The Hidden Subgroup Problem in Certain Nilpotent p-Groups

A report summarizing the work completed as a QUASAR research assistant under Professor Nevins at the University of Ottawa

Anna B. Kis

January 2021 - April 2021

Abstract. Quantum computers promise efficient algorithms for solving the Hidden Subgroup Problem (HSP) in certain groups. The following report will outline the HSP and the relevant research being conducted in this field, including some open problems. Its main focus, however, will be the usage of the Clebsch-Gordon transform to efficiently solve the HSP in a specific class of extraspecial p-groups. Finally, the success of this methodology for other groups, specifically nilpotent wreath product groups, will be explored.

Contents

Chapter 1

Introduction

1.1 Overview

The Hidden Subgroup Problem (HSP) is a relevant problem in quantum computing, due to the increased efficiency of algorithms implemented on such computers, using techniques such as the quantum Fourier transform (QFT), over their classical counterparts [19]. Furthermore, the hardness of this problem is related to the security of a variety of cryptographic schemes; most notably, Shor's algorithm for factoring integers solves the HSP in the abelian case [26], which is relevant for RSA schemes. Furthermore, the graph isomorphism problem and shortest vector problem are equivalent to a certain subset of the HSP in the symmetric and dihedral groups, respectively, and thus finding an efficient algorithm for these open problems would indicate that currently relevant cryptographic schemes may not be secure in a post-quantum world [19].

The following report will begin by introducing the HSP and some relevant results, and will provide a summary of relevant representation theory. Then, in Chapter 2, it will discuss extraspecial p-groups and two closely related algorithms for solving the HSP in such groups which both rely on a Clebsch-Gordon transform and exploit the conjugacy classes and representation theory of the groups at hand. Finally, in Chapter 3 a certain class of wreath product groups will be explored in order to adapt the methodology in Chapter 2 to this other class of groups.

While definitions will be given when considered necessary, a basic background in group theory, linear algebra, and quantum information theory is assumed.

1.2 Hidden Subgroup Problem

First, we must define the Hidden Subgroup Problem (HSP). Consider a group G and a set X and suppose there is a *hiding function* $f : G \to X$ with the property that, for some *hidden subgroup* H of G, f is constant

and distinct on the left cosets of H. That is, for all $g, h \in G$, it has the property that

$$f(gH) = f(hH) \Leftrightarrow g^{-1}h \in H$$

The goal of the HSP is to find a generating set for H given repeated evaluations of f. Note that the function f is unknown.

Of course, one could simply query the function on each element $g \in G$, and thus after $|G|$ queries H can be completely determined. While this suffices for small groups, it is not nearly efficient enough for groups of larger order. As such, algorithms for solving the HSP aim to reduce the query complexity to $O(polylog(|G|))$, which includes the quantum part of the algorithm and any classical post-processing [19].

A related problem is the "Hidden Subgroup Conjugacy Problem" (HSCP), where instead of a generating set for the hidden subgroup H all that needs to be determined is which conjugacy class the subgroup belongs to. For some groups, solving the HSCP followed by some post-processing allows one to solve the HSP.

The standard algorithm for solving the HSP in a group G with hiding function f and hidden subgroup H, as described in [6] and [19], is as follows:

1. Prepare a uniform superposition over the group G with an additional "output" register,

$$|G\rangle|0\rangle = \frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle|0\rangle$$

2. Apply the function f on each $g \in G$,

$$|G\rangle|f(G)\rangle = \frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle|f(g)\rangle$$

3. Measure the second register to obtain some value $f(g_0)$, which collapses to state so that only states which contain that value in the second register. These are precisely the elements in the coset g_0H. One can then discard the second register, obtaining the *coset state*

$$|g_0H\rangle = \frac{1}{\sqrt{|H|}} \sum_{h \in H} |g_0h\rangle$$

   Note that g_0 is a uniformly random element. As such, the above state, called a *pure state*, may equivalently be represented by a *density matrix*, which corresponds to a completely mixed state,

$$\rho_H = \frac{1}{|G|} \sum_{g \in G} |gH\rangle\langle gH|$$

4. Compute the QFT on the coset state, resulting in the state

$$\sum_{\sigma \in \widehat{G}} \sum_{i,j=0}^{d_\sigma} \sqrt{\frac{d_\sigma}{|G||H|}} \Big(\sum_{h \in H} \sigma(g_0h))_{i,j} |\sigma, i, j\rangle$$

   where $\widehat{G}$ is a complete set of irreducible representations of G, and d_σ denotes the dimension of σ.

5. One can then measure the above state. *Weak* Fourier sampling results in only measuring an irrep label σ: this is sufficient for abelian and many nearly-abelian groups. On the other hand, *strong* Fourier sampling measures the label σ and indices i, j.

6. Finally, based on repeated measurements, conduct classical post-processing to extract the hidden subgroup.

Of course, when the group is non-abelian the existence of an efficient QFT, post-processing, and useful choice of basis for the irreps is not guaranteed. As such, the general non-abelian case remains an open problem.

Aside from an efficient algorithm for the abelian case [26], other noteworthy algorithms have been found, namely for "nearly abelian" groups. Namely, [10] gives an algorithm for finding the normal core of a hidden subgroup in a nonabelian group, thus providing an efficient algorithm to solve the HSP when the hidden subgroup is normal. Numerous positive results have been given for the Weyl-Heisenberg groups [2], [17], [13], as well as other groups with nilpotency class of two [14]. Furthermore, there have been a variety of algorithms given for different classes of semidirect product groups. This includes [20], which provided an algorithm for affine groups and q-hedral groups $\mathbb{Z}_p \rtimes \mathbb{Z}_q$ under certain conditions for p, q; [25], which examines wreath product groups of the form $\mathbb{Z}_2^n \wr \mathbb{Z}_2$; and [12], which looked specifically at $\mathbb{Z}_{p^r}^m \rtimes \mathbb{Z}_p$ as a black-box group.

There are numerous open problems which remain. While it has been shown that using a polynomial number of entangled registers one can information-theoretically solve the HSP in an arbitrary group [9], this is by no means efficient. However, exploiting entangled registers does provide some positive results, as will be shown in subsequent sections. Furthermore, while Kuperberg gives a $2^{O(\sqrt{(}\log(N)))}$-time and -quantum space algorithm for determining an order two hidden subgroup of the dihedral group, implemented as a sort of "quantum sieve" and relying on the abelian Fourier transform, [18], with an optimal measurement given in [3], no significant improvements have been made on the efficiency of this algorithm. Since the dihedral HSP is equivalent to the $f(n)$-uniform shortest vector problem (uSVP); that is, the SVP in which it is guaranteed that there is a unique nonzero vector which is shorter than all other, non-parallel, non-zero vectors by a factor of $f(n)$ [16], finding an efficient solution, or proving its hardness, would have important implications for post-quantum cryptography.

Similarly, the HSP for symmetric groups S_n is equivalent to solving the graph isomorphism and automorphism problems, which has applications in zero-knowledge proofs [22]. Unfortunately, mainly negative results have been shown for this group: strong Fourier sampling in some arbitrary basis cannot efficiently solve the HSP in this group [22].

There are, of course, a variety of other algorithms, groups, and results, which not have been mentioned here, including some for infinite groups. For further information any of the papers cited above provide useful background, and specifically [19] is recommended as an in-depth introduction to the HSP and recent research.

1.3 Representation Theory

The following section will provide some useful definitions. Unless otherwise stated, these definitions and theorems are modified from [27]. For additional information, Steinberg's book [27] or the self-contained summary of the HSP by Lomont [19], which includes relevant information on representation theory, are useful reads.

Definition 1 (Representation)**.** Suppose G is a group and V a vector space over $\mathbb{C}$. Then, a homomorphism $\phi : G \to GL(V)$ is called a *representation* of G. The *degree* of a representation d_ϕ is the dimension of V.

Note that one could consider a vector space over any field $\mathbb{F}$ instead, but for the remainder of this report we will assume that the vector space is finite dimensional over the complex numbers, and that the group G is finite.

Definition 2 (Equivalence)**.** Let G be a group and let $\sigma : G \to GL(V), \rho : G \to GL(W)$ be two representations of G, where V, W are vector spaces. Then, σ, ρ are said to be *equivalent* if there is a linear isomorphism $T : V \to W$ satisfying the relation

$$T\sigma_g T^{-1} = \rho_g$$

for all $g \in G$. In this case, write $\sigma \sim \rho$.

Definition 3 (G-invariant subspace)**.** Let G be a group and $\phi : G \to GL(V)$ a representation. Then, a subspace W of V is called *G-invariant* if $\phi(g)w \in W$ for all $w \in W$.

Definition 4 (Irreducible)**.** A representation $\phi : G \to GL(V)$ of a group G is called *irreducible* if the only $G-$invariant subspaces of V are V and $\{0\}$.

For brevity, the remainder of this report will refer to these irreducible representations as **irreps**.

Definition 5 (Character)**.** The *character* of a representation is defined as the trace of the matrix representation. Specifically, given a representation $\rho : G \to GL(V)$ for a group G, its character is a group homomorphism $\chi : Gto\mathbb{C}$ is given by $\chi = tr(\rho)$.

Note that the character of a representation is constant on conjugacy classes, due to the fact that the $Tr(A^{-1}BA) = Tr(B)$ for matrices A, B. This gives a one-to-one correspondence between conjugacy classes of a group and its unique characters.

Definition 6 (Restriction)**.** Consider a group G with representation $\phi : G \to GL(V)$ and with a subgroup $H \leqslant G$. Then, a *restriction* of ϕ to H is given as $\phi|_H : H \to GL(V)$ where $\phi|_H(h) = \phi(h)$ for all $h \in H$.

Definition 7. Consider a group H which is a subgroup of G with a representation $\phi : H \to GL(W)$ with dimension d_ϕ. Then, the *induced representation* of ϕ to a representation of G is a $d_\phi[G : H]$-dimensional representation denoted $Ind_H^G \phi : G \to GL(W)$ where W is a $d_\phi[G : H]$-dimensional space given by

$$W = \oplus_{t \in T} V_t$$

where T is a complete set of coset representatives of $[G : H]$. Then, if one writes $g \in G$ as $g = t_g h_g$ for some $t_g \in T, h_g \in H$, then the action of g on this larger vector space W is given by

$$gW = t_g h_g(\oplus_{t \in T} V_t) = \oplus_{t \in T} h_g V_{t_g t}$$

As an important result, recall that a matrix U is unitary if $U^\dagger U = UU^\dagger = I$.

Proposition 1.3.0.0.1 (3.2.4 [27]). *Let G be a finite group and $\phi : G \to GL(V)$ a representation. Then, any such representation is equivalent to a unitary representation.*

This is relevant due to the importance of unitary matrices in quantum mechanics.

Chapter 2

Extraspecial p-Groups

2.1 Overview

Let us begin with a few definitions before exploring the nature of extraspecial p-groups.

Definition 8 (p-group)**.** Let p be a prime. Then, a *p-group* is a group in which every element has order p^k for some $k \geqslant 0$.

If such a group is finite then we must have that $|G| = p^n$ for some $n \in \mathbb{N}$. There are a number of interesting properties of such groups. This section will explore some relevant groups and their properties in the hopes of generalizing the HSP to some class of $p-$groups.

Definition 9 (Frattini subgroup)**.** The *Frattini subgroup* of a group G, denoted $\phi(G)$, is the intersection of all maximal proper subgroups of G.

Some noteworthy properties of Frattini subgroups, given in [1] include:

1. It is a characteristic subgroup of G – that is, a subgroup where for all $\psi \in Aut(G)$, $\psi(\phi(G)) = \phi(G)$.
2. If $G/\phi(G)$ is cyclic then so is G
3. If G is a p-group then $\phi(G)$ is the smallest normal subgroup such that $G/\phi(G)$ is elementary abelian – that is, a subgroup where every element has order p.

Definition 10 (Commutator subgroup)**.** Given a group G, its *commutator subgroup* (or derived subgroup) is the group

$$G' = \langle \{[g, h] : g, h \in G\} \rangle$$

where $[g, h] = g^{-1}h^{-1}gh$.

Finally, recall that the center of a group is the subgroup of elements which commutes with every element in the group. Specifically, it is given as

$$Z(G) = \{h \in G : gh = hg \forall g \in G\}$$

and if G is abelian then $Z(G) = G$.

Definition 11 (Extraspecial p-group)**.** Let p be a prime and let G be a p-group. G is said to be an *extraspecial p-group* if $Z(G) = \phi(G) = G'$ and $|Z(G)| = p$. Notice that this implies that $G/Z(G)$ is an elementary abelian $p-$group.

Definition 12 (Upper central series)**.** Let G be a group. The *upper central series* of G is the tower

$$\{1\} = Z_0 \lhd Z_1 \lhd Z_2...$$

where $Z_{i+1} = \{x \in G : [x, g] \in Z_i \ \forall g \in G\}$. In addition, $Z_1 = Z(G)$ and so one can define Z_{i+1} instead according to the relation $Z_{i+1}/Z_i = Z(G/Z_i)$.

Definition 13 (Lower central series)**.** Let G be a group. Then, the *lower central series* of G is the tower

$$G = A_0 \rhd A_1 \rhd A_2...$$

where $A_{i+1} = [A_i, G] = \langle [a, g] : a \in A_i, g \in G \rangle$. Clearly, $A_1 = G'$.

Definition 14 (Nilpotent group)**.** A *nilpotent* group of *class* n, or, more briefly, a *nil-n* group, is a group G where $A_n = \{1\}$, or, equivalently, $Z_n = G$.

