_s \in G \mid \epsilon_m^{k_s} Z^{b_s} \in \mathcal{S}$ for some $k_s \in \mathbb{Z}_m\} \subseteq G$. Claim: $\mathcal{S}_0 \leq \mathcal{S}$. We have:

(i) Since the identity I belongs to $\mathcal{S}$ and $I = \epsilon_m^0 Z^0$, we have $I \in \mathcal{S}_0$.

(ii) Let $s, t \in \mathcal{S}_0$. Then we have $s = \epsilon_m^{k_s} Z^{b_s}$ and $t = \epsilon_m^{k_t} Z^{b_t}$ for some $k_s, k_t \in \mathbb{Z}_m$ and $b_s, b_t \in G$. Since $\mathcal{S}$ is a subgroup of $\mathcal{P}_G$, it follows that $\epsilon_m^{k_s+k_t} Z^{b_s+b_t} = st \in \mathcal{S}$ for some $k_s, k_t \in \mathbb{Z}_m$ and $b_s, b_t \in G$. Thus $st \in \mathcal{S}_0$.

(iii) Let $s \in \mathcal{S}_0$. Then we have $s = \epsilon_m^{k_s} Z^{b_s}$ for some $k_s \in \mathbb{Z}_m$ and $b_s \in G$. Since $s \in \mathcal{S}$ and $\mathcal{S}$ is a subgroup of $\mathcal{P}_G$, we have $\epsilon_m^{-k_s} Z^{-b_s} = s^{-1} \in \mathcal{S}$. Thus $s^{-1} \in \mathcal{S}_0$.

The claim follows. Claim: $B \leq G$. We have:

(i) Since the identity I belongs to $\mathcal{S}$ and $I = \epsilon_m^0 Z^0$, it follows that the identity 0 of G belongs to B.

(ii) Let $b_s, b_t \in B$. Then we have that $s := \epsilon_m^{k_s} Z^{b_s}$ and $t := \epsilon_m^{k_t} Z^{b_t}$ belong to $\mathcal{S}$ for some $k_s, k_t \in \mathbb{Z}_m$. Since $\mathcal{S}$ is a subgroup of $\mathcal{P}_G$, it follows that $\epsilon_m^{k_s+k_t} Z^{b_s+b_t} = st \in \mathcal{S}$ for some $k_s, k_t \in \mathbb{Z}_m$. Thus $b_s + b_t \in B$.

(iii) Let $b_s \in B$. Then we have that $s := \epsilon_m^{k_s} Z^{b_s} \in \mathcal{S}$ for some $k_s \in \mathbb{Z}_m$. Since $\mathcal{S}$ is a subgroup of $\mathcal{P}_G$, we have $\epsilon_m^{-k_s} Z^{-b_s} = s^{-1} \in \mathcal{S}$. Thus $-b_s \in B$.

The claim follows.

Now, define $\alpha : B \to \mathcal{S}_0$ by $\alpha(b) = \epsilon_m^{k_s} Z^{b_s}$, where $s \in \mathcal{S}_0$ is such that $b_s = b$, and define $\beta : \mathcal{S}_0 \to \mathbb{Z}_m$ by $\beta(s) = k_s$. Since $\mathcal{S} \cap \mathcal{N}$ is trivial, α is a well-defined function. Since β maps $s = \epsilon^{k_s} Z^{b_s}$ to k_s, it is immediate that β is a well-defined function. It is a straightforward proof that α and β are homomorphisms. Put $\psi = \beta\alpha$. It follows that $\psi : B \to \mathbb{Z}_m$ is a well-defined

$\mathbb{Z}_m$-homomorphism defined by $\psi(b) = k_s$, where $s \in \mathcal{S}_0$ is such that $b_s = b$. Let $i : B \to G$ be the inclusion map. We have the following diagram of $\mathbb{Z}_m$-modules:

$$\begin{array}{ccccc} 0 & \longrightarrow & B & \xrightarrow{i} & G \\ & & \downarrow{\scriptstyle \psi} & & \\ & & \mathbb{Z}_m & & \end{array}$$

The $\mathbb{Z}$-module $\mathbb{Z}_m$ is divisible and the ring $\mathbb{Z}$ is a PID, so the $\mathbb{Z}$-module $\mathbb{Z}_m$ is injective by Lemma 4.6.7, implying that ψ extends to a $\mathbb{Z}_m$-homomorphism $G \to \mathbb{Z}_m$, which equals ι_γ for some $\gamma \in G$ (by the remarks preceding Lemma 3.2.2), making the following diagram commutative:

$$\begin{array}{ccccc} 0 & \longrightarrow & B & \xrightarrow{i} & G \\ & & \downarrow{\scriptstyle \psi} & \swarrow{\scriptstyle \iota_\gamma} & \\ & & \mathbb{Z}_m & & \end{array}$$

Put $|v\rangle = \sum_{s\in\mathcal{S}} s|\mu\rangle$, where $\mu = -\gamma$. First, it follows that $|v\rangle \in V_{\mathcal{S}}$, so it remains to be shown that $|v\rangle \neq 0$. We have, for some $k_s \in \mathbb{Z}_m$ and $a_s, b_s \in G$,

$$|v\rangle = \left(\sum_{s\in\mathcal{S}} \epsilon_m^{k_s} X^{a_s} Z^{b_s}\right)|\mu\rangle = \sum_{a\in G} \sum_{\substack{s\in\mathcal{S} \\ a_s = a}} \epsilon_m^{k_s} \epsilon_m^{b_s\circ\mu} |\mu + a\rangle.$$

It is enough to show that the projection $|v\rangle_\mu$ of $|v\rangle$ onto the subspace $\mathbb{C}|\mu\rangle$ of $\mathbb{C}G$ is nonzero. We have

$$|v\rangle_\mu = \left(\sum_{s\in\mathcal{S}_0} \epsilon_m^{k_s} \epsilon_m^{b_s\circ\mu}\right)|\mu\rangle$$

for some $k_s \in \mathbb{Z}_m$ and $a_s, b_s \in G$. For each $s \in \mathcal{S}_0$, we have

$$\epsilon_m^{k_s} \epsilon_m^{b_s\circ\mu} = \epsilon_m^{k_s} \epsilon_m^{b_s\circ(-\gamma)} = \epsilon_m^{k_s} \epsilon_m^{-\gamma\circ b_s} = \epsilon_m^{k_s - \iota_\gamma(b_s)} = \epsilon_m^{k_s - \iota_\gamma i(b_s)} = \epsilon_m^{k_s - \psi(b_s)} = \epsilon_m^{k_s - k_s} = 1,$$

so $|v\rangle_\mu = |S_0|\,|\mu\rangle \neq 0$, as desired.

□

4.6.9 Corollary. *Let W be a subspace of $\mathbb{C}G$. If W is nontrivial, then the stabilizer subgroup $\mathcal{S}_W$ of W is an abelian subgroup of $\mathcal{P}_G$.*

Proof. Suppose W is nontrivial. By the previous theorem, $\mathcal{S}_W \cap \mathcal{N}$ is trivial, and thus $\mathcal{S}_W$ is isomorphic to its image under the canonical epimorphism $\mathcal{P}_G \to \mathcal{P}_G/\mathcal{N}$. Since $\mathcal{N}$ contains the commutator subgroup of $\mathcal{P}_G$ by Lemma 4.4.1, it follows that $\mathcal{P}_G/\mathcal{N}$ is abelian. Therefore, $\mathcal{S}_W$ is abelian.

□

4.6.10 Example. Assume $G = \mathbb{Z}_2 \oplus \mathbb{Z}_3$. Put $m = 12$ so that m is a multiple of the set $\{4, 6\}$. Set $S_0 = X^{(1,1)}$ and $S_1 = Z^{(1,0)}$. Let $\mathcal{S}$ be the subgroup of $\mathcal{P}_G$ generated by the set $\{S_0, S_1\}$. Recall the definition of $\circ$ from Section 2.2, and observe that

$$(1,1) \circ (1,0) = \frac{12}{2}(1 \cdot 1) + \frac{12}{3}(1 \cdot 0) = 6,$$

and thus

$$S_0 S_1 = X^{(1,1)} Z^{(1,0)} = \epsilon_{12}^{-(1,1)\circ(1,0)} Z^{(1,0)} X^{(1,1)} = \epsilon_{12}^{-6} S_1 S_0 \neq S_1 S_0.$$

It follows that $\mathcal{S}$ is nonabelian. Applying the contrapositive of the previous corollary, it follows that $V_{\mathcal{S}}$ is trivial.

Let W be a nontrivial subspace of $\mathbb{C}G$ so that $\mathcal{S}_W$ is abelian (by the previous corollary).

4.6.11 Definition. An *error* E (on W) is any unitary operator on $\mathbb{C}G$ restricted to W.

4.6.12 Definition. [RP11, (11.2), p. 259] Let $B_W = \{|w_1\rangle, |w_2\rangle, \ldots, |w_\ell\rangle\}$ be an (orthonormal) basis for W. A finite set $\mathcal{E} = \{E_1, E_2, \ldots, E_k\}$ of unitary transformations $E_i : \mathbb{C}G \to \mathbb{C}G$

is said to be a *correctable set of errors* for W if there exists a matrix M with entries m_{ij} such that

$$\langle w_a|E_i^* E_j|w_b\rangle = m_{ij}\delta_{ab}$$

for all $|w_a\rangle, |w_b\rangle \in W$ and $E_i, E_j \in \mathcal{E}$, where δ_{ab} is the Kronecker delta function.

4.6.13 Note. The condition in the previous definition guarantees that two errors never take two codewords to the same state, and the errors in $\mathcal{E}$ avoid giving information about the state and hence do not affect the quantum computation.

4.6.14 Note. Even though errors can be any unitary operators on $\mathbb{C}G$ by definition, we henceforth restrict the errors to be elements of $\mathcal{P}_G$.

4.6.15 Note. [RP11, (11.4), p. 282] Let $\mathcal{E} = \{E_1, E_2, \ldots, E_k\}$ be a set of errors on $\mathbb{C}G$. Observe that if $E_i^* E_j \in \mathcal{S}_W$ for some $1 \leq i, j \leq k$, then $\langle w_a|E_i^* E_j|w_b\rangle = \langle w_a|w_b\rangle = \delta_{ab}$. In particular, if $i = j$, then since E_i is unitary, we have $E_i^* E_j = I \in \mathcal{S}_W$. If $E_i^* E_j \notin C(\mathcal{S}_W)$ for some $1 \leq i, j \leq k$, then $E_i^* E_j$ does not commute with some $S \in \mathcal{S}_W$, and thus

$$\langle w_a|E_i^* E_j|w_b\rangle = \langle w_a|E_i^* E_j S|w_b\rangle = \epsilon_m^\ell \langle w_a|S E_i^* E_j|w_b\rangle = \epsilon_m^\ell \langle w_a|E_i^* E_j|w_b\rangle$$

for some $\ell \in \mathbb{Z}_m \backslash \{0\}$, whence it follows that $\langle w_a|E_i^* E_j|w_b\rangle = 0$ since $\langle w_a|E_i^* E_j|w_b\rangle \in \mathbb{C}$.

It follows that any set $\mathcal{E} = \{E_1, E_2, \ldots, E_k\}$ of errors that satisfies the property that, for each $1 \leq i, j \leq k$, either $E_i^* E_j \in \mathcal{S}_W$ or $E_i^* E_j \notin C(\mathcal{S}_W)$ is a correctable set of errors by the previous definition.

4.6.16 Definition. Let A be a linear operator over $\mathbb{C}$ and $\lambda \in \mathbb{C}$ be an eigenvalue of A. We denote the λ-eigenspace of A by $V_{(\lambda,A)}$.

For the remainder of the section, let $E \in \mathcal{P}_G$, and let $\{S_1, S_2, \ldots, S_t\}$ be an independent generating set for $\mathcal{S}_W$.

4.6.17 Theorem. *For each $1 \leq r \leq t$ there exists a unique $k_r \in \mathbb{Z}_m$ such that $EW \subseteq V_{(\epsilon_m^{k_r}, S_r)}$.*

Proof. Since $E, S_r \in \mathcal{P}_G$ for all $1 \leq r \leq t$, it follows from Theorem 4.2.7 that $S_r E|w\rangle = \epsilon_m^{k_r} E S_r|w\rangle = \epsilon_m^{k_r} E|w\rangle$, and thus $E|w\rangle \in V_{(\epsilon_m^{k_r}, S_r)}$ for all $1 \leq r \leq t$ and any $|w\rangle \in W$. Hence $EW \subseteq V_{(\epsilon_m^{k_r}, S_r)}$. Suppose there is some $1 \leq r \leq t$ such that there are $j_r, k_r \in \mathbb{Z}_m$ with $EW \subseteq V_{(\epsilon_m^{j_r}, S_r)} \cap V_{(\epsilon_m^{k_r}, S_r)}$. Let $|w\rangle$ be a nonzero vector in W. We have

$$\epsilon_m^{j_r} E|w\rangle = S_r E|w\rangle = \epsilon_m^{k_r} E|w\rangle,$$

which implies $(\epsilon_m^{j_r} - \epsilon_m^{k_r}) E|w\rangle = 0$. Since E is invertible being an element of $\mathcal{P}_G$ and $|w\rangle \neq 0$, we have $E|w\rangle \neq 0$. It follows that $\epsilon_m^{j_r} - \epsilon_m^{k_r} = 0$, which implies $j_r = k_r$. The claim follows.

□

4.6.18 Definition. Let the notation be as in the previous theorem. The *syndrome* of E (relative to the subspace W and the set $\{S_1, S_2, \ldots, S_t\}$) is the t-tuple $(k_1, k_2, \ldots, k_t)$.

4.6.19 Definition. Let the notation be as in the previous theorem. We say an error E is *detectable* (relative to the subspace W and the set $\{S_1, S_2, \ldots, S_t\}$) if, given $(k_1, k_2, \ldots, k_t)$ is the syndrome of E, $k_i \neq 0$ for some $1 \leq i \leq t$.

4.6.20 Note. Let the notation be as in the previous theorem. Since any abelian subgroup of a group is necessarily contained in its centralizer (in the group), we have $\mathcal{S}_W \subseteq C_{\mathcal{P}_G}(\mathcal{S}_W) =: C(\mathcal{S}_W)$. Let $|w\rangle \in W$. We have either $E \in C(\mathcal{S}_W)$ or $E \notin C(\mathcal{S}_W)$. In the latter case, $E \notin C(S_W)$ implies E does not commute with some $S_\ell \in \mathcal{S}$, and thus the syndrome of E equals $(k_1, k_2, \ldots, k_t)$ with $k_\ell \neq 0$. Thus E is detectable. In the former case, either $E \in \mathcal{S}_W$ or $E \in C(\mathcal{S}_W) \backslash \mathcal{S}_W$. If $E \in S_W$, then $E|w\rangle = |w\rangle$, so E does not affect $|w\rangle$, and even though E

is undetectable, E does not need to be corrected. If $E \in C(S_W)\backslash\mathcal{S}_W$, then for all $S \in \mathcal{S}_W$, we have

$$SE|w\rangle = ES|w\rangle = E|w\rangle.$$

Thus $EW \subseteq V_{(+1,S)}$ for all $S \in \mathcal{S}$. Hence the syndrome of E equals $(0, \ldots, 0)$ and is therefore undetectable by syndrome measurements. When such a situation occurs, we may wish to define an encoding based on the action of E so that, while E cannot be detected, we can define our encoding such that we still take E into account. An example at the end of the section will illustrate this idea.

