Czech Technical University in Prague
Faculty of Nuclear Sciences and Physical Engineering
Department of Physics

Programme: Mathematical Physics

Clifford Groups in Quantum Computing

MASTER'S THESIS

Author: Vojtěch Teska
Supervisor: prof. Ing. Jiří Tolar, DrSc
Submitted in: May 2018

Prohlášení

Prohlašuji, že jsem svou diplomovou práci vypracoval samostatně a použil jsem pouze podklady uvedené v přiloženém seznamu.

Nemám závažný důvod proti použití tohoto školního díla ve smyslu § 60 zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon).

V Praze dne:

Podpis:

Název práce:
Cliffordovy grupy v kvantovém počítání

Autor: Vojtěch Teska

Obor: Matematická Fyzika

Druh práce: Dipolomová práce

Vedoucí práce: prof. Ing. Jiří Tolar, DrSc
Katedra fyziky FJFI ČVUT v Praze
Konzultanti: Ing. Petr Novotný, PhD
Katedra fyziky FJFI ČVUT v Praze
Mgr. Miroslav Korbelář, PhD
Katedra matematiky FEL ČVUT v Praze

Abstrakt: Nejprve jsou definovány gradace *-algebry $M_N(\mathbb{C})$. Je dána klasifikace jim příslušných MAD-grup a vysvětlen jejich vztah k Pauliho grupě. Dále jsou definovány Weylova-Heisenbergova grupa a Cliffordova grupa. Je zaveden aparát krátkých exaktních posloupností a možnost popisu omezené Cliffordovy grupy jako polopřímého součinu pomocí jejího zdvihu je prozkoumána. Jsou zavedeny Cliffordovy grupy pro složené kvantové systémy. Je zkoumán alternativní popis těchto grup pomocí zobecnění konečné symplektické grupy. Je vysvětlen význam Cliffordových grup pro kvantové počítání. Dále je vysvětlen jejich vztah k dosud nevyřešeném problému existence symetrických informačně kompletních měření (SIC-POVMs) v libovolné dimenzi. Evoluční grupa konečného harmonického oscilátoru je definována a popsána v nízkých dimenzích.
Klíčová slova: Weylova-Heisenbergova grupa, Cliffordova grupa, Gottesmanova-Knillova věta, SIC-POVMs, konečný kvantový oscilátor

Title:
Clifford Groups in Quantum Computing

Author: Vojtěch Teska

Abstract: First, the gradings of the *-algebra $M_N(\mathbb{C})$ are defined. The classification of their corresponding MAD-groups is given and their relation to the Pauli group is explained. Next, the Weyl-Heisenberg group and the Clifford group are defined. The apparartus of short exact sequences is introduced and the possibility of description of the Restricted Clifford group as a semidirect product using its lift is examined. Clifford groups of composite quantum systems are defined. Alternative description of these groups using a generalization of the finite symplectic group is examined. The significance of Clifford groups in quantum computing is explained. Furthermore, their relation to the unsolved prolem of existence of symmetric informationally complete measurements (SIC-POVMs) in arbitrary dimension is explained. The evolution group of a finite quantum oscillator is defined and it is descibed in small dimensions.
Key words: Weyl-Heisenberg group, Clifford group, Gottesman-Knill theorem, SIC-POVMs, finite quantum oscillator

Contents

Acknowledgements

I would like to thank prof. Miloslav Havlíček, prof. Jiří Tolar, Miroslav Korbelář and Petr Novotný for help with writing my thesis. I also thank my parents for support during my studies.

Introduction

The aim of this thesis is to give an overview of the properties of the Weyl-Heisenberg, Pauli and Clifford groups and examine their use in mathematics as well as some applications in the field of quantum computing. In the first chapter, we describe the use of the Pauli group to define a fine grading of the algebra $M_N(\mathbb{C})$, its relationship with the MAD-groups and the finite group $SL(2, \mathbb{Z}_N)$.

In the second chapter, we proceed to the definition of the Weyl-Heisenberg group and the Clifford group as its normalizer in the group of unitary matrices. Before proceeding, we give a summary of necessary preliminaries from group theory including the first two isomorphism theorems, properties of exact sequences and semidirect products. In the final part of the second chapter, we examine the short exact sequences for the restricted Clifford group.

In the third chapter the lifts of the Clifford group to the group $U(N)$ of $N \times N$ unitary matrices are examined. The lift is a finite subgroup of $U(N)$, which finds applications in quantum computing. It turns out that there are multiple ways to define the lifts even if one of the generating matrices is fixed. We examine basic properties of the lifts such its centre and the order of their generators. In the final part of the third chapter we ask whether a lift can be chosen in such way that it would define a splitting homomorphism in the short exact sequence for the Restricted Clifford group in the case of odd N.

In the fourth chapter, we define and describe the Clifford groups of composite systems using the new group $\mathrm{Sp}_{[n_1,\dots,n_k]}$. In the first part of this chapter, we go through the necessary steps that need to be done in preparation for the definition and for the finding of generators of $\mathrm{Sp}_{[n_1,\dots,n_k]}$. In the second part, we prove that a quotient of the Clifford group of a composite system is isomorphic to $\mathrm{Sp}_{[n_1,\dots,n_k]}$.

The final chapter is divided into three parts, each giving a brief overview of some application of Clifford groups in mathematical physics. The first section describes the fundamental notions of quantum computing and the significance of Clifford groups in connection with the Gottesman-Knill theorem. In the next section, we examine symmetric informationally complete positive operator valued measures (SIC-POVMs). Some basic properties are proven and we explain why Clifford groups are used in their construction. The final section of this thesis is dedicated to the study of the finite quantum oscillator where the Clifford group serves as an analogue of canonical transformations.

Notation

$\widehat{n}$	the set $\{1, 2, 3, ..., n\}$
$\bullet^*$	involution
$\bullet^H$	hermitian adjoining
$M_N(\mathbb{C})$	the *-algebra of $N \times N$ complex matrices
$\sigma(A)$	spectrum of a linear operator A
I	identity operator
Π_N	Pauli group of an N-level quantum system
Ad_A	inner automorphism of $M_n(\mathbb{C})$ generated by an invertible matrix A
$U(N)$	the group of $N \times N$ unitary matrices
$U_D(n)$	the group of diagonal unitary $n \times n$ matrices
$H(N)$	the Weyl-Heisenberg group in dimension N
$C(N)$	the restricted Clifford group in dimension N
$H \leq G$	H is a subgroup of G
$N \lhd G$	N is a normal subgroup of G
1_G	the unit element in the group G
$\rtimes$	semidirect product
$\mathcal{C}_N$	the lift of the restricted Clifford group to $U(N)$
$C(n_1, ..., n_k)$	the restricted Clifford group of a composite system
$\mathrm{Sp}_{[n_1,...,n_k]}$	the generalized symplectic group

Chapter 1

Automorphisms of the Pauli grading

1.1 Gradings of *-algebras

We define the state of a given quantum system as a ray (one-dimensional subspace) in a complex separable Hilbert space, which is called a state space of this system. If the state space is finite dimensional of dimension N (therefore isomorphic to the space $\mathbb{C}^N$), we call this system an N-level quantum system. The observables of an N-level quantum system are described by self-adjoint linear operators on the state space of a given system, as hermitian $N \times N$ matrices. The set of all complex $N \times N$ matrices, denoted $M_N(\mathbb{C})$, is a complex linear associative *-algebra with a multiplicative unit.

The following definition describes properties of the involution of algebras of operators on Hilbert spaces. Spectral values of a hermitian observable are real numbers interpreted as possible outcomes of measurement.

The following definition does not require associativity of multiplication or existence of multiplicative unit and therefore it is possible to define involution on other types of complex linear algebras as well.

Definition 1.1.1. *Let $\mathcal{A}$ be a complex linear algebra. Involution (also called involutive antiautomorphism) in $\mathcal{A}$ is a map $* : \mathcal{A} \to \mathcal{A}$ satisfying:*

1. $(\xi a + b)^* = \overline{\xi} a^* + b^*$ *for all* $\xi \in \mathbb{C}$ *and for all* $a, b \in \mathcal{A}$,
2. $(a^*)^* = a$ *for all* $a \in \mathcal{A}$,
3. $(ab)^* = b^* a^*$ *for all* $a, b \in \mathcal{A}$.

*The element a^* is called the adjoint element of a. If $a \in \mathcal{A}$ satisfies $a^* = a$, it is called self-adjoint. The pair $(\mathcal{A}, *)$ is called an involutive algebra or *-algebra.*

From this point onward, we will refer to a complex linear associative *-algebra with multiplicative unit simply as *-algebra.

In this chapter, we give a definition and an overview of properties of the Pauli grading (see [1] [2], [3]) of $M_N(\mathbb{C})$. In the following chapters, we study other interesting mathematical notions connected with automorphisms of $M_N(\mathbb{C})$. It is obvious that in the case of the algebra $M_N(\mathbb{C})$ of complex $N \times N$ matrices, the role of involution is played by Hermitian conjugation [2].

Definition 1.1.2. *A grading Γ of a *-algebra $\mathcal{A}$ is a decomposition of $\mathcal{A}$ into direct sum of subspaces*

$$\Gamma : \quad \mathcal{A} = \bigoplus_{i \in I} \mathcal{A}_i \tag{1.1}$$

such that for any pair of indices $i, j \in I$ there exists an index $k \in I$ with the property

$$\mathcal{A}_i \mathcal{A}_j = \{AB | A \in \mathcal{A}_i, B \in \mathcal{A}_j\} \subseteq \mathcal{A}_k$$

and for every index $l \in I$ there exists $m \in I$ such that

$$\mathcal{A}_l^* = \{A^* | A \in \mathcal{A}_l\} \subseteq \mathcal{A}_m$$

The most obvious question one tends to ask upon seeing this definition is whether it is possible to further divide the subspaces which constitutie the grading into smaller ones in such a way that this new decomposition would still be a grading. This process, regardless of how it is done, is called refining.

Definition 1.1.3. *Let $\mathcal{A}$ be a *-algebra and let Γ be a grading of $\mathcal{A}$. A grading $\tilde{\Gamma}$ is called a refinement of Γ if for each $\tilde{\mathcal{A}}_i$ constituting $\tilde{\Gamma}$ there exists $\mathcal{A}_j$ constituting Γ such that $\tilde{\mathcal{A}}_i \subseteq \mathcal{A}_j$. A grading which cannot be refined further is called fine [1], [2], [3].*

Trivially, a grading consisting only of subspaces of dimension one is fine. Gradings of *-algebras can be constructed is by using certain groups of *-automorphisms. These are *-preserving maps on a given *-algebra, as described in the following definition.

Definition 1.1.4. *Let $\mathcal{A}$ and $\mathcal{B}$ be *-algebras. A map $\psi : \mathcal{A} \to \mathcal{B}$ is called a *-morphism if*

1. *$\psi(\xi a + b) = \xi\psi(a) + \psi(b)$ for all $\xi \in \mathbb{C}$ and for all $a, b \in \mathcal{A}$,*
2. *$\psi(ab) = \psi(a)\psi(b)$ for all $a, b \in \mathcal{A}$,*
3. *$\psi(a^*) = (\psi(a))^*$ for all $a \in \mathcal{A}$.*

*If ψ is a bijection, then it is called a *-isomorphism, furthermore if $\mathcal{A} = \mathcal{B}$, then ψ is called a *-automorphism [2].*

Now we describe how certain gradings of a finite dimensional *-algebra $\mathcal{A}$ are obtained by looking at the group Aut $(\mathcal{A})$ of all its *-automorphisms. If $\psi \in$ Aut $(\mathcal{A})$ is diagonalizable and $x, y \in \mathcal{A}$ are its eigenvectors with eigenvalues $\mu, \nu \in \mathbb{C} \setminus \{0\}$ respectively. Then

$$\psi(xy) = \psi(x)\psi(y) = (\mu x)(\nu y) = (\mu\nu)xy \quad \text{and} \quad (\psi(x))^* = (\mu x)^* = \overline{\mu} x^*.$$

This means that xy is either an eigenvector of ψ with the eigenvalue $\mu\nu$ or the zero element and that x^* is an eigenvector of ψ corresponding to $\overline{\mu}$. The given automorphism ψ therefore leads to a decomposition of $\mathcal{A}$ into the sum of eigenspaces of ψ:

$$\Gamma : \quad \mathcal{A} = \bigoplus_{\lambda \in \sigma(\psi)} \text{Ker } (\psi - \lambda I)$$

which satisfies the definition of a grading [2].

Refinements of a given grading can be obtained by adjoining further diagonalizable *-automorphisms commuting with ψ. Suppose that $\phi, \psi \in \text{Aut } \mathcal{A}$ are diagonalizable and satisfy $\psi \circ \phi = \phi \circ \psi$. It follows that for any eigenvector a of ψ with the eigenvalue λ it holds that

$$\lambda\phi(a) = \phi(\lambda a) = (\phi \circ \psi)(a) = (\psi \circ \phi)(a) = \psi(\phi(a)) \text{ i.e. } \phi(a) \in \text{Ker } (\psi - \lambda I)$$

and so Ker $(\psi - \lambda I)$ is ϕ-invariant. Diagonalizability of ϕ implies that ϕ is diagonalizable on Ker $(\psi - \lambda I)$ for each $\lambda \in \sigma(\psi)$ and therefore defines a refinement of Γ [2], [4].

Moreover, since the automorphism ψ is invertible, i.e. $0 \notin \sigma(\psi)$, we obtain $\psi(a) = \lambda a \Rightarrow \psi^{-1}(a) = \frac{1}{\lambda}a$. Thus ψ^{-1} has the same eigenspaces as ψ only corresponding to the inverses of their respective eigenvalues.

These observations imply that a *-automorphism and its inverse define the same grading. Therefore a given grading Γ and its refinements are induced by a group G of commuting invertible diagonalizable *-automorphisms. If Γ is fine, then the corresponding group G must be maximal, i.e. for all $\psi \in \text{Aut } \mathcal{A} \setminus G$ there exists some $\phi \in G$ such that $\psi\phi \neq \phi\psi$. Maximal groups of commuting diagonalizable invertible *-automorphisms shall be called MAD-groups (maximal abelian diagonalizable) of a *-algebra $\mathcal{A}$ [2], [4].

Conversely, if a given grading of *-algebra $\mathcal{A}$ is given, it defines a particular abelian subgroup Diag $\Gamma \subset \text{Aut } \mathcal{A}$, defined below [4].

Definition 1.1.5. *Let (1.1) be a grading of a *-algebra $\mathcal{A}$.* Diag Γ *is the group consisting of those *-automorphisms $\psi \in \text{Aut } \mathcal{A}$ which satisfy*

1. *$\psi(\mathcal{A}_i) = \mathcal{A}_i$ for all $i \in I$,*
2. *$\psi(x) = \lambda_i x$ for all $x \in \mathcal{A}$ and for all $i \in I$, where $\lambda_i \neq 0$ depends only on ψ and $i \in I$.*

1.2 Pauli group

There exists a classification of all MAD-groups of the *-algebra $M_N(\mathbb{C})$ which uses the Pauli group as its foundation. This section is dedicated to the definition and description of the basic properties of this group.

Definition 1.2.1. *Let $N \in \mathbb{N}$. Denote the N-th primitive root of unity* $\exp(2\pi i/N)$ *by ω_N. We define the special diagonal matrix*

$$Q_N = \text{diag } (1, \omega_N, \omega_N^2, ..., \omega_N^{N-1})$$

and the special $N \times N$ permutation matrix

$$P_N = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & 0 & \cdots & 0 & 0 \end{pmatrix}.$$

The unitary matrices P_N and Q_N are both of order N. They appear in finite-dimensional quantum mechanics (FDQM), where their integral powers play the role of exponentiated operators of position and momentum. These matrices satisfy the commutation relation

$$P_N Q_N = \omega_N Q_N P_N, \quad \text{also} \quad [P_N, Q_N] := P_N Q_N P_N^{-1} Q_N^{-1} = \omega_n I_N. \tag{1.2}$$

which can be verified easily by direct computation [2], [4].

Definition 1.2.2. *The discrete Pauli group Π_N of an N-level quantum system is defined as the group generated by powers of P_N and Q_N.*

$$\Pi_N = \langle P_N, Q_N \rangle = \{\omega_N^i Q_N^j P_N^k | i, j, k = 0, 1, 2, ..., N-1\}.$$

Pauli group has N^3 elements and it follows from equation (1.2) that two elements of the Pauli group of the form $X_{ab} = Q^a P^b, a, b \in \mathbb{Z}_N$ satisfy

$$X_{cd} X_{ab} = \omega_N^{ad-bc} X_{ab} X_{cd}, \tag{1.3}$$

for every $a, b, c, d \in \mathbb{Z}_N$, with operations modulo N. Note that if N is even, then $(Q_N P_N)^N = -I_N$ and if N is odd, then $(Q_N P_N)^N = I_N$.

We define an analogue of the standard inner product on $M_N(\mathbb{C})$, which is called the Hilbert-Schmidt inner product.

Definition 1.2.3. *Let $A, B \in M_N(\mathbb{C})$. The Hilbert-Schmidt inner product of A and B is defined as $\langle A, B \rangle = \mathrm{Tr}(A^H B)$ [2].*

Lemma 1.2.1. *For all different pairs of indices $(a, b) \neq (c, d)$, the matrices X_{ab} and X_{cd} are orthogonal with respect to the Hilbert-Schmidt inner product.*

Proof. Let $(a, b) \neq (c, d)$, then

$$\langle X_{ab}, X_{cd} \rangle = \langle Q_N^a P_N^b, Q_N^c P_N^d \rangle = \mathrm{Tr}((Q_N^a P_N^b)^H Q_N^c P_N^d) = \mathrm{Tr}(P_N^{-b} Q_N^{-a} Q_N^c P_N^d) \tag{1.4}$$

and since trace is invariant under cyclic permutation of matrices,

$$\langle X_{ab}, X_{cd} \rangle = \mathrm{Tr}(P_N^d P_N^{-b} Q_N^{-a} Q_N^c). \tag{1.5}$$

Without loss of generality, we can assume that $c \geq a$ and $d \geq b$, giving the result

$$\langle X_{ab}, X_{cd} \rangle = \mathrm{Tr}(P_N^{d-b} Q_N^{c-a}). \tag{1.6}$$

If $b \neq d$, then P_N^{d-b} is a traceless matrix multiplied by a diagonal matrix Q_N^{c-a}, giving a traceless matrix. In the case $b = d$ and $c > a$, a diagonal matrix with powers of ω_N on the diagonal is obtained. It follows that

$$\mathrm{Tr}(\mathrm{diag}\ (1, \omega_N^{c-a}, \omega_N^{2(c-a)}, ..., \omega_N^{(n-1)(c-a)})) = \sum_{i=0}^{n-1} \omega_N^{i(c-a)} = \frac{\omega_N^{N(c-a)} - 1}{\omega_N^{c-a} - 1} = 0. \tag{1.7}$$

□

1.3 Pauli grading of $M_N(\mathbb{C})$ and its symmetries

Definition 1.3.1. *The Pauli grading of $M_N(\mathbb{C})$ is the decomposition*

$$\Gamma_{\Pi_N}: \quad M_N(\mathbb{C}) = \bigoplus_{(r,s)\in\mathbb{Z}_N\times\mathbb{Z}_N} \mathcal{A}_{rs}, \tag{1.8}$$

where $\mathcal{A}_{rs} = \mathbb{C}X_{rs}$.