Nilpotent groups are related to p groups in a number of ways. First, all p groups are nilpotent. Specifically, extraspecial p groups are nil-2 groups.

Claim 2.1.0.0.1. *Let G be an extraspecial p group of order p^{2n+1}. Then, G is a nil-2-potent group.*

Proof. We know that $Z(G) = G' \cong Z_p$ for an extraspecial p group G. Then,

$$Z_2 = \{x \in G : [x, g] \in Z(G), \forall g \in G\} = G$$

since $Z(G) = [G, G]$ and so $[x, g] \in Z(G) \forall x, g \in G$. We thus get the upper central series

$$1 \lhd Z(G) \lhd G$$

Equivalently, we could instead consider the lower central series. Since $A_1 = G' = [G, G] = Z(G) \cong Z_p$,

$$A_2 = \langle [z, g] : z \in Z(G), g \in G \rangle = \{1\}$$

since $Z(G)$ commutes with everything and so $[z, g] = 1 \forall g \in G, z \in Z(G)$, where 1 is the identity. Thus, we have the lower central series

$$G \rhd G' \rhd 1$$

□

By definition, we can see that Z_{i+1}/Z_i is an abelian group and so it is solvable. In addition, if G is finite and nilpotent then it is isomorphic to a direct product of its Sylow p-groups, all of which are normal in G ([7]).

This means that for a finite nilpotent group G, if we can find an algorithm to solve the HSP in Sylow p-groups, then, since computing the direct product is efficient, and since all the Sylow subgroups are unique, we can efficiently determine the HSP in the nilpotent group. Finally, elements of coprime order commute. This makes finite nilpotent groups "almost abelian".

Suppose G is an extraspecial p-group as defined above. Let us examine $[\ ,\ ] : G \times G \to G$ in this case, using the methodology in [15], in order to justify that only two classes of such groups exist, distinguished by their exponent.

Let $g, h, k \in G$. Then, since $G' = Z(G)$ we know that all elements in G' commute with G. Then,

$$\begin{aligned}[gh, k] &= (gh)^{-1}k^{-1}(gh)k = h^{-1}g^{-1}k^{-1}ghk \\ &= h^{-1}(g^{-1}k^{-1}gk)k^{-1}hk = [g, k]h^{-1}k^{-1}hk \\ &= [g, k][h, k]\end{aligned}$$

and

$$(gh)^n = g^n h^n [h, g]^{\frac{n(n-1)}{2}}.$$

Let G be an extraspecial p-group of order p^{2n+1} (by [15] there are no extraspecial groups of order p^{2n}). Then, $Z(G) \cong \mathbb{Z}_p$, and one can identify the vector space $V = Z_p^{2n}$ with $G/Z(G) = \{(0, b, c)Z(G) : b, c \in \mathbb{Z}_p^n\} \cong \mathbb{Z}_p^{2n}$ where **(b,c)** $= (0, b, c)Z(G)$. Then,

Claim 2.1.0.0.2. *The map $b : G/Z(G) \times G/Z(G) \to Z(G)$ given by $\underline{(\boldsymbol{g}, \boldsymbol{h})} = [g, h]$ is bilinear and skew symmetric.*

Proof. Let $\mathbf{x} = (x_1, x_2), \mathbf{y} = (y_1, y_2), \mathbf{z} = (z_1, z_2) \in V$ and a, c scalars. Then, we have already shown that $[gh, k] = [g, k][h, k], g, h, k \in G$. Then, since G is a group and thus closed, if we set $g := ax, h := cy, k := z$ we can see that

$$\begin{aligned}b(\mathbf{ax+cy}, \mathbf{z}) &= [ax + cy, z] = [g + h, k] = [g, k] + [h, k] \\ &= [ax, z] + [cy, z] = a[x, z] + c[y, z] = ab(\mathbf{x}, \mathbf{z}) + cb(\mathbf{y}, \mathbf{z})\end{aligned}$$

The other side follows from a similar proof.

To show that b is skew symmetric, note that it is alternating; that is, $b(\mathbf{x}, \mathbf{x}) = 0$. This is because $[x, x] = e_G$ where e is the identity in G. Since $Z(G) \cong \mathbb{F}_p$ which is an additive group we have that $e_G \cong 0$ and so $b(\mathbf{x}, \mathbf{x}) = [x, x] = e_G = 0$ as required.

Now, since b is bilinear we must have that $0 = b(x - y, y - x) = b(x, y - x) - b(y, y - x) = b(x, y) - b(x, x) - b(y, y) + b(y, x) = b(x, y) + b(y, x)$ and thus $b(x, y) = -b(y, x)$. Thus, it is also skew symmetric.

Finally, let us check that the Jacobi identity holds: that is, that

$$b(x, b(y, z)) + b(y, b(z, x)) + b(z, b(x, y)) = 0$$

Since our vector space V is spanned by $\{e, f\}$ for standard basis vector over the field $\mathbb{F}_p$ we can simply check the Jacobi identity for these two vectors, since it must hold for the rest of V by linearity. Note that $e = (1, 0) \cong (0, 1, 0)Z(G) \in G/Z(G)$ and $f = (0, 1) \cong (0, 0, 1)Z(G) \in G/Z(G)$. Then,

$$b(e, b(e, f)) + b(e, b(f, e)) + b(f, b(e, e)) = b(e, b(e, f)) - b(e, b(e, f)) + b(f, 0) = 0$$

as required. □

Unfortunately, this is not quite a Lie algebra, but perhaps we can find one later.

Now, in order to distinguish between the two classes of extraspecial p-groups, [15] defines a second map $q : G/Z(G) \to Z(G)$ as well, given by $q(\mathbf{g}) = g^p$.

Then, the following lemma is given in [15]:

Lemma 2.1.0.0.1. *Given a vector space V with basis $\{v_1, ..., v_n\}$ over $\mathbb{F}_p$, a bilinear map $b : V \times V \to \mathbb{F}_p$, and a map $q : V \to \mathbb{F}_p$,*

$$G = \langle v_1, ..., v_n, z | z^p = 1, v_i^p = q(v_i), [v_i, z] = 1, [v_i, v_j] = b(v_i, v_j) \rangle,$$

where $Z(G) = \langle z \rangle$, is an extraspecial p-group.

Using this lemma the two classes of extraspecial p-groups of order p^3 are given in [15] as:

$$H_{p^3} = \{e, f, z : e^p = f^p = z^p = 1, [e, z] = [f, z] = 1, [e, f] = z\}$$

$$M_{p^3} = \{e, f, z : e^p = 1, f^p = z, z^p = 1, [e, z] = [f, z] = 1, [e, f] = z\}$$

Where the map q is the zero map for H_{p^3} and a non-zero linear map where $q(e) = 0, q(f) = 0$ for symplectic basis elements e, f of V.

To give a general definition which does not rely on b, q, the following classification is given in [24] for groups of order p^{2n+1}:

$$\begin{aligned} H_{p^{2n+1}} = \{&e_1, ..., e_n, f_1, ..., f_n, z : [e_i, e_j] = [f_i, f_j] = [e_i, f_j] = 1, i \neq j, \\ &[e_i, z] = [f_i, z] = 1, [e_i, f_i] = z, e_i^p = f_i^p = z_i^p\} \end{aligned}$$

$$\begin{aligned} M_{p^{2n+1}} = \{&e_1, ..., e_n, f_1, ..., f_n, z : [e_i, e_j] = [f_i, f_j] = [e_i, f_j] = 1, i \neq j, \\ &[e_i, z] = [f_i, z] = 1, [e_i, f_i] = z, e_i^p = z_i^p = f_j = 1, j \neq n, f_n^p = z\} \end{aligned}$$

Where $e_1, ..., e_n, f_1, ..., f_n$ gives a basis for $\mathbb{Z}_p^2 n$ and z for $\mathbb{Z}_p$; alternatively, they are generating elements for $G/Z(G)$ and $Z(G)$, respectively.

It is also mentioned in [15] that all extraspecial p-groups of order p^{2n+1}, $p \neq 2$, are the central product of either n copies of H_{p^3} or $n - 1$ copies of H_{p^3} and one copy of M_3, where "central product" of two groups G, H is defined as the factor group $\frac{G \times H}{N}$ and where $N = \{(z^{-1}, \theta(z) : z \in Z(G)\}$ is a normal group and θ is an isomorphism between $Z(G), Z(H)$.

2.1.1 $H_{p^{2n+1}}$

Suppose $p \neq 2$ and consider the group which will be referred to as the "Weyl-Heisenberg group" in subsequent sections, with the notation $H_{p^{2n+1}} = W_p = \{(a, b, c) : a \in \mathbb{F}_p, b, c \in \mathbb{F}_p^n\}$. This group, which corresponds to extraspecial p-groups of exponent p, will be discussed in depth later in its relation to the HSP. For this reason its subgroup structure and representation theory will be omitted in this section and discussed later. This subsection will aim to better understand the nature of this group by relating it to Lie algebras.

Consider the $n+2$ by $n+2$ matrix representing group elements,

$$g = \begin{bmatrix} 1 & c & a \\ 0 & I_n & b \\ 0 & 0 & 1 \end{bmatrix}$$

in $GL_{n+2}(\mathbb{F}_p)$, where c, b are vectors in $\mathbb{F}_p^n$. Then we have a vector space

$$W = \left\{ \begin{bmatrix} 0 & c & a \\ 0 & [0] & b \\ 0 & 0 & 0 \end{bmatrix} : c, b \in \mathbb{F}_p^n, a \in \mathbb{F}_p \right\}$$

In fact, W is the Lie algebra of W_p; firstly, let $b : W \times W \to W$ be a map where $b(x, y) = xy - yx$. This is a skew-symmetric, bilinear map which satisfied the Jacobi identity and thus W is a Lie algebra. The following are the basis elements:

Lemma 2.1.1.0.1. *W is a (restricted) Lie algebra with the associated map $b : W \times W \to W$ given by $b(x, y) = xy - yx$.*

Proof. Clearly, W is a vector space with basis elements

$$X_i = \begin{bmatrix} 0 & e_i^T & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, Y_i = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & e_i \\ 0 & 0 & 0 \end{bmatrix}, Z = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

where e_i is the i^{th} standard basis element in $\mathbb{F}_p^n$.

Let $a = (a_1, ..., a_n), b = (a_1, ..., a_n) \in \mathbb{F}_p^n, c \in \mathbb{F}_p$, and let $X = \sum_{i \leqslant n} X_i, Y = \sum_i Y_i, A, B, C \in W$. Then, the map b is bilinear:

$$b(aA + cB, C) = (aA + cB)C - C(aA + cB) = a(AC - CA) + c(BC - CB) = ab(A, C) + cb(B, C)$$

Skew-symmetric:

$$b(A, B) = AB - BA = -(BA - AB) = -b(B, A)$$

And satisfies the Jacobi identity; it suffices, by bilinearity, to simply check for basis elements:

$$b(X_i, b(Y_j, Z)) + b(Y_i, b(Z, X_i)) + b(Z, b(X_i, Y_j)) = b(X_i, 0) + b(Y_j, 0) + b(Z, X_{ij}) = 0$$

where X_{ij} is X_i if $i = j$, otherwise it is all zeroes.

For elements $A \in W$ we have the $p-$operation taking $A \mapsto A^{[}p]$ defined by raising A to the power p; that is, we define $A^{[}p] := A^p$, making W a restricted Lie algebra. □

Then it is clear to see that $b(X_i, Y_i) = Z$, $b(X_i, Y_j) = b(X_i, Z) = b(Y_i, Z) = b(X_i, X_j) = b(Y_i, Y_j) = b(Z, Z) = 0$.

Lemma 2.1.1.0.2. *W is the (restricted) Lie algebra of the group W_p.*

Proof. Note that while we have defined W_p over $\mathbb{F}_p$ it is often generalized for elements in R, in which case one can form a real Matrix Lie group and proper associated Lie algebra. However, if one restricts the Lie group to the integers, and then reduces $\mod p$ with a $p-$operator, then we the current construction remains.

Now, we must show that for all $t \in \mathbb{F}_p, A \in W$, $exp(tA) \in W_p$, where $exp : W \to W_p$ is given by

$$exp(v) = \sum_{n=0}^{\infty} \frac{1}{n!} v^n \ \forall \ v \in W$$

Any element $A \in W$ can be written as $A = \sum_i (a_i X_i + b_i y_i) + cZ$ and thus as

$$\begin{pmatrix} 0 & \sum_i a_i e_i^T & c \\ 0 & 0 & \sum_i b_i e_i \\ 0 & 0 & 0 \end{pmatrix}.$$

Then,

$$\begin{aligned} exp(tA) &= \sum_{n=0}^{\infty} \frac{t^i}{i!} A^i \\ &= I_{i+2} + \sum_{n=1}^{2} \frac{t^i}{i!} A^i \\ &= I_{n+2} + tA + \sum_j \frac{t^2}{2} \begin{pmatrix} 0 & 0 & a_j b_j \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 1 & t\sum_j a_j e_j^T & \sum_j \frac{1}{2} a_j b_j t^2 + ct \\ 0 & 1 & t\sum_j b_j e_j \\ 0 & 0 & 1 \end{pmatrix} \in W_p \end{aligned}$$

□

Note that W is not only a vector space, but a group under addition, as well, with the identity element being the zero matrix.