For the following, let $\mathcal{E} := \{E_1, E_2, \ldots, E_k\} \subseteq \mathcal{P}_G$ be a collection of errors, and for $1 \leq \ell \leq k$, let $s_\ell := (k_{\ell 1}, k_{\ell 2}, \ldots, k_{\ell t})$ denote the syndrome of E_ℓ relative to the subspace W and the set $\{S_1, S_2, \ldots, S_t\}$.

4.6.21 Theorem. *Let $1 \leq i, j \leq k$. We have that $s_i \neq s_j$ if and only if $E_i^* E_j \notin C(\mathcal{S}_W)$.*

Proof. For the forward direction, suppose $(k_{i1}, k_{i2}, \ldots, k_{it}) = s_i \neq s_j = (k_{j1}, k_{j2}, \ldots, k_{jt})$. Thus there is some $1 \leq r \leq t$ such that $k_{ir} \neq k_{jr}$, so $\epsilon_m^{k_{jr}-k_{ir}} \neq 1$. Fix $1 \leq r \leq t$ such that $k_{ir} \neq k_{jr}$. Recall from the previous theorem that $E_i W \subseteq V_{(\epsilon_m^{k_{ir}}, S_r)}$ and $E_j W \subseteq V_{(\epsilon_m^{k_{jr}}, S_r)}$ so that $S_r E_i|w\rangle = \epsilon_m^{k_{ir}} E_i|w\rangle = \epsilon_m^{k_{ir}} E_i S_r|w\rangle$ and $S_r E_j|w\rangle = \epsilon_m^{k_{jr}} E_j|w\rangle = \epsilon_m^{k_{jr}} E_j S_r|w\rangle$ for any $|w\rangle \in W$. By the commutation relations in $\mathcal{P}_G$, $S_r^* E_i^* S_r E_i$, $S_r^* E_j^* S_r E_j \in \{\epsilon_m^k I \mid k \in \mathbb{Z}_m\}$, and thus $S_r E_i = \epsilon_m^{k_{ir}} E_i S_r$ and $S_r E_j = \epsilon_m^{k_{jr}} E_j S_r$. Rearranging the first equation in the previous sentence, we obtain

$$\begin{aligned} S_r E_i = \epsilon_m^{k_{ir}} E_i S_r &\implies S_r = \epsilon_m^{k_{ir}} E_i S_r E_i^* \\ &\implies \epsilon_m^{-k_{ir}} E_i^* S_r = S_r E_i^*. \end{aligned}$$

Thus

$$S_r E_i^* E_j = (\epsilon_m^{-k_{ir}} E_i^* S_r) E_j = \epsilon_m^{-k_{ir}} E_i^* (\epsilon_m^{k_{jr}} E_j S_r) = \epsilon_m^{k_{jr}-k_{ir}} E_i^* E_j S_r \neq E_i^* E_j S_r.$$

Therefore, $E_i^* E_j \notin C(\mathcal{S}_W)$.

For the other direction, we argue by contraposition. Suppose $(k_{i1}, k_{i2}, \ldots, k_{it}) = s_i = s_j = (k_{j1}, k_{j2}, \ldots, k_{jt})$. Thus $k_{ir} = k_{jr}$ for all $1 \leq r \leq t$, and we have $\epsilon_m^{k_{jr}-k_{ir}} = 1$ for all $1 \leq r \leq t$. Fix $1 \leq r \leq t$. Recall from the previous theorem that $E_i W \subseteq V_{(\epsilon_m^{k_{ir}}, S_r)}$ and $E_j W \subseteq V_{(\epsilon_m^{k_{jr}}, S_r)}$ so that $S_r E_i |w\rangle = \epsilon_m^{k_{ir}} E_i |w\rangle = \epsilon_m^{k_{ir}} E_i S_r |w\rangle$ and $S_r E_j |w\rangle = \epsilon_m^{k_{jr}} E_j |w\rangle = \epsilon_m^{k_{jr}} E_j S_r |w\rangle$ for any $|w\rangle \in W$. By the commutation relations in $\mathcal{P}_G$, $S_r^* E_i^* S_r E_i$, $S_r^* E_j^* S_r E_j \in \{\epsilon_m^k I \mid k \in \mathbb{Z}_m\}$, and thus $S_r E_i = \epsilon_m^{k_{ir}} E_i S_r$ and $S_r E_j = \epsilon_m^{k_{jr}} E_j S_r$. Rearranging the first equation in the previous sentence, we obtain

$$\begin{aligned} S_r E_i = \epsilon_m^{k_{ir}} E_i S_r &\implies S_r = \epsilon_m^{k_{ir}} E_i S_r E_i^* \\ &\implies \epsilon_m^{-k_{ir}} E_i^* S_r = S_r E_i^*. \end{aligned}$$

Thus

$$S_r E_i^* E_j = (\epsilon_m^{-k_{ir}} E_i^* S_r) E_j = \epsilon_m^{-k_{ir}} E_i^* (\epsilon_m^{k_{jr}} E_j S_r) = \epsilon_m^{k_{jr}-k_{ir}} E_i^* E_j S_r = E_i^* E_j S_r.$$

Since r was arbitrary, it follows that $S_r E_i^* E_j = E_i^* E_j S_r$ for all $1 \leq r \leq t$. The claim follows. □

4.6.22 Corollary. *If $s_i \neq s_j$ for all $1 \leq i, j \leq k$ with $i \neq j$, then $\mathcal{E}$ is correctable.*

Proof. Immediate by the previous theorem and Note 4.6.15.

□

4.6.23 Corollary. *Let $|w\rangle \in W$. If $E_i^* E_j \in \mathcal{S}_W$ for some $1 \leq i, j \leq k$, then the state $E_j|w\rangle$ can be returned to the state $|w\rangle$ by applying either E_i^* or E_j^* to $E_j|w\rangle$.*

Proof. Assume $E_i^* E_j \in \mathcal{S}_W$ for some $1 \leq i, j \leq k$. Applying E_i^* or E_j^* to $E_j|w\rangle$, we obtain $E_i^* E_j|w\rangle = |w\rangle$ or $E_j^* E_j|w\rangle = I|w\rangle = |w\rangle$, respectively. The claim follows.

□

4.6.24 Example. Assume $G = \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$. We wish to encode $\mathbb{C}\mathbb{Z}_3$ into $\mathbb{C}G$. Put $m = 12$ so that m is a multiple of the set $\{4, 6, 6\}$. Set $S_0 = X^{(1,0,0)}$ and $S_1 = X^{(0,0,2)} Z^{(0,1,0)}$. Let $\mathcal{S}$ be the subgroup of $\mathcal{P}_G$ generated by the set $\{S_0, S_1\}$. First, we observe that

$$(1,0,0) \circ (0,1,0) = \frac{12}{2}(1 \cdot 0) + \frac{12}{3}(0 \cdot 1) + \frac{12}{3}(0 \cdot 0) = 0,$$

and thus $X^{(1,0,0)} Z^{(0,1,0)} = \epsilon_{12}^{-(1,0,0)\circ(0,1,0)} Z^{(0,1,0)} X^{(1,0,0)} = Z^{(0,1,0)} X^{(1,0,0)}$ by Theorem 4.1.6. Therefore,

$$\begin{aligned} S_0 S_1 &= X^{(1,0,0)} X^{(0,0,2)} Z^{(0,1,0)} \\ &= X^{(0,0,2)} Z^{(0,1,0)} X^{(1,0,0)} \\ &= S_1 S_0. \end{aligned}$$

Now, observe that $o(S_0) = o(X^{(1,0,0)}) = o(1,0,0) = 2$. Also, $o(X^{(0,0,2)}) = 3$ and $o(Z^{(0,1,0)}) = 3$, so $\ell := \operatorname{lcm}(3,3) = 3$. Since ℓ is odd, $o(S_1) = 3$ by Theorem 4.2.10. The elements of $\mathcal{S}$ are thus

$$I,$$

$$S_0 = X^{(1,0,0)},$$

$$S_1 = X^{(0,0,2)} Z^{(0,1,0)},$$

$$S_1^2 = (X^{(0,0,2)} Z^{(0,1,0)})(X^{(0,0,2)} Z^{(0,1,0)}) = X^{(0,0,1)} Z^{(0,2,0)},$$

$$S_0 S_1 = (X^{(1,0,0)})(X^{(0,0,2)} Z^{(0,1,0)}) = X^{(1,0,2)} Z^{(0,1,0)},$$

$$S_0 S_1^2 = (X^{(1,0,0)})(X^{(0,0,1)} Z^{(0,2,0)}) = X^{(1,0,1)} Z^{(0,2,0)}.$$

Put $T := X^{(1,1,0)} Z^{(0,0,2)}$. Observe by Theorem 4.2.9 that $T^k = \epsilon_{12}^{\frac{k(k-1)}{2}(1,1,0)\circ(0,0,2)} X^{k(1,1,0)} Z^{k(0,0,2)} = X^{k(1,1,0)} Z^{k(0,0,2)}$ since $(1,1,0) \circ (0,0,2) = 0$. Thus $T^2 = X^{(0,2,0)} Z^{(0,0,1)}$, $T^3 = X^{(1,0,0)}$, $T^4 = X^{(0,1,0)} Z^{(0,0,2)}$, and $T^5 = X^{(1,2,0)} Z^{(0,0,1)}$. Therefore, $T, T^2 \notin \mathcal{S}$, but $T^3 = S_0 \in \mathcal{S}$, and thus $T^4|w\rangle = T(T^3|w\rangle) = T|w\rangle$ and $T^5|w\rangle = T^2(T^3|w\rangle) = T^2|w\rangle$ for all $|w\rangle \in W$, so T^4 and T^5 are equal to T and T^2 on the vectors in W, respectively.

Recall from Definition 3.4.1 that $(a,b) * (c,d) = b \circ c - a \circ d$ for all $a, b, c, d \in G$. Since

$$\big((1,1,0),(0,0,2)\big) * \big((1,0,0),(0,0,0)\big) = (0,0,2) \circ (1,0,0) - (1,1,0) \circ (0,0,0) = 0$$

and

$$\big((1,1,0),(0,0,2)\big) * \big((0,0,2),(0,1,0)\big) = (0,0,2) \circ (0,0,2) - (1,1,0) \circ (0,1,0) = \frac{12}{3}(2 \cdot 2) - \frac{12}{3}(1 \cdot 1) = 0,$$

we have, by Note 4.2.8,

$$\begin{aligned} TS_0 &= X^{(1,1,0)} Z^{(0,0,2)} X^{(1,0,0)} \\ &= \epsilon_{12}^{((1,1,0),(0,0,2)) * ((1,0,0),(0,0,0))} X^{(1,0,0)} X^{(1,1,0)} Z^{(0,0,2)} \\ &= S_0 T \end{aligned}$$

and

$$\begin{aligned} TS_1 &= X^{(1,1,0)} Z^{(0,0,2)} X^{(0,0,2)} Z^{(0,1,0)} \\ &= \epsilon_{12}^{((1,1,0),(0,0,2)) * ((0,0,2),(0,1,0))} X^{(0,0,2)} Z^{(0,1,0)} X^{(1,1,0)} Z^{(0,0,2)} \\ &= X^{(0,0,2)} Z^{(0,1,0)} X^{(1,1,0)} Z^{(0,0,2)} \\ &= S_1 T. \end{aligned}$$

Thus $T \in C(\mathcal{S})\backslash\mathcal{S}$. By Note 4.6.20, T is not detectable as an error. We let T define an encoding of $\mathbb{C}\mathbb{Z}_6$ into $\mathbb{C}G$ by the following assignment:

$$
\begin{aligned}
|0\rangle &\mapsto T^0|000\rangle = |000\rangle, \\
|1\rangle &\mapsto T^1|000\rangle = |110\rangle, \\
|2\rangle &\mapsto T^2|000\rangle = |020\rangle, \\
|3\rangle &\mapsto T^3|000\rangle = |100\rangle, \\
|4\rangle &\mapsto T^4|000\rangle = |010\rangle, \\
|5\rangle &\mapsto T^5|000\rangle = |120\rangle.
\end{aligned}
$$

Now that we have $\mathcal{S}$ written explicitly, we can invoke Theorem 4.6.2 and construct our stabilizer code by mapping $|g\rangle$, for each $g \in G$, to $|\tilde{g}\rangle = |\mathcal{S}|^{-1/2} \sum_{s\in\mathcal{S}} s|g\rangle$. Let $g \in G$. We have that $g = (g_1, g_2, g_3)$ for some $g_1 \in \mathbb{Z}_2$, $g_2 \in \mathbb{Z}_3$, and $g_3 \in \mathbb{Z}_3$, and thus:

$$
\begin{aligned}
&I|g_1g_2g_3\rangle = |g_1g_2g_3\rangle = |g_1\rangle|g_2\rangle|g_3\rangle, \\
&S_0|g_1g_2g_3\rangle = X^{(1,0,0)}|g_1g_2g_3\rangle = |(1+g_1)\rangle|g_2\rangle|g_3\rangle, \\
&S_1|g_1g_2g_3\rangle = X^{(0,0,2)}Z^{(0,1,0)}|g_1g_2g_3\rangle = \epsilon_{12}^{4g_2}|g_1\rangle|g_2\rangle|2+g_3\rangle, \\
&S_1^2|g_1g_2g_3\rangle = X^{(0,0,1)}Z^{(0,2,0)}|g_1g_2g_3\rangle = \epsilon_{12}^{8g_2}|g_1\rangle|g_2\rangle|1+g_3\rangle, \\
&S_0S_1|g_1g_2g_3\rangle = X^{(1,0,2)}Z^{(0,1,0)}|g_1g_2g_3\rangle = \epsilon_{12}^{4g_2}|1+g_1\rangle|g_2\rangle|2+g_3\rangle, \\
&S_0S_1^2|g_1g_2g_3\rangle = X^{(1,0,1)}Z^{(0,2,0)}|g_1g_2g_3\rangle = \epsilon_{12}^{8g_2}|1+g_1\rangle|g_2\rangle|1+g_3\rangle.
\end{aligned}
$$