We see that the Pauli grading is indeed a grading of $M_N(\mathbb{C})$ since equation (1.3) implies that the result of multiplication of two subspaces again lies in a subspace labeled by $\mathbb{Z}_N \times \mathbb{Z}_N$. Furthermore, the involution only permutes these subspaces since P_N and Q_N are unitary matrices. The subspaces $\mathcal{A}_{rs}$ are orthogonal for distinct elements of $\mathbb{Z}_N \times \mathbb{Z}_N$ according to Lemma 1.2.1.

The following definitions are given in a general form for a grading of an arbitrary *-algebra. For the sake of clarity we include them in this section.

Definition 1.3.2. *The symmetry group of a grading (1.1) is a subgroup* Aut Γ *of* Aut $\mathcal{A}$ *consisting of those *-automorphisms ϕ which satisfy*

$$\phi(\mathcal{A}_i) = (A_j) \tag{1.9}$$

for some $j \in I$ [4].

We give a brief overview of properties of normal groups, which will be used in the section 2.2 for describing short exact sequences and semidirect products (see [5]).

Definition 1.3.3. *Let G be a group, $N \leq G$ its subgroup. We say that N is a normal subgroup of G, denoted $N \lhd G$, if $\mathcal{N}_G(N) = G$.*

Theorem 1.3.1. *Let N be a subgroup of the group G. The following statements are equivalent:*

1. *$N \lhd G$*
2. *$gN = Ng$ for all $g \in G$*
3. *$gNg^{-1} \subset N$ for all $g \in G$*

4. the multiplication of left cosets $uN \cdot vN := (uv)N$ is well-defined

5. N is the kernel of some homomorphism $\phi : G \to H$, where H is a group.

Next, we introduce the formalism of group actions which will be used throughout this text.

Definition 1.3.4. *A group action of a group G on a set S is a map $a : G \times S \to S$ satisfying the following properties*

1. $a(g_1, a(g_2, s)) = a(g_1 g_2, s)$ for all $g_1, g_2 \in G$ and $s \in S$

2. $a(1, s) = s$ for all $s \in S$.

We often use the notation $a(g, s) = g \cdot s$ for all $g \in G$ and $s \in S$ [5].

Definition 1.3.5. *The kernel of the action a is the set of elements of G that act trivially on every elements of S*

$$\text{Ker } a = \{g \in G | a(g, s) = s, \ \forall s \in S\}.$$

The stabilizer of s in G is the set of elements of G that fix the element s

$$\text{Stab } s = \{g \in G | a(g, s) = s\}.$$

An action is called faithful if its kernel is the unit element [5].

Remark 1.3.1. *The equation (1.9) defines a permutation $\overline{\phi}$ of the elements of I, so we have a permutation representation Δ_Γ of* Aut Γ *given by*

$$\overline{\phi} = \Delta_\Gamma(\phi), \quad \phi \in \text{Aut } \Gamma.$$

(see [4])

Definition 1.3.6. *The kernel of Δ_Γ is called the stabilizer of Γ in* Aut Γ

$$\text{Stab } \Gamma = \text{Ker } \Delta_\Gamma = \{\phi \in \text{Aut } \mathcal{A} | \phi(\mathcal{A}_i) = \mathcal{A}_i, \forall i \in I\}.$$

Definition 1.3.7. *Let G be a group, $K \subset G$. Normalizer $\mathcal{N}_G(K)$ of the set K in the group G is the subgroup*

$$N_G(K) = \{g \in G | gKg^{-1} = K\}. \tag{1.10}$$

Let Γ be a fine grading. The symmetry group Aut Γ is the normalizer of Stab Γ in Aut $\mathcal{A}$:

$$\text{Aut } \Gamma = \mathcal{N}(\text{Stab } \Gamma) = \{\phi \in \text{Aut } \mathcal{A} | \phi(\text{Stab } \Gamma)\phi^{-1} \subset \text{Stab } \Gamma\}. \tag{1.11}$$

Remark 1.3.2. Stab Γ *is a normal subgroup of* Aut Γ *with the quotient group isomorphic to the permutation representation of* Aut Γ *on I,*

$$\text{Aut } \Gamma / \text{Stab } \Gamma \cong \Delta_\Gamma(\text{Aut } \Gamma).$$

Now let us consider a grading of $M_N(\mathbb{C})$ constructed by using diagonalizable *-automorphisms, as described in the first section. The following theorem is the first step in classification of such gradings achieved by giving complete description of all MAD-groups which exist in Aut $(M_N(\mathbb{C}))$ [1], [2].

Definition 1.3.8. *Let $A \in M_N(\mathbb{C})$ be an invertible matrix. We define the inner automorphism Ad_A as $Ad_A(X) = A^{-1}XA$ for all $X \in M_N(\mathbb{C})$ [2], [4].*

Theorem 1.3.2. *All *-automorphisms ψ of $M_N(\mathbb{C})$ can be written in the form $\psi = Ad_U$ for some unitary matrix U. Moreover, if U and V are unitary and $Ad_U = Ad_V$, then there exists $\varphi \in [0, 2\pi)$ such that $V = e^{i\varphi}U$.*

It was shown in [1], [2] that there is a one-to-one correspondence between MAD-groups and unitary Ad-groups (defined below).

Definition 1.3.9. *A subgroup $\mathscr{G}$ of $U(N)$ shall be called a unitary Ad-group if*

1. *For any pair $U, V \in \mathscr{G}$ there exists $\omega \in \mathbb{C}$ such that $UV = \omega VU$.*
2. *$\mathscr{G}$ is maximal, i.e. for each $M \notin \mathscr{G}$ there exists $U \in \mathscr{G}$ such that $UM \neq \omega MU$ for all $\omega \in \mathbb{C}$.*

The classification of all unitary Ad-groups was given in [1] using tensor products of Pauli groups of certain dimensions and the group $U_D(m)$ of $m \times m$ diagonal unitary matrices [1], [2].

Theorem 1.3.3. *$\mathscr{G} \subseteq U(N)$ is a unitary Ad-group if and only if it is unitarily conjugated to one of the finite groups*

$$\Pi_{\pi_1} \otimes \Pi_{\pi_2} \otimes \Pi_{\pi_3} \otimes ... \otimes \Pi_{\pi_s} \otimes U_D(N/\pi_1\pi_2\pi_3...\pi_s)$$

where $\pi_1, \pi_2, \pi_3, ..., \pi_s$ are powers of primes and their product divides N [1], [2].

This classification implies that Π_N itself is the simplest unitary Ad-group and the corresponding fine grading of $M_N(\mathbb{C})$ obtained by the process described in the first section is the Pauli grading (1.8). Let us denote the MAD group Ad_{Π_N} by $\mathscr{P}_N$. It is an Abelian subgroup of Aut $M_N(\mathbb{C})$ with generators Ad_{P_N} and Ad_{Q_N},

$$\mathscr{P}_N = \{Ad_{Q_N^i P_N^j} | (i, j) \in \mathbb{Z}_N \times \mathbb{Z}_N\}. \tag{1.12}$$

It is obvious that $\mathscr{P}_N$ has N^2 elements which stabilize Pauli's grading, since taking the generators one sees that

$$Ad_{P_N} X_{rs} = \omega_N^{-r} X_{rs}, \quad Ad_{Q_N} X_{rs} = \omega_n^s X_{rs}. \tag{1.13}$$

Moreover, $\mathscr{P}_N =$ Stab Γ_{Π_N} since $\mathscr{P}_N$ is maximal.

Now, we wish to describe the group Aut Γ_{Π_N} in terms of some other groups. We begin by looking at the generators of the stabilizer Stab Γ_{Π_N}. Since the matrices P_N and Q_N have the same spectra, they are similar with a unitary similarity matrix F_N such that $F_N^{-1} P_N F_N = Q_N$. Such F_N is not determined uniquely. We choose the matrix given in the following definition.

Definition 1.3.10. *The matrix F_N of the discrete Fourier transformation in dimension N is defined as follows:*

$$(F_N)_{ij} = \frac{1}{\sqrt{N}}\omega_N^{-ij} \quad \textit{for } i,j \in \mathbb{Z}_N. \tag{1.14}$$

Remark 1.3.3. *It is easy to verify that $(F_N^2)_{ij} = \delta_{i,-j}$ for $i,j \in \mathbb{Z}_N$ and that $F_N^4 = I_N$ [4].*

In addition, the matrices P_N and $P_N Q_N$ are similar with a unitary similarity matrix D_N. Analogously, we choose one D_N.

Definition 1.3.11. *Put $\varepsilon = 1$ if N is odd, and $\varepsilon = \sqrt{\omega_N}$ if N is even. Denote $d_j^{(N)} = \varepsilon^j \omega_N^{\binom{j}{2}}$ for $j \in \mathbb{Z}_N$. The discrete phase transformation matrix in dimension N is defined as*

$$D_N = \mathrm{diag}\ (d_0^{(N)}, d_1^{(N)}, d_2^{(N)}, ..., d_{N-1}^{(N)}). \tag{1.15}$$

A simple calculation gives $D_N Q_N D_N^{-1} = Q_N$ and $P_N Q_N = \varepsilon D_N P_N D_N^{-1}$. If Ad_X induces a permutation of elements in $\mathscr{P}_N$, then there must exist $a,b,c,d \in \mathbb{Z}_N$ such that

$$XQ_N X^{-1} = \mu Q_N^a P_N^b \quad \text{and} \quad XP_N X^{-1} = \nu Q_N^c P_N^d, \tag{1.16}$$

where $|\mu| = |\nu| = 1$. We define an equivalence relation between the elements X, Y of the set $A_N = \{X \in M_N(\mathbb{C}) | \mathrm{Ad}_X \in \mathrm{Aut}\ \Gamma_{\Pi_N}\}$ by

$$X \sim Y \Leftrightarrow X = e^{i\varphi} Y \quad \text{for some} \quad \varphi \in [0, 2\pi). \tag{1.17}$$

To each equivalence class of Ad-actions Ad_X a quadruple of elements in $a,b,c,d \in \mathbb{Z}_N$ is assigned by (1.16). In matrix notation, we obtain

$$\mathrm{Ad}_X \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \tag{1.18}$$

$$\mathrm{Ad}_X \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{1.19}$$

Now using equations (1.16) and the commutation relation 1.2, we get

$$\mathrm{Ad}_X(P_N Q_N) = \omega_N \mathrm{Ad}_X(Q_N P_N) \Rightarrow \omega_N^{ad-1} = \omega_N^{bc}. \tag{1.20}$$

This result can be rewritten in the form [2], [4], [6]

$$\det \begin{pmatrix} a & c \\ b & d \end{pmatrix} = ad - bc = 1 \mod N. \tag{1.21}$$

Another way of expressing this result is in terms of a bilinear antisymmetric non-degenerate (symplectic) form on the phase space $\mathbb{Z}_N \times \mathbb{Z}_N$. Namely, the form q_N : $\mathbb{Z}_N \times \mathbb{Z}_N \to \mathbb{Z}_N$, where

$$q_N((i,j),(k,l)) = jk - il = (i,j) \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} k \\ l \end{pmatrix} = \det \begin{pmatrix} j & i \\ k & l \end{pmatrix} = 1 \mod N. \tag{1.22}$$

These observations were taken further. Using the fact that elements of $\mathscr{P}_N$ itself stabilize Pauli grading and if the properties of the indices a, b, c, d are examined, it follows that that $\mathcal{N}(\mathscr{P}_N))/\mathscr{P}_N$ is isomorphic to a known group, as stated in the following theorem [2].

Theorem 1.3.4. *The quotient group $\mathcal{N}(\mathscr{P}_N))/\mathscr{P}_N$ is isomorphic to the group $SL(2, \mathbb{Z}_N)$, which is the group of 2×2 matrices with entries form $\mathbb{Z}_N$ with determinant equal to 1 modulo N.*

Lemma 1.3.1. *$SL(2, \mathbb{Z}_N)$ is generated by the matrices [4]*

$$F = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \textit{and} \quad D = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}. \tag{1.23}$$

We see that the matrices $F, D \in SL(2, \mathbb{Z}_N)$ correspond to the Ad-actions of the matrices F_N and D_N respectively, hence we arrive to the following corollary [2], [4].

Corollary 1.3.1. *The normalizer $\mathcal{N}(\mathscr{P}_N)$ of the group $\mathscr{P}_N$ in* Aut $M_N(\mathbb{C})$ *is generated by*

$$Ad_F, Ad_D, Ad_P \quad \textit{and} \quad Ad_Q.$$

Chapter 2

Clifford group of a simple N-level quantum system

2.1 The Weyl-Heisenberg group

Definition 2.1.1. *Put $\tau_N = -\sqrt{\omega_N}$. We define the Weyl-Heisenberg group $H(N)$ as follows [6]:*

$$H(N) = \Pi_N = \{\omega_N^i Q_N^j P_N^k | i, j, k = 0, 1, 2, ..., N-1\} \quad \textit{for odd } N, \tag{2.1}$$

$$H(N) = \{\tau_N^i Q_N^j P_N^k | i = 0, 1, 2, ..., 2N-1; j, k = 0, 1, 2, ..., N-1\} \quad \textit{for even } N. \tag{2.2}$$

Note that for odd N, the Weyl-Heisenberg group $H(N)$ is by definition equal to the Pauli group Π_N, but this is not true in the case of even N, where the Weyl-Heisenberg group is larger and contains the Pauli group as a subgroup. The reason for this inconvenient definition will be explained in the third chapter.

The centre $Z(H(N))$ of $H(N)$ is the set of all those elements of $H(N)$ which commute with all elements of $H(N)$. For odd N we have

$$Z(H(N)) = \{1, \omega_N, \omega_N^2, ..., \omega_N^{N-1}\} \tag{2.3}$$

and for even N

$$Z(H(N)) = \{1, \tau_N, \tau_N^2, ..., \omega_N^{2N-1}\}. \tag{2.4}$$

Since the centre is a normal subgroup, we can consider the quotient group $H(N)/Z(H(N))$. Its elements are the cosets labelled by pairs of exponents $(j, k) \in \mathbb{Z}_N \times \mathbb{Z}_N$. We see that the correspondence

$$Q_N^j P_N^k Z(H(N)) = \{\tau_N^i Q_N^j P_N^k | i = 0, 1, 2, ..., 2N-1\} \mapsto (j, k) \tag{2.5}$$

and the analogous correspondence for odd N is an isomorphism of abelian groups and therefore the three groups $\mathscr{P}_N$, $H(N)/Z(H(N))$ and $\mathbb{Z}_N \times \mathbb{Z}_N$ are isomorphic.

Definition 2.1.2. *The Clifford group of dimension N is the normalizer of $H(N)$ in the group $U(N)$ of unitary operators in dimension N.*

It turns out that the structure of the normalizer is rather difficult to describe in general. In order to get insight into the structure of the normalizer, the restricted Clifford group is defined [6].

Definition 2.1.3. *The Restricted Clifford group $C(N)$ of dimension N is defined as the quotient group*

$$C(N) = \mathcal{N}_{U(N)}(H(N))/U(1). \tag{2.6}$$

2.2 Normal subgroups and isomorphism theorems

In this section, we prove the first two isomorphism theorems.

Theorem 2.2.1 (The First Isomorphism Theorem)**.** *Let $\psi : G \to H$ be a homomorphism. Then*

1. $\mathrm{Im}\ \psi$ *is a subgroup of* H
2. $\mathrm{Ker}\ \psi$ *is a normal subgroup of* G
3. $\mathrm{Im}\ \psi \cong H/\mathrm{Ker}\ \psi$

In particular, if ψ is surjective, then $G/(\mathrm{Ker}\ \psi) \cong H$.

Proof. The first point is trivial. Analogously, it is easy to see that $\mathrm{Ker}\ \psi$ is a subgroup of H. Take arbitrary $g \in G$ and $k \in \mathrm{Ker}\ \psi$ and denote 1_G. We obtain

$$\psi(g^{-1}kg) = (\psi(g))^{-1}\psi(k)\psi(g) = (\psi(g))^{-1}\psi(g) = 1_H \Rightarrow g^{-1}kg \in \mathrm{Ker}\ \psi, \tag{2.7}$$

therefore by definition $\mathrm{Ker}\ \psi \lhd G$.

To prove the third statement, we denote $K = \mathrm{Ker}\ \psi$ and define a new mapping $\Phi : G/K \to H$ by $\Phi(gK) = \psi(g)$ for all $g \in G$. First, we need to ensure that Φ is well defined, i.e. $\forall g_1, g_2 \in G : g_1K = g_2K \Rightarrow \Phi(g_1K) = \Phi(g_2K)$. It is well-known that $g_1K = g_2K \Leftrightarrow g_1^{-1}g_2 \in K = \mathrm{Ker}\ \psi$. Thus $\psi(g_1^{-1}g_2) = 1_H \Rightarrow \psi(g_1) = \psi(g_2)$ and Φ is well-defined. Second, we need to prove that Φ preserves multiplication; taking any $g_1, g_2 \in G$, we obtain $\Phi(g_1Kg_2K) = \Phi(g_1g_2K) = \psi(g_1g_2) = \psi(g_1)\psi(g_2) = \Phi(g_1K)\Phi(g_2K)$.

Finally, we see that $\mathrm{Im}\ \Phi = \{\Phi(gK)|g \in G\} = \{\psi(g)|g \in G\} = \mathrm{Im}\ \psi$ and $\Phi(g_1K) = \Phi(g_2K) \Rightarrow \psi(g_1) = \psi(g_2) \Rightarrow g_1^{-1}g_2 \in K$ and $g_1K = g_2K$ as above. □

Theorem 2.2.2 (The Second or Diamond Isomorphism Theorem)**.** *Let G be a group, A, B its subgroups satisfying $A \leq \mathcal{N}_G(B)$. Then $AB \leq G$, $B \lhd AB$, $A \cap B \lhd A$ and $AB/B \cong A/(A \cap B)$.*

Proof. It is shown in [5] that AB is indeed a subgroup of G. Since $A \leq \mathcal{N}_G(B)$ by assumption and $B \leq \mathcal{N}_G(B)$ trivially, we see that $AB \leq \mathcal{N}_G(B)$ i.e. B is a normal subgroup of AB.

Since B is normal in AB, the quotient group AB/B is well-defined. Let $\psi : A \to AB/B$ be defined as $\psi(a) = aB$ for all $a \in A$. Since the group operation in AB/B is well-defined, we have

$$\psi(a_1a_2) = (a_1a_2)B = a_1B \cdot a_2B = \psi(a_1)\psi(a_2) \quad \forall a_1, a_2 \in A. \tag{2.8}$$

It follows from the definition that ψ is surjective. The kernel of ψ consists of elements $a \in A$ such that $aB = 1B$, which are the elements $a \in B$, i.e. Ker $\psi = A \cap B$. By the First Isomorphism Theorem, $A \cap B \lhd A$ and $A/(A \cap B) \cong AB/B$. $\square$

2.3 Group extensions and exact sequences

In this section, we formulate the theory of short exact sequences and their relation to group extensions. We follow the approach used in [7].