Claim 2.1.1.0.1. *The set of matrices given by $exp(W) = \{exp(w) : w \in W\}$ forms a group. Specifically, $exp(W) = W_p$*

Proof. We have already seen that $exp(W) \subset W_p$ Then, we have seen that $\forall A \in W$, $exp(A)$ terminates, since A^3 is the zero matrix. Also, $|W| = p^{2n+1} = |W_p|$ and since it is surjective and injective. Thus, this map has

an inverse, $log : W_p \to W$ given by

$$\log(h) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{(h-I)^n}{n}$$

Since $exp(W) = W_p$ and W_p is a group, $exp(W)$ is a group. □

Then, since $X_i^2 = Y_i^2 = Z^2 = 0$, we obtain the following basis elements for W_p

$$x_i = exp(X_i) = I_{n+2} + X_i = \begin{bmatrix} 1 & e_i^T & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$y_i = exp(Y_i) = I_{n+2} + Y_i = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & e_i \\ 0 & 0 & 1 \end{bmatrix}$$

$$z = exp(Z) = I_{n+2} + Z+ = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Now, we can define the map $[\ ,\ ] : W_p \to W_p$ by

$$[g, h] = exp(b(\log(g), \log(h))),$$

Claim 2.1.1.0.2. *The map $[,]$ defined above has the property that $\forall g, h, k \in W_p$ and scalars a, b, $[g^a h^b, k] = [g, k]^a [h, k]^b$ and $[g, h^a k^b] = [g, h]^a [g, k]^b$. It is also skew symmetric, and satisfies a variant of the Jacobi identity (with the operation being matrix multiplication).*

Proof. Let $g = exp(G), h = exp(H), k = exp(K)k, g, h \in W_p, G, H, K \in W$ and let $a, c \in \mathbb{F}_p$. Note that in W_p we are working with matrix multiplication, whereas in W our operation is addition. Then,

$$\begin{aligned} [g^a h^c, k] &= exp(b(aG + cH, K)) = exp(ab(G, K) + cb(H, K)) \\ &= exp(a(GK - KG) + c(HK - KH)) \\ &= exp(ab(G, K))exp(cb(H, K))* \\ &= exp(b(G, K))^a exp(b(H, K))^c = [g, k]^a [h, k]^c \end{aligned}$$

since $(GK - KG)(HK - KH) = GKHK - GK^2H - KGHK + KGKH$ and $(HK - KH)(GK - KG) = HKGK - HK^2G - KHGK + KHKG$.

Then, notice that $\forall A, B \in W, AB$ is the upper triangular matrix with a potentially non-zero value in the upper rightmost corner and zeroes everywhere else. Then, $\forall A, B, C, D \in W, ABCD = 0_{n+2}$. Thus, $(GK - KG)(HK - KH) = 0 = (HK - KH)(GK - KG)$ and thus the equality at * follows. The other side follows in a similar manner.

Next,

$$[g,h] = exp(b(g,h)) = exp(-b(h,g)) = [h,g]^{-1}$$

and thus $[,]$ is skew symmetric.

Finally, let us check a modified Jacobi identity on the basis elements.

$$\begin{aligned}[x_i,[y_j,z]][y_j[z,x_i]][z,[x_i,y_i] &= exp(b(X_i,b(Y_j,Z)))exp(b(Y_i,b(Z,X_i)))exp(b(Z,b(X_i,Y_j))) \\ &= exp(b(X_i,0))exp(b(Y_i,0))exp(b(Z,X_{ij})) \\ &= exp(0)exp(0)exp(0) = I_{n+2}\end{aligned}$$

Since $exp(0) = I_{n+2}$. Thus, this identity holds. □

By the way it is defined and the above claim, $[,]$ satisfies the same relations as b. That is, $[x_i,y_i] = z, [x_i,y_j] = [x_i,x_j] = [z,z] = [y_i,y_j] = I$

Additionally, notice that $\forall g \in W_p, g^p = exp(p\log(g)) = exp(0) = 1$, since we are working over $\mathbb{F}_p$, so the order of each element is p (or one).

This gives us the Weyl-Heisenberg group, as expected. Notice that it satisfies the requirements given in the definition for $H_{p^{2n+1}}$

Using these relations let us confirm that the properties of an extraspecial group hold; that is, that $Z(G) = \phi(G) = G'$ and $|Z(G)| = p$ for $G = W_p$. First, however, let us relate the map $[,]$ defined above to the standard commutator map.

Lemma 2.1.1.0.3. *Let $[,]$ be as defined above. Then, $\forall g,h \in W_p$, $[g,h] = g^{-1}h^{-1}gh$*

Proof. Let $g,h \in W_p, G = log(g), H = log(h) \in W$. Then,

$$[g,h] = exp(b(G,H)) = exp(GH - HG)$$

Alternatively, consider

$$g^{-1}h^{-1}gh = (hg)^{-1}gh = exp(-HG + GH)$$

Thus, $[g,h] = g^{-1}h^{-1}gh$. □

Notice that the image of $[,]$ is, in fact, contained in the center of W_p, since $GH - HG = aZ, a \in \mathbb{F}_p$, and thus $W_p' = \{[g,h] : g,h \in W_p\} \subset Z(W_p)$. We wish to show that this is, in fact, an equality.

Claim 2.1.1.0.3. *Let W_p' be the commutator subgroup of W_p. Then, $W_p' = \{exp(dZ) : d \in \mathbb{F}_p\}$*

Proof. Consider $W_p' = \langle [g,h] : g,h \in W_p \rangle$. In this case this corresponds to

$$W_p' = \{[g,h] : g,h \in W_p\} = \{exp(b(G,H)) : G = log(g), H = log(h), g,h \in W_p\}$$

Since

$$\begin{aligned}
b(G,H) &= b(\sum_i (a_i X_i + b_i Y_i + cZ, \sum_j a'_j X_j + b'_j Y'_j + c'Z) \\
&= \sum_i (a_i b(X_i, \sum_j a'_j X_j + b'_j Y'_j + cZ) + b_i b(Y_i, \sum_j a'_j X_j + b'_j Y'_j + cZ) + cb(Z, \sum_j a'_j X_j + b'_j Y'_j + c'Z)) \\
&= \sum_{i,j} (a_i(a'_j b(X_i, X_j) + b'_j b(X_i, Y_j) + c'b(X_i, Z)) + b_i(a'_j b(Y_i, X_j) + b'_j b(Y_i, Y_j) \\
&\quad + c'b(Y_i, Z)) + c(a'_j b(Z, X_j) + b'_j b(Z, Y_j) + c'b(Z, Z))) \\
&= \sum_i (a_i b'_i Z + b_i b'_i Z + c b'_i Z) \\
&= dZ, \text{ for some } d \in \mathbb{F}_p.
\end{aligned}$$

Thus we have that $W'_p = \{exp(dZ) : d \in \mathbb{F}_p\}$. □

Claim 2.1.1.0.4. *Let W'_p be as defined above. Then, $W'_p \neq \{I_{n+2}\}$. That is, there exists at least one element $d \in \mathbb{F}_p^*$ such that $exp(dZ) \in W'_p$. In fact, $|W'_p| = p$ and thus $|W'_p| \cong \mathbb{F}_p$*

Proof. Recall that $[x_i, y_i] = z$. Thus, simply take $d = 1$. Then,

$$[x_i, y_i] = z = exp(Z) \Rightarrow exp(Z) \in W'_p \Rightarrow W'_p \neq \{I_{n+2}\}$$

In addition, we know that $[,]$ is a bilinear map. As such, forall $a \in \mathbb{F}_p$, since $exp(Z) \in W_{p'}$ we have that

$$[ax_i, y_i] = exp(aZ) \in W'_p$$

and thus $|W'_p| = p$ (it cannot contain more than p elements by how it is defined).

Finally, we have a natural isomorphism $\psi : W'_p \to \mathbb{F}_p$ given by $\psi(exp(aZ)) = a$. This is clearly a surjective and injective map. It also has the homomorphism property:

$$\psi(exp(aZ + bZ)) = \psi(exp((a+b)Z)) = a + b = \psi(exp(aZ)) + \psi(exp(bZ))$$

□

Then, since $W'_p \cong \mathbb{F}_p$ and $Z(W_p) \cong \mathbb{F}_p$ we get that $W'_p \cong Z(W_p)$

Alternatively, we would show that the center and W'_p are equal by examining the center, $Z(W_p) = \{g \in W_p : gh = hg \forall h \in W_p\}$, more closely.

Notice that $b(X,Y) = XY - YX = 0 \Leftrightarrow X, Y$ commute. If the two matrices commute then $e^{X+Y} = e^X e^Y$. Now, suppose $g \in Z(W_p)$. Then, for all $h \in W_p$,

$$hg = gh \Rightarrow g^{-1}hgh^{-1} = 1 \Rightarrow [g, h^{-1}] = 1 \in W'_p$$

Similarly, let $k = [g, h] = dz \in W_p'$. Then, for all $x \in W_p$,

$$[k, x] = exp(b(log(k), log(x))) = exp(\sum_i (a_i b(dZ, X_i) + b_i b(dZ, Y_i) + c_i b(dZ, Z))) = exp(0) = I$$

and thus k, x commute and so $k \in Z(W_p)$. Thus, $Z(W_p) = W_p' \cong \mathbb{F}_p$ which is an elementary abelian p-group and so W_p is extraspecial, as expected.

2.1.1.1 $M_{p^{2n+1}}$

Once again, assume $p \neq 2$ and consider the other class of extraspecial p groups, $M_{p^{2n+1}}$, of exponent p^2. For brevity let us denote $M := M_{p^{2n+1}}$. We will begin by considering the case when $n = 1$;that is, $|M| = p^3$.

First, let $z \in M$ be an element such that $\langle z \rangle = Z(M)$ and let $f \in M$ be an element of order p^2 where $f^p = z$.

Since M is a semidirect product; that is, $M \cong \mathbb{Z}_{p^2} \rtimes_\phi \mathbb{Z}_p$, we need to determine how $\mathbb{Z}_p$ acts on $\mathbb{Z}_{p^2}$. We know that it acts non-trivially, since M is nonabelian.

That is, for elements $(a, b), (a', b') \in M$, where $a, a' \in \mathbb{Z}_{p^2}, b, b' \in \mathbb{Z}_p$, we have the group operation

$$(a, b)(a', b') = (a + \phi_b(a'), b + b')$$

We must now determine the homomorphism $\phi : \mathbb{Z}_p \to Aut(\mathbb{Z}_{p^2})$.

Fix an element $y \in \mathbb{Z}_p$. Since $\phi_y : \mathbb{Z}_{p^2} \to \mathbb{Z}_{p^2}$ is an isomorphism we must have that $\phi_y(0) = 0$ and $\langle x \rangle = \langle \phi_y(x) \rangle, x \in \mathbb{Z}_{p^2}$; that is, it must map generators to generators.

Since the elements that generate $\mathbb{Z}_{p^2}$ are of the form $(g + pk), k \geqslant 0, 1 \leqslant g \leqslant p - 1$ we have that $\phi_y(x) = (g + py)x$. However, since we must have that $\phi_0(x) = x$ we are required to take $g = 1$. It is then easy to see that $\phi_0(x) = x = (1 + pp)x = \phi_p(x)$ and $\phi_y(0) = 0$.

That is, we have the group operation

$$(a, b)(a', b') = (a + (1 + pb)a', b + b')$$

Next, we need to find the generators of M. Since $f^{p^2} = 1$, an obvious choice is $f = (1, 0) \in M, 1 \in \mathbb{Z}_{p^2}$. Similarly, $e = (0, 1) \in M, 1 \in \mathbb{Z}_p$.

To find the final generator, consider

$$[e, f] = e^{-1} f^{-1} e f = (0, -1)(-1, 0)(0, 1)(1, 0) = (p, 0)$$

and call this z. Clearly, $z^p = (p, 0)^p = (0, 0)$.

Remark 2.1.1.1.1. *A final way to think about this group is as a matrix group representing the linear functions $\mathbb{Z}_{p^2} \to \mathbb{Z}_{p^2}$ given by $x \mapsto ax + b$ where $a = 1 \mod p$, $a, b \in \mathbb{Z}_{p^2}$. We can then write each element in M as*

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

In this case, we have the following three generators:

$$E = \begin{pmatrix} 1-p & p \\ 0 & 1 \end{pmatrix},\ F = \begin{pmatrix} 1+p & 1 \\ 0 & 1 \end{pmatrix},\ Z = \begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix}$$

Then, since

$$F^x = \begin{pmatrix} 1+px & x+\binom{x}{2}p \\ 0 & 1 \end{pmatrix},\ E^x = \begin{pmatrix} 1-xp & xp \\ 0 & 1 \end{pmatrix},\ Z^x = \begin{pmatrix} 1 & xp \\ 0 & 1 \end{pmatrix}$$

Thus it is clear that $F^p = Z$, $F^{p^2} = E^p = Z^p = I_2$. In addition, the matrices satisfy the relations required for an extraspecial group. Additionally, Z clearly generates the center.

We now have defined the extraspecial p-group

$$M = \{e, f, z : [z, f] = [e, z] = e_M, [e, f] = z, e^p = z^p = f^{p^2} = e_M\}$$

where z generates $Z(M)$ and e_M denotes the identity element.

We wish to associate the quotient $M/Z(M)$ and $Z(M)$ with a vector space. Note that we have already done most of the work in the discussion above. Call the associated vector spaces V, V', respectively. Since $Z(M) = \{(px, 0) : x \in \mathbb{F}_p\}$ we have that V' is simply $\mathbb{F}_p$. Also, we know that $dim V = 2$, and that it must be a vector space over $\mathbb{F}_p$ and

$$M/Z(M) = \{(a, b)Z(M) : a, b \in \mathbb{F}_p\}$$

with p^2 elements. Each element has order p: suppose $(a, b)Z(M) \in M/Z(M)$. Then, $((a, b)Z(M))^x = (a, b)^x Z(M) = (a(x + \binom{x}{2}pb), xb)Z(M) = Z(M)$ if $x = p$.