Thus

$$
\begin{aligned}
|g_1\tilde{g_2}g_3\rangle &= \frac{1}{\sqrt{6}}(I + S_0 + S_1 + S_1^2 + S_0S_1 + S_0S_1^2)|g_1g_2g_3\rangle \\
&= \frac{1}{\sqrt{6}}(|g_1\rangle|g_2\rangle|g_3\rangle + |(1+g_1)\rangle|g_2\rangle|g_3\rangle + \epsilon_{12}^{4g_2}|g_1\rangle|g_2\rangle|2+g_3\rangle + \epsilon_{12}^{8g_2}|g_1\rangle|g_2\rangle|1+g_3\rangle
\end{aligned}
$$

$$+ \epsilon_{12}^{4g_2}|1+g_1\rangle|g_2\rangle|2+g_3\rangle + \epsilon_{12}^{8g_2}|1+g_1\rangle|g_2\rangle|1+g_3\rangle).$$

We have

$$\begin{aligned}
|\tilde{0\bar{0}0}\rangle &= \frac{1}{\sqrt{6}}(|000\rangle + |100\rangle + |002\rangle + |001\rangle + |102\rangle + |101\rangle).\\
|\tilde{1\bar{1}0}\rangle &= \frac{1}{\sqrt{6}}(|110\rangle + |010\rangle + \epsilon_{12}^{4}|112\rangle + \epsilon_{12}^{8}|111\rangle + \epsilon_{12}^{4}|012\rangle + \epsilon_{12}^{8}|011\rangle).\\
|\tilde{0\bar{2}0}\rangle &= \frac{1}{\sqrt{6}}(|020\rangle + |120\rangle + \epsilon_{12}^{8}|022\rangle + \epsilon_{12}^{4}|021\rangle + \epsilon_{12}^{8}|122\rangle + \epsilon_{12}^{4}|121\rangle).\\
|\tilde{1\bar{0}0}\rangle &= \frac{1}{\sqrt{6}}(|100\rangle + |000\rangle + |102\rangle + |101\rangle + |002\rangle + |001\rangle).\\
|\tilde{0\bar{1}0}\rangle &= \frac{1}{\sqrt{6}}(|010\rangle + |110\rangle + \epsilon_{12}^{4}|012\rangle + \epsilon_{12}^{8}|011\rangle + \epsilon_{12}^{4}|112\rangle + \epsilon_{12}^{8}|111\rangle).\\
|\tilde{1\bar{2}0}\rangle &= \frac{1}{\sqrt{6}}(|120\rangle + |020\rangle + \epsilon_{12}^{8}|122\rangle + \epsilon_{12}^{4}|121\rangle + \epsilon_{12}^{8}|022\rangle + \epsilon_{12}^{4}|021\rangle).
\end{aligned}$$

Observe that $|\tilde{0\bar{0}0}\rangle = |\tilde{1\bar{0}0}\rangle$, $|\tilde{1\bar{1}0}\rangle = |\tilde{0\bar{1}0}\rangle$, and $|\tilde{0\bar{2}0}\rangle = |\tilde{1\bar{2}0}\rangle$, which is due to the fact that $T^3 \in \mathcal{S}$. Put $\overline{|0\rangle} = |\tilde{0\bar{0}0}\rangle$, $\overline{|1\rangle} = |\tilde{0\bar{2}0}\rangle$, and $\overline{|2\rangle} = |\tilde{0\bar{1}0}\rangle$. By Note 4.6.3, it follows that our stabilizer code is the subspace of $\mathbb{C}G$ spanned by the set $\left\{\overline{|0\rangle}, \overline{|1\rangle}, \overline{|2\rangle}\right\}$ and the linear transformation $U : \mathbb{C}\mathbb{Z}_3 \to \mathbb{C}G$ that maps $|0\rangle \mapsto \overline{|0\rangle}$, $|1\rangle \mapsto \overline{|1\rangle}$, and $|2\rangle \mapsto \overline{|2\rangle}$ is an encoding of $\mathbb{C}\mathbb{Z}_3$. Also, observe that $I|\tilde{0\bar{0}0}\rangle = |\tilde{0\bar{0}0}\rangle$, $T^2|\tilde{0\bar{0}0}\rangle = |\tilde{0\bar{2}0}\rangle$, and $T^4|\tilde{0\bar{0}0}\rangle = |\tilde{0\bar{1}0}\rangle$, and thus T^2 acts in an equivalent manner on the stabilizer code as $X \in \mathcal{P}_{\mathbb{Z}_3}$ does on the set $\{|0\rangle, |1\rangle, |2\rangle\}$. Therefore, T^2 is an error belonging to $C(\mathcal{S})\backslash\mathcal{S}$ that we have used to define an encoding, which was discussed at the end of Note 4.6.20.

4.7 Automorphisms of the Pauli Algebra of G

Recall again that $G = \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_n}$ for some $n, m_i \in \mathbb{Z}^+$ and m is a fixed common multiple of the set $\{2m_i \mid 1 \leq i \leq n\}$.

For the following theorem, set $XZ(a,b) := X^a Z^b$, for $a, b \in G$. Also, recall from Theorem 4.3.4 that $\mathcal{P}_G$ has presentation $\langle S \mid R \rangle$, where

$$S = \{\epsilon_m^k I, X^g, Z^h \mid k \in \mathbb{Z}_m, g, h \in G\},$$
$$R = \{X^0, Z^0, \epsilon_m^0 I, X^{g+h}X^{-h}X^{-g}, Z^{g+h}Z^{-h}Z^{-g}, (\epsilon_m^{j+k}I)(\epsilon_m^{-k}I)(\epsilon_m^{-j}I),$$
$$(\epsilon_m^k I)X^g(\epsilon_m^{-k}I)X^{-g}, (\epsilon_m^k I)Z^g(\epsilon_m^{-k}I)Z^{-g}, (\epsilon_m^{g\circ h}I)X^g Z^h X^{-g} Z^{-h} \mid g, h \in G, j, k \in \mathbb{Z}_m\}.$$

For the following, let S and R be defined as they are above.

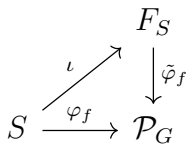
4.7.1 Theorem. *Let f be a symplectomorphism of $\overline{G}$, and define the function $\varphi_f : S \to \mathcal{P}_G$ by*

$$\varphi_f(X^g) = \varphi_f(XZ(g,0)) = \epsilon_m^{[\pi_1(f(g,0))\circ\pi_2(f(g,0))]/2} XZ(f(g,0)),$$
$$\varphi_f(Z^h) = \varphi_f(XZ(0,h)) = \epsilon_m^{[\pi_1(f(0,h))\circ\pi_2(f(0,h))]/2} XZ(f(0,h)),$$
$$\varphi_f(\epsilon_m^k I) = \epsilon_m^k I,$$

where $\pi_i : \overline{G} \to G$ is the projection onto the i^{th} coordinate. Then φ_f extends to an endomorphism of $\mathcal{P}_G$.

Proof. By Corollary 4.3.2, it suffices to check that $\tilde{\varphi}_f(r) = I$ for all $r \in R$, where $\tilde{\varphi}_f : F_S \to \mathcal{P}_G$ is the unique homomorphism afforded by the universal property of free groups (Theorem

4.3.1). In the statement of the universal property of free groups, we have that $\iota : S \to F_S$ is the inclusion map and $\tilde{\varphi}_f \iota = \varphi_f$, so for all $s \in S$, $\tilde{\varphi}_f(s) = \tilde{\varphi}_f \iota(s) = \varphi_f(s)$. We have the following diagram:



First, observe that

$$\varphi_f(X^0) = \varphi_f(XZ(0,0)) = \epsilon_m^{[\pi_1(f(0,0)) \circ \pi_2(f(0,0))]/2} XZ(f(0,0)) = \epsilon_m^{[\pi_1(0,0) \circ \pi_2(0,0)]/2} XZ(0,0) = I,$$
$$\varphi_f(Z^0) = \varphi_f(XZ(0,0)) = I,$$
$$\varphi_f(\epsilon_m^0 I) = \epsilon_m^0 I = I.$$

Thus $\tilde{\varphi}_f(X^0) = \varphi_f(X^0) = I$, $\tilde{\varphi}_f(Z^0) = \varphi_f(Z^0) = I$, and $\tilde{\varphi}_f(\epsilon_m^0 I) = \varphi_f(\epsilon_m^0 I) = I$. Now, let $g, h \in G$. Claim: $\tilde{\varphi}_f(X^{g+h}) = \tilde{\varphi}_f(X^g)\tilde{\varphi}_f(X^h)$. We have

$$\begin{aligned}
\tilde{\varphi}_f(X^{g+h}) &= \varphi_f(X^{g+h}) \\
&= \varphi_f(XZ(g+h,0)) \\
&= \epsilon_m^{[\pi_1(f(g+h,0)) \circ \pi_2(f(g+h,0))]/2} XZ(f(g+h,0)) \\
&= \epsilon_m^{[(\pi_1(f(g,0)) + \pi_1(f(h,0))) \circ (\pi_2(f(g,0)) + \pi_2(f(h,0)))]/2} \\
&\quad \cdot X^{\pi_1(f(g+h,0))} Z^{\pi_2(f(g+h,0))} \\
&= \epsilon_m^{[\pi_1(f(g,0)) \circ \pi_2(f(g,0)) + \pi_1(f(g,0)) \circ \pi_2(f(h,0)) + \pi_1(f(h,0)) \circ \pi_2(f(g,0)) + \pi_1(f(h,0)) \circ \pi_2(f(h,0))]/2} \\
&\quad \cdot X^{\pi_1(f(g,0))} X^{\pi_1(f(h,0))} Z^{\pi_2(f(g,0))} Z^{\pi_2(f(h,0))} \\
&= \epsilon_m^{[\pi_1(f(g,0)) \circ \pi_2(f(g,0)) + \pi_1(f(g,0)) \circ \pi_2(f(h,0)) + \pi_1(f(h,0)) \circ \pi_2(f(g,0)) + \pi_1(f(h,0)) \circ \pi_2(f(h,0))]/2} \\
&\quad \cdot \epsilon_m^{-\pi_1(f(h,0)) \circ \pi_2(f(g,0))} X^{\pi_1(f(g,0))} Z^{\pi_2(f(g,0))} X^{\pi_1(f(h,0))} Z^{\pi_2(f(h,0))}
\end{aligned}$$

$$
\begin{aligned}
&= \epsilon_m^{[\pi_1(f(g,0))\circ\pi_2(f(h,0))+\pi_1(f(h,0))\circ\pi_2(f(g,0))]/2}\epsilon_m^{-\pi_1(f(h,0))\circ\pi_2(f(g,0))} \\
&\quad \cdot \left(\epsilon_m^{\pi_1(f(g,0))\circ\pi_2(f(g,0))/2} X^{\pi_1(f(g,0))} Z^{\pi_2(f(g,0))}\right) \\
&\quad \cdot \left(\epsilon_m^{\pi_1(f(h,0))\circ\pi_2(f(h,0))/2} X^{\pi_1(f(h,0))} Z^{\pi_2(f(h,0))}\right) \\
&= \epsilon_m^{[\pi_1(f(g,0))\circ\pi_2(f(h,0))+\pi_1(f(h,0))\circ\pi_2(f(g,0))]/2}\epsilon_m^{-\pi_1(f(h,0))\circ\pi_2(f(g,0))} \\
&\quad \cdot \left(\epsilon_m^{\pi_1(f(g,0))\circ\pi_2(f(g,0))/2} XZ(f(g,0))\right) \\
&\quad \cdot \left(\epsilon_m^{\pi_1(f(h,0))\circ\pi_2(f(h,0))/2} XZ(f(h,0))\right) \\
&= \epsilon_m^{[\pi_1(f(g,0))\circ\pi_2(f(h,0))-\pi_1(f(h,0))\circ\pi_2(f(g,0))]/2} \cdot \varphi_f(XZ(g,0))\varphi_f(XZ(h,0)) \\
&= \epsilon_m^{[(\pi_1(f(h,0)),\pi_2(f(h,0)))*(\pi_1(f(g,0)),\pi_2(f(g,0)))]/2}\varphi_f(XZ(g,0))\varphi_f(XZ(h,0)) \\
&= \epsilon_m^{f(h,0)*f(g,0)/2}\varphi_f(XZ(g,0))\varphi_f(XZ(h,0)) \\
&= \epsilon_m^{(h,0)*(g,0)/2}\varphi_f(XZ(g,0))\varphi_f(XZ(h,0)) \\
&= \epsilon_m^{0}\varphi_f(XZ(g,0))\varphi_f(XZ(h,0)) \\
&= \varphi_f(XZ(g,0))\varphi_f(XZ(h,0)) \\
&= \varphi_f(X^g)\varphi_f(X^h) \\
&= \tilde{\varphi}_f(X^g)\tilde{\varphi}_f(X^h).
\end{aligned}
$$

The claim follows. Thus for all $a \in G$, we have $\tilde{\varphi}_f(X^a)\tilde{\varphi}_f(X^{-a}) = \tilde{\varphi}_f(X^{a-a}) = \tilde{\varphi}_f(X^0) = I$ so that $\tilde{\varphi}_f(X^{-a}) = \tilde{\varphi}_f(X^a)^{-1}$. We have

$$
\begin{aligned}
\tilde{\varphi}_f(X^{g+h}X^{-h}X^{-g}) &= \tilde{\varphi}_f(X^{g+h})\tilde{\varphi}_f(X^{-h})\tilde{\varphi}_f(X^{-g}) \\
&= \tilde{\varphi}_f(X^{g})\tilde{\varphi}_f(X^{h})\tilde{\varphi}_f(X^{-h})\tilde{\varphi}_f(X^{-g}) \\
&= \tilde{\varphi}_f(X^{g})\tilde{\varphi}_f(X^{-g}) \\
&= I.
\end{aligned}
$$

Similarly, $\tilde{\varphi}_f(Z^{g+h}Z^{-h}Z^{-g}) = I$. We also have

$$\begin{aligned}
\tilde{\varphi}_f((\epsilon_m^{j+k}I)(\epsilon_m^{-k}I)(\epsilon_m^{-j}I)) &= \tilde{\varphi}_f(\epsilon_m^{j+k}I)\tilde{\varphi}_f(\epsilon_m^{-k}I)\tilde{\varphi}_f(\epsilon_m^{-j}I) \\
&= \varphi_f(\epsilon_m^{j+k}I)\varphi_f(\epsilon_m^{-k}I)\varphi_f(\epsilon_m^{-j}I) \\
&= (\epsilon_m^{j+k}I)(\epsilon_m^{-k}I)(\epsilon_m^{-j}I) \\
&= I.
\end{aligned}$$

Additionally, we have

$$\begin{aligned}
\tilde{\varphi}_f((\epsilon_m^{k}I)X^{g}(\epsilon_m^{-k}I)X^{-g}) &= \tilde{\varphi}_f(\epsilon_m^{k}I)\tilde{\varphi}_f(X^{g})\tilde{\varphi}_f(\epsilon_m^{-k}I)\tilde{\varphi}_f(X^{-g}) \\
&= \tilde{\varphi}_f(\epsilon_m^{k}I)\tilde{\varphi}_f(X^{g})\tilde{\varphi}_f(\epsilon_m^{-k}I)\tilde{\varphi}_f(X^{g})^{-1} \\
&= \varphi_f(\epsilon_m^{k}I)\tilde{\varphi}_f(X^{g})\varphi_f(\epsilon_m^{-k}I)\tilde{\varphi}_f(X^{g})^{-1} \\
&= (\epsilon_m^{k}I)\tilde{\varphi}_f(X^{g})(\epsilon_m^{-k}I)\tilde{\varphi}_f(X^{g})^{-1} \\
&= (\epsilon_m^{k}I)(\epsilon_m^{-k}I)\tilde{\varphi}_f(X^{g})\tilde{\varphi}_f(X^{g})^{-1} \\
&= I.
\end{aligned}$$

The proof for $\tilde{\varphi}_f((\epsilon_m^{k}I)Z^{g}(\epsilon_m^{-k}I)Z^{-g}) = I$ is similar.