Definition 2.3.1. *Let K, H, G be groups and let $\beta : K \to G$ and $\alpha : G \to H$ be homomorphisms. The sequence of two morphisms β, α*

$$K \xrightarrow{\ \beta\ } G \xrightarrow{\ \alpha\ } H \tag{2.9}$$

is called exact in G if Im β = Ker α.

Remark 2.3.1. *Exactness in G means that $\alpha \circ \beta(k) = 1_H$ for every $k \in K$ and simultaneously every $g \in G$ satisfying $\alpha(g) = 1_H$ can be written in the form $g = \beta(k)$ for some suitable $k \in K$.*

Lemma 2.3.1. *The sequence $1 \xrightarrow{\ \beta\ } G \xrightarrow{\ \alpha\ } H$ is exact if and only if α is a injective. The sequence $K \xrightarrow{\ \beta\ } G \xrightarrow{\ \alpha\ } 1$ is exact if and only if β is an surjective.*

Proof. In the first case, the sequence is exact iff Im $\beta = 1_G =$ Ker $\alpha \Leftrightarrow \alpha$ is a injective. In the second case, the sequence is exact iff Im β = Ker $\alpha = G$, which by definition means that β is surjective. $\square$

Definition 2.3.2. *Let $G_1, G_2, G_3, ..., G_n$ be groups. A longer sequence*

$$G_1 \longrightarrow G_2 \longrightarrow G_3 \longrightarrow ... \longrightarrow G_{n-1} \longrightarrow G_n, \tag{2.10}$$

where each arrow represents some group homomorphism, is called exact if it is exact in all the middle groups $G_2, G_3, ..., G_{n-1}$, i.e. each subsequence

$$G_{i-1} \longrightarrow G_i \longrightarrow G_{i+1} \tag{2.11}$$

is exact in G_i for all $i \in \{2, 3, 4, ..., n-1\}$.

Definition 2.3.3. *Let K, H, G be groups and let $\beta : K \to G$ and $\alpha : G \to H$ be homomorphisms. A short exact sequence is an exact sequence of homomorphisms*

$$1 \longrightarrow K \xrightarrow{\beta} G \xrightarrow{\alpha} H \longrightarrow 1. \tag{2.12}$$

Exactness in K means that β is a group injective and exactness in G implies that α is a a surjective. Furthermore, exactness in G means that $\mathrm{Im}\ (\beta) = \mathrm{Ker}\ (\alpha)$. These facts imply that $\beta(K) \lhd G$. In addition, the first isomorphism theorem implies that $G/\beta(K) \cong H$. Conversely, every normal subgroup $N \lhd G$ leads to a short exact sequence

$$1 \longrightarrow N \longrightarrow G \longrightarrow G/N \longrightarrow 1, \tag{2.13}$$

where the morphisms are the insertion $N \to G$ and the projection $G \to G/N$, respectively.

Definition 2.3.4. *Let a short exact sequence be given as in (2.12). We say that the middle group G is an extension of the group H by the group K. This extension is called split if there exists homomorphism $\gamma : H \to G$, called splitting morphism, such that $\alpha \circ \gamma = id_H$, where id_H denotes the identity map on H. A short exact sequence (2.12), for which the splitting homomorphisms exists is called a split short exact sequence.*

For example, the direct product $G \times H$ of two groups G and H is an extension of H by G

$$1 \longrightarrow G \xrightarrow{\beta} G \times H \xrightarrow{\alpha} H \longrightarrow 1 \tag{2.14}$$

with the morphisms $\beta(g) = (g, 1)$ for all $g \in G$ and $\alpha((g, h)) = h$ for all $(g, h) \in G \times H$. In this case, the splitting morphism is defined by $\gamma(h) = (1, h)$ for all $h \in H$.

Definition 2.3.5. *Let us have two short exact sequences with the same ends K and H and with distinct middle groups G and G'. Then we say that the two extensions G and G' are equivalent if there exists a group isomorphism $\psi : G \to G'$ such that the diagram*

$$\begin{tikzcd}
1 \arrow[r] & K \arrow[r] \arrow[d, "id_K"'] & G \arrow[r] \arrow[d, "\psi"'] & H \arrow[r] \arrow[d, "id_H"'] & 1 \\
1 \arrow[r] & K \arrow[r] & G' \arrow[r] & H \arrow[r] & 1
\end{tikzcd} \tag{2.15}$$

commutes, i.e. if we consider the diagram to be an oriented graph, where the groups act as vertices and the arrows act as arcs in the graph, then all directed paths with the same start and endpoint will yield the same result.

For example, taking the direct products $G \times K$ and $K \times G$ of groups G and K, we can easily see that

$$\begin{tikzcd}
1 \arrow[r] & G \arrow[r] \arrow[d, "id_K"'] & G \times K \arrow[r] \arrow[d, "\psi"'] & K \arrow[r] \arrow[d, "id_H"'] & 1 \\
1 \arrow[r] & G \arrow[r] & K \times G \arrow[r] & K \arrow[r] & 1
\end{tikzcd} \tag{2.16}$$

where ψ is defined as $\psi((g,k)) = (k,g)$ for all $(g,k) \in G \times K$ is a commutative diagram, so $G \times K$ and $K \times G$ are equivalent extensions of G by the group K.

Now we proceed to define a generalization of the direct product. Let G, H be groups, let Aut G denote the group of all automorphisms of G and let $\Theta : H \to \text{Aut } G$ be a homomorphism. Each automorphism $\Theta(h) : G \to G$ shall be denoted as $[\Theta(h)](g) = h \bullet g$ for all $g \in G$ and all $h \in H$.

For every $g_1, g_2 \in G$ and every $h \in H$ we have

$$h \bullet (g_1 g_2) = [\Theta(h)](g_1 g_2) = [\Theta(h)](g_1)[\Theta(h)](g_2) = (h \bullet g_1)(h \bullet g_2). \tag{2.17}$$

and

$$(h_1 h_2) \bullet g = [\Theta(h_1 h_2)](g) = [\Theta(h_1) \circ \Theta(h_2)](g) = [\Theta(h_1)]([\Theta(h_2)](g)) = h_1 \bullet (h_2 \bullet g) \tag{2.18}$$

for all $h, h_1, h_2 \in H$ and all $g, g_1, g_2 \in G$. In particular we have

$$1_H \bullet g = [\Theta(1_H)](g) = id_G(g) = g \tag{2.19}$$

$$h \bullet 1_G = [\Theta(h)](1_G) = 1_G \tag{2.20}$$

for all $g \in G$ and $h \in H$.

Definition 2.3.6. *Let G, H be groups, let $\Theta : H \to \text{Aut } G$ be a homomorphism. We define the semidirect product $G \rtimes_\Theta H$ of the groups G and H with respect to Θ as a groupoid, where the underlying set is the cartesian product $G \times H$ and the binary operation*

$$(G \rtimes_\Theta H) \times (G \rtimes_\Theta H) \to G \rtimes_\Theta H \tag{2.21}$$

is defined as

$$(g_1, h_1)(g_2, h_2) = (g_1(h_1 \bullet g_2), h_1 h_2) = (g_1[\Theta(h_1)](g_2), h_1 h_2) \tag{2.22}$$

for all $g_1, g_2 \in G$ and $h_1, h_2 \in H$.

Theorem 2.3.1. *Let G, H be groups, let $\Theta : H \to \text{Aut } G$ be a morphism. Then the semidirect product $G \rtimes_\Theta H$ is a group where the unit element is $(1_G, 1_H)$ and the inverse element to $(g, h) \in G \rtimes_\Theta H$ is given by $(h^{-1} \bullet g^{-1}, h^{-1})$.*

Proof. First, we prove associativity of the grupoid operation. Consider arbitrary $g_1, g_2, g_3 \in G$ and $h_1, h_2, h_3 \in H$. We have

$$\begin{aligned}
(g_1, h_1)\big((g_2, h_2)(g_3, h_3)\big) &= (g_1, h_1)\big(g_2(h_2 \bullet g_3), h_2 h_3\big) = \\
= \Big(g_1\big(h_1 \bullet (g_2(h_2 \bullet g_3))\big), h_1(h_2 h_3)\Big) &= \Big(g_1(h_1 \bullet g_2)\big(h_1 \bullet (h_2 \bullet g_3)\big), (h_1 h_2) h_3\Big) = \\
= \Big(\big(g_1(h_1 \bullet g_2)\big)\big((h_1 h_2) \bullet g_3\big), (h_1 h_2) h_3\Big) &= \big(g_1(h_1 \bullet g_2), h_1 h_2\big)(g_3, h_3) = \\
&= \big((g_1, h_1)(g_2, h_2)\big)(g_3, h_3),
\end{aligned}$$

thus associativity is proven.

Now let $(g,h) \in G \rtimes_\Theta H$. Using equations (2.19) and (2.20),we have

$$(1_G, 1_H)(g,h) = (1_G(1_H \bullet g), 1_H h) = (g,h), \tag{2.23}$$

$$(g,h)(1_H, 1_G) = (g(h \bullet 1_G), h1_H) = (g,h), \tag{2.24}$$

proving the existence of the unit element.

It remains to prove that $(h^{-1} \bullet g^{-1}, h^{-1})$ is an inverse element of (g,h). Again, we utilise equations (2.19) and (2.20):

$$(h^{-1} \bullet g^{-1}, h^{-1})(g,h) = \big((h^{-1} \bullet g^{-1})(h^{-1}g), h^{-1}h\big) = \big(h^{-1} \bullet (g^{-1}g), 1_H\big) = \tag{2.25}$$

$$= (h^{-1} \bullet 1_G, 1_H) = (1_G, 1_H) \tag{2.26}$$

$$(g,h)(h^{-1} \bullet g^{-1}, h^{-1}) = \big(g(h \bullet (h^{-1} \bullet g^{-1})), h^{-1}h\big) = \big(g((hh^{-1}) \bullet g^{-1}), 1_H\big) = \tag{2.27}$$

$$= \big(g(1_H \bullet g^{-1}), 1_H\big) = (gg^{-1}, 1_H) = (1_G, 1_H), \tag{2.28}$$

concluding the proof. □

If $\Theta : H \to \text{Aut } G$ is the trivial homomorphism, which acts as $h \mapsto id_G$ for all $h \in H$, then $G \rtimes_\Theta H$ is the direct product $G \times H$, as can be easily verified. In this sense, semidirect product is a generalization of the direct product. Taking $H = \text{Aut } G$ and $\Theta = id_{\text{Aut } G}$, we obtain another group, called the holomorph of G, usually denoted $\text{Hol}(G)$ with multiplication defined by $(g_1, \phi_1)(g_2, \phi_2) = (g_1\phi(g_2), \phi_1\phi_2)$ for all $g_1, g_2 \in G$ and $\phi_1, \phi_2 \in \text{Aut } G$.

Each semidirect product $G \rtimes_\Theta H$ can be described in terms of exact sequences. By (2.22) and (2.20), $(g_1, 1_H)(g_2, 1_H) = (g_1g_2, 1_H)$ for all $g_1, g_2 \in G$. Thus we obtain a monomorphism $\beta : G \to G \rtimes_\Theta H$ defined by $\beta(g) = (g, 1_H)$ for all $g \in G$. It is easy to see that $\alpha : G \rtimes_\Theta H \to H, \alpha((g,h)) = h$ for all $(g,h) \in G \rtimes_\Theta H$ is an epimorphism and $\text{Im } \beta = \text{Ker } \alpha$. These homomorphisms define an exact sequence

$$1 \longrightarrow G \xrightarrow{\beta} G \rtimes_\Theta H \xrightarrow{\alpha} H \longrightarrow 1. \tag{2.29}$$

Futhermore, $\gamma : H \to G \rtimes_\Theta H$, defined $\gamma(h) = (1_G, h)$ for all $h \in H$ is a splitting homomorphism satisfying $\alpha \circ \gamma = id_H$, so (2.29) is a split short exact sequence.

Now denote $G_0 = \beta(G)$ and $H_0 = \gamma(H)$. The subgroups G_0 and H_0 satisfy the conditions $G_0 \cap H_0 = 1_{G \rtimes_\Theta H}$ and $G_0H_0 = G \rtimes_\Theta H$. Considering the converse of this result, the following theorem is obtained.

Theorem 2.3.2. *Each group G with subgroups N, S such that $N \lhd G$, $NS = G$ and $N \cap S = 1$ is isomorphic to some semidirect product. Explicitly, if $\Theta : S \to \text{Aut } N$ maps each $s \in S$ to the automorphism $[\Theta(s)]$ defined by $[\Theta(s)](n) = sns^{-1}$ for every $n \in N$, then the isomorphism $\Phi : N \rtimes_\Theta S \to G$ is defined by the equation $\Phi((n,s)) = ns$.*

Proof. Since $N \lhd G$, conjugation by $s \in S$ is an automorphism of the subgroup N. Each element $g \in G$ can be written in the form $g = ns$, where $n \in N$ and $s \in S$ and because $N \cap S = 1$, n and s are determined uniquely. Furthermore, $(n_1 s_1)(n_2 s_2) = n_1(s_1 n_2 s_1^{-1})s_1 s_2 = n_1[\Theta(s_1)](n_2)s_1 s_2$. By comparison with (2.22), it is obvious that $\Phi((n,s)) = ns$ is a homomorphism and since n and s are determined uniquely, it is an isomorphism. $\square$

The above theorem can be expressed in the form of the diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & N & \xrightarrow{\beta} & N \rtimes_\Theta S & \xrightarrow{\alpha} & S & \longrightarrow & 1 \\ & & {\scriptstyle id_N}\downarrow & & {\scriptstyle \Phi}\downarrow & & {\scriptstyle \psi}\downarrow & & \\ 1 & \longrightarrow & N & \longrightarrow & G & \xrightarrow{p} & G/N & \longrightarrow & 1. \end{array} \tag{2.30}$$

In this diagram, both rows are split short exact sequences. In the bottom row, p is the projection of G on the quotient group G/N. The middle vertical map is the isomorphism from the above theorem and the right vertical map ψ is the isomorphism $\psi : S \cong G/N$ which is the special case of the map from the Diamond Isomorphism Theorem with $G = NS$ and $1_G = N \cap S$. Since

$$\Phi \circ \beta(n) = \Phi((n,1)) = n \quad \text{and} \quad \psi \circ \alpha(n,s) = \psi(s) = sN = p \circ \Phi((n,s)), \tag{2.31}$$

the diagram (2.30) is commutative.

Corollary 2.3.1. *Every split short exact sequence*

$$1 \longrightarrow K \xrightarrow{\beta} G \xrightarrow{\alpha} H \longrightarrow 1 \tag{2.32}$$

defines an isomorphism $G \cong K \rtimes_\Theta H$ *for some suitable* $\Theta : H \to \text{Aut }(K)$.

Proof. Let (2.32) be split by $\gamma : H \to G$. We shall prove that the groups $N = \beta(K)$ and $S = \gamma(H)$ satisfy the assumptions in Theorem 2.3.2. Trivially, $N \lhd G$. Now let $g \in N \cap S$, then there exist $k \in K$ and $h \in H$ such that $g = \beta(k) = \gamma(h)$, so $h = \alpha \circ \gamma(h) = \alpha(\beta(k)) = 1_H \Rightarrow g = \gamma(1_H) = 1_G$.

Finally, let $g \in G$ be an arbitrary element. We choose $g = ns$, where $s = \gamma \circ \alpha(g) \in \gamma(H) = S$ and $n = gs^{-1}$. We get

$$\alpha(s) = \alpha \circ \gamma \circ \alpha(g) = id_H(\alpha(g)) = \alpha(g) \tag{2.33}$$

which implies

$$\alpha(n) = \alpha(g)\alpha(s^{-1}) = \alpha(s)(\alpha(s))^{-1} = \alpha(g)\alpha(g)^{-1} = 1_H. \tag{2.34}$$

Thus $n \in \text{Ker } \alpha = \beta(K) = N$, i.e. $G = NS$. $\square$

2.4 The restricted Clifford Group as a semidirect product

Our aim is to describe the Restricted Clifford Group as a semidirect product of already known groups. The first step is given by the following theorem.

Theorem 2.4.1. *The Restricted Clifford group is isomorphic to the normalizer of $\mathscr{P}_N$ in* Aut $(M_N(\mathbb{C}))$.

Proof. Denote the coset $[X] = \{e^{i\varphi}X\} \in C(N)$, where X lies in the Clifford group and $\varphi \in [0, 2\pi)$. We define the map $\Phi : C(N) \to \mathcal{N}_{\text{Aut }(M_N(\mathbb{C}))}(\mathscr{P}_N)$ by $\Phi([X]) = Ad_X$ for all $X \in C(N)$.

First, we shall verify that the map Φ is well-defined and that $\Phi([X])$ lies in $\mathcal{N}_{\text{Aut }(M_N(\mathbb{C}))}(\mathscr{P})$. Let $X, X' \in [X]$. Then

$$\Phi(X') = Ad_{X'} = Ad_{e^{i\varphi}X} = Ad_X = \Phi(X), \tag{2.35}$$

so the image does not depend on the choice of representative elements of $[X]$, thus we can use the notation $\Phi([X])$. Let $[X] \in C(N)$. Next, we will prove that $\Phi([X]) = Ad_X$ belongs to $\mathcal{N}_{\text{Aut }(M_N(\mathbb{C}))}(\mathscr{P}_N)$. For all $i, j \in \mathbb{Z}_N$, we get

$$\mathrm{Ad}_X \mathrm{Ad}_{Q^iP^j}(\mathrm{Ad}_X)^{-1} = \mathrm{Ad}_{XQ^iP^jX^{-1}} = \mathrm{Ad}_{\mu Q^kP^l} = \mathrm{Ad}_{Q^kP^l} \in \mathscr{P}_N, \tag{2.36}$$

where the pair $k, l \in \mathbb{Z}_N$ depends on $[X]$ and i, j, and where μ is some power of ω_N or τ_N, if N is odd or even, respectively. Thus $\Phi([X]) \in \mathcal{N}_{\text{Aut }(M_N(\mathbb{C}))}(\mathscr{P})$.

Second, we will prove that Φ is homomorphism. Let $[X], [Y] \in C(N)$, then by definition $[X][Y] = [XY]$, so

$$\Phi([X][Y]) = \Phi([XY]) = \mathrm{Ad}_{XY} = Ad_X Ad_Y = \Phi([X])\Phi([Y]). \tag{2.37}$$

Now, we examine the kernel Ker Φ:

$$[X] \in \text{Ker } \Phi \Leftrightarrow Ad_X = Ad_I \Leftrightarrow X = e^{i\varphi}I \Leftrightarrow [X] = [I], \tag{2.38}$$

i.e. Ker $\Phi = \{[I]\}$, therefore Φ is injective.