Then, we have that V must be $\mathbb{Z}_p \times \mathbb{Z}_p$ since $M/Z(M)$ is abelian with nontrivial elements having order p and with p^2 elements.

V has the basis $\{(1, 0), (0, 1)\}$, which corresponds to our choice of f, e (or F,E) from before. That is, we can identify e with $(0, 1)$ and f with $(1, 0)$. In addition, identify $1 \in \mathbb{F}_p \cong V'$ with z. More precisely, we have $W = V \oplus V'$, and thus define $\pi : M \to W$ by

$$\pi(e) = (0, 1, 0), \pi(f) = (1, 0, 0), \pi(z) = (0, 0, 1)$$

Then clearly $\pi(x) = (\pi_1(x), \pi_2(x))$ where $\pi_1 : M \to V,\ \pi_2 : M \to V'$, $\pi_1(e) = (0, 1), \pi_1(f) = (1, 0), \pi_1(z) = (0, 0)$, and $\pi_2(z) = 1$ and zero for e, f.

Now, focusing on $V \subset W$, with elements of the form $(a, b),\ a, b \in \mathbb{F}_p$ and let $s : V \times V \to \mathbb{F}_p$ be the map

$$s((a, b), (a', b')) = ab' - ba'$$

This is a symplectic bilinear form, and notice that

$$s((1, 0), (0, 1)) = 1, s((1, 0), (1, 0)) = s((0, 1), (0, 1)) = 0$$

Let $\phi : W \to V$ be the map $\phi((a, b, c)) = (a, b)$. Then, we can extend the map s to W by $S : W \times W \to W$ which is given by

$$S((a, b, c), (d, e, f)) = (0, 0, s(\phi(a, b, c), \phi(d, e, f)))$$

Finally, notice that this map S corresponds to the commutator $[,]$ given for the group M, and, in fact, its image is the center of M. That is, our defining relations are preserved, and we could define $b : M \times M \to M$ by

$$b(g,h) = \pi^{-1}S(\pi(g),\pi(h)).$$

Then, clearly,

$$b(e,f) = \pi^{-1}S((0,1,0),(1,0,0)) = \pi^{-1}(0,0,1) = z$$
$$b(e,e) = b(f,f) = \pi^{-1}(0,0,0) = e_M$$
$$b(e,z) = b(f,z) = \pi^{-1}(0,0,0) = e_M$$

2.1.1.2 Subgroup structure of M

This section will outline some relevant subgroups of M.

Recall the group operation $(a,b)(a',b') = (a + (1+pb)a', b+b')$; then for elements $(a,b),(x,y) \in M$,

$$(-(1-pb)a,-b)(x,y)(a,b) = (a((1-bp)x + yp), y) \tag{2.1}$$

Claim 2.1.1.2.1. *$N = \langle(1,0)\rangle \cong \mathbb{Z}_{p^2}$ is a normal subgroup of M.*

Proof. Since

$$(1,0)^k = (k,0) \in N$$

and thus we have a cyclic abelian group. Since $|N| = p^2$ and $(1,0)^{p^2} = (0,0)$ we have that $N \cong \mathbb{Z}_{p^2}$. Finally, let $(a,b) \in M$, so that $(a,b)^{-1} = ((pb-1)a,-b)$. Then,

$$(-a(1-pb),-b)(x,0)(a,b) = ((1-pb)x,0) \in N$$

and thus $N \lhd M$. □

In fact, this is not the only normal subgroup: we have p^2-1 generators for non-trivial normal subgroups $\langle(x,0)\rangle \lhd M, x \in \mathbb{Z}_{p^2}$, although if $gcd(x,p^2) = 1$ then $\langle(x,0)\rangle = \langle(1,0)\rangle$. Thus we have two nontrivial unique normal subgroups of this form, N from above and $\langle(p,0)\rangle$, the latter being the only subgroup of that form as $\langle(py,0)\rangle = \langle(p,0)\rangle$ since $(py,0)^x = (pyx,0) = (p(yx),0) = (p,0)^{yx}$. A third normal subgroup is given by $\langle(p,1)\rangle$, which can be shown to be normal using Equation 2.1 with (x,y) = (p,y) since

$$(a((1-pb)p + yp), y) = (ap(1+y), y) \in \langle(p,y)\rangle$$

In particular, this holds when $y = 1$ as above. However, we do have $p-1$ distinct groups $\langle(p,y)\rangle, y \in \mathbb{Z}_p^*$ since

$$(p,y)^x = (px,yx) \notin \langle(p,1)\rangle$$

To summarize, we have the following normal groups:

$$N = \langle(1,0)\rangle, N_y := \langle(p,y)\rangle, y \in \mathbb{Z}_p, \langle e,f\rangle, \langle e,z\rangle$$

Let $A_{a,b} = \langle(a,b)\rangle = \{(a(x + \binom{x}{2}pb), xb) : x \in \mathbb{Z}_{p^2}\},\ a \in \mathbb{Z}_{p^2}, b \in \mathbb{Z}_p$

Claim 2.1.1.2.2. *$A_{a,b}$ is an abelian subgroup of M of order p^2*

Proof. Clearly, since $A_{a,b}$ is cyclic it must be abelian. Then, let x be the smallest nonzero power where $(a,b)^x = (0,0)$. We then get the equation

$$(a,b)^x = (a(x + \binom{x}{2}pb), xb) = (0,0) \Rightarrow xb = 0 \ mod \ p, x + \binom{x}{2}pb = 0 \ mod \ p^2$$

where we know that $o(b) = p$ and so x must be a multiple of p, say $x = py$. Then, $\binom{x}{2}pb = \frac{py(py-1)pb}{2} = 0 \ mod \ p^2$ for any value of y.

Finally, we are left with $ax = apy = 0 \ mod p^2 \Rightarrow py = p^2 \Rightarrow y = p$. Thus, $x = p^2$. Since x is the order of (a,b) we get that $|A_{a,b}| = p^2$. □

2.1.1.3 Representation theory

Now, let us briefly discuss the representations of this group. Note that we will be using the notation e, f, z and $(0,1), (1,0), (p,0)$ interchangeably when denoting elements in M.

First, since $Z(M) \cong \mathbb{Z}_p$, and because M is an extraspecial p-group, we know that $M/Z(M) = \{(a,b)Z(M) : a, b \in \mathbb{F}_p\} \cong \mathbb{Z}_p \times \mathbb{Z}_p$ and thus we have the p^2 representations

$$\chi_{(a,b)}(c,d) = \omega^{ac+bd}, \ \omega = e^{\frac{2\pi i}{p}}, a, b \in \mathbb{Z}_p, (c,d) \in M$$

Next, since $Z(M) \cong \mathbb{Z}_p$, it has p one dimensional representations $\phi_k(px, 0) = \omega^{kpx}$, $0 \leqslant k < p$. Also, $Z(M) \lhd N$, and thus

$$N/Z(M) = \{(xp, 0)Z(M) : x \in \mathbb{Z}_p\}.$$

Thus, we can induce ϕ_k to a representation of N, determined by its behavior on the coset representatives $t_i := (ip, 0), i \in \mathbb{Z}_p$ of N/Z_p. Let $g = (x, 0) \in N$ and recall that $(p, 0)$ generates $Z(M)$. Then,

$$(x.0) \cdot \sum_i (ip, 0) \otimes (p, 0) = \sum_i (x + ip, 0) \otimes (p, 0)$$

and thus we are simply permuting the characters.

Alternatively, consider inducing this in matrix form, obtaining

$$\text{Ind}\phi_k(g) = \sum_{i,j \in \mathbb{Z}_p} \phi_k(t_j^{-1} g t_i)' e_i$$

where $\phi_k(g)' = 0 if g \notin Z(M)$ and e_i is a standard basis vector for C^p. Since $(-jp, 0)(x, 0)(ip, 0) = (x + p(i - j), 0)$,

$$\phi_k(t_j^{-1} g t_i)' = \begin{cases} \omega^{k(i-j)}, x = 0 \mod p \\ 0, \text{ else} \end{cases}$$

In fact, since N is cyclic of order p^2 it has p^2 character representations. Let ψ denote the representation of N. Then,

$$\psi_k(x,0) = (e^{\frac{2\pi i}{p^2}})^{kx}, k, x \in \mathbb{F}_{p^2}$$

Notice that if we restrict this to elements in $Z(M)$ we get $\psi_l(py,0) = \omega^{ly}$. This directly corresponds to the p characters of the center when $l \leqslant p$.

That is, since $l \in \mathbb{Z}_{p^2}$ we can write $l = a + pk$ for some $a, k \in \mathbb{Z}_p$. Then, we know that

$$\text{Ind}_{Z(M)}^{N} \phi_k(x,0) = \oplus_{a \in \mathbb{Z}_p} \psi_{a+kp}$$

is a $p-$dimensional diagonal matrix and thus the direct sum of characters.

Then, $\psi_{a+kp}(x,0) = (e^{\frac{2\pi i}{p^2}})^{x(a+kp)}$. Since this is true for all values of a we can take $a = 0$ to obtain

$$\psi_{kp}(x,0) = (e^{\frac{2\pi i}{p}})^{kx} = \phi_k(px,0)$$

Finally, recall that the elements in N are of the form $(a + pb, 0) = f^a z^b$. Thus,

$$\psi_{pk}(a + pb, 0) = (e^{\frac{2\pi i}{p^2}})^{(a+pb)(kp)} = \omega^{ak}$$

Thus, we can restrict ourselves to p distinct irreps of N, as these induce to p distinct irreps of M. These can be defined by $\psi_k(px,0) = 1, \psi_k(x,0) = \omega^{kx}, x \in \mathbb{Z}_p, k \in \mathbb{Z}_p$.

Now, since $N \lhd M$ we can induce ψ_k to a representation of M. Note that if $k = 0$ then the induced representation of ψ_0 would decompose as a direct sum of the one-dimensional irreps $\chi_{0,0}$ defined above and so choose instead $k \in \mathbb{Z}_p^*$.

We have the quotient

$$M/N = \{(0,a)N : a \in \mathbb{Z}_p\}$$

Denote the p coset representatives by $h_i = (0,i),\ i \in \mathbb{Z}_p$.

Let $g = (a,b) \in M$. Then, $h_j^{-1} g h_i = ((1-pj)a, b+i-j)$, which is an element of N if $(b - j + i) = 0 \mod p$. Then,

$$\text{Ind}\psi_k(g) = \sum_{i,j \in \mathbb{Z}_p} \psi_k(h_j^{-1} g h_i)' e_i$$

where e_i is a standard basis vector for $\mathbb{C}^p$ and

$$\psi_k(h_j^{-1} g h_i)' = \begin{cases} \psi_k((1-pj)a, 0), b + i - j = 0 \mod p, \\ 0, \text{ else} \end{cases}$$

Alternatively, consider the action of generators e, f, z. Let σ_k denote the final, p-dimensional representation of M. Then, any element in N is of the form f^x for some $x \in \mathbb{Z}_{p^2}$, and the coset representative $h_i = e^i$.Then,

$$e \sum_{i \in \mathbb{Z}_p} e^i \otimes v = \sum_{i \in \mathbb{Z}_p} e^{i+1} \otimes v$$

and thus this is simply a permutation of basis vectors. This then implies

$$\sigma_k(e) = \sum_{i\in\mathbb{Z}_p} |i+1\rangle\langle i|$$

Then, since $[e, f] = z$ we get that $fe = efz^{-1}$. We can generalize this to obtain $fe^k = (ez^{-1})^k f$, since z, f commute. e, z also commute and so we get the relation $fe^k = e^k z^{-k} f$. Recall that $f^p = z$ and so we could simply write this as $fe^k = e^k f^{1-pk}$. Thus,

$$f\sum_{i\in\mathbb{Z}_p} e^i \otimes v = \sum_{i\in\mathbb{Z}_p} e^i f^{1-pi} \otimes v = \sum_{i\in\mathbb{Z}_p} e^i \otimes \omega^{-ik} v$$

This gives us the corresponding representation

$$\sigma_k(f) = \sum_{i\in\mathbb{Z}_p} \omega^{-ik} |i\rangle\langle i|$$

Finally, since z, e commute and $z = f^p$ we get

$$z\sum_{i\in\mathbb{Z}_p} e^i \otimes v = \sum_{i\in\mathbb{Z}_p} e^i z \otimes v = \sum_{i\in\mathbb{Z}_p} e^i \otimes \omega^k v$$

and thus

$$\sigma_k(z) = \sum_{i\in\mathbb{Z}_p} \omega^k |i\rangle\langle i|$$

Now, since any element in M can be written as $e^x f^y z^k = e^x f^{y+pl}$ since

$$f^y e^x z^l = f^y z^l e^x = f^{y+pl} e^x = e^x f^{(y+pl)(1-px)} = e^x f^{y+p(l-xy)}$$

we can compute

$$e^x f^{y+pl} \sum_{i\in\mathbb{Z}_p} e^i \otimes v = \sum_{i\in\mathbb{Z}_p} e^{x+i} f^{y+p(l-yi)} \otimes v = \sum_{i\in\mathbb{Z}_p} e^{x+i} \otimes \omega^{k(l-yi)} v$$

Thus we get that

$$\sigma_k(e^x f^y z^l) = \sum_{i\in\mathbb{Z}_p} \omega^{k(l-yi)} |x+i\rangle\langle i|$$

which gives us $p-1$ p^n-dimensional representations, with $k \in \mathbb{Z}_p^*$.