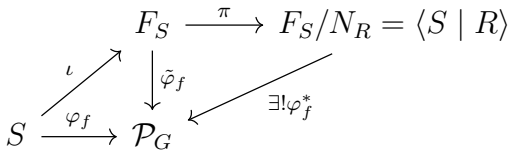
Lastly, we prove that $\tilde{\varphi}_f((\epsilon_m^{g\circ h}I)\cdot(X^gZ^hX^{-g}Z^{-h})) = I$. We have

$$\begin{aligned}
\tilde{\varphi}_f((\epsilon_m^{g\circ h}I)\cdot(X^gZ^hX^{-g}Z^{-h})) &= \tilde{\varphi}_f(\epsilon_m^{g\circ h}I)\tilde{\varphi}_f(X^{g})\tilde{\varphi}_f(Z^{h})\tilde{\varphi}_f(X^{-g})\tilde{\varphi}_f(Z^{-h}) \\
&= \varphi_f(\epsilon_m^{g\circ h}I)\varphi_f(X^{g})\varphi_f(Z^{h})\varphi_f(X^{-g})\varphi_f(Z^{-h}) \\
&= (\epsilon_m^{g\circ h}I)\cdot(\epsilon_m^{\pi_1(f(g,0))\circ\pi_2(f(g,0))/2}XZ(f(g,0))) \\
&\quad\cdot(\epsilon_m^{\pi_1(f(0,h))\circ\pi_2(f(0,h))/2}XZ(f(0,h))) \\
&\quad\cdot(\epsilon_m^{\pi_1(f(-g,0))\circ\pi_2(f(-g,0))/2}XZ(f(-g,0))) \\
&\quad\cdot(\epsilon_m^{\pi_1(f(0,-h))\circ\pi_2(f(0,-h))/2}XZ(f(0,-h)))
\end{aligned}$$

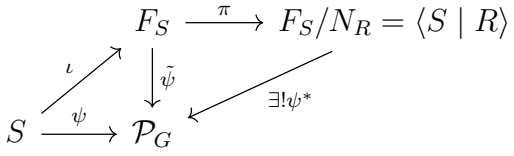
$$
\begin{aligned}
&= (\epsilon_m^{g\circ h} I) \cdot (\epsilon_m^{\pi_1(f(g,0))\circ\pi_2(f(g,0))/2} XZ(f(g,0))) \\
&\quad \cdot (\epsilon_m^{\pi_1(f(0,h))\circ\pi_2(f(0,h))/2} XZ(f(0,h))) \\
&\quad \cdot (\epsilon_m^{(-\pi_1(f(g,0)))\circ(-\pi_2(f(g,0)))/2} XZ(f(-g,0))) \\
&\quad \cdot (\epsilon_m^{(-\pi_1(f(0,h)))\circ(-\pi_2(f(0,h)))/2} XZ(f(0,-h))) \\
&= (\epsilon_m^{g\circ h} I) \cdot (\epsilon_m^{\pi_1(f(g,0))\circ\pi_2(f(g,0))/2} XZ(f(g,0))) \\
&\quad \cdot (\epsilon_m^{\pi_1(f(0,h))\circ\pi_2(f(0,h))/2} XZ(f(0,h))) \\
&\quad \cdot (\epsilon_m^{\pi_1(f(g,0))\circ\pi_2(f(g,0))/2} XZ(f(-g,0))) \\
&\quad \cdot (\epsilon_m^{\pi_1(f(0,h))\circ\pi_2(f(0,h))/2} XZ(f(0,-h))) \\
&= (\epsilon_m^{g\circ h} I) \cdot (\epsilon_m^{\pi_1(f(g,0))\circ\pi_2(f(g,0))} I) \cdot (\epsilon_m^{\pi_1(f(0,h))\circ\pi_2(f(0,h))} I) \\
&\quad \cdot XZ(f(g,0))XZ(f(0,h))XZ(f(-g,0))XZ(f(0,-h)) \\
&= (\epsilon_m^{g\circ h} I) \cdot (\epsilon_m^{\pi_1(f(g,0))\circ\pi_2(f(g,0))} I) \cdot (\epsilon_m^{\pi_1(f(0,h))\circ\pi_2(f(0,h))} I) \\
&\quad \cdot (X^{\pi_1(f(g,0))} Z^{\pi_2(f(g,0))})(X^{\pi_1(f(0,h))} Z^{\pi_2(f(0,h))}) \\
&\quad \cdot (X^{-\pi_1(f(g,0))} Z^{-\pi_2(f(g,0))})(X^{-\pi_1(f(0,h))} Z^{-\pi_2(f(0,h))}) \\
&= (\epsilon_m^{g\circ h} I) \cdot (\epsilon_m^{\pi_1(f(g,0))\circ\pi_2(f(g,0))} I) \cdot (\epsilon_m^{\pi_1(f(0,h))\circ\pi_2(f(0,h))} I) \\
&\quad \cdot (\epsilon_m^{(\pi_1(f(0,h)),\pi_2(f(0,h)))*(-\pi_1(f(g,0)),-\pi_2(f(g,0)))} I) \\
&\quad \cdot (X^{\pi_1(f(g,0))} Z^{\pi_2(f(g,0))})(X^{-\pi_1(f(g,0))} Z^{-\pi_2(f(g,0))}) \\
&\quad \cdot (X^{\pi_1(f(0,h))} Z^{\pi_2(f(0,h))})(X^{-\pi_1(f(0,h))} Z^{-\pi_2(f(0,h))}) \\
&= (\epsilon_m^{g\circ h} I) \cdot (\epsilon_m^{\pi_1(f(g,0))\circ\pi_2(f(g,0))} I) \cdot (\epsilon_m^{\pi_1(f(0,h))\circ\pi_2(f(0,h))} I) \\
&\quad \cdot (\epsilon_m^{f(0,h)*f(-g,0)} I) \\
&\quad \cdot X^{\pi_1(f(g,0))}(Z^{\pi_2(f(g,0))} X^{-\pi_1(f(g,0))}) Z^{-\pi_2(f(g,0))} \\
&\quad \cdot X^{\pi_1(f(0,h))}(Z^{\pi_2(f(0,h))} X^{-\pi_1(f(0,h))}) Z^{-\pi_2(f(0,h))} \\
&= (\epsilon_m^{g\circ h} I) \cdot (\epsilon_m^{\pi_1(f(g,0))\circ\pi_2(f(g,0))} I) \cdot (\epsilon_m^{\pi_1(f(0,h))\circ\pi_2(f(0,h))} I) \\
&\quad \cdot (\epsilon_m^{(0,h)*(-g,0)} I) \\
&\quad \cdot X^{\pi_1(f(g,0))}(\epsilon_m^{-\pi_1(f(g,0))\circ\pi_2(f(g,0))} X^{-\pi_1(f(g,0))} Z^{\pi_2(f(g,0))}) Z^{-\pi_2(f(g,0))} \\
&\quad \cdot X^{\pi_1(f(0,h))}(\epsilon_m^{-\pi_1(f(0,h))\circ\pi_2(f(0,h))} X^{-\pi_1(f(0,h))} Z^{\pi_2(f(0,h))}) Z^{-\pi_2(f(0,h))}
\end{aligned}
$$

$$
\begin{aligned}
&= (\epsilon_m^{g\circ h} I) \cdot (\epsilon_m^{\pi_1(f(g,0))\circ\pi_2(f(g,0))} I) \cdot (\epsilon_m^{\pi_1(f(0,h))\circ\pi_2(f(0,h))} I) \\
&\quad \cdot (\epsilon_m^{-g\circ h} I) \\
&\quad \cdot X^{\pi_1(f(g,0))} (\epsilon_m^{-\pi_1(f(g,0))\circ\pi_2(f(g,0))} X^{-\pi_1(f(g,0))} Z^{\pi_2(f(g,0))}) Z^{-\pi_2(f(g,0))} \\
&\quad \cdot X^{\pi_1(f(0,h))} (\epsilon_m^{-\pi_1(f(0,h))\circ\pi_2(f(0,h))} X^{-\pi_1(f(0,h))} Z^{\pi_2(f(0,h))}) Z^{-\pi_2(f(0,h))} \\
&= (\epsilon_m^{\pi_1(f(g,0))\circ\pi_2(f(g,0))} I) \cdot (\epsilon_m^{\pi_1(f(0,h))\circ\pi_2(f(0,h))} I) \\
&\quad \cdot (\epsilon_m^{-\pi_1(f(g,0))\circ\pi_2(f(g,0))} I)(\epsilon_m^{-\pi_1(f(0,h))\circ\pi_2(f(0,h))} I) \\
&\quad \cdot (X^{\pi_1(f(g,0))} X^{-\pi_1(f(g,0))})(Z^{\pi_2(f(g,0))} Z^{-\pi_2(f(g,0))}) \\
&\quad \cdot (X^{\pi_1(f(0,h))} X^{-\pi_1(f(0,h))})(Z^{\pi_2(f(0,h))} Z^{-\pi_2(f(0,h))}) \\
&= I.
\end{aligned}
$$

Thus $\tilde{\varphi}_f(r) = I$ for all $r \in R$, so we can apply Corollary 4.3.2, which implies φ_f extends to a homomorphism $\varphi_f^* : \langle S \mid R \rangle \to \mathcal{P}_G$. We have the following diagram:

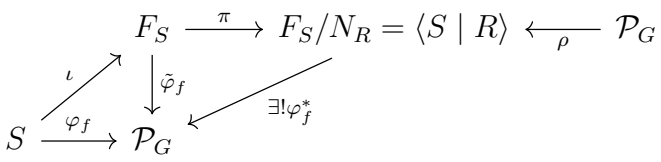


Now, recall the following diagram from Theorem 4.3.4, with φ replaced by ψ in the proof of that theorem:



In the proof of Theorem 4.3.4, $\psi : S \to \mathcal{P}_G$ was the inclusion map and $\psi^* : F_S/N_R \to \mathcal{P}_G$ was the homomorphism extension granted by Corollary 4.3.2 that was found to be an isomorphism. In Note 4.3.5, we observed that for all $s \in S$, $\psi^*(sN_R) = \psi^*\pi(s) = \tilde{\psi}(s) = \tilde{\psi}\iota(s) = \psi(s) = s$.

Put $\rho = (\psi^*)^{-1}$. Then $\rho : \mathcal{P}_G \to F_S/N_R$ is a well-defined isomorphism with $\rho(s) = sN_R$ for all $s \in S$. Therefore, we may update the diagram of this theorem with



Put $\overline{\varphi_f} = \varphi_f^* \rho$. It follows that $\overline{\varphi_f} : \mathcal{P}_G \to \mathcal{P}_G$ is a homomorphism. The claim follows.

□

4.7.2 Note. Let the language be as in the proof of the previous theorem. Observe that, for all $s \in S$, we have

$$\overline{\varphi_f}(s) = \varphi_f^* \rho(s) = \varphi_f^*(sN_R) = \varphi_f^* \pi(s) = \tilde{\varphi}_f(s) = \tilde{\varphi}_f \iota(s) = \varphi_f(s).$$

We apply this observation to the following theorem.

4.7.3 Theorem. *Let f and g be symplectomorphisms of $\overline{G}$, and let $\overline{\varphi_f}$ and $\overline{\varphi_g}$ denote the endomorphisms of $\mathcal{P}_G$ that f and g afford by Theorem 4.7.1, respectively. We have $\overline{\varphi_f}\,\overline{\varphi_g} = \overline{\varphi_{fg}}$.*

Proof. It is straightforward to prove that fg is a symplectomorphism of $\overline{G}$. Thus fg affords the endomorphism $\overline{\varphi_{fg}}$ of $\mathcal{P}_G$ by the previous theorem.