Finally, for any $\psi \in \mathcal{N}_{\text{Aut }(M_N(\mathbb{C}))}(\mathscr{P}_N)$ there exists some $X \in U(N)$ such that $\psi = \mathrm{Ad}_X$ [1]. Then $\Phi([X]) = \mathrm{Ad}_X = \psi$, hence Φ is also surjective. $\square$

In the rest of this section, we will attempt to describe $C(N)$ as a semidirect product. For the sake of brevity, we shall use the notation $\rtimes$ instead of $\rtimes_\Theta$ and $\mathscr{N}$ will replace $\mathcal{N}_{\text{Aut }(M_N(\mathbb{C}))}$. We start by recapitulating the known results

$$\mathscr{P}_N \cong \mathbb{Z}_N \times \mathbb{Z}_N, \tag{2.39}$$
$$\mathcal{N}(\mathscr{P}_N)/\mathscr{P}_N \cong SL(2, \mathbb{Z}_N). \tag{2.40}$$

Now let us examine the short exact sequence

$$1 \longrightarrow \mathscr{P}_N \longrightarrow \mathcal{N}(\mathscr{P}_N) \longrightarrow \mathcal{N}(\mathscr{P}_N)/\mathscr{P}_N \longrightarrow 1. \tag{2.41}$$

Using Theorem 2.4.1, and the above results, we will construct a new short exact sequence and prove that it has a splitting homomorphism. Let us consider the sequence

$$1 \longrightarrow \mathbb{Z}_N \times \mathbb{Z}_N \xrightarrow{\beta} \mathcal{N}(\mathscr{P}_N) \xrightarrow{\alpha} SL(2, \mathbb{Z}_N) \longrightarrow 1, \tag{2.42}$$

where

$$\beta((i,j)) = Ad_{Q^i P^j} \quad \forall i, j \in \mathbb{Z}_N \tag{2.43}$$

and

$$\alpha(\psi) = \Phi \circ p(\psi) \quad \forall \psi \in \mathcal{N}(\mathscr{P}_N), \tag{2.44}$$

where Φ is the isomorphism $\Phi : \mathcal{N}(\mathscr{P}_N)/\mathscr{P}_N \to SL(2,\mathbb{Z}_N)$ and $p : \mathcal{N}(\mathscr{P}_N) \to \mathcal{N}(\mathscr{P}_N)/\mathscr{P}_N$ is the projection. We see that β is a injective and $\alpha = \Phi \circ p$ is surjective. It follows from the definitions of α and β that Im β = Ker α, thus (2.42) is indeed a short exact sequence.

We would like to define a map $\gamma : SL(2,\mathbb{Z}_N) \to \mathcal{N}(\mathscr{P}_N)$ by its action on the generators of $SL(2,\mathbb{Z}_N)$, for example

$$\gamma\left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\right) = \mathrm{Ad}_D, \quad \gamma\left(\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\right) = \mathrm{Ad}_F,$$

and prove that

$$\alpha \circ \gamma = id_{SL(2,\mathbb{Z}_N)}. \tag{2.45}$$

However, it is not even clear if such map is well-defined, since there are multiple ways how to express elements of $\mathscr{N}(\mathscr{P}_N)$ in terms of its generators $\mathrm{Ad}_F, \mathrm{Ad}_D, \mathrm{Ad}_P$ and Ad_Q. Furthermore, by checking the smallest non-trivial group $SL(2,\mathbb{Z}_2)$, we see that if such γ could be defined, is would not be a homomorphism, since

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

is of order 2 and $\gamma\left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\right) = \mathrm{Ad}_{D_2}$ is of order 4, so γ does not preserve multiplication. In the next chapter, we explore different possibilities of defining D_N and ask whether these can be used to construct the splitting homomorphism.

We conclude this chapter with calculating the order of $SL(2,\mathbb{Z}_N)$. Let

$$N = p_1^{k_1} p_2^{k_2} p_3^{k_3} \ldots p_r^{k_r}$$

be the prime decomposition of N, where $p_1, p_2, p_3, \ldots, p_r$ are prime numbers and $k_i \in \mathbb{N}$ for all $i \in \widehat{r}$. Then

$$|SL(2,\mathbb{Z}_N)| = N^3 \prod_{i=1}^{r} \left(1 - \frac{1}{p_i^2}\right). \tag{2.46}$$

The orders of $\mathcal{P}_N$ and $SL(2,\mathbb{Z}_N)$ for small N are given in the following table (see [6]).

N	$\vert\mathcal{P}_N\vert$	$\vert SL(2,\mathbb{Z}_N)\vert$
2	4	6
3	9	24
4	16	48
5	25	120
6	36	144
7	49	336
8	64	384

Chapter 3

Lifts of the restricted Clifford group to $U(N)$

3.1 Non-uniqueness of the phase transformation D_N

In this section, we explore various ways in which one can define the phase transformation D_N. In previous chapters we discovered that the group $\mathcal{N}(\mathscr{P}_N)/\mathscr{P}_N$ is generated by $\mathrm{Ad}_{F_N}, \mathrm{Ad}_{D_N}$ which are spanned by the equivalence classes of the matrices F_N and D_N in the restricted Clifford group $C(N)$. F_N and D_N satisfy the equations

$$F_N P_N F_N^{-1} = Q \quad \text{and} \quad F_N Q_N F_N^{-1} = P_N^{-1} \tag{3.1}$$

and

$$D_N Q_N D_N^{-1} = \mu Q_N \quad \text{and} \quad D_N P_N D_N^{-1} = \nu P_N Q_N, \tag{3.2}$$

where $|\mu| = |\nu| = 1$. For the sake of clarity, we will omit the subscript N in parts of the following text.

By means of determinants, we find that $\mu^N = 1$ and $\nu^N \det(Q) = \nu^N \omega^{\sum_{k=1}^{N-1} k} = \nu^N \omega^{\frac{1}{2}N(N-1)} = 1$, i.e.

$$\nu^N = \omega^{\frac{1}{2}N(1-N)}. \tag{3.3}$$

Since DQD^{-1} should belong to $H(N)$, we see that $\mu = \omega^i$ for some $i \in \mathbb{Z}_N$. Using this fact the equations (3.2) can be simplified. Consider the matrix $\tilde{D} = DP^i$, which belongs to the same equivalence class as Ad_D in the group $\mathcal{N}(\mathscr{P}_N)$. The first equation gives

$$\tilde{D} Q \tilde{D}^{-1} = DP^i QP^{-i} D^{-1} = \omega^{-i} DQD^{-1} = Q. \tag{3.4}$$

The second in (3.2) equation is invariant with respect to this choice:

$$\tilde{D} Q \tilde{D}^{-1} = DP^i PP^{-i} D^{-1} = D^{-1} PD = \nu PQ. \tag{3.5}$$

Therefore we can consider just the case $\mu = 1$ and all other cases can be derived from this one by applying the above transformation.

The first equation in (3.2) now reads $DQD^{-1} = Q$. Since Q is a diagonal matrix with distinct elements on the diagonal, it follows that D must be a diagonal matrix as well. Let us designate its elements by $D_{ij} = d_i\delta_{ij}$, where $i, j \in \mathbb{Z}_N$.

We write the matrix elements of the second equation in (3.2):

$$\sum_{k\in\mathbb{Z}_N} d_i\delta_{ik}\ \delta_{k,j-1} = \nu \sum_{k,l\in\mathbb{Z}_N} \delta_{i,k-1}\ \omega^k\delta_{k,l}\ d_l\delta_{lj} \tag{3.6}$$

$$d_i\delta_{i,j-1} = \nu d_j\omega^j\delta_{i,j-1} \tag{3.7}$$

$$d_{i+1} = \nu^{-1}d_i\omega^{-i} \tag{3.8}$$

for all matrix elements in $i, j \in \mathbb{Z}_N$. Equation (3.8) is a recurrence relation starting at $i = 0$ with the initial condition $d_N = d_0$. Since D is a diagonal unitary matrix, we must choose the starting point as $d_0 = \exp(i\varphi), \varphi \in \mathbb{R}$. Solving this recurrence is easy, for example by induction we find that $d_k = \exp(i\varphi)\nu^{-k}\omega^{\frac{-k}{2}(k+1)}$ for all $k \in \mathbb{Z}_N$. The initial condition $d_0 = d_N$ is fulfilled because of the equation (3.3):

$$d_N = \exp(i\varphi)\nu^{-N}\omega^{\frac{-N}{2}(N+1)} = \exp(i\varphi)\omega^{\frac{N}{2}(N-1)}\omega^{\frac{-N}{2}(N+1)} = \exp(i\varphi)\omega^{-N} = \exp(i\varphi) = d_0. \tag{3.9}$$

This gives us the final result

$$D = e^{i\varphi}\text{diag}\ (1, \nu^{-1}\omega^{-1}, \nu^{-2}\omega^{-3}, ..., \nu^{-k}\omega^{\frac{-1}{2}k(k+1)}, ..., \nu^{-N+1}\omega^{\frac{-1}{2}N(N-1)}), \tag{3.10}$$

where ν is some solution of (3.3) and $\varphi \in \mathbb{R}$.

Now we proceed to solve the equation (3.3). First, we consider the case of odd N, i.e. $N = 2k + 1, k \in \mathbb{N}$. We get

$$\nu^{2k+1} = \omega^{\frac{1}{2}(2k+1)(1-2k-1)} = \omega^{-k(2k+1)} = (\omega^{(2k+1)})^{-k} = 1^{-k} = 1, \tag{3.11}$$

hence $\nu^N = 1$, i.e. $\nu = \exp(\frac{2\pi im}{N}) = \omega^m$ where $m = 0, 1, 2, ..., N - 1$.

Second, we consider the case of even N, i.e. $N = 2k, k \in \mathbb{N}$. We obtain

$$\nu^{2k} = \omega^{\frac{1}{2}2k(1-2k)} = \omega^{k-2k^2} = \omega^k(\omega^{-2k})^k = \omega^k 1^k = \omega^k = -1, \tag{3.12}$$

thus $\nu^N = \omega^{\frac{N}{2}} = -1$, i.e. $\nu = \sqrt{\omega}\exp(\frac{2\pi im}{N}) = \sqrt{\omega}\omega^m$, where $m = 0, 1, 2, ..., N - 1$.

These results explain why the Weyl-Heisenberg group $H(N)$ had to be defined differently for N odd and N even in Definition 2.1.1. Namely, ν in equation (3.2) should belong to $H(N)$ by definition of the Clifford group.

3.2 Order of the phase transformation D_N

Theorem 3.2.1. *Let $\varphi = 0$. Then D is of order N for N odd and D is of order $2N$ for N even.*

Proof. Order of D is equal to $r \in \mathbb{N}$ if and only if r is the smallest natural number such that $d_k^r = 1$ for all $k \in \mathbb{Z}_N$, i.e. $\nu^{-rk}\omega^{\frac{-1}{2}rk(k+1)} = 1$ for all $k \in \mathbb{Z}_N$. First, we examine the case of N odd, where $\nu = exp(\frac{2\pi im}{N})$, where $m = 0, 1, 2, ..., N-1$ is given. A system of equivalent modular equations is obtained:

$$mkr + \frac{1}{2}k(k+1)r = 0 \mod N \quad \text{for all} \quad k \in \mathbb{Z}_N. \tag{3.13}$$

We write the same equation for $k+1$ and then subtracting the k-th equation. We get

$$mr + \frac{1}{2}r(k^2 + 3k + 2 - k^2 - k) = mr + kr + r = 0 \mod N. \tag{3.14}$$

By choosing $k = 1$ in (3.13) we see that $(m+1)r = 0 \mod N$, therefore by subtracting again, the final system of equations $kr = 0 \mod N, k \in \mathbb{Z}_N$ is obtained. The smallest natural solution is $r = N$, since there exists $k \in \mathbb{Z}_N$ such that $\gcd(k, N) = 1$. Conversely, $r = N$ satisfies (3.13) for all $k \in \mathbb{Z}_N$ and all possible choices of m.

Second, we examine the case of N even, where

$$\nu = \sqrt{\omega}\exp\left(\frac{2\pi im}{N}\right) = \exp\left(\frac{2\pi i}{N}(m + \frac{1}{2})\right).$$

Analogously, we obtain

$$2\left((m + \frac{1}{2})kr + \frac{1}{2}k(k+1)r\right) = 0 \mod 2N \quad \text{for all} \quad k \in \mathbb{Z}_N. \tag{3.15}$$

We proceed in the same fashion by writing the same equation for $k+1$ and then subtracting the k-th equation. We get

$$(2m+1)r + 2(k+1)r = (2m + 2k + 3)r = 0 \mod 2N. \tag{3.16}$$

By choosing $k = 0$ in equation (3.16), we see that $(2m+3)r = 0 \mod 2N$ which implies $2kr = 0 \mod 2N$ for all $k \in \mathbb{Z}_N$, therefore $(2m+1)r = 0 \mod 2N$ for any arbitrary choice of m. The smallest natural solution is $r = 2N$, since there exists $m \in \mathbb{Z}_N$ such that $\gcd(m, 2N) = 1$. Conversely, one can easily verify that $r = 2N$ is a solution of (3.15). $\square$

A special case of this theorem has been proven in [8].

3.3 Lifts of the Restricted Clifford group

Definition 3.3.1. *The lift of the restricted Clifford group in dimension N into the group $U(N)$ is the group $\mathcal{C}_N$ generated by the matrices P_N, Q_N, S_N, D_N, i.e.*

$$\mathcal{C}_N = \langle P_N, Q_N, F_N, D_N \rangle, \tag{3.17}$$

where D_N is given by equation (3.10) with $\varphi = 0$.

We see that in dimension N, there are N lifts of $C(N)$.

Remark 3.3.1. *$\mathcal{C}_N$ is a finite subgroup of $\mathcal{N}_{U(N)}(H(N))$.*

Remark 3.3.2. *Since $Q_N = F_N P_N F_N^3$, we see that $\mathcal{C}_N = \langle P_N, F_N, D_N \rangle$.*

Remark 3.3.3. *We see that $\mathrm{Ad}(\mathcal{C}_N) = \mathcal{N}(\mathscr{P}_N) \cong C(N)$.*

Remark 3.3.4. *The centre of the Weyl-Heisenberg group $Z(H(N))$ is equal to the centre of $\mathcal{C}_N$.*

Theorem 3.3.1. *$H(N)$ is a normal subgroup of $\mathcal{C}_N$.*

Proof. For N odd, it is sufficient to prove that $\omega_N I_N \in \mathcal{C}_N$. Using the commutation relation 1.2, we have

$$P_N Q_N P_N^{N-1} Q_N^{N-1} = \omega_N I_N,$$

so all elements of $H(N) = \{\omega_N^i Q^j P_N^k | i,j,k = 0,1,2,...,N_1\}$ can be generated by the matrices P_N and Q_N.

For N even, we have $\omega_N^{N/2} = -1$. In this case, ω_N can be generated by P_N and Q_N in the same manner as above. Furthermore, we utilise the matrix D_N:

$$D_N P_N D_N^{2N-1} P_N^{N-1} Q_N^{N_1} = \nu_N I_N. \tag{3.18}$$

We can choose $\nu_N = \exp(\pi i/N)$ and generate $\tau_N = (-1)\nu_N$ using the matrices P_N, Q_N and D_N.

Since $H(N)$ is normal in $N_{U(N)}(H(N))$ and $\mathcal{C}_N$ is a subgroup of $N_{U(N)}(H(N))$ which contains $H(N)$, we have $H(N) \lhd \mathcal{C}_N$ □

For $N = 2$, we can generate the whole group $\mathcal{C}_2$ just using matrices F_2 and D_2. Since

$$F_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad D_2 = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix},$$

we can easily see that $D_2^2 = Q_2$ and since $F_2^{-1} = F_2$, we have $F_2 D_2^2 F_2 = P_2$. Moreover, there are only two possible choices for D_2, namely

$$D_2^{(1)} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \quad \text{and} \quad D_2^{(2)} = (D_2^{(1)})^3 \begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix}, \tag{3.19}$$

we reach the conclusion that this is true for all possible choices of D_2. Similar result holds for odd N, but the matrices P_N and Q_N are constructed in a different way and using just one specific choice of D_N [8]. To prove this statement, we need the following lemma.

Lemma 3.3.1. *For N odd and $\nu = 1$, it holds that $Q \in \langle F_N, D_N \rangle$.*

Proof. In this proof we shall omit the subscript N. Since $D_{ij} = d_i\delta_{ij}$ and $F^2_{ij} = \delta_{i,-j}$, we have

$$[F^2, D]_{ij} = (F^2DF^2D^{-1})_{ij} = \sum_{k,l,m\in\mathbb{Z}_N} \delta_{i,-k}d_k\delta_{kl}\delta_{l,-m}d_m^{-1}\delta_{mj} = \tag{3.20}$$

$$= \sum_{l\in\mathbb{Z}_N} d_l d_j^{-1}\delta_{i,-l}\delta_{l,-j} = d_{-j}d_j^{-1}\delta_{ij} \tag{3.21}$$

for all $i, j \in \mathbb{Z}_N$. We know that $d_j = \nu^j\omega^{\frac{j}{2}(j+1)}$ for all $j \in \mathbb{Z}_N$, so

$$d_{-j}d_j^{-1} = \nu^{-j}\omega^{\frac{-j}{2}(-j+1)}(\nu^j\omega^{\frac{j}{2}(j+1)})^{-1} = \nu^{-2j}\omega^{\frac{j}{2}(1-j)-\frac{j}{2}(j+1)} = \nu^{-2j}\omega^{-j}. \tag{3.22}$$

N is an odd number, so $\nu = 1$ can be chosen and thus $[F^2, D]_{ij} = \omega^{-j}\delta_{ij} = Q^{-1}_{ij}$. Thus we have $Q = [F^2, D]^{-1} = [D, F^2] = DF^2D^{N-1}F^2$. □

Theorem 3.3.2. *For N odd, there exists a lift $\mathcal{C}_N$ such that $\mathcal{C}_N = \langle F_N, D_N\rangle$.*

Proof. F_N is of order 4, so using Lemma 3.3.1, we have

$$D_NF_N^2D_N^{N-1}F_N^2 = Q_N, \quad F_NQ_NF_N^3 = P_N. \tag{3.23}$$

Thus we have managed to generate both Q_N and P_N using only F_N and D_N. □

3.4 Lifts and semidirect products

Theorem 3.2.1 implies that a map $\gamma : SL(2, \mathbb{Z}_N) \to \mathcal{N}(\mathscr{P}_N)$ defined on the generating set of $SL(2, \mathbb{Z}_N)$ in the same manner as in equation (2.4), i.e.

$$\gamma\left(\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\right) = \mathrm{Ad}_D, \quad \gamma\left(\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}\right) = \mathrm{Ad}_F,$$

cannot preserve multiplication in even dimensions $N = 2k, k \in \mathbb{N}$. The sufficient condition for γ to be a homomorphism in even dimensions is that there exists a lift of $C(N)$ into $U(N)$ such that its generators satisfy the same relations as the generators of $SL(2, \mathbb{Z}_N)$ up to a phase factor.

This approach would result in a construction of a projective unitary representation of the group $SL(2, \mathbb{Z}_N)$ on the vector space $\mathbb{C}^N$. The defining relations of $SL(2, \mathbb{Z}_N)$ using the above matrices are known for $N = p^k$ where $p > 2$ is a prime number and $k \in \mathbb{N}$.