2.1.2 General group of exponent p^2

Now that we understand M when $|M| = p^3$, let us look at the general case,

$$\begin{aligned} M_{p^{2n+1}} =& \{e_1, ..., e_n, f_1, ..., f_n, z : [e_i, e_j] = [f_i, f_j] = [e_i, f_j] = 1, i \neq j, \\ & [e_i, z] = [f_i, z] = 1, [e_i, f_i] = z, e_i^p = z_i^p = f_j^p = 1, j \neq n, f_n^p = z\} \end{aligned}$$

Claim 2.1.2.0.1. *The group $M_{p^{2n+1}}$ can be obtained using the central product: $M_{p^{2n+1}} \cong M \circ H_p \circ H_p \circ ... \circ H_p$ where H_p appears $n-1$ times and $\circ$ denotes the central product.*

Proof. A concrete proof is given in [15, Theorem 4.3], however this will be discussed informally below.

Consider one copy of M, H_p, with both having centers isomorphic to $\mathbb{Z}_p$ with the isomorphism $z^i \mapsto i \mod p$. Let $\psi : Z(M) \to Z(H_p$ be the isomorphism $\psi(z^i) = z^i$. Then, we have the group

$$N = \{(g^{-1}, \psi(g)) : g \in Z(M)\} = \{(z^{-i}, z^i) : i \in \mathbb{Z}_p\}$$

which is normal in $M \times H_p$. Notice that $(z^i, z^i) \in N \Rightarrow i = 0$. Then, since $M \times H_p = \{(e^a f^b z^c, x^i y^j z^k) : b \in \mathbb{Z}_{p^2}, a, c, i, j, k \in \mathbb{Z}_p\}$ we get that

$$M \circ H_p = M \times H_p / N = \{(e^a f^b z^c, x^i y^j z^k)N : b \in \mathbb{Z}_{p^2}, a, c, k, i, j \in \mathbb{Z}_p, p - c \neq k\}$$

Then, we have an isomorphism $\psi : M \circ H_p \to M_{p^5}$ which maps generators as follows:

$$\psi((e,0)N) = e_1, \psi((0,x)N) = e_2, \psi((f,0)N) = f_1, \psi((0,y)N) = f_2, \psi((z,0)N) = z$$

since then the identities are satisfied, with $f_1^p = z$.

Next, consider

$$H_p \circ H_p = \{(x^a y^b z^c, x^i y^j z^k)N : a, b, c, i, j, k \in \mathbb{Z}_p, p - c \neq k\}$$

where $N = \{(z^{-i}, z^i) : i \in \mathbb{Z}_p\}$.

Then, this is isomorphic to W_p with $|W_p| = p^5$ with an isomorphism $\rho : H_p \circ H_p \to W_p$ which, defined on generators, is

$$\rho((x,0)N) = x_1, \rho((y,0)N) = y_1, \rho((0,x)N) = x_2, \rho((0,y)N) = y_2, \rho((z,0)N) = \rho((0,z)N) = z$$

Then, in the general case, we have W_p with $|W_p| = 2(n-1)+1 = 2n-1$ where $x_i \cong (0, ..., x, 0..., 0) \in \circ^{n-1} H_p$; that is, one can think of it as i^{th} standard basis vector for $\mathbb{Z}_p^{n-1}$ except with x in place of the one. The same is true for y_i.

Then, consider

$$M \circ H_{p^{2n-1}} = \{(e^a f^b z^c, \sum_{i,j \in \mathbb{Z}_p} x_i^l y_j^m z^k)N : b \in \mathbb{Z}_{p^2}, l, m, c, a \in \mathbb{Z}_p, p - c \neq k\}$$

where x_i, y_i are the i^{th} standard basis element as discussed above and in Section 2.1.1.

We then have the isomorphism $\phi : M \circ H_{p^{2n-1}} \to M_{p^{2n+1}}$ given by

$$\phi((0,x_i)N) = e_{i+1}, \phi((e,0)N) = e_1, \phi((0,y_j)N) = f_{j+1}, \phi((f,0)N) = f, \phi((z,0)N) = \phi((0,z)N) = z,$$

where "0" denotes the identity. Then, letting 1 denote the identity, we see that,

$$e_i^p = f_i^p = z^p = 1, f^p = z, [e_i, f_i] = [e_i, f] = z$$

□

2.1.2.1 HSP in M

The following subsection will briefly summarize the subgroups of M discussed above, with a focus on solving the HSP in this group.

Consider the subgroups of M. These include the normal subgroups

$$N = \langle f \rangle \cong \mathbb{Z}_{p^2}, N_y = \langle e^y z \rangle, y \in \mathbb{Z}_p$$

Notice that $Z(M) \subset N, N_y$. Also, $\langle f^i, e^j \rangle = M \ \forall i, j \neq 0 \mod p$.

Next, consider $\langle e \rangle \cong \mathbb{Z}_p$, which is an abelian subgroup. In fact, the remaining subgroups are the cyclic subgroups

$$A_{a,b} = \langle f^a e^b \rangle = \{ f^{a(x+\binom{x}{2}pb)} e^{xb} : x \in \mathbb{Z}_{p^2} \}$$

where $a \in \mathbb{Z}_{p^2}, b \in \mathbb{Z}_p$. If $a = pc, c \neq 0$ then $A_{pc,b} = \langle z^c e^b \rangle = N_b$. Similarly, if $b = 0$ then $A_{a,0} = \langle f^a \rangle \cong \mathbb{Z}_{p^2}$. Finally, $a = 0$ gives us $\langle e \rangle$.

Let us try to determine which subgroups are distinct. First, notice that since e, z commute we have that

$$A_{pc,b} = \langle z^c e^b \rangle = \{ z^{cx} e^{bx} : x \in \mathbb{Z}_p \}$$

Then, all such subgroups are isomorphic; that is, $A_{pc,b} \cong A_{p,1} \cong \mathbb{Z}_p \times \mathbb{Z}_p, c, b \in \mathbb{Z}_p^*$.

Some are also equivelant; take $A_{pc,c} = \langle z^c e^c \rangle$ for example, with elements $z^{cx} e^{cx}$. If we let $cx = 1 \mod p$ then this is simply $A_{p,1}$.

In addition, consider any $A_{pc,d} = \langle z^c e^d \rangle$ where every element if of the form $z^{cx} e^{dx}$. If we choose x such that $cx = 1 \mod p$ we get the element ze^{dx}, and since this is a cyclic group we have $A_{pc,d} = \langle ze^{dx} \rangle = A_{p,dx} = N_{dx}$

Then, in order to solve the HSP we wish to determine the value of a, b.

Claim 2.1.2.1.1. *Let $A_{a,b}$ be a cyclic group as described above. Then, if $a \neq 0$ then $Z(M) \leqslant A_{a,b}$ and the group has order p^2. Otherwise, $Z(M) \cap A_{0,b} = \{1\}$ and every element in $A_{0,b}$ has order p or 1.*

Proof. Let $A_{a,b} = \langle x \rangle$ where $x = f^a e^b$. Then, since this is a cyclic group, $x^p \in A_{a,b}$, where

$$x^p = (f^a e^b)^p = f^{a(p+\binom{p}{2}pb)} e^{bp} = f^{ap} = z^a$$

Suppose $a \neq 0$. Then, since $A_{a,b}$ is a group we have that $\langle z^a \rangle \leqslant A_{a,b} \Rightarrow Z(M) \leqslant A_{a,b}$ since $\langle z^a \rangle = \langle z \rangle$ and clearly, $(z^a)^p = z^{ap} = 1$.

On the other hand, suppose $a = 0$. Then $x^p = z^a = 1$ and we must have that $|A_{0,b}| = p$, which forces all elements to have order p or 1. Let $y \in Z(M) \cap A_{0,b}$. Then, $y = z^i = x^k$ for some $i, k \in \mathbb{Z}_p$. Since $x = e^b$ we have that

$$x^k = e^{kb} \in Z(M) \Leftrightarrow kb = 0 \Rightarrow i = 0$$

Thus, we have that $y = 1$ and so the intersection is simply $\{1\}$. □

Now, we will consider one of the reductions given in [13]. Let $\pi : M \to V$ be the map given by $\pi(e^i f^j z^k) = E^i F^j$ where V is a two-dimensional vector space with basis $\{E, F\}$, $i, j \in \mathbb{Z}_p$ and let $G = \{\pi(x) : x \in M\}$. This is analogous to what was done in Section 2.3. In fact, this vector space is isomorphic to $M/Z(M)$ with basis $\{eZ(M), f(Z(M))\}$

Then, let us define the group operation on G by $\pi(x) \star \pi(y) = \pi(xy)$ for elements in G. That is, if $E^a F^b, E^i F^j \in G$ then $E^a F^b \star E^i F^j = E^{a+i} F^{b+j}$ and $G \cong M/Z(M) \cong \mathbb{Z}_p \times \mathbb{Z}_p$ and is thus abelian.

Finally, by [13, Lemma 2] we have that finding $A_{a,b}Z(M)$ can be reduced to finding $\pi(A_{a,b}Z(M))$ in G. Since G is abelian this is simply an analogue of the abelian HSP.

Then, if $Z(M) \leqslant A_{a,b}$ then $A_{a,b}Z(M) = A_{a,b}$ and so one can immediately find $A_{a,b}$. On the other hand, if $Z(M) \cap A_{a,b} = \{1\}$ then we have shown that there is no element of order p^2 in $A_{a,b}$. Thus, this subgroup is isomorphic to a subgroup in H_p and so one can use the methodology for solving the HSP in H_p. Then, if f is the hiding function, one can restrict f to $A_{a,b}$ and then extend to a function F on H_p which hides the group isomorphic to $A_{a,b}$ in H_p. Specifically in [13] F is defined on elements $\bar{x}^i \bar{y}^j \bar{z}^k \in H_p$ and $e^i z^k \in A_{a,b} \leqslant M$ as

$$F(\bar{x}^i \bar{y}^j \bar{z}^k) = (j, f(e^i z^k))$$

This is true for the general group $M_{p^{2n+1}}$, as well, where if $Z(M) \cap A_{a,b} = \{1\}$ then $A_{a,b}$ is isomorphic to a subgroup of $H_{p^{2n+1}}$. In this case the hiding function would be

Now, in [13] an algorithm is given which requires four entangled coset states, however in [17] this is reduced to two states when solving a group of exponent p. We will attempt to use the latter methodology for solving the HSP in M and $M_{p^{2n+1}}$. First, recall that when solving the HSP in W_p and H_p, we were relying on the conjugacy classes of $A_{a,b}$. Thus let us first determine what these are in M.

Claim 2.1.2.1.2. *The conjugate groups of $A_{a,b}$ are of the form $A_{\alpha,b}$ for some $\alpha \in \mathbb{Z}_{p^2}$.*

Proof. Let $A_{a,b} = \langle f^a e^b \rangle$, $f^u e^y z^k \in M$. Then, consider conjugation on the generator:

$$(f^u e^y z^k)^{-1}(f^a e^b)(f^u e^y z^k) = (f^a e^b z^{bu-ab-ay})$$

If $a = 0$ then this is simply $e^b z^{bu} \in A_{pbu,b}$ and so $\alpha = pbu$. Notice that $Z(M) \leqslant A_{\alpha,b}$ in this case. In fact,

$$A_{pbu,b} = \langle e^b z^{bu} \rangle = \langle e z^u \rangle \lhd M$$

Otherwise, if $a \neq 0$, then $(f^a e^b z^{bu-ab-ay}) \in A_{a,b}$ since $Z(M) \leqslant A_{a,b}$ and so $z^{bu-ab-ay} \in A_{a,b}$. That is, $A_{a,b}$ is normal. □

Now, if $a = pk, k \neq 0$ then $A_{a,b} = \langle e^b z \rangle \lhd M$, if $a = 0$ then $A_{a,b} = \langle e^b \rangle$ which is simply $\langle e \rangle M$ if $b \neq 0$, and if $a \neq 0 \mod p$ then $A_{a,b} \lhd M$ and if $b \neq 0$ then, in fact, $A_{a,b} = M$.

Then, the only non-normal case is when $a = 0$.

Claim 2.1.2.1.3. *$A_{0,b} = \langle e^b \rangle \cong H$ where $H \leqslant H_p$. Specifically, $H = \{1\}$ if $b = 0$. Otherwise, $H = \langle x \rangle$.*

Proof. Suppose we have the group $A_{0,b} \leqslant M$. First, suppose $b = 0$. Then, $A_{0,b} = \langle 1 \rangle = \{1\}$, which is clearly isomorphic to $\{1\} \leqslant H_p$.

Next, suppose $b \neq 0$. Then let $\psi : A_{0,b} \to Z_p$ be given by $\psi(e^i) = i, i \in \mathbb{Z}_p$. This is clearly an isomorphism and so $A_{0,b} \cong \mathbb{Z}_p$.

Let $H = \langle x \rangle$ where x is a generator of H_p such that $x^p = 1$, and let $\phi : H \to Z_p$ be the isomorphism $\phi(x^i) = i, i \in \mathbb{Z}_p$.