Let $a \in G$. To improve readability, set $g(a, 0) = x$. By the previous note, we have that $\overline{\varphi_\alpha}(s) = \varphi_\alpha(s)$ for all $s \in S$, where α is a symplectomorphism of $\overline{G}$. Then we have

$$\begin{aligned}
\overline{\varphi_f}\,\overline{\varphi_g}(X^a) &= \overline{\varphi_f}(\varphi_g(X^a)) \\
&= \overline{\varphi_f}\left(\epsilon_m^{\pi_1(x)\circ\pi_2(x)/2} X^{\pi_1(x)} Z^{\pi_2(x)}\right) \\
&= \epsilon_m^{\pi_1(x)\circ\pi_2(x)/2} \overline{\varphi_f}\left(X^{\pi_1(x)}\right) \overline{\varphi_f}\left(Z^{\pi_2(x)}\right)
\end{aligned}$$

$$
\begin{aligned}
&= \epsilon_m^{\pi_1(x)\circ\pi_2(x)/2} \varphi_f\left(X^{\pi_1(x)}\right) \varphi_f\left(Z^{\pi_2(x)}\right) \\
&= \epsilon_m^{\pi_1(x)\circ\pi_2(x)/2} I \\
&\quad \cdot \left(\epsilon_m^{\pi_1(f(\pi_1(x),0))\circ\pi_2(f(\pi_1(x),0))/2} X^{\pi_1(f(\pi_1(x),0))} Z^{\pi_2(f(\pi_1(x),0))}\right) \\
&\quad \cdot \left(\epsilon_m^{\pi_1(f(0,\pi_2(x)))\circ\pi_2(f(0,\pi_2(x)))/2} X^{\pi_1(f(0,\pi_2(x)))} Z^{\pi_2(f(0,\pi_2(x)))}\right) \\
&= \epsilon_m^{\pi_1(x)\circ\pi_2(x)/2} \epsilon_m^{\pi_1(f(\pi_1(x),0))\circ\pi_2(f(\pi_1(x),0))/2} \epsilon_m^{\pi_1(f(0,\pi_2(x)))\circ\pi_2(f(0,\pi_2(x)))/2} \\
&\quad \cdot X^{\pi_1(f(\pi_1(x),0))} Z^{\pi_2(f(\pi_1(x),0))} X^{\pi_1(f(0,\pi_2(x)))} Z^{\pi_2(f(0,\pi_2(x)))} \\
&= \epsilon_m^{\pi_1(x)\circ\pi_2(x)/2} \epsilon_m^{\pi_1(f(\pi_1(x),0))\circ\pi_2(f(\pi_1(x),0))/2} \epsilon_m^{\pi_1(f(0,\pi_2(x)))\circ\pi_2(f(0,\pi_2(x)))/2} \\
&\quad \cdot X^{\pi_1(f(\pi_1(x),0))} \\
&\quad \cdot \left(\epsilon_m^{\pi_2(f(\pi_1(x),0))\circ\pi_1(f(0,\pi_2(x)))} X^{\pi_1(f(0,\pi_2(x)))} Z^{\pi_2(f(\pi_1(x),0))}\right) Z^{\pi_2(f(0,\pi_2(x)))} \\
&= \epsilon_m^{\pi_1(x)\circ\pi_2(x)/2} \epsilon_m^{\pi_1(f(\pi_1(x),0))\circ\pi_2(f(\pi_1(x),0))/2} \epsilon_m^{\pi_1(f(0,\pi_2(x)))\circ\pi_2(f(0,\pi_2(x)))/2} \\
&\quad \cdot \epsilon_m^{\pi_2(f(\pi_1(x),0))\circ\pi_1(f(0,\pi_2(x)))} X^{\pi_1(f(\pi_1(x),\pi_2(x)))} Z^{\pi_2(f(\pi_1(x),\pi_2(x)))}
\end{aligned}
$$

For increased readability, we set $\gamma = [\pi_1(x) \circ \pi_2(x) + \pi_1(f(\pi_1(x), 0)) \circ \pi_2(f(\pi_1(x), 0)) + \pi_1(f(0, \pi_2(x))) \circ \pi_2(f(0, \pi_2(x)))]/2 + \pi_2(f(\pi_1(x), 0)) \circ \pi_1(f(0, \pi_2(x)))$. Simplifying γ, we obtain

$$
\begin{aligned}
\gamma &= [\pi_1(x) \circ \pi_2(x) \\
&\quad + \pi_1(f(\pi_1(x), 0)) \circ \pi_2(f(\pi_1(x), 0)) + \pi_1(f(0, \pi_2(x))) \circ \pi_2(f(0, \pi_2(x))) \\
&\quad + 2(\pi_2(f(\pi_1(x), 0)) \circ \pi_1(f(0, \pi_2(x))))]/2 \\
&= [\pi_1(x) \circ \pi_2(x) \\
&\quad + \pi_1(f(\pi_1(x), 0)) \circ \pi_2(f(\pi_1(x), 0)) + \pi_1(f(0, \pi_2(x))) \circ \pi_2(f(0, \pi_2(x))) \\
&\quad + \pi_2(f(\pi_1(x), 0)) \circ \pi_1(f(0, \pi_2(x))) + \pi_2(f(\pi_1(x), 0)) \circ \pi_1(f(0, \pi_2(x)))]/2 \\
&= [\pi_1(x) \circ \pi_2(x) \\
&\quad + \pi_1(f(\pi_1(x), 0)) \circ \pi_2(f(\pi_1(x), 0)) + \pi_2(f(\pi_1(x), 0)) \circ \pi_1(f(0, \pi_2(x))) \\
&\quad + \pi_1(f(0, \pi_2(x))) \circ \pi_2(f(0, \pi_2(x))) + \pi_2(f(\pi_1(x), 0)) \circ \pi_1(f(0, \pi_2(x)))]/2
\end{aligned}
$$

$$
\begin{aligned}
&= [\pi_1(x) \circ \pi_2(x) \\
&\quad + \pi_2(f(\pi_1(x), 0)) \circ \ [\pi_1(f(\pi_1(x), 0)) + \pi_1(f(0, \pi_2(x)))] \\
&\quad + \pi_1(f(0, \pi_2(x))) \circ \ [\pi_2(f(0, \pi_2(x))) + \pi_2(f(\pi_1(x), 0))]]/2 \\
&= [\pi_1(x) \circ \pi_2(x) \\
&\quad + \pi_2(f(\pi_1(x), 0)) \circ \pi_1(f(\pi_1(x), \pi_2(x))) \\
&\quad + \pi_1(f(0, \pi_2(x))) \circ \pi_2(f(\pi_1(x), \pi_2(x)))]/2 \\
&= [\pi_1(x) \circ \pi_2(x) \\
&\quad + \pi_2(f(\pi_1(x), 0)) \circ \pi_1(f(x)) \\
&\quad + \pi_1(f(0, \pi_2(x))) \circ \pi_2(f(x))]/2 \\
&= [\pi_1(x) \circ \pi_2(x) + \\
&\quad + \pi_2(f(\pi_1(x), 0)) \circ \pi_1(f(x)) + \Big(\pi_2(f(0, \pi_2(x))) \circ \pi_1(f(x)) - \pi_2(f(0, \pi_2(x))) \circ \pi_1(f(x))\Big) \\
&\quad + \pi_1(f(0, \pi_2(x))) \circ \pi_2(f(x))]/2 \\
&= [\pi_1(x) \circ \pi_2(x) \\
&\quad + \pi_2(f(\pi_1(x), \pi_2(x))) \circ \pi_1(f(x)) \\
&\quad - \pi_2(f(0, \pi_2(x))) \circ \pi_1(f(x)) + \pi_1(f(0, \pi_2(x))) \circ \pi_2(f(x))]/2 \\
&= [\pi_1(x) \circ \pi_2(x) \\
&\quad + \pi_2(f(x)) \circ \pi_1(f(x)) \\
&\quad - \pi_2(f(0, \pi_2(x))) \circ \pi_1(f(x)) + \pi_1(f(0, \pi_2(x))) \circ \pi_2(f(x))]/2 \\
&= [\pi_1(x) \circ \pi_2(x) \\
&\quad + \pi_2(f(x)) \circ \pi_1(f(x)) \\
&\quad + [(\pi_1(f(x)), \pi_2(f(x))) * (\pi_1(f(0, \pi_2(x))), \pi_2(f(0, \pi_2(x))))]]/2 \\
&= [\pi_1(x) \circ \pi_2(x) \\
&\quad + \pi_2(f(x)) \circ \pi_1(f(x)) \\
&\quad + [f(x) * f(0, \pi_2(x))]]/2 \\
&= [\pi_1(x) \circ \pi_2(x)
\end{aligned}
$$

$$
\begin{aligned}
&+ \pi_2(f(x)) \circ \pi_1(f(x)) \\
&+ [x * (0, \pi_2(x))]]/2 \\
&= [\pi_1(x) \circ \pi_2(x) \\
&+ \pi_2(f(x)) \circ \pi_1(f(x)) \\
&[(\pi_1(x), \pi_2(x)) * (0, \pi_2(x))]]/2 \\
&= [\pi_1(x) \circ \pi_2(x) \\
&+ \pi_2(f(x)) \circ \pi_1(f(x)) \\
&[\pi_2(x) \circ 0 - \pi_1(x) \circ \pi_2(x)]]/2 \\
&= [\pi_1(x) \circ \pi_2(x) \\
&+ \pi_1(f(x)) \circ \pi_2(f(x)) \\
&- \pi_1(x) \circ \pi_2(x)]/2 \\
&= \pi_1(f(x)) \circ \pi_2(f(x))/2 \\
&= \pi_1(fg(a,0)) \circ \pi_2(fg(a,0))/2.
\end{aligned}
$$

Thus

$$
\begin{aligned}
\overline{\varphi_f}\,\overline{\varphi_g}(X^a) &= \epsilon_m^{\gamma} X^{\pi_1(f(x))} Z^{\pi_2(f(x))} \\
&= \epsilon_m^{\pi_1(fg(a,0)) \circ \pi_2(fg(a,0))/2} X^{\pi_1(fg(a,0))} Z^{\pi_2(fg(a,0))} \\
&= \overline{\varphi_{fg}}(X^a).
\end{aligned}
$$

By a similar argument, for any $b \in G$, we have $\overline{\varphi_f}\,\overline{\varphi_g}(Z^b) = \overline{\varphi_{fg}}(Z^b)$. We also have that $\overline{\varphi_f}\,\overline{\varphi_g}(\epsilon_m^k I) = \overline{\varphi_f}(\epsilon_m^k I) = \epsilon_m^k I = \overline{\varphi_{fg}}(\epsilon_m^k I)$ for all $k \in \mathbb{Z}_m$. Since $\overline{\varphi_f}$ and $\overline{\varphi_g}$ are endomorphisms of $\mathcal{P}_G$, we have for any $a, b \in G$ and $k \in \mathbb{Z}_m$ that

$$
\begin{aligned}
\overline{\varphi_f}\,\overline{\varphi_g}(\epsilon_m^k X^a Z^b) &= \left[\overline{\varphi_f}\,\overline{\varphi_g}(\epsilon_m^k I)\right] \left[\overline{\varphi_f}\,\overline{\varphi_g}(X^a)\right] \left[\overline{\varphi_f}\,\overline{\varphi_g}(Z^b)\right] \\
&= \left[\overline{\varphi_{fg}}(\epsilon_m^k)\right] \left[\overline{\varphi_{fg}}(X^a)\right] \left[\overline{\varphi_{fg}}(Z^b)\right] \\
&= \overline{\varphi_{fg}}(\epsilon_m^k X^a Z^b).
\end{aligned}
$$

Therefore, we have $\overline{\varphi_f}\,\overline{\varphi_g} = \overline{\varphi_{fg}}$, as claimed.

□

4.7.4 Corollary. *If f is a symplectomorphism of $\overline{G}$, then the endomorphism $\overline{\varphi_f}$ of $\mathcal{P}_G$ that f affords by Theorem 4.7.1 is an automorphism of $\mathcal{P}_G$.*

Proof. Let f be a symplectomorphism of $\overline{G}$. Thus f is an automorphism of $\overline{G}$ and hence a permutation of $\overline{G}$. Therefore, f^{-1} exists, and it is also a symplectomorphism of $\overline{G}$. Therefore, the endomorphism $\overline{\varphi_{f^{-1}}}$ of $\mathcal{P}_G$ that f^{-1} affords by Theorem 4.7.1 exists. By the previous corollary, we have $\overline{\varphi_f}\,\overline{\varphi_{f^{-1}}} = \overline{\varphi_{ff^{-1}}} = \overline{\varphi_{\mathbf{1}_{\overline{G}}}}$, where $\mathbf{1}_{\overline{G}}$ is the identity symplectomorphism on $\overline{G}$. By Theorem 4.7.1, the function $\varphi_{\mathbf{1}_{\overline{G}}} : S \to \mathcal{P}_G$ is defined by

$$\varphi_{\mathbf{1}_{\overline{G}}}(X^g) = \varphi_{\mathbf{1}_{\overline{G}}}(XZ(g,0)) = \epsilon_m^{[\pi_1(g,0)\circ\pi_2(g,0)]/2} XZ(g,0) = \epsilon_m^{(g\circ 0)/2} XZ(g,0) = XZ(g,0) = X^g,$$
$$\varphi_{\mathbf{1}_{\overline{G}}}(Z^h) = \varphi_{\mathbf{1}_{\overline{G}}}(XZ(0,h)) = \epsilon_m^{[\pi_1(0,h)\circ\pi_2(0,h)]/2} XZ(0,h) = \epsilon_m^{(0\circ h)/2} XZ(0,h) = XZ(0,h) = Z^h,$$
$$\varphi_{\mathbf{1}_{\overline{G}}}(\epsilon_m^k I) = \epsilon_m^k I,$$

so it follows that $\overline{\varphi_{\mathbf{1}_{\overline{G}}}}$ is the identity map on $\mathcal{P}_G$. Hence $(\overline{\varphi_f})^{-1}$ exists and is equal to $\overline{\varphi_{f^{-1}}}$. Thus $\overline{\varphi_f}$ is a bijection, which shows $\overline{\varphi_f}$ is an automorphism of $\mathcal{P}_G$. The claim follows.

□

Before we go further, we present a result from elementary linear algebra as a lemma.

4.7.5 Lemma. *Let V be a vector space over a field K and let B be a basis of V. If W is a vector space and $\alpha : B \to W$ is a function, then there exists a unique linear map $\beta : V \to W$ that extends α. The map β is defined by $\beta\left(\sum_{b\in B} k_b b\right) = \sum_{b\in B} k_b \alpha(b)$, for any $k_b \in K$ with $k_b = 0$ for all but finitely many b.*

4.7.6 Lemma. *The set $\{X^g Z^h \mid g, h \in G\}$ is a basis of $\overline{\mathcal{P}_G}$.*

Proof. Claim: $\{X^g Z^h \mid g, h \in G\}$ is linearly independent over $\mathbb{C}$. Let $T \subseteq G$. Suppose $\sum_{g,h \in T} c_{(g,h)} X^g Z^h = \mathbf{0}$ for some $c_{(g,h)} \in \mathbb{C}$, where $\mathbf{0}$ denotes the zero matrix in $\overline{\mathcal{P}_G}$. Let $a \in G$. Then we have

$$\sum_{g,h \in T} c_{(g,h)} \epsilon_m^{h \circ a} |a + g\rangle = \sum_{g,h \in T} c_{(g,h)} \epsilon_m^{h \circ a} X^g |a\rangle = \sum_{g,h \in T} c_{(g,h)} X^g Z^h |a\rangle = \mathbf{0}|a\rangle = \overline{0},$$

where $\overline{0}$ denotes the zero vector belonging to $\mathbb{C}G$. Since $\{|b\rangle \mid b \in G\}$ is a basis for $\mathbb{C}G$, it follows that $c_{(g,h)} \epsilon_m^{h \circ a} = 0$ for all $g, h \in T$, which due to the fact that $\epsilon_m^{h \circ a} \neq 0$ for any $h \in T$, we must have that $c_{(g,h)} = 0$ for all $g, h \in T$. The claim follows.