Theorem 3.4.1. *Let $A = \begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}$, $B = \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$ and let $N = p^k$ where $p > 2$ is a prime number and $k \in \mathbb{N}$. Then A, B satisfy the relations*

$$A^4 = 1, \quad B^N = 1, \quad (AB)^3 = A^2, \quad (AB^{\lambda^{-1}}AB^{\lambda})^3 = 1 \quad \text{and} \quad (AB^{\lambda^{-1}}AB^{2\lambda})^2 = A^2,$$

where λ is chosen such that λ and -1 generate the group of invertible integers modulo N, denoted $U(\mathbb{Z}_{p^k})$.

Proof. Proven in [9]. □

The advantage of this approach is that it is rather straightforward, but it is very complicated to actually verify the relations given in Theorem 3.4.1. However, to our knowledge the presentation of $SL(2, \mathbb{Z}_N)$ for odd N such that $N \neq p^k$ is not known, so this approach cannot be used in all cases.

In [10], a more general approach to the construction of a projective representation of $C(N)$ for odd N has been found, using the Pontryagin dual.

Definition 3.4.1. *Let G be a group. The Pontryagin dual $\overline{G}$ of G is the group of all homomorphisms $\chi : G \to U(1)$.*

Consider the group $\mathbb{Z}_N$, where N is odd. The Pontryagin dual $\overline{\mathbb{Z}_N}$ is the group of all homomorphisms $\chi_a : \mathbb{Z}_N \to U(1)$ of the form $\chi_a(k) = e^{\frac{2\pi i}{N}ka}$ for all $a, k \in \mathbb{Z}_N$ with multiplication defined by $\chi_a \chi_b = \chi_{a+b \mod N}$. We see that $\overline{\mathbb{Z}_N}$ is isomorphic to $\mathbb{Z}_N$.

Denote $K = \mathbb{Z}_N \times \overline{\mathbb{Z}_N}$. For each $k = (x, \chi) \in K$, we construct a unitary operator on the Hilbert space $\ell^2(\mathbb{Z}_N) = \mathbb{C}_N$ with the standard inner product defined by

$$W_k f(u) = \chi(u - \frac{1}{2}x) f(u - x) \quad \text{for all} \quad f \in \ell^2(\mathbb{Z}_N), u \in \mathbb{Z}_N, \tag{3.24}$$

where the vector $f(u)$ is defined as the u-th vector of the standard basis of $\mathbb{C}^N$, using the numbering starting with 0.

We see that

$$\begin{aligned} W_{(k,\chi_0)} f(u) &= f(u - k) \\ W_{(0,\chi_l)} f(u) &= e^{\frac{2\pi i}{N} l} f(u) = \omega_N^l f(u). \end{aligned}$$

for all $k, l, u \in \mathbb{Z}_N$, so in matrix form, these operators correspond to the matrices P_N^k and Q_N^l respectively. Using this construction, we obtained the Weyl-Heisenberg group as a representation of the direct product $\mathbb{Z}_N \times \mathbb{Z}_N$, called the Schrödinger representation.

Furthermore, it is suggested in [10] that using Mackey's theorem, we can construct a ray representation of $(\mathbb{Z}_N \times \mathbb{Z}_N) \rtimes SL(2, \mathbb{Z}_N)$ for odd N, called the Weil representation. This result gives the splitting homomorphism γ in the short exact sequence (2.42).

Chapter 4

Clifford groups of composite systems

4.1 Composite quantum systems

In this chapter, we examine Clifford groups of quantum systems where the state space $\mathscr{H} = \mathscr{H}_1 \otimes ... \otimes \mathscr{H}_k$ is a tensor product of Hilbert spaces of smaller dimension. Such quantum systems are called composite systems. We consider them to be composed of several simple systems, each with its own state space $\mathscr{H}_i$. We will denote the set $\{1, 2, 3, ..., k\}$ by $\widehat{k}$ for every $k \in \mathbb{N}$ and n_i will denote the dimension of $\mathscr{H}_i$ for every $i \in \widehat{k}$.

Let us recall the properties of the matrix tensor (Krönecker) product $\otimes$. Let $A, B \in M_k(\mathbb{C})$ and $C, D \in M_l(\mathbb{C})$, $\alpha \in \mathbb{C}$. Then

1. $(A \otimes C)(B \otimes D) = AB \otimes CD$
2. $\alpha(A \otimes C) = (\alpha A) \otimes C = A \otimes (\alpha C)$
3. $A \otimes C = I_{kl}$ if and only if there exists $\alpha \in \mathbb{C}, \alpha \neq 0$ such that $A = \alpha I_k$ and $C = \alpha^{-1} I_l$ (see [11]).

We define the Weyl-Heisenberg group of a composite system in a similar fashion as in the case of a simple system. Denote

$$H(n_1) \otimes ... \otimes H(n_k) := \{X_1 \otimes ... \otimes X_k | X_i \in H(n_i) \text{ for every } i \in \widehat{k}\}. \tag{4.1}$$

It is clear that $H(n_1) \otimes ... \otimes H(n_k)$ is a group isomorphic to the direct product $H(n_1) \times ... \times H(n_k)$.

Definition 4.1.1. *Let $n_1, ..., n_k \in N$. We define the Clifford group of a composite system consisting of Hilbert spaces of dimensions $n_1, ...n_k$ as the normalizer of $H(n_1) \otimes ... \otimes H(n_k)$ in the group $U(n_1 \cdots n_k)$. The restricted Clifford group of a composite system consisting* *of Hilbert spaces of dimension $n_1, ...n_k$ shall be denoted $C(n_1, ..., n_k)$ and is defined as the quotient*

$$C(n_1, ..., n_k) := \mathcal{N}_{U(n_1 \cdots n_k)}(H(n_1) \otimes ... \otimes H(n_k))/U(1). \tag{4.2}$$

We define an analogue of $\mathscr{P}_N$ for composite systems, as given in [11]:

Definition 4.1.2. *Let $n_1, ..., n_k \in \mathbb{N}$, $n_1...n_k = N$. We define*

$$\mathscr{P}_{(n_1,...,n_k)} = \{\mathrm{Ad}_{M_1 \otimes ... \otimes M_k} | M_i \in H(n_i)\}. \tag{4.3}$$

We denote the generators of the Weyl-Heisenberg group $H(n_1) \otimes ... \otimes H(n_k)$ by

$$A_{2i_1} = I_{n_1...n_i - 1} \otimes P_{n_i} \otimes I_{n_{i+1}...n_k}, \quad A_{2i} = I_{n_1...n_i - 1} \otimes Q_{n_i} \otimes I_{n_{i+1}...n_k} \tag{4.4}$$

*for $i \in \widehat{k}$ and the corresponding *-automorphisms*

$$e_j = \mathrm{Ad}_{A_j} \quad \text{for } j \in \widehat{2k}. \tag{4.5}$$

It follows from Theorem 1.3.3 that $\mathscr{P}_{(n_1,...,n_k)}$ is a MAD-group. Explicit proof for the bipartite case was given in [12].

4.2 The symmetry group $\mathrm{Sp}_{[n_1,...,n_k]}$

In this section, we define the symmetry group $\mathrm{Sp}_{[n_1,...,n_k]}$ as a matrix subgroup of $\mathcal{M}_{[n_1,...,n_k]}$, which is the endomorphism ring of $\mathbb{Z}_{n_1} \times ... \times \mathbb{Z}_{n_k}$, and examine its properties. This group shall be constructed in several steps. Through the remainder of this chapter, let $n_1, n_2, n_3, ..., n_k \in \mathbb{N}$ be fixed natural numbers and let $M_n(R)$ denote the ring of $n \times n$ matrices with entries from a given ring R. Our construction starts with the definition of a set of block matrices and follows the same steps as in [11].

Definition 4.2.1. *Let $\mathcal{M}_{[n_1,...,n_k]}$ be a set of $k \times k$ matrices H composed of 2×2 blocks*

$$H_{ij} = \frac{n_i}{\gcd(n_i, n_j)} A_{ij} \tag{4.6}$$

where $A_{ij} \in M_2(\mathbb{Z}_{n_i})$ for $i, j \in \widehat{k}$ are 2×2 matrices over $\mathbb{Z}_{n_i}$.

Definition 4.2.2. *We define the set*

$$\mathcal{S}_{[n_1,...,n_k]} = \left\{ H \in M_k(M_2(\mathbb{Z})) | A_{ij} \in M_2(\mathbb{Z}); H_{ij} = \frac{n_i}{\gcd(n_i, n_j)} A_{ij}; i, j \in \widehat{k} \right\}. \tag{4.7}$$

Using a special matrix

$$D = \mathrm{diag}\ (\frac{\mathrm{lcm}(n_1, ..., n_k)}{n_1} I_2, ..., \frac{\mathrm{lcm}(n_1, ..., n_k)}{n_k} I_2) \tag{4.8}$$

we define an equivalence $\equiv$ *on* $\mathcal{S}_{[n_1,...,n_k]}$*:*

$$H \equiv G \;\Leftrightarrow\; DH \equiv_{\mathrm{lcm}(n_1,...,n_k)} DG, \quad \text{where } H, G \in \mathcal{S}_{[n_1,...,n_k]}. \tag{4.9}$$

Furthermore, let $H \in \mathcal{S}_{[n_1,...,n_k]}$ *consist of elements* $H_{ij} = \frac{n_i}{\gcd(n_i,n_j)} A_{ij}$*, where* $A_{ij} \in M_2(\mathbb{Z}_{n_i})$*. The adjoint element* H^* *of* H *is defined by*

$$(H^*)_{ij} = \frac{n_i}{\gcd(n_i,n_j)} A^T_{ji}. \tag{4.10}$$

For convenience, we denote $\ell = \mathrm{lcm}(n_1, ..., n_k)$*.*

The above definitions imply the following properties of $\mathcal{M}_{[n_1,...,n_k]}$: let $a, b, d, n \in \mathbb{Z}, d|n$. Then the congruence $\frac{n}{d}a = \frac{n}{d}b$ is equivalent to $a \equiv b \mod d$, so we see that $\mathcal{M}_{[n_1,...,n_k]} = \mathcal{S}_{[n_1,...,n_k]}/_{\equiv}$.

Let $i, j, m \in \widehat{k}$. Then $\frac{n_i}{\gcd(n_i,n_j)} | \frac{n_i}{\gcd(n_i,n_m)} \frac{n_m}{\gcd(n_m,n_j)}$. Indeed $\gcd(n_m, n_j) \cdot \gcd(n_i, n_m)$ divides both $n_i n_m$ and $n_j n_m$, hence $\gcd(n_j, n_m) \cdot \gcd(n_i, n_m)$ divides

$$\gcd(n_i n_m, n_j n_m) = n_m \gcd(n_i, n_j),$$

giving

$$\frac{n_m \gcd(n_i, n_j)}{\gcd(n_i, n_m) \gcd n_j, n_m} \in \mathbb{Z}.$$

Using the above observations, we get that $\mathcal{S}_{[n_1,...,n_k]}$ is a subring of $M_k(M_2(\mathbb{Z}))$. It is easy to verify that $DH = (H^*)^T D$ for every $H \in \mathcal{S}_{[n_1,...,n_k]}$.

Next, we prove that $\equiv$ is a ring congruence on $\mathcal{S}_{[n_1,...,n_k]}$, which implies that $\mathcal{M}_{[n_1,...,n_k]}$ is a ring with respect to the usual matrix multiplication and addition. It is enough to prove that $\mathcal{I} := \{H \in \mathcal{S}_{[n_1,...,n_k]} | H \equiv 0\}$ is an ideal in $\mathcal{S}_{[n_1,...,n_k]}$ and the rest is obvious. Let $G, H \in \mathcal{S}_{[n_1,...,n_k]}$ and $H \in \mathcal{I}$. Then $DH \equiv_\ell 0$, so $D(GH) \equiv_\ell (G^*)^T(DH) \equiv_\ell 0 \Rightarrow GH \in \mathcal{I}$.

Furthermore, $\mathcal{M}_{[n_1,...,n_k]}$ has a natural action on the group $\mathbb{Z}^2_{n_1} \times ... \times \mathbb{Z}^2_{n_k}$ via the matrix multiplication. Clearly, $\mathbb{Z}^2_{n_1} \times ... \times \mathbb{Z}^2_{n_k}$ can be viewed as $\mathbb{Z}^{2k}$ factorised by the following equivalence:

$$x \equiv y \Leftrightarrow Dx \equiv_\ell Dy, \quad x, y \in \mathbb{Z}^{2k}. \tag{4.11}$$

It is sufficient to show that $H \equiv G$ and $x \equiv y$ imply that $Hx \equiv Gy$ for $G, H \in \mathcal{S}_{[n_1,...,n_k]}$ and $x, y \in \mathbb{Z}^{2k}$. Let $DH \equiv_\ell DG$ and $Dx \equiv_\ell Dy$. Then $DHx \equiv_\ell (DG)x \equiv_\ell (G^*)^T(Dx) \equiv_\ell (G^*)^T(Dy) \equiv_\ell DGy$, and thus $Hx \equiv Gy$. Finally, we observe that $\mathcal{M}_{[n_1,...,n_k]}$ is a finite set of matrices closed under usual matrix multiplication containing the unit matrix, i.e. it is a finite monoid.

Properties of the adjoint operation $*$ defined above mean that $\mathcal{S}_{[n_1,...,n_k]}$ and $\mathcal{M}_{[n_1,...,n_k]}$ are involutive rings, also called *-rings. Indeed, let $H, G \in \mathcal{S}_{[n_1,...,n_k]}$. It is easy to see that $(H^*)^* = H$ and $(H+G)^* = H^*+G^*$. Now let $H_{ij} = \frac{n_i}{\gcd(n_i,n_j)} A_{ij}$ and $G_{ij} = \frac{n_i}{\gcd(n_i,n_j)} B_{ij}$,

$A_{ij}, B_{ij} \in M_2(\mathbb{Z})$ for all $i, j = 1, ..., k$. Then

$$(G^*H^*)_{ij} = \sum_{l=1}^{k} \frac{n_i}{\gcd(n_i, n_l)} \frac{n_l}{\gcd(n_l, n_j)} B_{li}^T A_{jl}^T =$$

$$= \frac{n_i}{\gcd(n_i, n_j)} \sum_{l=1}^{k} \frac{n_l \gcd(n_i, n_j)}{\gcd(n_i, n_l) \gcd(n_l, n_j)} (A_{jl} B_{li})^T = (HG)^*_{ij},$$

so $(HG)^* = G^*H^*$. We shall prove that the operation $*$ is well-defined on $\mathcal{M}_{[n_1,...,n_k]}$. Let $DH \equiv_\ell DG$. Then $DH^* \equiv_\ell H^T D \equiv_\ell G^T D \equiv_\ell DG^*$, so $H^* \equiv G^*$. Now we proceed to the definition of $\mathrm{Sp}_{[n_1,...,n_k]}$.

Definition 4.2.3. *Denote* $J = \mathrm{diag}\ (J_2, ..., J_2) \in \mathcal{M}_{[n_1,...,n_k]}$ *where* $J_2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. *Put* $\mathrm{Sp}_{[n_1,...,n_k]} = \{H \in \mathcal{M}_{[n_1,...,n_k]} | H^*JH = J\}$.

Lemma 4.2.1. *Let M be a finite monoid and let the map $x \mapsto x^*$ satisfy $(x^*)^* = x$ and $(xy)^* = y^*x^*$ for all $x, y \in M$. Let j be an element of M such that $j^*j = 1$. Then $G = \{x \in M | x^*jx = j\}$ is a group.*

Proof. We see that $1 \in G$. Let $x, y \in G$. Then $(xy)^*j(xy) = y^*(x^*jx)y = y^*jy = j$, hence $xy \in G$ and G is closed under multiplication. Since $j^*j = 1$, j has a left inverse j^* and therefore it is invertible, where $j^* = j^{-1}$. It can be easily verified that $j, j^* \in G$. For any $x \in G$, we have $x^*jx = j$, hence $(j^*x^*j)x = 1$. Thus x is invertible, $x^{-1} = j^*x^*j$ and $1 = xx^{-1} = xj^*x^*j$ which implies that $j^{-1} = j^* = xj^*x^*$. Applying the $*$ operation, we get $j = xjx^* = (x^*)^*jx^*$, so $x^* \in G$ and therefore $x^{-1} = j^*x^*j \in G$, so G forms a group. □

Remark 4.2.1. *It can be shown that $xjx^* = j$ implies $x^*jx = j$ and vice versa. By a similar argument as in the final part of the proof above, i.e. $G == \{x \in M | x^*jx = j\} = \{x \in M | xjx^* = j\}$.*

Corollary 4.2.1. $\mathrm{Sp}_{[n_1,...,n_k]}$ *is a finite subgroup of the monoid* $\mathcal{M}_{[n_1,...,n_k]}$.

4.3 Characterization of the group $\mathrm{Sp}_{[n_1,...,n_k]}$

In this section, we are going to find the elements of $\mathrm{Sp}_{[n_1,...,n_k]}$ which generate the whole group in the same manner as in [11]. Note that

$$SL(2, \mathbb{Z}_{n_1}) \times ... \times SL(2, \mathbb{Z}_{n_k}) \cong \{\mathrm{diag}\ (H_1, ..., H_k) | H_i \in M_2(\mathbb{Z}_{n_i}), \det H_i \equiv_{n_i} 1, i \in \widehat{k}\},$$

so we can consider $SL(2, \mathbb{Z}_{n_1}) \times ... \times SL(2, \mathbb{Z}_{n_k})$ to be naturally embedded into $\mathrm{Sp}_{[n_1,...,n_k]}$.

Definition 4.3.1. *Let $\ell \in \mathbb{Z}$, $1 \leq i < j \leq k$. We define special matrices $G_{ij}(\ell) \in \mathcal{M}_{[n_1,\dots,n_k]}$ consisting of 2×2 blocks*

$$(G_{ij}(\ell))_{rs} = \begin{cases} I_2, & \text{if } r = s \\ \frac{n_r}{\gcd(n_r,n_s)}\ell \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, & \text{if } (r,s) = (i,j) \text{ or } (r,s) = (j,i) \\ 0, & \text{otherwise} \end{cases} \tag{4.12}$$

where $r, s \in \widehat{k}$.