Thus, $A_{0,b} \cong H$. Recalling our notation in Section 2.2.3 for the cyclic subgroups, H is in fact $A_{0,b} = A_{0,1} = \langle (0,1,0) \rangle$. □

Thus, we can simply use the procedure in Section 2.2.3 to solve the HSP when our hidden subgroup is $A_{0,b}$. As such, given a hiding function f and hidden subgroup $A_{a,b}$ we can proceed as follows:

First, query $f(1)$ and $f(z^i)$ for some $i \in \mathbb{Z}_p^*$. If $f(1) = f(z^i)$ then $Z(M) \leqslant A_{a,b}$ and so $A_{a,b} \lhd M$. In this case, one can use the efficient algorithm given by [10] for normal subgroups, discussed in Section **??**.

If $f(1) \neq f(z^i)$ then our hidden subgroup is of the form $A_{0,b} = \langle e^b \rangle \cong H \leqslant H_p$ where $H = \langle (0,b,0) \rangle$ is an abelian subgroup of H_p. Thus, we can use the methodology of [2] or [17] to solve for b. In fact, it suffices to simply determine if $b = 0$ or $b \neq 0$ since $b = 0 \Rightarrow A_{0,0} = \{1\}$ and $b \neq 0 \Rightarrow A_{0,b} = A_{0,1} = \langle e \rangle$.

2.1.2.2 HSP in $M_{p^{2n+1}}$

In the above section we saw that solving the HSP in M reduces to either solving the HSP in H_p or solving using the method for normal subgroups.

Now, consider

$$\begin{aligned} M_{p^{2n+1}} =& \{e_1, ..., e_n, f_1, ..., f_n, z : [e_i, e_j] = [f_i, f_j] = [e_i, f_j] = 1, i \neq j, \\ & [e_i, z] = [f_i, z] = 1, [e_i, f_i] = z, e_i^p = z_i^p = f_j^p = 1, j \neq n, f_n^p = z\} \end{aligned}$$

with normal subgroups

$$N = \langle f \rangle \cong \mathbb{Z}_{p^2}, N_{I,J} = \langle f_1^{i_1}, ..., f_n^{i_n}, e_1^{j_1}, ..., e_n^{j_n} \rangle$$

where $I = (i_1, ..., i_n) \in \mathbb{Z}_p^{n-1} \times \mathbb{Z}_{p^2}$ where at least one $i_k \neq 0$, $J = (j_1, ..., j_n) \in \mathbb{Z}_p^n$. Clearly, if $j_n \neq 0$ or $j_a, i_a \neq 0$ then, since $f_n^p = [f_a, e_a] = z$ $Z(M_{p^{2n+1}})$ is contained in the subgroup; otherwise this is not a normal subgroup and is instead the abelian subgroup discussed below. For brevity call the center Z'.

Also, we have the the cyclic abelian subgroups

$$K_{A,B} = \langle f_1^{a_1} ... f_n^{a_n} e_1^{b_1} ... e_n^{b_n} \rangle$$

where $A = (a_1, ..., a_n) \in \mathbb{Z}_p^{n-1} \times \mathbb{Z}_{p^2}, B = (b_1, ..., b_n) \in \mathbb{Z}_p^n$.

Recall that $f_n^p = z$ and so if $a_n \neq 0$ then $Z' \subset K_{A,B}$, since $Z' = [M, M]$, and so $K_{A,B} \lhd M_{p^{2n+1}}$.

If $a_n = 0$ then the subgroup is

$$K_{A,B} = \langle f_1^{a_1} ... f_{n-1}^{a_{n-1}} e_1^{b_1} ... e_n^{b_n} \rangle$$

and since $z^i \notin K_{A,B}$ we have that $Z' \cap K_{A,B} = \{1\}$. As before, since all elements in $K_{A,B}$ in this case have order p or 1, $K_{A,B} \cong H \leqslant W_p$.

Recall the non-normal subgroups of W_p are

$$A_{i,J,K} = \langle (i, J, K) \rangle = \langle z^i x_1^{j_1} ... x_n^{j_n} y_1^{k_1} ... y_n^{k_n} \rangle$$

for $J, K \in \mathbb{Z}_p^n, i \in \mathbb{Z}_p$.

If we let $i = 0$ and $k_n = 0$ then $A_{i,J,K} \cong K_{A,B}$ with an isomorphim $\psi : K_{A,B} \to A_{i,J,K}$ given by $\psi(e_i) = x_i, \psi(f_i) = y_i$. If we then solve the HSP for $A_{i,J,K}$ using the methodology in [17] we can solve for $K_{A,B}$.

As such, as before, we first need to determine if the hidden subgroup is normal by checking if $f(1) = f(z)$ for a hiding function f. If it is then proceed using the method for normal groups; see Section **??** for details. If it isn't then use the methodology in [17], where we can define the function f on W_p as F, as seen in [13], where $F(x_1^{i_1}, ..., x_n^{i_n}, y_1^{j_1}, ..., y_n^{j_n}, z^l) = (i_1, f(x_2^{i_2}, ..., x_n^{i_n}, y_1^{j_1}, ..., y_n^{j_n}, z^l)$

2.1.3 Conclusion

Since solving the HSP in extraspecial p-groups of exponent p^2 can be reduced to solving the HSP in extraspecial p-groups of exponent p, the latter case will be focused on in the subsequent sections, beginning with the Heisenberg group – that is, groups of the form H_{2n+1} when $n = 1$, followed by the more general case, for all n.

2.2 Heisenberg Group

This section will examine the Heisenberg group. It will give a slightly different construction to the one discussed above, and will closely follow the paper [2]. This section will begin with a discussion of the representation theory of this group, followed by an implementation of the Clebsch-Gordon (CG) transform given in [2]. Finally, the method given in that paper for solving the HSP will be described.

Let $H_p = (\mathbb{Z}_p \times \mathbb{Z}_p) \rtimes \mathbb{Z}_p$ be the Heisenberg group with multiplication defined as

$$(a, b, c)(a', b', c') = (a + a' + b'c, b + b', c + c')$$

2.2.1 Representation theory

Then, we know that there is a bijection between degree one representations of H_p and irreps of H_p/H_p' by a lemma from [27], where H_p' denotes the commutator subgroup of H_p.

Since

$$(x,y,z)(a,b,c)(-x+yz,-y,-z) = (a-yc+bz,b,c)$$

we can see that elements of the form $(a,0,0)$ are in the center of H_p, which is the commutator subgroup in this case. In addition, we have a series of other subgroups:

There are a series of normal groups, generated by $N_i = \{(a,xi,x) : a,x \in \mathbb{Z}_p\}$, for each $i \in \mathbb{Z}_p$. There is an additional normal group $N = \{(a,b,0) : a,b \in \mathbb{Z}_p\} \cong \mathbb{Z}_p \times \mathbb{Z}_p$; thus there are a total of $p+1$ normal subgroups.

We also have a series of subgroups of order p: p^2 subgroups $A_{a,b} = \{(a,b,1)^x : x \in \mathbb{Z}_p\}$ and p subgroups $A_k = \langle (k,1,0) \rangle$.

Now, notice that $H_p' \cong \mathbb{Z}_p \lhd H_p$ and $H_p/H_p' = \{(0,a,b) + H_p' | a,b \in \mathbb{Z}_p\} \cong \mathbb{Z}_p \times \mathbb{Z}_p$ is an abelian group. Thus, we can use it to find the degree one representations of H_p. As in the previous section, these can be denoted

$$\chi_{(x,y)}(a,b,c) = \omega^{by+cx}, (x,y) \in \mathbb{Z}_p \times \mathbb{Z}_p,\ \omega = e^{\frac{2\pi i}{p}}$$

There are p^2 such degree one representations. Thus, there are $p-1$ representations left, each with degree p, since $p^2(p-1) + p^2 = |H_p|$.

Recall that $N = \langle (1,0,0),(0,1,0) \rangle \lhd H_p$. This is an abelian subgroup and thus has unique degree one representations given by $\psi_{x,y}(a,b,0) = \omega^{ay+by}, 0 \leqslant x,y < p$. In addition, consider $H_p' = \langle (1,0,0) \rangle$ which has 1-dimensional representations $\phi_k(a,0,0) = \omega^{ak},\ 0 \leqslant k < p$. Since $H_p' \lhd N$ we can induce ϕ_k to a representation of N by noting that the coset representatives of N/H_p' are $T = \{(0,i,0) : i \in \mathbb{Z}_p\}$; denote each representative $t_i = (0,i,0)$.

Then, the action of any $(a,b,0) \in N$ on the induced representation is given by

$$(a,b,0) \cdot \sum_{i,j \in \mathbb{Z}_p} (0,i,0) \otimes (j,0,0)) = \sum_{i,j \in \mathbb{Z}_p} (0,i+b,0) \otimes \phi_a(j,0,0)$$

Let π denote this induced representation. Then, we can consider how it acts on $g = (a,b,c)$ instead by noting that $t_j^{-1} g t_i = (a, b+i-j, 0)$ for each $t_i, t_j \in T$. Then,

$$\pi_g = \sum_{i,j \in \mathbb{Z}_p} \phi'_{t_j^{-1} g t_i} e_i$$

where $\phi'_h = 0 if h \notin H_p'$ and e_i is a standard basis vector for C^p. We then end up with a permutation matrix with the entries ϕ_a. As expected, when $b = 0$ this is simply $\phi_a \otimes I_p$.

Now, consider $\psi_{x,y}|_{H_p'} \cong \phi_x$; this can be seen easily if one lets $\psi_{x,y}|_{H_p'} = \psi_{x,0}$. Then, by Schur's lemma we know that $\mathrm{Hom}_{H_p'}(\psi|_{H_p'}, \phi) = \mathbf{C}$ and, by Frobenius reciprocity, the same is true for $\mathrm{Hom}_{H_p'}(\psi, \pi)$. It then

follows that $\pi_x = \psi_{x,0}$ so we can define $\pi_x(0,b,0) = 1$, and thus we have $\pi_x(a,b,0) = \omega^{ax}$ which is one dimensional and thus irreducible.

Now, one can induce this to a representation of the whole group H_p by determining how it acts on the generators $(1,0,0),(0,1,0),(0,0,1)$. Since $H_p/N = \{(0,0,i)+N \ : \ i \in \mathbb{Z}_p\}$, $|H_p/N| = p$ and the vector space being induced to is $\mathbf{C}^p$, we have the usual basis vectors $\{e_i \ : i \in \mathbb{Z}_p\}$. Then,

$$(0,0,1)\sum_{i\in\mathbb{Z}_p}(0,0,i)\otimes v = \sum_{i\in\mathbb{Z}_p}(0,0,1+i)\otimes v$$

which is just a "reshuffling" of sorts; that is, for the representation $\sigma : G \to GL(V^3)$ we get that

$$\sigma_k(0,0,1) = \sum_{i\in\mathbb{Z}_p}|i+1\rangle\langle i|$$

Similarly, consider

$$\begin{aligned}(0,1,0)\sum_{i\in\mathbb{Z}_p}(0,0,i) \ \otimes \ v &= \sum_{i\in\mathbb{Z}_p}(0,1,i) \ \otimes \ v = \sum_{i\in\mathbb{Z}_p}(0,0,i)(-i,1,0) \ \otimes \ v \\ &= \sum_{i\in\mathbb{Z}_p}(0,0,i) \ \otimes \ \psi_k(-i,1,0)v \\ &= \sum_{i\in\mathbb{Z}_p}(0,0,i) \ \otimes \ \psi_k(-i,1,0)v \\ &= \sum_{i\in\mathbb{Z}_p}(0,0,i) \ \otimes \ \omega^{-i}v\end{aligned}$$

We can reindex i and thus define the action of σ_k as

$$\sigma_k(0,1,0) = \sum_{i\in\mathbb{Z}_p}\omega^{ik}|i\rangle\langle i|$$

Combining the above calculations one can get the final solution:

$$\sigma_k(a,b,c) = \omega^{ak}\sum_{i\in\mathbb{Z}_p}\omega^{ibk}|i+c\rangle\langle c|$$

2.2.2 Clebsch-Gordan Transform

Now, we are ready to try the Clebsch-Gordan (CG) transform described in [2]. First, let us start with two degree one representations. This clearly yields a one-dimensional irrep:

$$\chi_{(x,y)}(a,b,c)\otimes \ \chi_{(u,v)}(a,b,c) = \omega^{by+cx}\otimes\omega^{bv+cu} = \omega^{b(v+y)+c(x+u)} = \chi_{(x+u,y+v)}(b,c)$$

Then, this is already an irrep and no CG transform must be enacted. Next, consider a degree 1 and degree p irrep:

$$\chi_{(x,y)}(a,b,c) \otimes \sigma_k(a,b,c) = \omega^{by+cx} \otimes \omega^{ak} \sum_{i \in \mathbb{Z}_p} \omega^{ibk} |i+c\rangle\langle c| = \omega^{ak+by+cx} \sum_{i \in \mathbb{Z}_p} \omega^{ibk} |i+c\rangle\langle c|$$

Notice that this is simply another p-dimensional irrep, call it σ_f. The question remains: what unitary matrix V would be able to transform the above equation into $\omega^{af} \sum_{i \in \mathbb{Z}_p} \omega^{ibf} |i+c\rangle\langle c|$?

The one given in the paper in equation (60) works.

Example 2.2.2.0.1. Suppose $p = 3$ and consider the irreps $\chi_{(2,1)}, \sigma_2$ acting on $(1,2,0)$.Then,

$$\sigma_k(2,0,1) = \begin{bmatrix} 0 & 0 & \omega \\ \omega & 0 & 0 \\ 0 & \omega & 0 \end{bmatrix},\ \chi_{(2,1)}(2,0,1) = \omega^2,\ \chi_{(x,y)}(a,b,c) \otimes \sigma_k(a,b,c) = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

$$V = (|2\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 2|)(|0\rangle\langle 0| + \omega^{-2}|1\rangle\langle 1| + \omega^{-1}|2\rangle\langle 2|) = \begin{bmatrix} 0 & \omega^{-2} & 0 \\ 0 & 0 & \omega^{-1} \\ 1 & 0 & 0 \end{bmatrix}$$

After applying this to the tensored representations we get

$$\sigma_f(2,0,1) = \begin{bmatrix} 0 & 0 & \omega \\ \omega & 0 & 0 \\ 0 & \omega & 0 \end{bmatrix}$$

And thus $f = 2$.