Claim: $\{X^g Z^h \mid g, h \in G\}$ spans $\overline{\mathcal{P}_G}$. Since $\epsilon_m^k \in \mathbb{C}$ for all $k \in \mathbb{Z}_m$, it follows that for all $k \in \mathbb{Z}_m$, we may take any occurrence of ϵ_m^k in a linear combination of elements from $\mathcal{P}_G$ as simply a scalar belonging to $\mathbb{C}$. Thus every element of $\overline{\mathcal{P}_G}$ can be expressed as a linear combination of elements from $\{X^g Z^h \mid g, h \in G\}$ over $\mathbb{C}$. The claim follows.

Therefore, $\{X^g Z^h \mid g, h \in G\}$ is a basis of $\overline{\mathcal{P}_G}$.

□

4.7.7 Corollary. *Let f be a symplectomorphism of $\overline{G}$, and let $\overline{\varphi_f}$ denote the automorphism of $\mathcal{P}_G$ afforded by f as in the statement of the previous corollary. Then $\overline{\varphi_f}$ can be extended to an inner automorphism of $\overline{\mathcal{P}_G}$.*

Proof. Put $B = \{X^g Z^h \mid g, h \in G\}$, and observe that $B \subset \mathcal{P}_G \subset \overline{\mathcal{P}_G}$. Let $\alpha_f : B \to \overline{\mathcal{P}_G}$ be defined as $\overline{\varphi_f}$ with domain restricted to B and codomain extended to $\overline{\mathcal{P}_G}$. By Lemma 4.7.6, B is a basis of $\overline{\mathcal{P}_G}$, and thus by Lemma 4.7.5, the function $\alpha_f : B \to \overline{\mathcal{P}_G}$ can be extended to a linear map $\beta_f : \overline{\mathcal{P}_G} \to \overline{\mathcal{P}_G}$ defined by $\beta_f \left(\sum_{g,h \in G} c_{(g,h)} X^g Z^h \right) = \sum_{g,h \in G} c_{(g,h)} \alpha_f(X^g Z^h)$, for $c_{(g,h)} \in \mathbb{C}$. Since f^{-1} exists and is also a symplectomorphism of $\overline{G}$, we can define $\alpha_{f^{-1}}$ and $\beta_{f^{-1}}$ similarly. By Theorem 4.7.3, $\overline{\varphi_f}\,\overline{\varphi_{f^{-1}}} = \overline{\varphi_{ff^{-1}}} = \overline{\varphi_{\mathbf{1}_{\overline{G}}}}$, where $\mathbf{1}_{\overline{G}}$ is the identity symplectomorphism on $\overline{G}$. Recall from Note 4.7.2 that $\overline{\varphi_f}(s) = \varphi_f(s)$, $\overline{\varphi_{f^{-1}}}(s) = \varphi_{f^{-1}}(s)$, and $\overline{\varphi_{\mathbf{1}_{\overline{G}}}}(s) = \varphi_{\mathbf{1}_{\overline{G}}}(s)$ for all $s \in S$. We have

$$
\begin{aligned}
\beta_f\left(\sum_{g,h\in G} c_{(g,h)}X^gZ^h\right) &= \sum_{g,h\in G} c_{(g,h)}\alpha_f(X^gZ^h)\\
&= \sum_{g,h\in G} c_{(g,h)}\overline{\varphi_f}(X^gZ^h)\\
&= \sum_{g,h\in G} c_{(g,h)}\overline{\varphi_f}(X^g)\overline{\varphi_f}(Z^h)\\
&= \sum_{g,h\in G} c_{(g,h)}\varphi_f(X^g)\varphi_f(Z^h)\\
&= \sum_{g,h\in G} c_{(g,h)}\left(\epsilon_m^{[\pi_1(f(g,0))\circ\pi_2(f(g,0))]/2}X^{\pi_1(f(g,0))}Z^{\pi_2(f(g,0))}\right)\\
&\quad\left(\epsilon_m^{[\pi_1(f(0,h))\circ\pi_2(f(0,h))]/2}X^{\pi_1(f(0,h))}Z^{\pi_2(f(0,h))}\right),\\
&= \sum_{g,h\in G} c_{(g,h)}\epsilon_m^{[\pi_1(f(g,0))\circ\pi_2(f(g,0))]/2}\epsilon_m^{[\pi_1(f(0,h))\circ\pi_2(f(0,h))]/2}\\
&\quad X^{\pi_1(f(g,0))}Z^{\pi_2(f(g,0))}X^{\pi_1(f(0,h))}Z^{\pi_2(f(0,h))},\\
&\iff \sum_{g,h\in G} c_{(g,h)}\epsilon_m^{[\pi_1(f(g,0))\circ\pi_2(f(g,0))]/2}\epsilon_m^{[\pi_1(f(0,h))\circ\pi_2(f(0,h))]/2}\\
&\quad X^{\pi_1(f(g,0))}\left(\epsilon_m^{\pi_1(f(0,h))\circ\pi_2(f(g,0))}X^{\pi_1(f(0,h))}Z^{\pi_2(f(g,0))}\right)Z^{\pi_2(f(0,h))}\\
&\iff \sum_{g,h\in G} c_{(g,h)}\epsilon_m^{[\pi_1(f(g,0))\circ\pi_2(f(g,0))]/2}\epsilon_m^{[\pi_1(f(0,h))\circ\pi_2(f(0,h))]/2}\epsilon_m^{\pi_1(f(0,h))\circ\pi_2(f(g,0))}\\
&\quad X^{\pi_1(f(g,h))}Z^{\pi_2(f(g,h))}.
\end{aligned}
$$

Thus

$$
\begin{aligned}
\beta_{f^{-1}}\beta_f\left(\sum_{g,h\in G} c_{(g,h)}X^gZ^h\right) &= \beta_{f^{-1}}\left(\sum_{g,h\in G} c_{(g,h)}\epsilon_m^{[\pi_1(f(g,0))\circ\pi_2(f(g,0))]/2}\epsilon_m^{[\pi_1(f(0,h))\circ\pi_2(f(0,h))]/2}\epsilon_m^{\pi_1(f(0,h))\circ\pi_2(f(g,0))}\right.\\
&\qquad \left. X^{\pi_1(f(g,h))}Z^{\pi_2(f(g,h))}\right)\\
&= \sum_{g,h\in G} c_{(g,h)}\epsilon_m^{[\pi_1(f(g,0))\circ\pi_2(f(g,0))]/2}\epsilon_m^{[\pi_1(f(0,h))\circ\pi_2(f(0,h))]/2}\epsilon_m^{\pi_1(f(0,h))\circ\pi_2(f(g,0))}\\
&\qquad \alpha_{f^{-1}}\left(X^{\pi_1(f(g,h))}Z^{\pi_2(f(g,h))}\right)
\end{aligned}
$$

$$
\begin{aligned}
&= \sum_{g,h\in G} c_{(g,h)} \epsilon_m^{[\pi_1(f(g,0))\circ\pi_2(f(g,0))]/2+[\pi_1(f(0,h))\circ\pi_2(f(0,h))]/2+\pi_1(f(0,h))\circ\pi_2(f(g,0))} \\
&\quad \overline{\varphi_{f^{-1}}}\left(X^{\pi_1(f(g,h))} Z^{\pi_2(f(g,h))}\right) \\
&= \sum_{g,h\in G} c_{(g,h)} \varphi_{f^{-1}}\left(\epsilon_m^{[\pi_1(f(g,0))\circ\pi_2(f(g,0))]/2+[\pi_1(f(0,h))\circ\pi_2(f(0,h))]/2+\pi_1(f(0,h))\circ\pi_2(f(g,0))}\right) \\
&\quad \overline{\varphi_{f^{-1}}}\left(X^{\pi_1(f(g,h))} Z^{\pi_2(f(g,h))}\right) \\
&= \sum_{g,h\in G} c_{(g,h)} \overline{\varphi_{f^{-1}}}\left(\epsilon_m^{[\pi_1(f(g,0))\circ\pi_2(f(g,0))]/2+[\pi_1(f(0,h))\circ\pi_2(f(0,h))]/2+\pi_1(f(0,h))\circ\pi_2(f(g,0))}\right) \\
&\quad \overline{\varphi_{f^{-1}}}\left(X^{\pi_1(f(g,h))} Z^{\pi_2(f(g,h))}\right) \\
&= \sum_{g,h\in G} c_{(g,h)} \overline{\varphi_{f^{-1}}}\Big(\epsilon_m^{[\pi_1(f(g,0))\circ\pi_2(f(g,0))]/2+[\pi_1(f(0,h))\circ\pi_2(f(0,h))]/2+\pi_1(f(0,h))\circ\pi_2(f(g,0))} \\
&\quad X^{\pi_1(f(g,h))} Z^{\pi_2(f(g,h))}\Big) \\
&= \sum_{g,h\in G} c_{(g,h)} \overline{\varphi_{f^{-1}}}\left(\overline{\varphi_f}\left(X^g Z^h\right)\right) \\
&= \sum_{g,h\in G} c_{(g,h)} \overline{\varphi_{f^{-1}f}}\left(X^g Z^h\right) \\
&= \sum_{g,h\in G} c_{(g,h)} \overline{\varphi_{\mathbf{1}_{\overline{G}}}}\left(X^g Z^h\right) \\
&= \sum_{g,h\in G} c_{(g,h)} \overline{\varphi_{\mathbf{1}_{\overline{G}}}}\left(X^g\right) \overline{\varphi_{\mathbf{1}_{\overline{G}}}}\left(Z^h\right) \\
&= \sum_{g,h\in G} c_{(g,h)} \varphi_{\mathbf{1}_{\overline{G}}}\left(X^g\right) \varphi_{\mathbf{1}_{\overline{G}}}\left(Z^h\right) \\
&= \sum_{g,h\in G} c_{(g,h)} X^g Z^h.
\end{aligned}
$$

It follows that $\beta_{f^{-1}}\beta_f$ (and similarly, $\beta_f\beta_{f^{-1}}$) is the identity map on $\overline{\mathcal{P}_G}$. Thus $\beta_f^{-1} = \beta_{f^{-1}}$ and β_f is a bijection. Hence β_f is an automorphism of $\overline{\mathcal{P}_G}$. By Theorem 4.5.6, β_f is an inner automorphism of $\overline{\mathcal{P}_G}$. □

4.8 Clifford Group

Recall again that $G = \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_n}$ for some $n, m_i \in \mathbb{Z}^+$ and m is a fixed common multiple of the set $\{2m_i \mid 1 \leq i \leq n\}$.

We define the *Clifford group $\mathcal{C}_G$ of G* to be the unitary normalizer of $\mathcal{P}_G$. Let f be a symplectomorphism of $\overline{G}$. By Corollaries 4.7.4 and 4.7.7, we proved that f affords an automorphism $\overline{\varphi_f}$ of $\mathcal{P}_G$ which can then be extended to an inner automorphism β_f of $\overline{\mathcal{P}_G}$. Thus there is an element $C_f \in \overline{\mathcal{P}_G}$ such that β_f acts as conjugation by C_f on $\overline{\mathcal{P}_G}$. Since $\mathcal{P}_G \subset \overline{\mathcal{P}_G}$, it follows that β_f maps $\mathcal{P}_G$ to itself since, for any $k \in \mathbb{Z}_m$ and $g, h \in G$, we have

$$\beta_f(\epsilon_m^k X^g Z^h) = \epsilon_m^k \alpha_f(X^g Z^h) = \epsilon_m^k \overline{\varphi_f}(X^g Z^h) = \overline{\varphi_f}(\epsilon_m^k)\overline{\varphi_f}(X^g Z^h) = \overline{\varphi_f}(\epsilon_m^k X^g Z^h),$$

and thus it follows that C_f maps $\mathcal{P}_G$ to itself via conjugation. Therefore, it follows that C_f belongs to the normalizer $N_{\mathrm{GL}(\mathbb{C}G)}(\mathcal{P}_G)$ of $\mathcal{P}_G$ in $\mathrm{GL}(\mathbb{C}G)$. We will not prove whether or not C_f is unitary in this paper (and hence an element of $\mathcal{C}_G$). This yields the following open problem:

4.8.1 Open Problem. Let f be a symplectomorphism of $\overline{G}$, let β_f denote the inner automorphism of $\overline{\mathcal{P}_G}$ afforded by f that is granted by Corollaries 4.7.4 and 4.7.7, and let C_f denote the element of $\overline{\mathcal{P}_G}$ with the property that $C_f^{-1} P C_f = \beta_f(P)$ for all elements P in $\mathcal{P}_G$. Is C_f unitary?

D. Gottesman states in "Fault Tolerant Quantum Computation with Higher-Dimensional Systems" [Got99, p. 1753] that the Clifford group of $G = \mathbb{Z}_k$, where $k \in \mathbb{Z}^+$, is generated by the Walsh-Hadamard operator W, the so-called phase operator P, and S_u operator, where u is a unit in $\mathbb{Z}_m$ (P and S_u will be generalized below). We will not prove and thus do not know if the generalized forms of the aforementioned operators generate the Clifford group $\mathcal{C}_G$ of G. This

yields the following open problem:

4.8.2 Open Problem. Do the generalized forms of the Walsh-Hadamard operator W, phase operator P, and S_u operator (u is a unit in $\mathbb{Z}_m$) generate the Clifford group $\mathcal{C}_G$ of G?

We will prove that each of the operators defined below are in fact unitary and thus belong to $\mathcal{C}_G$.

A quick check shows that each of the following maps is a symplectomorphism of $\overline{G}$:

(1) $(a, b) \mapsto (-b, a)$,

(2) $(a, b) \mapsto (a, a + b)$,

(3) $(a, b) \mapsto (ua, u^{-1}b)$, where u is a unit in $\mathbb{Z}_m$.

Treating $(a, 0)$ and $(0, b)$ separately, we observe that

(1) $(a, 0) \mapsto (0, a)$ and $(0, b) \mapsto (-b, 0)$,

(2) $(a, 0) \mapsto (a, a)$ and $(0, b) \mapsto (0, b)$,

(3) $(a, 0) \mapsto (ua, 0)$ and $(0, b) \mapsto (0, u^{-1}b)$, where u is a unit in $\mathbb{Z}_m$.