Lemma 4.3.1. *$G_{ij}(\ell) = G_{ij}(1)^{\ell}$ for every $\ell \in \mathbb{Z}$ and $1 \leq i < j \leq k$. Furthermore $G_{ij}(1) \in \mathrm{Sp}_{[n_1,\dots,n_k]}$.*

Proof. First let us consider a permutation π of the set $\widehat{k}$. Clearly, it induces an isomorphism $\phi_\pi : \mathcal{M}_{[n_1,\dots,n_k]} \to \mathcal{M}_{[n_{\pi(1)},\dots,n_{\pi(k)}]}$. Obviously $H \in \mathrm{Sp}_{[n_1,\dots,n_k]} \Leftrightarrow \phi_\pi(H) \in \mathrm{Sp}_{[n_1,\dots,n_k]}$ for every $H \in \mathcal{M}_{[n_1,\dots,n_k]}$, so it is sufficient to show our assertion for G_{12} only. This is equivalent to the case $k = 1$, which was already proven in [12]. $\square$

Corollary 4.3.1. *Let $u = (a, b)^T \in \mathbb{Z}^2$. Then there exist $A, B \in SL(2,\mathbb{Z})$ such that $Au = (0, \gcd(a, b))^T$ and $Bu = (\gcd(a, b), 0)^T$.*

Proof. We can assume that $u \neq 0$. Then there are $k, l \in \mathbb{Z}$ such that $ka + lb = \gcd(a, b)$. Let us denote $d = \gcd(a, b)$. Then we simply put

$$A = \begin{pmatrix} b/d & -a/d \\ k & l \end{pmatrix} \quad \text{and} \quad B = J_2 A, \tag{4.13}$$

thus concluding the proof. $\square$

Denote $\mathcal{G}$ the subgroup of $\mathrm{Sp}_{[n_1,\dots,n_k]}$ generated by $SL(2,\mathbb{Z}_{n_1}) \times \dots \times SL(2,\mathbb{Z}_{n_1})$ and $\{G_{ij}(1) | 1 \leq i < j \leq k\}$. We are aiming to prove that $\mathcal{G} = \mathrm{Sp}_{[n_1,\dots,n_k]}$. Some auxiliary results are needed.

Consider the elements of $\mathcal{S}_{[n_1,\dots,n_k]}$ as $k \times k$ matrices consisting of 2×2 blocks. Let Σ_k be the set of k-th columns of all the elements of $\mathcal{S}_{[n_1,\dots,n_k]}$ and similarly, let Σ_k^* be the set of k-th rows of all the elements of $\mathcal{S}_{[n_1,\dots,n_k]}$. We see that the involution $*$ on $\mathcal{S}_{[n_1,\dots,n_k]}$ induces a bijection $\Sigma_k \to \Sigma_k^*$.

The congruence $\equiv$ on $\mathcal{S}_{[n_1,\dots,n_k]}$ induces naturally equivalences on both Σ_k and Σ_k^*, so for $U, V \in \Sigma_k$ such that $U \equiv V$ and for $G, H \in \mathcal{S}_{[n_1,\dots,n_k]}$ such that $G \equiv H$ we have $U^* \equiv V^*$, $GU \equiv HV$ and, finally, $(GU)^* = U^*G^*$. Put $\Omega_k = \Sigma_k/_{\equiv}$ and $\Omega_k^* = \Sigma_k^*/_{\equiv}$. By the preceding observations, we have a well-defined map $\Omega_k \to \Omega_k^*$ induced by $*$ and a natural action of the ring $\mathcal{M}_{[n_1,\dots,n_k]}$ on the set Ω_k.

Lemma 4.3.2. *Let $U, V \in \Sigma_k, U \equiv V$ and $T, R \in \Sigma_k^*, T \equiv R$. Then $TU \equiv_{n_k} VR$.*

Proof. Clearly, there are $G, H \in \mathcal{S}_{[n_1,...,n_k]}$ such that U and V are last columns of G, respectively H and $G \equiv H$. Analogously, there exist $M, N \in \mathcal{S}_{[n_1,...,n_k]}$ such that T and R are the last columns of M, respectively N. Then TU, respectively VR is the block on the (k,k)-position of the matrix GM (or HN). By (4.11), we have $GM \equiv HN$ and thus $TU \equiv_{n_k} VR$. □

Now we define the set

$$\Delta_k = \{[U] \in \Omega_k | U^* J U \equiv_{n_k} J_2\}. \tag{4.14}$$

By Lemma 4.3.2, Δ_k is well-defined and using the above observations, it can be easily seen that Δ_k is invariant under the action of the group $\mathrm{Sp}_{[n_1,...,n_k]}$, since this action is a restriction of the action of $\mathcal{M}_{[n_1,...,n_k]}$ on the set Ω_k.

Definition 4.3.2. *Let G be a group acting on a non-empty set S. The action of G is called transitive, if given two elements $a, b \in S$ there exists $g \in G$ such that $b = g \cdot a$. Alternatively, we say that G acts transitively on S.*

Lemma 4.3.3. *$\mathcal{G}$ acts transitively on Δ_k.*

Proof. We will consider an element of Ω_k as an ordered pair of its columns, (v, u) where $u, v \in \mathbb{Z}_{n_1} \times ... \times \mathbb{Z}_{n_k}$. For $v^0 := (0, ..., 0, 1, 0)^T$ and $u^0 = (0, ..., 0, 0, 1)$, (v^0, u^0) belongs to Δ_k.

Now assume that some $(v, u) \in \Delta_k$ is given. To prove our assertion, we construct for some $n \in \mathbb{N}$ a sequence of pairs $(v, u) = (v_0, u_0), ..., (v_{n-1}, u_{n-1}), (v_n, u_n)$ in Δ_k ending with (v^0, u^0) and another sequence of matrices $H_1, ..., H_n$ in $\mathcal{G}$ such that $(v_{j+1}, u_{j+1}) = H_{j+1}(v_j, u_j)$ for $j = 0, 1, ..., n-1$. We denote $d_{(i,j)} = \frac{n_i}{\gcd(n_i, n_j)}$. We shall divide the proof into four steps.

1. By Corollary 4.3.1, there are $B_i \in SL(2, \mathbb{Z}_{n_i})$ for every $i \in \widehat{k}$ such that for $H_1 = \mathrm{diag}\ (B_1, ..., B_k) \in \mathcal{G}$ we have

$$u_1 := H_1 u = \Big((d_{(1,k)} a_1, 0), ..., (d_{(k,k)} a_k, 0) \Big)^T \quad \text{for some} \quad a_i \in \mathbb{Z}_{n_i}. \tag{4.15}$$

2. Let

$$v_1 := H_1 v = (d_{(1,k) b_1}, d_{(1,k) c_1}, ..., d_{(k,k)} b_k, d_{(k,k)} c_k)^T. \tag{4.16}$$

then by the definition of Δ_k, we have $\sum_{i=1}^k d_{(k,i)} d_{(i,k)} a_i c_i \equiv_{n_k} -1$. Put $H_2 = \mathrm{diag}\ (I_2, ..., I_2, B) \in \mathcal{G}$, where $B = \begin{pmatrix} 1 & 0 \\ c_k & 1 \end{pmatrix}$. Then

$$u_2 := H_2 u_1 = \Big((d_{(1,k)} a_1), ..., (d_{(k-1,k-1)} a_{k-1}, 0), (a_k, a_k c_k) \Big)^T. \tag{4.17}$$

By induction, on $1 \leq m \leq k-1$, we get that $H_{m+2} = G_{mk}(c_m)$. Next,

$$u_{m+2} := H_{m+2}u_{m+1} \tag{4.18}$$
$$= \left(..., (d_{(m+1,k)}a_{m+1}, 0), ..., (d_{(k-1,k)}a_{k-1}, 0), (a_k, a_k c_k + \sum_{i=0}^{m} d_{(k,i)}d_{(i,k)}a_i c_i)\right)^T, \tag{4.19}$$

so $u_{k+1} = (..., a_k, -1)^T$.

3. Using a similar argument as in the first step, we get that there exists some $H_{k+2} \in \mathcal{G}$ such that

$$u_{k+2} := H_{k+2}u_{k+1} = \left((0, d_{(1,k)}a'), ..., (0, d_{(k-1,k-1)}a'_k), (1, 0)\right)^T \tag{4.20}$$

for some $a'_i \in \mathbb{Z}_{n_i}$. Put $H_{k+3} = G_{1,k}(-a'_1) \cdots G_{k,k}(-a'_k) \in \mathcal{G}$. Then

$$u_{k+3} := H_{k+3}u_{k+2} = (0, ..., 0, 1, 0)^T. \tag{4.21}$$

4. Again, by a similar argument as in the first step, we get that there is $H_{k+4} \in \mathcal{G}$ satisfying

$$u_{k+4} := H_{k+4}u_{k+3} = (0, ..., 0, 1)^T \tag{4.22}$$

and

$$v_{k+4} := \left((0, d_{(1,k)}b'_1), ..., (0, d_{(k-1,k)}b'_{k-1}), (b', c')\right)^T \tag{4.23}$$

for some $b'_i \in \mathbb{Z}_{n_i}$ and $b', c' \in \mathbb{Z}_{n_k}$. If follows from definition of Δ_k that $b' \equiv_{n_k} 1$. Put $B' = \begin{pmatrix} 1 & 0 \\ -c' & 1 \end{pmatrix}$. Then for $H_{k+5} := \mathrm{diag}\ (I_2, ..., B') \in \mathcal{G}$, we get

$$u_{k+5} := H_{k+5}u_{k+4} = (0, ..., 0, 1)^T \tag{4.24}$$

and

$$v_{k+5} := H_{k+5}v_{k+4} = \left((0, d_{(1,k)}b'_1), ..., (0, d_{(k-1,k)}b'_{k-1}), (1, 0)\right)^T. \tag{4.25}$$

We arrive to an analogous situation to the third step, thus there exists $H_{k+6} \in \mathcal{G}$ such that the vector

$$u_{k+6} := H_{k+6}u_{k+5} = (0, ..., 0, 1)^T \tag{4.26}$$

stays unchanged, and $v_{k+6} := (0, ..., 0, 1, 0)^T$.

□

Lemma 4.3.4. *Let $H \in \mathcal{M}_{[n_1,\dots,n_{k-1}]}$ and assume $T \in \Sigma^*_{k-1}$ is such that $\begin{pmatrix} H & 0 \\ T & I_2 \end{pmatrix} \in \mathrm{Sp}_{[n_1,\dots,n_k]}$. Then $T = 0$ and $H \in \mathrm{Sp}_{[n_1,\dots,n_{k-1}]}$.*

Proof. Clearly, there exists $U \in \Sigma_k$ such that $T = U^*$. Then we get that

$$\begin{pmatrix} J & 0 \\ 0 & J_2 \end{pmatrix} = \begin{pmatrix} H^* & U \\ 0 & I_2 \end{pmatrix} \begin{pmatrix} J & 0 \\ 0 & J_2 \end{pmatrix} \begin{pmatrix} H & 0 \\ U^* & I_2 \end{pmatrix} = \begin{pmatrix} H^*JH + UJU^* & UJ_2 \\ J_2U^* & J_2 \end{pmatrix}. \tag{4.27}$$

Therefore we obtain $U^* = 0$ which implies $T = 0$. Thus $H^*JH = J$. $\square$

Theorem 4.3.1. *The group $\mathrm{Sp}_{[n_1,\dots,n_k]}$ is generated by $SL(2,\mathbb{Z}_{n_1}) \times \dots \times SL(2,\mathbb{Z}_{n_1})$ and $\{G_{ij}(1) | 1 \le i < j \le k\}$.*

Proof. Let $G \in \mathrm{Sp}_{[n_1,\dots,n_k]}$ and let $U \in \Sigma_k$ be its last column. Then $U \in \Delta_k$ and there is $A \in \mathcal{G}$ such that

$$AG = \begin{pmatrix} H & 0 \\ T & I_2 \end{pmatrix} \quad \text{for some} \quad H \in \mathcal{M}_{[n_1,\dots,n_{k-1}]} \quad \text{and} \quad T \in \Sigma^*_k. \tag{4.28}$$

Using Lemma 4.3.4, we have $T = 0$ and $H \in \mathrm{Sp}_{[n_1,\dots,n_{k-1}]}$. By repeating this procedure several times, we find $\tilde{A} \in \mathcal{G}$ such that $\tilde{A}G = I_{2k}$, thus $G = \tilde{A}^{-1} \in \mathcal{G}$ and $\mathcal{G} = \mathrm{Sp}_{[n_1,\dots,n_k]}$. $\square$

4.4 The normalizer of $\mathscr{P}_{(n_1,\dots,n_k)}$

In this section, we aim to completely describe the quotient group of the normalizer by the group $\mathscr{P}_{(n_1,\dots,n_k)}$. We will consider the matrices of $\mathcal{M}_{[n_1,\dots,n_{k-1}]}$ to be $2k \times 2k$ matrices instead of taking them as $k \times k$ matrices consisting of 2×2 blocks. First, we transcribe the definition of the group $\mathrm{Sp}_{[n_1,\dots,n_k]}$ into this new language and prove an auxiliary technical lemma [11].

Lemma 4.4.1. *Let $H = (h_{ij})_{i,j=1}^{2k} \in \mathcal{M}_{[n_1,\dots,n_k]}$, $h_{ij} = \frac{n_{\lceil i/2 \rceil}}{\gcd(n_{\lceil i/2 \rceil}, n_{\lceil j/2 \rceil})} a_{ij}$, $a_{ij} \in \mathbb{Z}_{n_{\lceil i/2 \rceil}}$ for $i,j \in \widehat{2k}$. Then $H \in \mathrm{Sp}_{[n_1,\dots,n_k]}$ if and only if*

$$\sum_{m=1}^{k} \frac{n_{\lceil i/2 \rceil}}{\gcd(n_m, n_{\lceil i/2 \rceil})} \frac{n_m}{\gcd(n_m, n_{\lceil j/2 \rceil})} (a_{2m-1,i}a_{2m,j} - a_{2m-1,j}a_{2m,i}) \equiv_{n_{\lceil i/2 \rceil}} w_{ij} \tag{4.29}$$

for every $i,j \in \widehat{2k}$, where $J_{ij} = w_{ij}; i,j \in \widehat{2k}$.

Proof. We only transcribe the equation $H^*JH = J$ using the definition of J. $\square$

Lemma 4.4.2. *For every endomorphism α of the ring $\mathbb{Z}^2_{n_1} \times \dots \times \mathbb{Z}^2_{n_k}$, there is a unique $H \in \mathcal{M}_{[n_1,\dots,n_k]}$ such that $\alpha(x) = Hx$ for every $x \in \mathbb{Z}^2_{n_1} \times \dots \times \mathbb{Z}^2_{n_k}$. The map $\Phi : \alpha \mapsto H$ is a ring homomorphism.*

Proof. Let $\{f_1, ..., f_{2k}\}$ be the canonical generating set of $\mathbb{Z}_{n_1}^2 \times ... \times \mathbb{Z}_{n_k}^2$. For every endomorphism α, there are $h_{ij} \in \mathbb{Z}$ such that $\alpha(f_j) = \sum_{i=1}^{2k} h_{ij} f_i$. The order of f_{2i-1} and f_{2i} is n_i for $i \in \widehat{k}$, so

$$1 = \alpha(n_i f_{2i-1}) = \sum_{j=1}^{2k} (n_i h_{j,2i-1}) f_j \tag{4.30}$$

for every $j \in \widehat{k}$. It follows that

$$\frac{n_i}{\gcd(n_i, n_j)} h_{2j-1,2i} \equiv_{n_j/\gcd(n_i,n_j)} 0 \quad \equiv_{n_j/\gcd(n_i,n_j)} \frac{n_i}{\gcd(n_i, n_j)} h_{2j,2i}. \tag{4.31}$$

We see that $h_{2j-1,2i}, h_{2j,2i} \in \frac{n_j}{\gcd(n_i,n_j)}\mathbb{Z}$ for every $j \in \widehat{k}$. Now consider h_{ij} modulo $n_{\lceil i/2 \rceil}$. Put $H = (h_{ij})_{i,j=1}^{2k} \in \mathcal{M}_{[}n_1, ...n_k]$ and the rest is easy. $\square$

The following notation will be used in the remainder of this chapter:

$$\mathcal{N}(\mathscr{P}_{(n_1,...,n_k)}) := \mathcal{N}_{\text{Aut }(M_{n_1...n_k}(\mathbb{C}))}(\mathscr{P}_{(n_1,...,n_k)})$$

and

$$\mathcal{N}(\mathscr{P}_n) := \mathcal{N}_{\text{Aut }(M_n(\mathbb{C}))}(\mathscr{P}_n).$$

Furthermore,

$$\mathcal{N}(\mathscr{P}_{n_1}) \times ... \times \mathcal{N}(\mathscr{P}_{n_k}) := \{\text{Ad}_{X_1 \otimes ... \otimes X_k} | X_i \in \mathcal{N}(\mathscr{P}_{n_i}), i \in \widehat{k}\}.$$

Let us consider the homomorphism $\Psi : \mathcal{N}(\mathscr{P}_{(n_1,...,n_k)}) \to \text{Aut } \mathscr{P}_{(n_1,...,n_k)}$, defined $\Psi(\text{Ad}_M)(\text{Ad}_X) := \text{Ad}_M \text{Ad}_X \text{Ad}_M^{-1}$ for every $M \in \mathcal{N}(\mathscr{P}_{(n_1,...,n_k)})$ and $X \in \mathscr{P}_{(n_1,...,n_k)}$. Obviously, Ker $\Psi = \mathscr{P}_{(n_1,...,n_k)}$. Put

$$\lambda_{ij} = \exp\left(2\pi i \frac{w_{ij}}{n_{\lceil i/2 \rceil}}\right) \tag{4.32}$$

for $i, j \in \widehat{2k}$, where w_{ij} are the entries of $J \in \text{Sp}_{[n_1,...n_k]}$. Using the commutation relations for the matrices P_{n_i} and Q_{n_i}, we obtain $A_i^m A_j^n = \lambda_{ij}^{mn} A_j^n A_i^m$ for all pairs $i, j \in \widehat{k}$ and $m, n \in \mathbb{Z}$.

Lemma 4.4.3. $\Phi \circ \Psi(\mathcal{N}(\mathscr{P}_{(n_1...n_k)})) \subseteq \text{Sp}_{[n_1,...n_k]}$.

Proof. See [11]. $\square$

Definition 4.4.1. *Let* $1 \leq i < j \leq k$. *Put*

$$T_{ij} = I_{n_{i+1}...n_{j-1}} \otimes Q_{n_j}^{\frac{n_j}{\gcd(n_i,n_j)}} \tag{4.33}$$

and

$$R_{ij} = I_{n_1...n_{i-1}} \otimes \text{diag }(I_{n_{i+1}...n_j}, T_{ij}, ..., T_{ij}^{n_i-1}) \otimes I_{n_{j+1}...n_k} \tag{4.34}$$

Lemma 4.4.4. *Let $1 \leq i < j \leq k$. Then $Ad_{R_{ij}} \in \mathcal{N}(\mathscr{P}_{(n_1 \ldots n_k)})$ and $\Phi \circ \Psi(Ad_{R_{ij}}) = G_{ij}(-1) \in \mathrm{Sp}_{[n_1,\ldots n_k]}$.*

Proof. See [11]. $\square$

In the case $k = 1$, denote $n_1 = n$. We obtain the already known result $\Phi \circ \Psi(\mathcal{N}(\mathscr{P}_n)) = SL(2, \mathbb{Z}_n)$. As an immediate consequence, we have the following corollary.

Corollary 4.4.1. $\Phi \circ \Psi(\mathcal{N}(\mathscr{P}_{n_1}) \times \ldots \times \mathcal{N}(\mathscr{P}_{n_k})) = SL(2, \mathbb{Z}_{n_1}) \times \ldots \times SL(2, \mathbb{Z}_{n_k})$.

Finally, we can prove the main theorems of this section [11].