Now, take two p dimensional irreps, σ_{k_1} and σ_{k_2}. Then,

$$\sigma_{k_1}(a,b,c) \otimes \sigma_{k_2} = \omega^{ak_1} \sum_{i \in \mathbb{Z}_p} \omega^{ibk_1} |i+c\rangle\langle c| \otimes \omega^{ak_2} \sum_{i \in \mathbb{Z}_p} \omega^{ibk_2} |i+c\rangle\langle c|$$

Which results in a p^2 dimensional matrix. Recall that there are p^2 1-dimensional representations. Then, this matrix may decompose into these, or it could instead decompose into a degree p representation with multiplicity p. Using the unitary matrices from [2] in the following example we will see that this depends on what the labels of the representations sum to; that is, if $k_1 + k_2 \neq [0]_p$ then the tensored representation is, in fact, reducible to p copies of $\sigma_{k_1+k_2}$. On the other hand, if this sum is 0 then this is a series of representations of degree 1.

Example 2.2.2.0.2. Suppose $p = 3$ and consider $\sigma_2(2,0,1)$ from before, as well as

$$\sigma_1(2,0,1) = \begin{bmatrix} 0 & 0 & \omega^2 \\ \omega^2 & 0 & 0 \\ 0 & \omega^2 & 0 \end{bmatrix}$$

For clarity let us use block matrix notation, where $[0]$ denotes the 3-by-3 zero matrix.

Begin by considering the case when $k_1 + k_2 \neq 0$, such as when the labels are $2, 2$, respectively. Then, we obtain:

$$\sigma_2(2,0,1) \otimes \sigma_2(2,0,1) = \begin{bmatrix} [0] & [0] & \omega\sigma_2(2,0,1) \\ \omega\sigma_2(2,0,1) & [0] & [0] \\ [0] & \omega\sigma_2(2,0,1) & [0] \end{bmatrix}$$

This is clearly

$$I_3 \otimes \omega^2 \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} = I_3 \otimes \sigma_1(2,0,1)$$

where I_3 is the 3-by-3 identity matrix, and using the unitary matrix defined in [2] would yield this same result. Notice that $2 + 2 = [1]_3$ as expected.

Finally, consider the case where $k_1 = 1, k_2 = 2, 1 + 2 = [0]_3$, and note that σ_0 is not defined. Then,

$$\sigma_1(2,0,1) \otimes \sigma_2(2,0,1) = I_3 \otimes \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

Using the unitary transform in [2], one can obtain

$$I_3 \otimes \begin{bmatrix} 1 & 0 & 0 \\ 0 & \omega^2 & 0 \\ 0 & 0 & \omega \end{bmatrix}$$

Which is simply a series of degree one representations. Note that this doesn't occur very often; with high probability after sampling the registers one obtains a representation of degree p that is the tensor of two degree p irreps.

2.2.3 HSP

Let us now look at solving the HSP for the Heisenberg group by using the methodology in [2]: the following section will act to interpret and explain the results of this paper. Note that we only need to consider the subgroups $A_{a,b}$ for this problem, as all other subgroups are normal in H_p and thus one can use the HSP method for normal groups to solve.

Recall that each element in $A_{a,b}$ can be written as $(ax + \binom{x}{2}b, xb, x)$. The conjugate subgroups of $A_{a,b}$ are $A_{c,b},\ c \in \mathbb{Z}_p$:

$$(x,y,z)(al + \binom{l}{2}b, lb, l)(-x + yz, -y, -z) = (l(a - y + bz) + \binom{l}{2}b, lb, l)$$

This will be important when considering the HSCP, as we can see that one only needs to know b to determine the conjugacy class of $A_{a,b}$.

In addition, the p^2 cosets of $A_{a,b}$ have coset representatives of the form $(l, m, 0),\ l, m \in \mathbb{Z}_p$, giving us the coset state

$$|(l,m,0)A_{a,b}\rangle = \frac{1}{\sqrt{p}} \sum_{h \in A_{a,b}} |(l,m,0)h\rangle = \frac{1}{p} \sum_{x \in \mathbb{Z}_p} |(l + xa + \binom{x}{2}b, m + xb, x)\rangle$$

We then have the mixed state

$$\rho_H = \rho_{A_{a,b}} = \frac{1}{p^2} \sum_{l,m \in \mathbb{Z}_p} |(l,m,0)H\rangle\langle(l,m,0)H|$$

Now, we wish to re-express ρ_H in terms of the irreducible representations discussed above. This can be done by performing a Fourier transform, which results in the density matrix

$$\hat{\rho_H} = \frac{1}{p^3} \oplus_\psi (\psi(H) \otimes I_{d_\psi}),\ \psi(H) = \sum_{h \in H} \psi(h)$$

for irreps ψ with degree d_ψ.

Specifically for the Heisenberg group, we know that the irreps are either of the form $\chi_{c,d}$ or σ_k from before. Thus,

$$\chi_{c,d}(H) = \sum_{x \in \mathbb{Z}_p} \chi_{c,d}(ax + \binom{x}{2}b, xb, x) = \sum_{x \in \mathbb{Z}_p} \omega^{dxb+cx} \tag{2.2}$$

$$\sigma_k(H) = \sum_{x \in \mathbb{Z}_p} \sigma_k(ax + \binom{x}{2}b, xb, x) = \sum_{x \in \mathbb{Z}_p} \omega^{(ax+\binom{x}{2})k} \sum_{i \in \mathbb{Z}_p} \omega^{ibxk} |i + x\rangle\langle i| \tag{2.3}$$

Notice that

$$\chi_{c,d}(A_{a,b}) = \begin{cases} p,\ db + c = 0 \\ 0,\ \text{else} \end{cases},$$

$$tr(\sigma_k((ax + \binom{x}{2}b, xb, x)) = p,\ \text{since } x = 0$$

Thus, $\hat{\rho_H}$ is a block-diagonal square matrix with dimension p^3, with the irreps on the diagonal. The probability of observing either a 1- or p-dimensional irrep can be calculated using the formula

$$P(\psi) = \frac{d_\psi}{p^3} \sum_{h \in H} tr(\psi(h))$$

. Thus,

$$P(\chi_{c,d}) = \frac{1}{p^3}\chi_{c,d}(A_{a,b}) = \begin{cases} \frac{1}{p^2},\ db + c = 0 \\ 0,\ \text{else} \end{cases}, P(\sigma_k) = \frac{1}{p}$$

For an arbitrary b there are p solutions to the equation $db + c = 0$. As such, the overall probability of observing a one-dimensional representation is $\frac{1}{p}$. Since probabilities must sum to 0, it follows that we will observe any p-dimensional representation with probability $\frac{p-1}{p}$, although this can be verified by noting that

there are $p-1$ p-dimensional representations, each with probability $\frac{1}{p}$ of being measured for an arbitrary subgroup, and so the overall probability is $\frac{p-1}{p}$.

Now, when solving the HSCP, we are trying to determine the conjugacy class of a subgroup. As such, our desired state, which contains a conjugate subgroup with uniform probability, is ([2, Eq. 36, 38])

$$\rho_{[H]} = \frac{1}{p^3} \sum_{g \in H_p} \rho_{gHg^{-1}} = \frac{1}{p^3} \sum_{g \in H_p} R_R(g) \rho_H R_R(g^{-1})$$

where R_R is the right regular representation. After performing the FT we have a state very similar to $\hat{\rho}$ ([2, Eq. 40]):

$$\rho_{[H]} = \oplus_\psi (c_\psi(H) I_{d_\psi} \otimes I_{d_\psi}),\ c_\psi(H) = \frac{1}{p^3 d_\psi} \sum_{h \in H} tr(\psi(h))^*$$

Now, since

$$c_{\chi_{c,d}}(H) = \begin{cases} \frac{1}{p^2},\ db + c = 0 \\ 0,\ \text{else} \end{cases} \quad , c_{\sigma_k} = \frac{1}{p^4} \sum_{x \in \mathbb{Z}_p} p = \frac{1}{p^2}$$

Now, suppose the hidden subgroup is the trivial subgroup. We then have that

$$tr(\sigma_k((0,0,0)) = p \implies P(\sigma_k) = \frac{1}{p} \implies P(\sigma) = \frac{p-1}{p}$$

$$P(\chi_{c,d}((0,0,0))) = \begin{cases} \frac{1}{p^2},\ c = 0 \\ 0 \text{ else} \end{cases} \quad \Rightarrow P(\chi) = \frac{1}{p}$$

Thus, the probability distribution for observing a particular representation for $A_{a,b}$ is the same as for the trivial group. For this reason, it is beneficial to consider multiple hidden subgroup states to solve the HSCP. This is done in [2, Section 5.2]. Denote these $\rho_{[H],m}$ where m is the multiplicity of the state. Then, consider

$$\rho_{[H],2} = \sum_{g \in H_p} \rho_{gHg^{-1}}^{\otimes 2} = \sum_{g \in H_p} R_R^{\otimes 2}(g) \rho_H^{\otimes 2} R_R^{\otimes 2}(g^{-1})$$

Consider $\rho_{[H]}$. This, when measured, yields a particular coset state ρ_K where K is a conjugate of H. Then, when considering the multi-copy state, $\rho_H^{\otimes 2}$ would yield a state, upon measurement, which is $\rho_K \otimes \rho_{K'}$, where K' is a potentially different conjugate subgroup of H. This would not be particularly useful. Instead, we wish to entangle the two coset states first before measuring, thus yielding a state of the form $\rho_K \otimes \rho_K$; this is the state we obtain if we measure $\rho_{[H],2}$

One can perform QFT on the two hidden subgroup states ρ_H to obtain a state which is in the basis with representations as described above. After measuring we are left with the tensor of two irrep labels, say $\psi_1 \otimes \psi_2$, and the space on which they act, $|1, ..., d_{\psi_1}\rangle \otimes |1, ..., d_{\psi_2}\rangle$. This will be the input for the CG transform. That is, we have the state $\psi_1(A_{a,b}) \otimes \psi_2(A_{a,b})$.

Now, there are four possible options for this state, as described in Section 2.2. The probability of observing a one-dimensional state is $\frac{1}{p}$, and thus the probability of observing a p-dimensional state is $1 - \frac{1}{p}$. Then,

$$P(\chi \otimes \chi) = \frac{1}{p^2}, P(\chi \otimes \sigma) = P(\sigma \otimes \chi) = \frac{p-1}{p^2}, P(\sigma \otimes \sigma) = (\frac{p-1}{p})^2$$

As such, the last case occurs with the highest probability. As discussed in Section 2.2 if we have two p-dimensional irreps so that $\sigma_{k_1} \otimes \sigma_{k_2}$ one must consider the sum $k_1 + k_2$. Since $k_1 + k_2 = [0]_p \Rightarrow k_1 = [-k_2]_p$, sampling such a tensor product occurs with probability $\frac{p-1}{p^2}$. Thus, with high probability, the sampled tensor product is two p-dimensional representations with $k_1 + k_2 \neq [0]_p$.

Consider the case where where have the state $\sigma_{k_1}(A_{a,b}) \otimes \sigma_{k_2}(A_{a,b})$ where $k_1 + k_2 = k' \neq [0]_p$, and recall (2.3). Then,

$$\begin{aligned}\sigma_{k_1}(A_{a,b}) \otimes \sigma_{k_2}(A_{a,b}) &= \sum_{x \in \mathbb{Z}_p} \omega^{(ax+\binom{x}{2}b)k_1} \sum_{i \in \mathbb{Z}_p} \omega^{ibxk_1} |i+x\rangle\langle i| \otimes \sum_{y \in \mathbb{Z}_p} \omega^{(ay+\binom{y}{2}b)k_2} \sum_{j \in \mathbb{Z}_p} \omega^{jbyk_2} |j+y\rangle\langle j| \\ &= \sum_{x,y \in \mathbb{Z}_p} \omega^{(ax+\binom{x}{2}b)k_1 + (ay+\binom{y}{2}b)k_2} \sum_{i,j} \omega^{ibxk_1 + jbyk_2} |i+x, j+y\rangle\langle i, j|\end{aligned}$$

The state we obtain will contain these irreps with high probability so that our state is $\rho_{k_1}(A_{a,b}) \otimes \rho_{k_2}(A_{a,b}) = \frac{1}{p^2}\sigma_{k_1}(A_{a,b}) \otimes \sigma_{k_2}(A_{a,b})$. We can conjugate this by the unitary matrix

$$W = \sum_{r,d \in \mathbb{Z}_p} |r-d\rangle\langle r| \otimes |(k_1 r + k_2 d)(k_1+k_2)^{-1}\rangle\langle d|$$

given in [2, Eq. 63], to obtain

$$\begin{aligned}\frac{1}{p^2} \sum_{x,y,r,d \in \mathbb{Z}_p} \omega^{(ax+\binom{x}{2}b+bxr)k_1 + (ay+\binom{y}{2}b+byd)k_2} |r-d+x-y\rangle\langle r-d| \\ \otimes |(k_1(r+x)+k_2(d+y))(k_1+k_2)^{-1}\rangle\langle (k_1 r + k_2 d)(k_1+k_2)^{-1}|\end{aligned}$$

Here, the second register may be measured; there are p possible outcomes. Since with the CG decomposition are irreps of interest lie on the diagonal we only need to consider the diagonal entries of the second register. These occur when $k_1 x + k_2 y = 0$; thus we can make the substitution $y = -k_2^{-1} k_1 x$. In addition, we can relabel $u = r - d$. This results in the density matrix

$$\frac{1}{p} \sum_{x,u \in \mathbb{Z}_p} \omega^{bk_1 x(\frac{x(1+k_2^{-1}k_1)}{2}+u)} |u + x(1+k_2^{-1}k_1)\rangle\langle u|$$

Finally, one can relabel this with $s_1 = u + x(1 + k_2^{-1}k_1)$ and collapse the result to the pure state

$$\frac{1}{\sqrt{p}} \sum_{s \in \mathbb{Z}_p} \omega^{ts^2} |s\rangle, \text{ where } t = \frac{k_1 k_2 b}{2(k_1+k_2)} \tag{2.4}$$

We wish to find b, however this requires a unitary transform which decomposes the state so it does not contain a square.