Recall from Theorem 4.7.1 and Corollary 4.7.4 that if f is a symplectomorphism of $\overline{G}$, then f affords the automorphism $\overline{\varphi_f}$ of $\mathcal{P}_G$, so the elements of Aut($\mathcal{P}_G$) corresponding to the symplectomorphisms above have the following actions, respectively (continuing to treat $(a, 0)$ and $(0, b)$ separately):

(1) $XZ(a, 0) \mapsto \epsilon_m^{[\pi_1(0,a)\circ\pi_2(0,a)]/2} XZ(0, a) = \epsilon_m^{[0\circ a]/2} XZ(0, a) = XZ(0, a)$ and
$XZ(0, b) \mapsto \epsilon_m^{[\pi_1(-b,0)\circ\pi_2(-b,0)]/2} XZ(-b, 0) = \epsilon_m^{[-b\circ 0]/2} XZ(-b, 0) = XZ(-b, 0)$,

(2) $XZ(a,0) \mapsto \epsilon_m^{[\pi_1(a,a)\circ\pi_2(a,a)]/2} XZ(a,a) = \epsilon_m^{[a\circ a]/2} XZ(a,a)$ and
$XZ(0,b) \mapsto \epsilon_m^{[\pi_1(0,b)\circ\pi_2(0,b)]/2} XZ(0,b) = \epsilon_m^{[0\circ b]/2} XZ(0,b) = XZ(0,b)$,

(3) $XZ(a,0) \mapsto \epsilon_m^{[\pi_1(ua,0)\circ\pi_2(ua,0)]/2} XZ(ua,0) = \epsilon_m^{[ua\circ 0]/2} XZ(ua,0) = XZ(ua,0)$ and
$XZ(0,b) \mapsto \epsilon_m^{[\pi_1(0,u^{-1}b)\circ\pi_2(0,u^{-1}b)]/2} XZ(0,u^{-1}b) = \epsilon_m^{[0\circ u^{-1}b]/2} XZ(0,u^{-1}b) = XZ(0,u^{-1}b)$,
where u is a unit in $\mathbb{Z}_m$.

Simplifying the notation, we obtain

(1) $X^a \mapsto Z^a$ and $Z^b \mapsto X^{-b}$,

(2) $X^a \mapsto \epsilon_m^{(a\circ a)/2} X^a Z^a$ and $Z^b \mapsto Z^b$,

(3) $X^a \mapsto X^{ua}$ and $Z^b \mapsto Z^{u^{-1}b}$, where u is a unit in $\mathbb{Z}_m$.

We point out that the operator described in (1) is the Walsh-Hadamard operator W defined in Definition 4.1.2. The operator described in (2) generalizes the phase operator P, and the one in (3) generalizes the S_u operator, where u is a unit in $\mathbb{Z}_m$ [Got99, p. 1753].

We have that the Walsh-Hadamard operator defined by $W = |G|^{-1/2} \sum_{b\in G} \sum_{a\in G} \epsilon_m^{a\circ b} |a\rangle\langle b|$ is unitary [HT03, p. 320], and thus $W \in \mathcal{C}_G$. Let u be a unit in $\mathbb{Z}_m$. Define the operators A and B_u on $\mathbb{C}G$ by

$$A = \sum_{g\in G} \epsilon^{g\circ g/2} |g\rangle\langle g|$$

and

$$B_u = \sum_{g\in G} |ug\rangle\langle g|.$$

It follows that $A^* = \sum_{g\in G} \epsilon^{-g\circ g/2} |g\rangle\langle g|$ and $B_u^* = \sum_{g\in G} |g\rangle\langle ug| = \sum_{h\in G} |u^{-1}h\rangle\langle h|$. A quick check shows that $AA^* = A^*A = I$ and $B_uB_u^* = B_u^*B_u = I$, and thus A and B_u are unitary.

4.8.3 Theorem. *We have* $AX^aA^* = \epsilon_m^{(a\circ a)/2}X^aZ^a$ *and* $AZ^bA^* = Z^b$ *for all* $a, b \in G$.

Proof. Let $g \in G$. By direct computation, we have

$$\begin{aligned}
AX^aA^*|g\rangle &= AX^a(\epsilon_m^{-g\circ g/2}|g\rangle) \\
&= \epsilon_m^{-g\circ g/2}A|a+g\rangle \\
&= \epsilon_m^{-g\circ g/2}(\epsilon_m^{(a+g)\circ(a+g)/2}|a+g\rangle) \\
&= \epsilon_m^{-g\circ g/2}(\epsilon_m^{(a\circ a+2a\circ g+g\circ g)/2}|a+g\rangle) \\
&= \epsilon_m^{a\circ a/2}\epsilon_m^{a\circ g}|a+g\rangle \\
&= \epsilon_m^{a\circ a/2}\epsilon_m^{a\circ g}X^a|g\rangle \\
&= \epsilon_m^{a\circ a/2}X^a(\epsilon_m^{a\circ g}|g\rangle) \\
&= \epsilon_m^{a\circ a/2}X^aZ^a|g\rangle,
\end{aligned}$$

for all $a \in G$. Thus $AX^aA^* = \epsilon_m^{(a\circ a)/2}X^aZ^a$ for all $a \in G$. Also,

$$\begin{aligned}
AZ^bA^*|g\rangle &= AZ^b(\epsilon_m^{-g\circ g/2}|g\rangle) \\
&= \epsilon_m^{-g\circ g/2}AZ^b|g\rangle \\
&= \epsilon_m^{-g\circ g/2}A(\epsilon_m^{b\circ g}|g\rangle) \\
&= \epsilon_m^{-g\circ g/2}\epsilon_m^{b\circ g}A|g\rangle \\
&= \epsilon_m^{-g\circ g/2}\epsilon_m^{b\circ g}(\epsilon_m^{g\circ g/2}|g\rangle) \\
&= \epsilon_m^{b\circ g}|g\rangle \\
&= Z^b|g\rangle,
\end{aligned}$$

for all $b \in G$. Thus $AZ^bA^* = Z^b$ for all $b \in G$.

□

4.8.4 Theorem. *We have* $B_uX^aB_u^* = X^{ua}$ *and* $B_uZ^bB_u^* = Z^{u^{-1}b}$.

Proof. Let $g \in G$. By direct computation, we have

$$\begin{aligned} B_u X^a B_u^* |g\rangle &= B_u X^a |u^{-1} g\rangle \\ &= B_u |a + u^{-1} g\rangle \\ &= |ua + g\rangle \\ &= X^{ua} |g\rangle, \end{aligned}$$

for all $a \in G$. Thus $B_u X^a B_u^* = X^{ua}$ for all $a \in G$. Also,

$$\begin{aligned} B_u Z^b B_u^* |g\rangle &= B_u Z^b |u^{-1} g\rangle \\ &= B_u (\epsilon_m^{b \circ (u^{-1} g)} |u^{-1} g\rangle) \\ &= B_u (\epsilon_m^{(u^{-1} b) \circ g} |u^{-1} g\rangle) \\ &= \epsilon_m^{(u^{-1} b) \circ g} B_u |u^{-1} g\rangle \\ &= \epsilon_m^{(u^{-1} b) \circ g} |g\rangle \\ &= Z^{u^{-1} b} |g\rangle, \end{aligned}$$

for all $b \in G$. Thus $B_u Z^b B_u^* = Z^{u^{-1} b}$ for all $b \in G$.

□

4.8.5 Note. It follows that A and B_u are the generalized phase operator P and S_u operator, respectively. In other words, $A = P$ and $B_u = S_u$. Therefore, we conclude that P and S_u are unitary, so $P, S_u \in \mathcal{C}_G$.

Assume $G = \mathbb{Z}_k$ ($k \in \mathbb{Z}^+$). The SUM operator, which acts on a pair of k-dimensional qudits called a *2-qudit*, is defined by $\mathrm{SUM}(|i\rangle|j\rangle) = |i\rangle|j + i\rangle$ for $i, j \in G$. We have that SUM is the generalization of the CNOT operator in greater than two dimensions [Got99, p. 1753]. We can also see how SUM acts on the generators of the 2-qudit Pauli group [Far14, p. 8], as follows:

$$X \otimes I \mapsto X \otimes X$$

$$I \otimes X \mapsto I \otimes X$$

$$Z \otimes I \mapsto Z \otimes I$$

$$I \otimes Z \mapsto Z^{-1} \otimes Z.$$

For the remainder of the section, assume $G = \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_n}$ for some $n, m_i \in \mathbb{Z}^+$.

4.8.6 Definition. We define the *generalized* SUM operator on $\mathbb{C}G \otimes \mathbb{C}G$ by $\mathrm{SUM}(|x\rangle|y\rangle) = |x\rangle|y + x\rangle$.

4.8.7 Note. Observe that $\mathrm{SUM}^{-1}(|x\rangle|y\rangle) = |x\rangle|y - x\rangle$.

4.8.8 Theorem. *Let $a, b, c, d \in G$. Then $X^a Z^b \otimes X^c Z^d$ is mapped to $X^a Z^{b-d} \otimes X^{c+a} Z^d$ via conjugation by the* SUM *operator.*

Proof. Let $x, y \in G$. Then

$$\begin{aligned}
\mathrm{SUM}(X^a Z^b \otimes X^c Z^d)\,\mathrm{SUM}^{-1}(|x\rangle|y\rangle) &= \mathrm{SUM}(X^a Z^b \otimes X^c Z^d)(|x\rangle|y - x\rangle) \\
&= \mathrm{SUM}(X^a Z^b |x\rangle \otimes X^c Z^d |y - x\rangle) \\
&= \mathrm{SUM}(\epsilon_m^{b \circ x} |a + x\rangle \otimes \epsilon_m^{d \circ (y-x)} |c + y - x\rangle) \\
&= \epsilon_m^{b \circ x} \epsilon_m^{d \circ (y-x)}\,\mathrm{SUM}(|a + x\rangle \otimes |c + y - x\rangle) \\
&= \epsilon_m^{b \circ x} \epsilon_m^{d \circ y - d \circ x}(|a + x\rangle \otimes |(a + x) + c + y - x\rangle) \\
&= \epsilon_m^{b \circ x} \epsilon_m^{d \circ y} \epsilon_m^{-d \circ x}(|a + x\rangle \otimes |a + c + y\rangle) \\
&= \epsilon_m^{b \circ x - d \circ x} \epsilon_m^{d \circ y}(X^a \otimes X^{a+c})(|x\rangle \otimes |y\rangle) \\
&= (X^a \otimes X^{a+c})(\epsilon_m^{(b-d) \circ x} |x\rangle \otimes \epsilon_m^{d \circ y} |y\rangle) \\
&= (X^a \otimes X^{a+c})(Z^{b-d} \otimes Z^d)(|x\rangle \otimes |y\rangle) \\
&= (X^a Z^{b-d} \otimes X^{c+a} Z^d)(|x\rangle|y\rangle).
\end{aligned}$$

The claim follows.

□

Chapter 5

Further Results

5.1 Pseudo-unitarity and a Generalization of the Walsh-Hadamard Operator

5.1.1 Theorem. *[Ser02, p. 145] Let A be a complex $j \times k$ matrix $(j, k \in \mathbb{Z}^+)$. There exists a unique complex $k \times j$ matrix A^+ that satisfies the following properties:*

(i) $AA^+A = A$

(ii) $A^+AA^+ = A^+$

(iii) $(AA^+)^* = AA^+$

(iv) $(A^+A)^* = A^+A$.

5.1.2 Definition. Let A be a complex $j \times k$ matrix $(j, k \in \mathbb{Z}^+)$. We define the *Moore-Penrose pseudo-inverse* of A to be the unique matrix A^+ of the previous theorem.

Let U be a complex matrix.

5.1.3 Definition. We say that U is *pseudo-unitary* by a factor of $z \in \mathbb{C}$ if

$$U^+ = zU^*.$$

5.1.4 Note. Observe that if U is pseudo-unitary by a factor of 1 and is invertible, then it is unitary.

5.1.5 Definition. Assume U is a square complex matrix. We say that U is *pseudo-idempotent* by a factor of $z \in \mathbb{C}$ if

$$U^2 = zU.$$

5.1.6 Definition. A *unitary representation* of a group H is a group homomorphism $\rho : H \to U(n)$, where $U(n)$ is the group of $n \times n$ unitary matrices under matrix multiplication.

5.1.7 Definition. For a finite abelian group H and a unitary representation ρ of H, define $U_{H,\rho} = |H|^{-1/2} \sum_{h \in H} \rho(h)$.

5.1.8 Definition. The matrix U is *Hermitian* if $U = U^*$.

Fix a finite abelian group H and a unitary representation ρ of H, and put $U = U_{H,\rho}$.

5.1.9 Lemma. *U is Hermitian.*

Proof. By direct computation, we see that

$$\begin{aligned} U^* &= \left(|H|^{-1/2} \sum_{h \in H} \rho(h) \right)^* \\ &= \overline{|H|^{-1/2}} \sum_{h \in H} \rho(h)^* \\ &= |H|^{-1/2} \sum_{h \in H} \rho(h)^{-1} \end{aligned}$$

$$
\begin{aligned}
&= |H|^{-1/2} \sum_{h \in H} \rho(h^{-1}) \\
&= U.
\end{aligned}
$$

□

5.1.10 Lemma. *U is pseudo-idempotent by a factor of $|H|^{1/2}$.*

Proof. By direct computation, we see that

$$
\begin{aligned}
U^2 &= UU \\
&= \left(|H|^{-1/2} \sum_{h \in H} \rho(h) \right) \left(|H|^{-1/2} \sum_{k \in H} \rho(k) \right) \\
&= |H|^{-1} \sum_{k \in H} \left(\sum_{h \in H} \rho(h) \right) \rho(k) \\
&= |H|^{-1} \sum_{k \in H} \sum_{h \in H} \rho(h)\rho(k) \\
&= |H|^{-1} \sum_{k \in H} \sum_{h \in H} \rho(h+k) \\
&= |H|^{-1/2} \sum_{k \in H} \left(|H|^{-1/2} \sum_{h \in H} \rho(h+k) \right) \\
&= |H|^{-1/2} \sum_{k \in H} U \\
&= |H|^{-1/2} |H| U \\
&= |H|^{1/2} U.
\end{aligned}
$$

□

5.1.11 Theorem. *U is pseudo-unitary by a factor of $|H|^{-1}$.*

Proof. The claim is that $U^+ = |H|^{-1} U^*$. It is enough to show that the four properties of Theorem 5.1.1 are satisfied with U^+ replaced by $|H|^{-1} U^*$.

(i) $U\left(|H|^{-1}U^*\right)U = U\left(|H|^{-1}U\right)U = |H|^{-1}U(UU) = |H|^{-1}U(|H|^{1/2}U) = |H|^{-1/2}(UU) = |H|^{-1/2}(|H|^{1/2}U) = U$.

(ii) Similar to (1).

(iii) $\left(U\left(|H|^{-1}U^*\right)\right)^* = \left(|H|^{-1}U^*\right)^* U^* = \overline{|H|^{-1}}UU^* = |H|^{-1}UU^* = U(|H|^{-1}U^*)$.

(iv) Similar to (3).

This proves the claim.

□

5.1.12 Definition. Let f be an endomorphism of G. Denote by W_f the linear operator on $\mathbb{C}G$ defined by $W_f|g\rangle = |G|^{-1/2}\sum_{h\in G}\epsilon_m^{f(g)\circ h}|h\rangle$. We call W_f the *Walsh-Hadamard operator afforded by* f.