Theorem 4.4.1. *The following statements hold:*

1. *$\mathcal{N}(\mathscr{P}_{(n_1,\ldots,n_k)})/\mathscr{P}_{(n_1,\ldots,n_k)} \cong \mathrm{Sp}_{[n_1,\ldots n_k]}$.*
2. *$\mathcal{N}(\mathscr{P}_{(n_1,\ldots,n_k)})$ is generated by $\mathcal{N}(\mathscr{P}_{n_1}) \times \ldots \times \mathcal{N}(\mathscr{P}_{n_k})$ and $\{Ad_{R_{ij}} | 1 \leq i < j \leq k\}$.*

Proof. We split the proof into two parts.

1. By Theorem 4.3.1, $\mathrm{Sp}_{[n_1,\ldots n_k]}$ is generated by $SL(2, \mathbb{Z}_{n_1}) \times \ldots \times SL(2, \mathbb{Z}_{n_k})$ and $\{G_{ij}(1) | 1 \leq i < j \leq k\}$. Thus, by Lemma 4.4.3, Lemma 4.4.4 and Corollary 4.4.1, we get that $\Phi \circ \Psi(\mathcal{N}(\mathscr{P}_{(n_1,\ldots,n_k)}))$. Using Lemma 4.4.2 and the observation that $\mathrm{Ker}\ \Psi = \mathscr{P}_{(n_1,\ldots,n_k)}$, we get that $\mathrm{Ker}\ \Phi \circ \Psi = \mathscr{P}_{(n_1,\ldots,n_k)}$. By the First Isomorphism Theorem, $\mathcal{N}(\mathscr{P}_{(n_1,\ldots,n_k)})/\mathscr{P}_{(n_1,\ldots,n_k)} \cong \mathrm{Sp}_{[n_1,\ldots n_k]}$.
2. Let N be the subgroup of $\mathcal{N}(\mathscr{P}_{(n_1,\ldots,n_k)})$ generated by the group $\mathcal{N}(\mathscr{P}_{n_1}) \times \ldots \times \mathcal{N}(\mathscr{P}_{n_k})$ and by the set $\{Ad_{R_{ij}} | 1 \leq i < j \leq k\}$. Then $\mathrm{Ker}\ \Phi \circ \Psi \subseteq \mathcal{N}(\mathscr{P}_{n_1}) \times \ldots \times \mathcal{N}(\mathscr{P}_{n_k}) \subseteq N$ and by Lemma 4.4.4, Corollary 4.4.1 and Theorem 4.3.1, $\Phi \circ \Psi(N) = \mathrm{Sp}_{[n_1,\ldots n_k]}$. Hence $N = \mathcal{N}(\mathscr{P}_{(n_1,\ldots,n_k)})$.

This concludes our proof. $\square$

Theorem 4.4.2. *There is a group $\mathcal{G}_{(n_1,\ldots,n_k)} \subseteq U(n_1 \ldots n_k)$ such that $\mathcal{N}(\mathscr{P}_{n_1 \ldots n_k}) = \{\mathrm{Ad}_M | M \in \mathcal{G}_{(n_1,\ldots,n_k)}\}$. The group $\mathcal{G}_{(n_1,\ldots,n_k)}$ is generated by the matrices*

$$\begin{gathered} I_{n_1 \ldots n_{i-1}} \otimes P_{n_i} \otimes I_{n_{i+1} \ldots n_k} \\ I_{n_1 \ldots n_{i-1}} \otimes Q_{n_i} \otimes I_{n_{i+1} \ldots n_k} \\ I_{n_1 \ldots n_{i-1}} \otimes D_{n_i} \otimes I_{n_{i+1} \ldots n_k} \\ I_{n_1 \ldots n_{i-1}} \otimes F_{n_i} \otimes I_{n_{i+1} \ldots n_k} \end{gathered}$$

for $i \in \widehat{k}$ and R_{ij} for $1 \leq i < j \leq k$.

Proof. Follows immediately from Theorem 4.4.1. $\square$

The above theorems describe the most general case of $\mathcal{N}(\mathscr{P}_{(n_1,\ldots,n_k)})/\mathscr{P}_{(n_1,\ldots,n_k)}$. Special cases have been studied before, for example in [13].

4.5 Short exact sequence for the restricted Clifford group of a composite system

In this section, we describe a short exact sequence for $C(n_1, ..., n_k)$. First, we need a correspondence between $C(n_1, ..., n_k)$ and $\mathcal{N}(\mathscr{P}_{(n_1,...,n_k)})$, given by the following theorem.

Theorem 4.5.1. *$C(n_1, ..., n_k)$ is isomorphic to $\mathcal{N}(\mathscr{P}_{(n_1,...,n_k)})$.*

Proof. Let X belong to $\mathcal{N}_{U(n_1 \cdots n_k)}(H(n_1) \otimes ... \otimes H(n_k))$. We define the map

$$\Xi : \mathcal{N}_{U(n_1 \cdots n_k)}(H(n_1) \otimes ... \otimes H(n_k)) \to \mathcal{N}(\mathscr{P}_{(n_1,...,n_k)})$$

by $\Xi(X) = \mathrm{Ad}_X$. First, we need to verify that Ξ is well-defined on the cosets $[X]$ for all elements of the Clifford group of the composite system. Indeed, let X and X' belong to the same equivalence class $[X] \in C(n_1, ..., n_k)$. Then $X' = e^{i\varphi}X, \varphi \in [0, 2\pi)$, so

$$\Xi(X) = \mathrm{Ad}_X = \mathrm{Ad}_{e^{i\varphi}X} = \Xi(e^{i\varphi}X) = \Xi(X'). \tag{4.35}$$

We omit the rest of the proof, since it is the same as the proof of Theorem 2.4.1, except replacing elements of $\mathscr{P}_N$ with elements of $\mathcal{N}(\mathscr{P}_{(n_1,...,n_k)})$. □

Now we come to the final result of this chapter. Let $\Lambda : \mathcal{N}(\mathscr{P}_{(n_1,...,n_k)})/\mathscr{P}_{(n_1,...,n_k)} \to \mathrm{Sp}_{[n_1,...n_k]}$ denote the isomorphism between these groups. It is easy to see that $\mathscr{P}_{(n_1,...,n_k)}$ is isomorphic to $(\mathbb{Z}^2_{n_1} \times ... \times \mathbb{Z}^2_{n_k})$, so $\beta : (\mathbb{Z}^2_{n_1} \times ... \times \mathbb{Z}^2_{n_k}) \to \mathcal{N}(\mathscr{P}_{(n_1,...,n_k)})$ given by

$$\beta((i_1, j_1, ..., i_k, j_k)) := \mathrm{Ad}_{Q^{i_1}_{n_1} P^{j_1}_{n_1} \otimes ... \otimes Q^{i_k}_{n_k} P^{j_k}_{n_k}} \tag{4.36}$$

for all $(i_1, j_1, ..., i_k, j_k) \in (\mathbb{Z}^2_{n_1} \times ... \times \mathbb{Z}^2_{n_k})$ is a monomorphism. Let $p : \mathcal{N}(\mathscr{P}_{(n_1,...,n_k)}) \to \mathcal{N}(\mathscr{P}_{(n_1,...,n_k)})/\mathscr{P}_{(n_1,...,n_k)}$ be the projection map. We define $\alpha : \mathcal{N}(\mathscr{P}_{(n_1,...,n_k)}) \to \mathrm{Sp}_{[n_1,...n_k]}$ as $\alpha = \Lambda \circ p$. It is surjective, because p is surjective and Λ is an isomorphism. We see that $\mathrm{Im}\ \beta = \mathscr{P}_{(n_1,...,n_k)} = \mathrm{Ker}\ \alpha$, hence we have a short exact sequence

$$1 \longrightarrow (\mathbb{Z}^2_{n_1} \times ... \times \mathbb{Z}^2_{n_k}) \xrightarrow{\beta} \mathcal{N}(\mathscr{P}_{(n_1,...,n_k)}) \xrightarrow{\alpha} \mathrm{Sp}_{[n_1,...n_k]} \longrightarrow 1. \tag{4.37}$$

If we wish to find a splitting homomorphism of the short exact sequence (4.37), we first need to be able to describe the short exact sequence for a simple system which seems to be an unsolved problem even in the case when all the subsystems have odd dimensions. This effort would require a definition of a lift of the restricted Clifford group of a composite system using all possible matrices which define the group $\mathcal{G}$ in Theorem 4.4.2.

Chapter 5

Applications of Clifford groups

5.1 Quantum computers and the Gottesman-Knill theorem

In this section, we give a brief overview of the relationship between Clifford groups and quantum computing. Quantum computation relies on the concept of quantum bit, or qubit for short. In a quantum computer, qubits are realized as physical systems, however for the sake of computation they are described as mathematical objects. The usefulness of this approach lies in the fact that it gives us the freedom to construct an abstract theory of quantum computation which does not depend on a concrete system for its realization.

Classical bit has two states, either 0 or 1, which correspond to electrical currents in their physical realization. Like a classical bit, qubit has a manifold of states. In analogy with the classical case, a qubit can be found in the states $|0\rangle$ and $|1\rangle$, which correspond to the states 0 and 1 of the classical bit. The difference between bits and qubits is that a qubit can be found in a state described by any complex linear combination of $|0\rangle$ and $|1\rangle$, often called superpositions [14]. The states $|0\rangle, |1\rangle$ are postulated to be linearly independent and are usually referred to as computational basis states. Put in another way, the state of a qubit is any one-dimensional subspace in the vector space $\mathbb{C}^2$.

We can examine a state of the classical bit in order to determine whether it is in the state of 0 or 1, computers do this whenever they read data from their memory. We cannot examine a qubit to determine its state, that is to find the values of α_0 and α_1 in the linear combination

$$|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$$

spanning the one-dimensional subspace describing the state. Instead, quantum mechanics tells us only probabilities. If we normalize $|\psi\rangle$ to length 1, then after performing a suitable measurements on a qubit, we can obtain either the result 0 with probability $|\alpha_0|^2$ or the result 1 with probability $|\alpha_1|^2$. Naturally, these probabilities must sum to 1. A simple generalization of this concept is the qudit, which is a quantum system with d basis states. Mathematically, we describe qudits by the vector space $\mathbb{C}^d$. The state of a qudit is described by a d-dimensional vector with unit norm.

Despite the strangeness of their behaviour, qubits exist in the physical world and their existence and behaviour have been validated by many experiments. There are many physical systems which can be used to realize qubits. These are, for example: two different polarizations of a photon, the alignment of a nuclear spin in a uniform magnetic field, the two spin states of a single electron orbiting a proton in a hydrogen atom etc. Naturally, much attention has been given to interpretation that might be associated with the superposition of states and the probabilistic nature of quantum mechanics.

Like a classical bit, a qubit can be used to store only a small amount of information. Recall that standard measurements on a qubit can yield only two results: either 0 or 1. Furthermore, measurement changes the state of a qubit, collapsing the superposition of states. After performing a measurement, qubit will be in the state that was measured. We conclude that a single qubit can store only one bit of information.

Even more interesting question to ask is how much information can be represented by a qubit if it is not measured? This might seem to be a nonsensical question, since how can one quantify information if it cannot be measured? Nevertheless, it seems that when we leave qubits to evolve naturally without measuring them, the information contained in all the continuous variables describing the state, like α_0 and α_1, is somehow stored. It can be shown that the potential amount of this extra hidden information grows exponentially with the number of qubits and it can be used to our benefit when performing calculations [14].

A quantum computer is a device which can perform operations on qubits in such a way that they can be used for performing the basic logical or mathematical operations. It is worth noting that quantum computers promise solving problems requiring exorbitant resources if they were to be solved by a classical computer. However, this requires the development of new quantum algorithms which appears to be a difficult problem, as there are many highly efficient classical algorithms. Hence a beneficial quantum algorithm must be faster than those available for classical computers. Taking the simplest system, the single qubit, we require that these operations preserve the norm, thus they are described by 2×2 unitary matrices. Some of the most important are the Pauli matrices

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{5.1}$$

and the phase gate D, the two-dimensional Fourier transformation (also called the Hadamard gate) and the $\pi/8$ gate (denoted T):

$$F_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad D = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 0 \\ 0 & \exp(\pi i/4) \end{pmatrix}. \tag{5.2}$$

These operations may be chained together in order to form quantum circuits, analogically to the way a classical computer performs logical operations to perform more complicated tasks. It can be shown that there exists a small universal set of operations (often called 'gates' in quantum computing language) that can be used to approximate any unitary

2×2 matrix with arbitrary accuracy. This theorem is a quantum version of the well-known construction of all possible logical operations from the gates AND, OR and NOT. There are several steps in the quantum analogue of this construction and they culminate with the proof that any unitary operation can be approximated to arbitrary accuracy using just the Hadamard, phase, $\pi/8$ and the CNOT gate, defined below:

$$\mathrm{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \tag{5.3}$$

The construction starts with a single qubit system, and it moves up to two-qubit systems by adding the CNOT gate. First, it is shown that the Hadamard, phase and $\pi/8$ gates can approximate any unitary operation on a single qubit and then the leap to two-qubit systems is made by proving that any unitary operation on two qubits may be expressed just using single-qubit operations and the CNOT gate. The proof of the general case for an arbitrary number of qubits is a more or less direct generalization of the above steps. It may appear at first that universal sets of gates are somehow connected to the group $C(N)$, but this is a coincidence, since there are many such small sets of universal quantum gates. The significance of this particular set lies in the familiarity most physicists have with this one, since it easy to perform calculations with it [14].

This construction says very little about efficiency, that is how many (polynomially or exponentially many) gates must be combined in order to create a given unitary transformation. There exist unitary transformation which require exponentially many gates to approximate. The goal of quantum computation is to find interesting sets of unitary transformations which can be performed efficiently and use them to perform calculations.

At this point, we know two classes of quantum algorithms which promise to solve problems which are practically unsolvable on classical computers. The first relies on Fourier transform and includes algorithms for solving factorization and discrete logarithm problems, providing exponential speedup over the best performing classical algorithms. The second class is based on Grover's algorithm for quantum searching. These provide a much less striking quadratic speedup over the classical ones.

Another important question which naturally arises is whether classical computers may be able to efficiently carry out calculations which will simulate the steps that quantum computer makes. The answer to this question is given by the Gottesman-Knill theorem [14].

Theorem 5.1.1 (Gottesman-Knill)**.** *Suppose a quantum computation is performed which involves only the following elements: state preparations in the computational basis, Hadamard gates, phase gates,* CNOT *gates, Pauli gates, and measurements of observables in the Pauli group (which includes measurement in the computational basis as a special case), together with the possibility of classical control conditioned on the outcome of such measurements. Such a computation may be efficiently simulated on a classical computer.*

This theorem basically states that all operations belonging to the Clifford group can be effectively simulated on a classical computer. It is interesting that a group which is constructed from simple mathematical operation on a group of matrices significant in physics does not, in fact, provide any benefit with regard to quantum computing.

The proof of the Gottesman-Knill theorem relies on the powerful stabilizer formalism of quantum computing [14]. The basic idea is that many quantum states can be more easily described by working with the operators whose action stabilizes them rather than the states themselves. Even more importantly, errors on the qubits and operations such as the Hadamard gate, the phase gate, the CNOT gate and the measurements in the computational basis are all easily described using this formalism. For example, if we take the state

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle), \tag{5.4}$$

we see that $\sigma_x \otimes \sigma_x|\psi\rangle = |\psi\rangle$ and $\sigma_z \otimes \sigma_z|\psi\rangle = |\psi\rangle$, that is $|\psi\rangle$ is stabilized by the operations $\sigma_x \otimes \sigma_x$ and $\sigma_z \otimes \sigma_z$. The usefulness of the stabilizer formalism lies in the clever use of group theory and its powerful tools.

The way in which the classical computer performs the simulation mentioned in the Gottesman-Knill theorem is simply to keep track of the generators of the stabilizer as the various operations are being performed during the computation. The Gottesman-Knill theorem highlights how subtle is the power of quantum computation. Of course, not all quantum computations can be described efficiently within the stabilizer formalism, but an impressive number may be.

We conclude that the significance of the Clifford group in quantum computing is that simple expanding it by a cleverly chosen unitary operation, we can obtain a new set of gates which cannot be efficiently simulated on a classical computer. It is in this sense a maximal known group which is not useful for quantum computing.

5.2 SIC-POVMs

SIC-POVM is an acronym for symmetric, informationally complete positive operator valued measure, which is a special type of quantum measurement. In quantum theory, measurements are represented by positive operator valued measures (POVMs). A POVM is called informationally complete, if its statistics determine the state on which the measurement is carried out. In order to be maximally efficient at determining the state, such measurement should also be of rank equal to one, i.e. the measurement operators should be positive multiples of projectors onto pure states (i.e. one-dimensional subspaces in the state space). Particularly interesting measurements are the ones which are symmetric, meaning that all pairwise inner products between the POVM elements are equal [15].

SIC-POVMs have been exactly described in dimensions $2-21$ and a few others; moreover numerical solutions have been calculated in every dimension up to 139 as well as a few higher ones [16]. This fact leads to the speculation that they might exist in every dimension. The proof for the existence of SIC-POVMs for arbitrary dimensions remains an open question, but is an ongoing field of research in the quantum information community. In this section, we give a definition of SIC-POVMs in finite dimension and describe some of their properties and their relation to Clifford groups [15].

Definition 5.2.1. *A SIC-POVM $\mathcal{S}$ in finite dimension N is a set of N^2 projectors $\{R_1, R_2, ..., R_{N^2}\} \subset M_N(\mathbb{C})$ of rank 1 satisfying*

$$\frac{1}{N}\sum_{j=1}^{N^2} R_i = I \tag{5.5}$$

$$\mathrm{Tr}(R_i R_j) = \frac{N\delta_{i,j}+1}{N+1} \quad \textit{for every} \quad i,j \in \widehat{N^2}. \tag{5.6}$$

Theorem 5.2.1. *The projectors $\{R_i\}$ constituting a SIC-POVM are linearly independent.*

Proof. Let us have a linear combination

$$\sum_{i=1}^{N^2} \alpha_i R_i = 0, \quad \alpha_i \in \mathbb{C}. \tag{5.7}$$

By applying the trace, we obtain

$$\sum_{i=1}^{N^2} \alpha_i \mathrm{Tr}(R_i) = \sum_{i=1}^{N^2} \alpha_i \mathrm{Tr}(R_i^2) = \sum_{i=1}^{N^2} \alpha_i = 0. \tag{5.8}$$

Let j be an arbitrary element of $\widehat{N^2}$. By multiplying equation (5.7) by R_j and calculating trace, we obtain

$$0 = \mathrm{Tr}(\sum_{i=1}^{N^2} \alpha_i R_i R_j) = \sum_{i=1}^{N^2} \alpha_i \mathrm{Tr}(R_i R_j) = \sum_{i=1}^{N^2} \alpha_i \frac{N\delta_{i,j}+1}{N+1} =$$
$$= \frac{1}{N+1}\left(N\alpha_j + \sum_{i=1}^{N^2} \alpha_i\right) = \frac{N}{N+1}\alpha_j.$$

Since j was arbitrarily chosen, $\alpha_j = 0$ for every $j \in \widehat{N^2}$, thus proving the theorem. ☐

We see that the complex linear combinations of projectors constituting a SIC-POVM span the whole algebra $M_N(\mathbb{C})$.