Written explicitly,

$$W_f = |G|^{-1/2}\sum_{b\in G}\sum_{a\in G}\epsilon_m^{f(b)\circ a}|a\rangle\langle b|.$$

5.1.13 Note. Observe that

$$\begin{aligned} W_f^* &= \left(|G|^{-1/2}\sum_{b\in G}\sum_{a\in G}\epsilon_m^{f(b)\circ a}|a\rangle\langle b|\right)^* \\ &= |G|^{-1/2}\sum_{b\in G}\sum_{a\in G}\left(\epsilon_m^{f(b)\circ a}|a\rangle\langle b|\right)^* \\ &= |G|^{-1/2}\sum_{a\in G}\sum_{b\in G}\epsilon_m^{-f(b)\circ a}|b\rangle\langle a|. \end{aligned}$$

5.1.14 Note. If f is the identity map on G, then W_f is the generalized Walsh-Hadamard operator as presented in [Holmes-Texier] as well as Definition 4.1.2. In this case, W_f is unitary.

It turns out that W_f is not always unitary, as the next example shows.

5.1.15 Example.

Assume that $G = \mathbb{Z}_4$, put $m = 8$, and let $f : \mathbb{Z}_4 \to \mathbb{Z}_4$ be the $\mathbb{Z}_8$-homomorphism given by $f(g) = 2g$. By definition of W_f, we have, for $g \in \mathbb{Z}_4$

$$\begin{aligned} W_f|g\rangle &= |\mathbb{Z}_4|^{-1/2} \sum_{h\in\mathbb{Z}_4} \epsilon_8^{f(g)\circ h}|h\rangle \\ &= \frac{1}{2}\sum_{h\in\mathbb{Z}_4} \epsilon_8^{2g\circ h}|h\rangle \\ &= \frac{1}{2}\sum_{h\in\mathbb{Z}_4} \epsilon_8^{2gh}|h\rangle \\ &= \frac{1}{2}\left(\epsilon_8^{2g\cdot 0}|0\rangle + \epsilon_8^{2g\cdot 1}|1\rangle + \epsilon_8^{2g\cdot 2}|2\rangle + \epsilon_8^{2g\cdot 3}|3\rangle\right) \\ &= \frac{1}{2}\left(|0\rangle + \epsilon_8^{2g}|1\rangle + |2\rangle + \epsilon_8^{2g}|3\rangle\right). \end{aligned}$$

For $g = 0, 2$, the formula above yields

$$W_f|0\rangle = \frac{1}{2}\left(|0\rangle + |1\rangle + |2\rangle + |3\rangle\right) = W_f|2\rangle.$$

Thus W_f is not injective, so W_f is not invertible. Therefore, W_f is not unitary.

5.1.16 Theorem. *Let f be an endomorphism of G. The Walsh-Hadamard transform W_f afforded by f is pseudo-unitary by a factor of $|\ker f|^{-1}$.*

Proof. The claim is that $W_f^+ = |\ker f|^{-1} W_f^*$. It is enough to show that the four properties of Theorem 5.1.1 are satisfied with U^+ replaced by $|\ker f|^{-1} W_f^*$. Let $g \in G$.

(i)

$$
\begin{aligned}
W_f\left(|\ker f|^{-1}W_f^*\right)W_f|g\rangle &= |\ker f|^{-1}W_fW_f^*\left(|G|^{-1/2}\sum_{h\in G}\epsilon_m^{f(g)\circ h}|h\rangle\right)\\
&= |G|^{-1/2}|\ker f|^{-1}W_f\left(\sum_{h\in G}\epsilon_m^{f(g)\circ h}W_f^*|h\rangle\right)\\
&= |G|^{-1/2}|\ker f|^{-1}W_f\left(\sum_{h\in G}\epsilon_m^{f(g)\circ h}|G|^{-1/2}\sum_{a\in G}\epsilon_m^{-f(a)\circ h}|a\rangle\right)\\
&= |G|^{-1}|\ker f|^{-1}\left(\sum_{h\in G}\epsilon_m^{f(g)\circ h}\sum_{a\in G}\epsilon_m^{-f(a)\circ h}W_f|a\rangle\right)\\
&= |G|^{-1}|\ker f|^{-1}\left(\sum_{h\in G}\epsilon_m^{f(g)\circ h}\sum_{a\in G}\epsilon_m^{-f(a)\circ h}|G|^{-1/2}\sum_{b\in G}\epsilon_m^{f(a)\circ b}|b\rangle\right)\\
&= |G|^{-3/2}|\ker f|^{-1}\left(\sum_{h\in G}\sum_{a\in G}\sum_{b\in G}\epsilon_m^{f(g)\circ h}\epsilon_m^{-f(a)\circ h}\epsilon_m^{f(a)\circ b}|b\rangle\right)\\
&= |G|^{-3/2}|\ker f|^{-1}\sum_{b\in G}\sum_{a\in G}\left(\sum_{h\in G}\epsilon_m^{f(g)\circ h}\epsilon_m^{-f(a)\circ h}\right)\epsilon_m^{f(a)\circ b}|b\rangle\\
&= |G|^{-3/2}|\ker f|^{-1}\sum_{b\in G}\sum_{a\in G}\left(\sum_{h\in G}\epsilon_m^{f(g-a)\circ h}\right)\epsilon_m^{f(a)\circ b}|b\rangle\\
&= |G|^{-3/2}|\ker f|^{-1}\sum_{b\in G}\sum_{a\in G}\left(\sum_{h\in G}\epsilon_m^{\iota_{f(g-a)}(h)}\right)\epsilon_m^{f(a)\circ b}|b\rangle
\end{aligned}
$$

Since $\iota_{f(g-a)} : G \to \mathbb{Z}_m$ is a homomorphism for each $a \in G$, $\iota_{f(g-a)}$ is either constant or balanced on G for each $a \in G$ by Theorem 2.2.6 . Let $a \in G$. Observe that $\iota_{f(g-a)}$ is constant on G if and only if $f(g-a)\circ h = \iota_{f(g-a)}(h) = 0$ for all $h \in G$, that is, if and only if $f(g-a) \in G^\perp = \{0\}$, which is true if and only if $g - a \in \ker f$, or $a \in g + \ker f$. Otherwise, if $\iota_{f(g-a)}$ is balanced on G, then by Theorem 2.2.7, $\sum_{h\in G}\epsilon_m^{\iota_{f(g-a)}(h)} = 0$. Therefore, the equation above becomes

$$
\begin{aligned}
W_f\left(|\ker f|^{-1}W_f^*\right)W_f|g\rangle &= |G|^{-3/2}|\ker f|^{-1}\sum_{b\in G}\sum_{a\in g+\ker f}\left(\sum_{h\in G}\epsilon_m^{\iota_{f(g-a)}(h)}\right)\epsilon_m^{f(a)\circ b}|b\rangle\\
&= |G|^{-3/2}|\ker f|^{-1}\sum_{b\in G}\sum_{a\in g+\ker f}\left(\sum_{h\in G}\epsilon_m^{\iota_0(h)}\right)\epsilon_m^{f(a)\circ b}|b\rangle\\
&= |G|^{-3/2}|\ker f|^{-1}\sum_{b\in G}\sum_{a\in g+\ker f}(|G|)\,\epsilon_m^{f(a)\circ b}|b\rangle
\end{aligned}
$$

$$
\begin{aligned}
&= |G|^{-1/2} |\ker f|^{-1} \sum_{b\in G} \sum_{a\in g+\ker f} \epsilon_m^{f(a)\circ b} |b\rangle \\
&= |G|^{-1/2} |\ker f|^{-1} \sum_{b\in G} \sum_{a\in g+\ker f} \epsilon_m^{f(g)\circ b} |b\rangle \\
&= |G|^{-1/2} |\ker f|^{-1} \sum_{b\in G} \epsilon_m^{f(g)\circ b} |b\rangle \left(\sum_{a\in g+\ker f} 1 \right) \\
&= |G|^{-1/2} |\ker f|^{-1} \sum_{b\in G} \epsilon_m^{f(g)\circ b} |b\rangle \left(|\ker f| \right) \\
&= |G|^{-1/2} \sum_{b\in G} \epsilon_m^{f(g)\circ b} |b\rangle \\
&= W_f |g\rangle.
\end{aligned}
$$

Therefore, $W_f \left(|\ker f|^{-1} W_f^* \right) W_f = W_f$.

(ii) The proof showing $\left(|\ker f|^{-1} W_f^* \right) W_f \left(|\ker f|^{-1} W_f^* \right) = |\ker f|^{-1} W_f^*$ is similar to (i).

(iii) We have

$$
\left(W_f \big(|\ker f|^{-1} W_f^* \big) \right)^* = \big(|\ker f|^{-1} W_f^* \big)^* W_f^* = |\ker f|^{-1} W_f W_f^* = W_f \big(|\ker f|^{-1} W_f^* \big).
$$

(iv) The proof showing $\left(\big(|\ker f|^{-1} W_f^* \big) W_f \right)^* = \big(|\ker f|^{-1} W_f^* \big) W_f$ is similar to (iii).

Therefore, $W_f^+ = |\ker f|^{-1} W_f^*$, so W_f is pseudo-unitary by a factor of $|\ker f|^{-1}$.

□

5.1.17 Definition. An endomorphism f of G is *self-adjoint* (*relative to* $\circ$) if $f(a) \circ b = a \circ f(b)$ for all $a, b \in G$.

For example, for $k \in \mathbb{Z}_m$ the endomorphism f of G given by $f(g) = kg$ is self-adjoint, since, for every $a, b \in G$ we have $f(a) \circ b = (ka) \circ b = k(a \circ b) = a \circ (kb) = a \circ f(b)$.

5.1.18 Theorem. *Let f and g be endomorphisms of G and assume that f is self-adjoint relative to $\circ$. Then for every $x \in G$,*

$$W_f W_g|x\rangle = \sum_{b \in -f^{-1}(g(x))} |b\rangle.$$

Proof. Let $x \in G$. Then

$$\begin{aligned}
W_f W_g|x\rangle &= W_f \left(|G|^{-1/2} \sum_{a \in G} \epsilon_m^{g(x)\circ a}|a\rangle \right) \\
&= |G|^{-1/2} \sum_{a \in G} \epsilon_m^{g(x)\circ a} W_f|a\rangle \\
&= |G|^{-1} \sum_{a \in G} \epsilon_m^{g(x)\circ a} \sum_{b \in G} \epsilon_m^{f(a)\circ b}|b\rangle \\
&= |G|^{-1} \sum_{a \in G} \sum_{b \in G} \epsilon_m^{g(x)\circ a + f(a)\circ b}|b\rangle \\
&= |G|^{-1} \sum_{a \in G} \sum_{b \in G} \epsilon_m^{g(x)\circ a + f(b)\circ a}|b\rangle \\
&= |G|^{-1} \sum_{b \in G} \sum_{a \in G} \epsilon_m^{f(b)\circ a - (-g(x)\circ a)}|b\rangle \\
&= |G|^{-1} \sum_{b \in G} \sum_{a \in G} \epsilon_m^{\iota_{f(b)}(a) - \iota_{-g(x)}(a)}|b\rangle \\
&= |G|^{-1} \sum_{b \in G} \sum_{a \in G} \epsilon_m^{(\iota_{f(b)} - \iota_{-g(x)})(a)}|b\rangle \\
&= |G|^{-1} \sum_{b \in G} \varphi(\iota_{f(b)} - \iota_{-g(x)})|b\rangle,
\end{aligned}$$

where we recall the definition of φ was given by Definition 2.2.3. Observe that $\iota_{-g(x)}$ is $\{-g(x)\}$-based by Theorem 2.2.5. By Definition 2.2.4, $\varphi(\iota_{f(b)} - \iota_{-g(x)}) = 0$ for all $b \in G$ such that $f(b) \in G \backslash \{-g(x)\}$. Equivalently, $\varphi(\iota_{f(b)} - \iota_{-g(x)}) = 0$ for all $b \in G$ such that $b \notin -f^{-1}(g(x))$. Observe that $\iota_{f(b)} - \iota_{-g(x)} = 0$ when $b \in -f^{-1}(g(x))$. Therefore,

$$\begin{aligned}
W_f W_g|x\rangle &= |G|^{-1} \sum_{b \in -f^{-1}(g(x))} \varphi(\iota_{f(b)} - \iota_{-g(x)})|b\rangle \\
&= |G|^{-1} \sum_{b \in -f^{-1}(g(x))} \varphi(0)|b\rangle
\end{aligned}$$

$$
\begin{aligned}
&= |G|^{-1} \sum_{b \in -f^{-1}(g(x))} \left(\sum_{a \in G} \epsilon_m^{0(a)} \right) |b\rangle \\
&= |G|^{-1} \sum_{b \in -f^{-1}(g(x))} \left(\sum_{a \in G} 1 \right) |b\rangle \\
&= |G|^{-1} |G| \sum_{b \in -f^{-1}(g(x))} |b\rangle \\
&= \sum_{b \in -f^{-1}(g(x))} |b\rangle,
\end{aligned}
$$

as claimed.

□

5.1.19 Corollary. *W_f^2 acts as the negation involution on the group G for any self-adjoint automorphism f of G, in other words $W_f^2|g\rangle = |-g\rangle$ for all $g \in G$.*

5.1.20 Corollary. *Let f be a self-adjoint automorphism of G. If $|G| = 2$, then W_f has order 2, and if $|G| > 2$, then W_f has order 4.*

Proof. The proof follows from Corollary 5.1.19. □

Bibliography

[Cho20] Adrian Cho. Ibm promises 1000-qubit quantum computer—a milestone—by 2023, September 2020. [Science Magazine; Online; posted 15-September-2020].

[Far14] J. M. Farinholt. An ideal characterization of the Clifford operators. *J. Phys. A*, 47(30):305303, 16, 2014.

[Got99] Daniel Gottesman. Fault-tolerant quantum computation with higher-dimensional systems. *Chaos Solitons Fractals*, 10(10):1749–1758, 1999.

[GS17] Philippe Gille and Tamás Szamuely. *Central simple algebras and Galois cohomology*, volume 165 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2017. Second edition of [MR2266528].

[HT03] Randall R. Holmes and Frédéric Texier. A generalization of the Deutsch-Jozsa quantum algorithm. *Far East J. Math. Sci. (FJMS)*, 9(3):319–326, 2003.

[Hun80] Thomas W. Hungerford. *Algebra*, volume 73 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1980. Reprint of the 1974 original.

[RP11] Eleanor Rieffel and Wolfgang Polak. *Quantum computing*. Scientific and Engineering Computation. MIT Press, Cambridge, MA, 2011. A gentle introduction.

[Ser02] Denis Serre. *Matrices*, volume 216 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2002. Theory and applications, Translated from the 2001 French original.

[Wei94] Charles A. Weibel. *An introduction to homological algebra*, volume 38 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1994.