Corollary 5.2.1. *The condition that projectors $\{R_i\}$ satisfying $\frac{1}{N}\sum_{j=1}^{N^2} R_j = I$ have equal pairwise inner products for $i \neq j$ fixes the value of this constant and the value of the trace of every R_i.*

Proof. Set $\mathrm{Tr}(R_iR_j) = a$ for all $i \neq j$, where $i, j \in \widehat{N^2}$. We observe

$$N = \mathrm{Tr}(I^2) = \frac{1}{N^2}\sum_{i,j=1}^{N^2} \mathrm{Tr}(R_iR_j) = \frac{1}{N^2}\Bigg(\sum_{i=1}^{N^2} \mathrm{Tr}(R_i) + \sum_{\substack{i,j=1\\ i\neq j}}^{N^2} \mathrm{Tr}(R_iR_j)\Bigg) = \tag{5.9}$$

$$= \frac{1}{N^2}\Bigg(\mathrm{Tr}\big(\sum_{i=1}^{N^2} R_i\big) + N^2(N^2-1)a\Bigg) = \frac{1}{N^2}\big(N^2 + N^2(N^2-1)a\big) \tag{5.10}$$

and solving for a, we have $\mathrm{Tr}(R_iR_j) = \frac{1}{N+1}$. Now consider arbitrary $i \in \widehat{N^2}$. We have

$$\mathrm{Tr}(R_i) = \mathrm{Tr}(R_iI) = \frac{1}{N}\sum_{j=1}^{N^2} \mathrm{Tr}(R_iR_j) = \frac{1}{N}\mathrm{Tr}(R_i) + \sum_{\substack{j=1\\ i\neq j}}^{N^2} \frac{1}{N(N+1)}. \tag{5.11}$$

After a simple calculation, we get

$$\frac{N-1}{N}\mathrm{Tr}(R_i) = \frac{N^2-1}{N(N+1)} \quad \Rightarrow \quad \mathrm{Tr}(R_i) = 1. \tag{5.12}$$

Thus we can write $\mathrm{Tr}(R_iR_j) = \frac{N\delta_{i,j}+1}{N+1}$ for every pair i, j, since $\{R_i\}$ are projectors. □

Every known SIC-POVM has a group covariance property [16], i.e. there exists a group Sym $\mathcal{S}$ of unitary operators leaving the set of operators $\mathcal{S}$ invariant under conjugation and the action of Sym $\mathcal{S}$ on $\mathcal{S}$ is transitive. In detail, this means that

$$UR_sU^H = R_{\pi(s)} \tag{5.13}$$

for every $U \in$ Sym $\mathcal{S}$ and every $s \in \widehat{N^2}$, where π is some permutation of the set of integers $1, 2, ..., N^2$. The transitivity of the action means that in order to specify a given SIC-POVM, we need only to specify a single projector R, which shall be called the fiducial projector. Unit vector ψ such that $R\psi = \psi$ shall be called the fiducial vector.

It has been shown that in prime dimension, if a SIC-POVM has a group covariance property, then it is necessarily covariant with respect to the Weyl-Heisenberg group of that dimension [17]. It seems that with a single exception in dimension 8, SIC-POVMs are always covariant with respect to this group. In the following, we will use the term "SIC-POVM" to refer specifically to a SIC-POVM covariant with respect to the N-dimensional Weyl-Heisenberg group.

Let $X_{ab} = Q_N^a P_N^b$ for some natural number N. The necessary and sufficient condition for a rank 1 projector R to be the fiducial projector for a Weyl-Heisenberg covariant SIC-POVM is

$$\mathrm{Tr}(RX_{ab}) = \frac{e^{i\varphi_{a,b}}}{\sqrt{N+1}} \tag{5.14}$$

for all $(a, b) \in \mathbb{Z}_N \setminus (0, 0)$, where $\varphi_{a,b} \in [0, 2\pi)$ depends on $(a, b) \in \mathbb{Z}_N \times \mathbb{Z}_N$ [16].

The Clifford group plays an important role in this theory. By definition, for any element U in the Clifford group, R is a fiducial projector of a Weyl-Heisenberg invariant SIC-POVM, whenever URU^H is. Furthermore, the extended Clifford group is defined analogously, containing antiunitary operators in addition to the elements of the regular Clifford group. Fiducial projectors and SIC-POVMs form disjoint orbits under the action of the (extended) Clifford group. SIC-POVMs on the same orbit of the (extended) Clifford group are unitarily or antiunitarily equivalent.

The existence of SIC-POVMs and their relation to the Weyl-Heisenberg group are (at the time of writing this thesis) unsolved problems which appear to be connected to other yet unresolved questions in mathematics, namely Hilbert's twelfth problem (studied extensively in number theory). We conclude this section with an example of fiducial vector in dimension $N = 2$. Note that there are eight fiducial vectors, all lying in the same orbit, in dimension 2, generating two SIC-POVMs. One of the fiducial vectors is given by

$$\vec{x} = \begin{pmatrix} \sqrt{\frac{3+\sqrt{3}}{6}} \\ e^{i\pi/4}\sqrt{\frac{3-\sqrt{3}}{6}} \end{pmatrix}. \tag{5.15}$$

When represented on the Bloch sphere, the eight fiducial vectors constitute a cube, and the two SIC-POVMs enact two regular tetrahedra respectively, which are related to each other by space inversion. The Clifford group corresponds to the rotational symmetry group of the cube and the extended Clifford group is related to the full symmetry group of the cube [17].

5.3 Finite quantum oscillator

Elements of the Clifford group can be used to construct a discrete analogue of time evolutions of the quantum harmonic oscillator in finite configuration space where the configuration variable q lies in the group $\mathbb{Z}_N$ for some natural N. The state space is spanned by the base $(|q\rangle)_{q\in\mathbb{Z}_N}$.

In a similar way as in the usual quantum mechanics, we define the fundamental operators P and Q by

$$P|q\rangle = |q+1\rangle \quad Q|q\rangle = \omega_N|q\rangle. \tag{5.16}$$

We see that matrix representations of these operators are the matrices P_N and Q_N, respectively. They span the Pauli group in dimension N. The analogue of linear canonical transformations in this system is the group $\mathcal{N}(\mathcal{P}_N)$, because it permutes the group of operators generated by P and Q.

In this section, we carry over the usual definition of a linear harmonic oscillator to the finite phase space using the finite Fourier transformation, which is represented by the unitary matrix F_N in the basis $(|q\rangle)_{q\in\mathbb{Z}_N}$.

In continuous quantum mechanics, the Hamiltonian of the harmonic oscillator commutes with the Fourier-Plancherel operator and so does its propagator. The analogue of the evolution group of the harmonic oscillator in the finite phase space is, according to [18], the maximal abelian subgroup of the $\mathcal{N}(\mathcal{P}_N)$ commuting with Ad_{F_N}. The corresponding transformations are "rotations" of the finite phase space.

In the Hilbert space $\mathbb{C}^N$ these transformations are represented by a restriction of the so-called Weil representations. In [18], a simplified case was considered when N is a prime number of the form $N = 4K \pm 1$, where $K \in \mathbb{N}$.

Definition 5.3.1. *The evolution group $\mathcal{R} \leq \mathcal{N}(\mathcal{P}_N)$ is the group of all $\mathrm{Ad}_X \in \mathcal{N}(\mathcal{P}_N)$ commuting with Ad_F.*

Since $\mathcal{N}(\mathcal{P}_N) \cong SL(2, \mathbb{Z}_N)$, we shall carry out all calculations in $SL(2, \mathbb{Z}_N)$. Any element of $\mathcal{N}(\mathcal{P}_N)$ commutes with Ad_F if and only if its image in $SL(2, \mathbb{Z}_N)$ commutes with $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, i.e.

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, \mathbb{Z}_N). \tag{5.17}$$

After an easy calculation, it can be seen that the solution is

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}, \quad a^2 + b^2 = 1 \mod N, \quad \text{where} \quad a, b \in \mathbb{Z}_N. \tag{5.18}$$

The subgroup of $SL(2, \mathbb{Z}_N)$ satisfying equation 5.18 will be denoted by $\mathcal{K}_N$. A simple calculation shows that $\mathcal{K}_N$ is an abelian group [18]:

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} a' & b' \\ -b' & a' \end{pmatrix} = \begin{pmatrix} a' & b' \\ -b' & a' \end{pmatrix} \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} aa' - bb' & ab' + a'b \\ -ab' - a'b & aa' - bb' \end{pmatrix}, \tag{5.19}$$

where

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}, \begin{pmatrix} a' & b' \\ -b' & a' \end{pmatrix} \in \mathcal{K}_N.$$

The properties of $\mathcal{K}_N$ are difficult to study in general, since they depend on the dimension N and the defining equation (5.18) is quadratic in both a and b. It is shown in [18] that the generator of the Weil representation of $\mathcal{K}_N$ in the case of $N = 4K \pm 1$ is the root $F_N^{1/K}$ of the Fourier matrix. In the remaining part of this section, we examine the cases of $N = 2, N = 3$ and $N = 4$.

First, we know that $SL(2, \mathbb{Z}_2)$ has only six elements and it is easy to check that the only ones satisfying the equation 5.18 are

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Thus the group $\mathcal{K}_2$ is isomorphic to the group $\mathbb{Z}_2$.

In the next case, $N = 3$, the group $SL(2, \mathbb{Z}_3)$ has 24 elements. By checking equation (5.18) for $a, b \in \mathbb{Z}_3$ we obtain the result that there are 4 elements in $\mathcal{K}_3$, namely

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \quad \text{and} \quad \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}.$$

It can be easily checked that these are the matrices corresponding to the powers of Ad_F in dimension 3, so they form a group isomorphic to the cyclic group $\mathbb{Z}_4$. Hence there are no other classes of equivalence in $C(3)/H(3)$ commuting with $[F]$ other than those generated by $[F]$ in agreement with [18] for $K = 1$.

Finally, we examine the case $N = 4$. The group $SL(2, \mathbb{Z}_4)$ has 48 elements and there are 8 solutions to equation (5.18), namely

$$\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}, \begin{pmatrix}0 & 3\\ 1 & 0\end{pmatrix}, \begin{pmatrix}3 & 0\\ 0 & 3\end{pmatrix}, \begin{pmatrix}0 & 1\\ 3 & 0\end{pmatrix},$$
$$\begin{pmatrix}2 & 1\\ 3 & 2\end{pmatrix}, \begin{pmatrix}1 & 2\\ 2 & 1\end{pmatrix}, \begin{pmatrix}2 & 3\\ 1 & 2\end{pmatrix} \quad \text{and} \quad \begin{pmatrix}3 & 2\\ 2 & 3\end{pmatrix}.$$

The first row represents matrices induced by Ad_F and thus forms a group isomorphic to the cyclic group $\mathbb{Z}_4$. The matrices

$$\begin{pmatrix}2 & 1\\ 3 & 2\end{pmatrix} \quad \text{and} \quad \begin{pmatrix}2 & 3\\ 1 & 2\end{pmatrix}$$

are of order 4 and the matrices

$$\begin{pmatrix}1 & 2\\ 2 & 1\end{pmatrix} \quad \text{and} \quad \begin{pmatrix}3 & 2\\ 2 & 3\end{pmatrix}$$

are of order 2. Hence the group $\mathcal{K}_4$ has 8 elements and does not contain an element of order 8, but it contains elements of order 4. We will prove that $\mathcal{K}_4$ is isomorphic to the group $\mathbb{Z}_4 \times \mathbb{Z}_2$, which can be defined by the presentation

$$\mathbb{Z}_4 \times \mathbb{Z}_2 = \langle A, F | F^4 = A^2 = 1, AF = FA \rangle. \tag{5.20}$$

We define the map $\phi : \mathcal{K}_4 \to \mathbb{Z}_4 \times \mathbb{Z}_2$ by

$$\begin{pmatrix}0 & 3\\ 1 & 0\end{pmatrix} \mapsto F, \quad \begin{pmatrix}1 & 2\\ 2 & 1\end{pmatrix} \mapsto A.$$

The extension of ϕ on products is defined as a morphism of the monoid of words constructed from the above matrices. It follows from the above observations on orders of elements in $\mathcal{K}_4$ and from the way $\mathcal{K}_4$ was constructed that these matrices satisfy the same relations as in presentation (5.20). Next, we verify that $\begin{pmatrix}0 & 3\\ 1 & 0\end{pmatrix}$ and $\begin{pmatrix}1 & 2\\ 2 & 1\end{pmatrix}$ generate the whole group $\mathcal{K}_4$. It remains to prove that

$$\begin{pmatrix}1 & 2\\ 2 & 1\end{pmatrix}\begin{pmatrix}0 & 3\\ 1 & 0\end{pmatrix} = \begin{pmatrix}2 & 3\\ 1 & 2\end{pmatrix}$$
$$\begin{pmatrix}1 & 2\\ 2 & 1\end{pmatrix}\begin{pmatrix}0 & 3\\ 1 & 0\end{pmatrix}^2 = \begin{pmatrix}1 & 2\\ 2 & 1\end{pmatrix}\begin{pmatrix}3 & 0\\ 0 & 3\end{pmatrix} = \begin{pmatrix}3 & 2\\ 2 & 3\end{pmatrix}$$
$$\begin{pmatrix}1 & 2\\ 2 & 1\end{pmatrix}\begin{pmatrix}0 & 3\\ 1 & 0\end{pmatrix}^3 = \begin{pmatrix}3 & 2\\ 2 & 3\end{pmatrix}\begin{pmatrix}0 & 1\\ 3 & 0\end{pmatrix} = \begin{pmatrix}2 & 1\\ 3 & 2\end{pmatrix}.$$

Thus $\mathcal{K}_4$ is generated by elements satisfying the presentation (5.20) and ϕ is an isomorphism of the groups $\mathbb{Z}_4 \times \mathbb{Z}_2$ and $\mathcal{K}_4$.

This result is not analogous with the continuous quantum mechanics, where the evolution group is generated by just one element. The discrete analogue of this requirement is that the evolution group for a finite system must be isomorphic to a cyclic group. This leads to the interpretation that the evolution group of the finite quantum oscillator in dimension $N = 4$ describes two independent systems. Clearly, the structure of the evolution group of the finite quantum oscillator depends on the dimension N of the state space. In [18] a partial solution to the problem of description of these groups was proposed.

Proposition 5.3.1. *For $N = 4K \pm 1$, the subgroup $\mathcal{K}_N$ of $SL(2, \mathbb{Z}_N)$ commuting with $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ is isomorphic to the cyclic group $\mathbb{Z}_{4K}$.*

Conclusion

This thesis was started with the definition of the Pauli group and its use for construction of a fine grading of the algebra $M_N(\mathbb{C})$. Next, we defined the restricted Clifford group of a simple quantum system and we gave a short exact sequence of $C(N)$ containing $\mathbb{Z}_N \times \mathbb{Z}_N$ and $SL(2, \mathbb{Z}_N)$. We discovered that in the general case the most obvious way of defining a splitting homomorphism γ cannot be used.

We followed up with examining the multiple ways to define the lift of the restricted Clifford group to the group of $N \times N$ unitary matrices and examined the orders of its generators. We have proven that in dimension $N = 2$ and in all odd dimensions, it is sufficient to use just the finite Fourier transformation and the phase transformation as generators of the lift. We note that a splitting homomorphism γ in the case of odd N has been found using a more general definition of the Weyl-Heisenberg group.

Then, we examined the restricted Clifford groups of composite quantum systems and described them in terms of the group $\mathrm{Sp}_{[n_1,\ldots,n_k]}$. We characterised the groups $\mathrm{Sp}_{[n_1,\ldots,n_k]}$ by finding its generators using group action. We proved that the restricted Clifford group of a composite system is isomorphic to the normalizer of the group $\mathscr{P}_{(n_1\ldots n_k)}$ in the group of *-automorphisms of $M_{n_1\ldots n_k}(\mathbb{C})$.

In the final chapter, we gave an overview of basic concepts of quantum computing and explained the significance of Clifford groups with regards to effective classical simulation of quantum computing stated by the Gottesman-Knill theorem. We proceeded to a brief introduction to SIC-POVMs, proving some basic properties and discovering that the standard definition is redundant. In the final section, the finite quantum oscillator was examined. We managed to define the evolution group of a quantum oscillator in such way that it exists in every dimension.

Bibliography

[1] V. Teska: Algebras of observables and quantum computing, Bachelor's Thesis at FNSPE Czech Technical University in Prague, 2016

[2] V. Teska: Algebras of observables and quantum computing, Research Thesis at FNSPE Czech Technical University in Prague, 2017

[3] J. Patera, H. Zassenhaus, On Lie gradings I, Lin. Alg. Appl. 112 (1989), 87-159

[4] M. Havlíček, J. Patera, E. Pelantová, J. Tolar: Automorphisms of the fine grading of $sl(n,\mathbb{C})$ associated with the generalized Pauli matrices, J. Math. Phys. 43 (2002), 1083-1094 (arxiv: math-ph/0311015)

[5] D. S. Dummit, R. M. Foote: *Abstract Algebra*, John Wiley and Sons, Hoboken, 2004

[6] J. Tolar: On Clifford groups in quantum computing, to be published in J. Phys: Conf. Series (2018)

[7] S. Mac Lane, G. Birkhoff: *Algebra*, ALFA, Bratislava 1974 (in Slovak)

[8] P. Bartoňová: Teorie grup a kvantové počítání, bakalářská práce FJFI ČVUT v Praze, 2017 (in Czech)

[9] P. R. Helm: A presentation for $SL(2,\mathbb{Z}_{p^r})$, Communications in Algebra 10 (1982), 1683-1688

[10] K. Dutta, A. Prasad: Combinatorics of finite abelian groups and Weil representations, Pacific J. of Math., 275 No. 2 (2015), 295-324

[11] M. Korbelář, J. Tolar: Symmetries of finite Heisenberg groups for multipartite systems, J. Phys. A: Math. Theor. 45 No. 28 (2012), 285305

[12] M. Korbelář, J. Tolar: Symmetries of finite Heisenberg group for composite systems, J. Phys. A: Math. Theor. 43 No. 37 (2010), 375302

[13] E. Pelantová, M. Svobodová, J. Tremblay: Fine grading of $sl(p^2,\mathbb{C})$ generated by tensor product of generalized Pauli matrices and its symmetries, J. Math. Phys. 47 (2006), 5341-5357

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

[15] A. Kalve, G. Gour: Construction of all general symmetric informationally complete measurements, J. Phys. A: Math. Theor. 47 (2014)

[16] M. Appleby, S. Flammia, G. McConnell, J. Yard: SICs and algebraic number theory, Found. Phys. 47 (2017), 1042.

[17] H. Zhu: SIC POVMs and Clifford groups in prime dimensions, J. Phys. A: Math. Theor. 43 (2010)

[18] R. Balian, C. Itzykson: Observations sur la mécanique quantique finie, C. R. Acad. Sc. Paris, 303, Série I, n° 16 (1986), 773-778 (in French)