Specifically in [2] it is claimed that there is a unitary transform

$$U_2 : \frac{1}{\sqrt{2}}(|\sqrt{t}\rangle + |-\sqrt{t}\rangle) \to |t\rangle \text{ and } U_2 : |0\rangle \to |0\rangle$$

See Claim 2.3.3.0.1 and the discussion below for some additional details.

Now, we can consider the above sum as being over $x \in \mathbb{Z}_p$ where $x = s^2$; then $s = \pm\sqrt{x}$, so Eq 2.4 becomes

$$\begin{aligned}\frac{1}{\sqrt{p}}(&\sum_{x\in\mathbb{Z}_p, x\neq 0, s=\sqrt{x}} \omega^{tx}|\sqrt{x}\rangle + \sum_{x\in\mathbb{Z}_p, x\neq 0, s=-\sqrt{x}} \omega^{tx}|-\sqrt{x}\rangle + |0\rangle) \\ &= \frac{1}{\sqrt{p}}(\sum_{x\in\mathbb{Z}_p, x\neq 0} \omega^{tx}(|\sqrt{x}\rangle + |-\sqrt{x}\rangle) + |0\rangle) \end{aligned} \tag{2.5}$$

Applying U_2 to Eq 2.5 we obtain

$$\sqrt{\frac{2}{p}} \sum_{x\in\mathbb{Z}_p, x\neq 0} \omega^{tx}|x\rangle + \frac{1}{\sqrt{p}}|0\rangle$$

Then, after an inverse QFT and measurement one obtains t with $P(t) = \frac{1}{2} + O(\frac{1}{p^2})$ from which one can determine b.

What if instead of a degree p representation we measure $\chi_{c_1,d_1} \otimes \chi_{c_2,d_2}$; that is, two degree one representations? In this case,

$$\chi_{c_1,d_1}(A_{a,b}) \otimes \chi_{c_2,d_2}(A_{a,b}) = \sum_{x_1,x_2} \omega^{b(x_1d_1+x_2d_2)+c_1x_1+c_2x_2} = \begin{cases} p^2, \text{ with prob } \frac{1}{p^2} \\ 0 \end{cases}$$

That is, given an arbitrary $\chi_{c_1,d_1} \otimes \chi_{c_2,d_2}$ we will measure the value p^2 with probability $\frac{1}{p^2}$. Since the probability of measuring a one-dimensional irrep is $\frac{1}{p}$ we have that the overall probability of measuring two one-dimensional irreps is $\frac{1}{p}\frac{1}{p}p^2\frac{1}{p^2} = \frac{1}{p^2}$. And so the probability of obtaining any information from this case is quite small. However, this would result in $\chi_{c_1+c_2,d_1+d_2}(A_{a,b})$ and so standard techniques could be used to solve, since c_1, c_2, d_1, d_2 are all known.

If one of the irreps is of degree one the process would be similar. The resulting state would be nonzero with probability $\frac{1}{p}$; overall the chance of this happening would be $\frac{2}{p^3}$. Since the label of each irrep is known determining b would be simple from $\chi_{c,d}$.

Finally, if both irreps are of degree p but $k_1 + k_2 = [0]_p$ then their direct product is a series of degree one representations. Thus, summing over all of it would yield similar results to above. In addition, this would occur with very small probability.

2.3 Weyl-Heisenberg Group

The following section interprets and describes the methodology and results of [17], which is similar to the methodology described in Section 2.2.3 by [2] but has been generalized to extraspecial p-groups of exponent p and order p^{2n+1} for any $n \geqslant 1$. Such groups are called Weyl-Heisenberg groups and are of the form $\mathbb{Z}_p^{n+1} \rtimes \mathbb{Z}_p^n$.

The definition of this group is very similar to that of the restricted Heisenberg group: $W_p = \{(a, b, c) : a \in \mathbb{Z}_p, b \in \mathbb{Z}_p^n, c \in \mathbb{Z}_p^n\}$ where the group operation is defined by

$$(a, b, c)(a', b', c') = (a + a' + b' \cdot c, b + b', c + c')$$

as before, except now $b' \cdot c$ is a dot product of vectors.

Let us denote the vector space $\mathbb{Z}_p^{2n}$ by V and let $\pi : W_p \to V$ be the projection map defined by $\pi((a, b, c)) = (b, c)$.

Claim 2.3.0.0.1. *The map π defined above is a homomorphism where $\pi(gh) = \pi(g) + \pi(h)\ \forall g, h \in W_p$*

Proof. Let $g = (a, b, c), h = (x, y, z) \in W_p$. Then, $gh = (a + x + yc, b + y, c + z) \in W_p$. Now,

$$\pi(gh) = \pi((a + x + yc, b + y, c + z)) = (b + y, c + z) = (b, c) + (y, z) = \pi(g) + \pi(h)$$

since V is a vector space and thus linear in addition. □

2.3.1 Subgroup structure

The subgroup structure of this group is a generalized version of the Heisenberg group.

Claim 2.3.1.0.1. *The center of the group W_p is the commutator subgroup $W_p' = \langle(1, 0, 0)\rangle \cong \mathbb{Z}_p$.*

Proof. W_p' is clearly a cyclic subgroup. As such, it commutes with every element of W_p:

Let $g = (a, b, c) \in W_p, (x, 0, 0) \in W_p'$. Then,

$$(a, b, c)(x, 0, 0) = (a + x, b, c) = (x, 0, 0)(a, b, c)$$

Also, it is normal:

$$(a, b, c)(x, 0, 0)(-a + bc, -b, -c) = (x - a + bc - ab, b - b, c - c) = (x, 0, 0) \in W_p'$$

However this also follows from the fact that W_p' is the kernel of π:

$$\pi((a, b, c)) = (0, 0) \Leftrightarrow (b, c) = (0, 0) \Leftrightarrow (a, b, c) \in W_p'$$

Since the kernel of a homomorphism is a normal subgroup, we get that W_p' must be normal in W_p.

Finally, let $\psi : W_p' \to Z_p$ be a map defined by $\psi(x,0,0) \to x$. This is an isomorphism:

It is clearly surjective. It is also injective: suppose $(x,0,0),(y,0,0) \in W_p'$. Then,

$$\psi((x,0,0)) = \psi((y,0,0)) \Leftrightarrow x = y \Leftrightarrow (x,0,0) = (y,0,0)$$

Finally, it has the homomorphism property:

$$\psi((x,0,0)(y,0,0)) = \psi((x+y,0,0)) = (x+y) = (x) + (y) = \psi((x,0,0)) + \psi((y,0,0))$$

Thus, we have that $W_p' \cong \mathbb{Z}_p$. □

In fact, more can be said about the vector space V: we can associate it with the quotient $W_p/W_p' = \{(0,b,c)W_p' : b,c \in \mathbb{Z}_p^n\}$. That is, recalling the projection map π, notice that this gives an isomorphism on $\{(0,b,c) : b,c \in \mathbb{Z}_p^n\}$. Thus, if we associate each coset with an element in the above set we see that π allows us to associate the quotient with $\mathbb{Z}_p^n$.

Next, we have the subgroups $N_i = \{(a,xi,x) : a \in \mathbb{Z}_p, x \in \mathbb{Z}_p^n\}, i \in \mathbb{Z}_p$, $N = \{(a,b,0) : a \in \mathbb{Z}_p, b \in \mathbb{Z}_p^n\}$.

Claim 2.3.1.0.2. *The subgroups N_i, N are normal.*

Proof. We know that for any two elements $g = (x,y,z), h = (a,b,c) \in W_p$,

$$ghg^{-1} = (a - yc + bz, b, c)$$

Now, suppose $h = (a,vi,v) \in N_i, v \in \mathbb{Z}_p^n$. Then,

$$ghg^{-1} = (a - yv + viz, vi, v) = \in N_i \text{ since } a - yv + viz \in \mathbb{Z}_p$$

Similarly, if $h = (a,b,0) \in N$ then

$$ghg^{-1} = (a + bz, b, 0) \in N \text{ since } a + bz \in \mathbb{Z}_p$$

□

Finally, we have cyclic subgroups of the form

$$H = \langle (a,b,c) \rangle = \{(ax + \binom{x}{2} b \cdot c, bx, cx) : a,x \in \mathbb{Z}_p . b,c \in \mathbb{Z}_p^n\}$$

These can be divided into two subclasses, with either c being the zero vector or a vector with only ones and zeroes as entries.

The first subclass, call this $A_{a,b,c}$ can be enumerated by allowing a to range through all of $\mathbb{Z}_p$ and b over $\mathbb{Z}_p^n$. On the other hand, there are $\sum_{i=1}^{n} \binom{n}{i}$ possible choices for c, with each c having i ones and $n-i$ zeroes.

The other subclass, $A_{a,b}$, is given by letting c be the zero vector, allowing a to range over all of $\mathbb{Z}_p$, and b to be vectors in $\mathbb{Z}_p^n$ with ones and zeroes as entries. Note that if b is the zero vector then this subgroup is simply the center. Not including $b = 0 \in \mathbb{Z}_p^n$ there are $\sum_{i=1}^{n} \binom{n}{i}$ choices for b.

Moving forward, a cyclic subgroup $H = \langle (a, b, c) \rangle$ will be considered to be generated as described above, in order to avoid considering duplicate subgroups; this will be referred to as "standard".

Claim 2.3.1.0.3. *Let $H = \langle (a, b, c) \rangle$ be a cyclic subgroup of W_p. Then its conjugate subgroups are of the form $\langle (\alpha, b, c) \rangle$, $\alpha \in \mathbb{Z}_p$. That is, its conjugacy class is determined by the value of b, c.*

Proof. Suppose $g = (d, y, z) \in W_p$ and let $h = (ax + \binom{x}{2} b \cdot c, bx, cx) \in H$ where $x \in \mathbb{Z}_p$. Then,

$$(d, y, z)(ax + \binom{x}{2} bc, bx, cx)(-d + yz, -y, -z) = ((a - cy + bz)x + \binom{x}{2} cb, bx, cx) \in A_{(a-cy+bz),b,c}$$

Since the values of y, z range over the whole group we have that the conjugate subgroups of H are all the subgroups $A_{\alpha,b,c}, \alpha \in \mathbb{Z}_p$. □

Since the subgroups N_i, N are normal subgroups we will not consider these in our analysis.

Consider a subgroup $H = (a, b, c)^x = (ax + \binom{x}{2} bc, xb, xc)$ and define the vector space $S_H = \{(b, c) : (a, b, c) \in H\} = \{\pi(h) : h \in H\}$. Our goal is to determine the value of b, c, since these determine the conjugacy class of H as per the claim above.

Now, we have that

$$S_H = \{\pi(h) : h \in H\} = \{(bx, cx) : x \in \mathbb{Z}_p\},$$

and all that we need to determine is the value of b, c.

Claim 2.3.1.0.4. *Suppose H, K are non-normal subgroups of W_p. Then, these are conjugate $\Leftrightarrow S_H = S_K$*

Proof. Suppose $H = \langle (a, b, c) \rangle, K = \langle (d, e, f) \rangle$, where the generators are of the standard form mentioned above.

Assume H, K are conjugate. This means that $b = e, c = f$. Then,

$$S_H = \{\pi(h) : h \in H\} = \{(bx, cx) : x \in \mathbb{Z}_p$$

$$S_K = \{\pi(k) : k \in K\} = \{(by, cy) : y \in \mathbb{Z}_p\}$$

These are clearly equal. However, this can also be shown be letting $(bx, cx) \in S_H$. Then, since $x \in \mathbb{Z}_p$ we know that $(bx, cx) \in S_K \Rightarrow S_H \subset S_K$. Finally, $|S_H| = p = |S_K$ and thus $S_H = S_K$.

To prove the reverse direction, suppose $S_H = S_K$. Then, we must have that

$$\forall (bx, cx) \in S_H, (bx, cx) \in S_K \Rightarrow (bx, cx) = (ey, fy)$$

Since this is true for all x, take $x \neq 0$, which implies that $y \neq 0$. Then,

$$\Rightarrow (bx, cx) - (ey, fy) = (bx - ey, cx - fy) = (0,0) \Leftrightarrow cx - fy = 0 = bx - ey$$

for some $y \in \mathbb{Z}_p$.

Since this is true $\forall x \in \mathbb{Z}_p$ consider $x = 1$. Then, $b = ey, c = fy, y \in \mathbb{Z}_p$. Then, $H = \langle (a, ey, fy) \rangle$. Similarly, we could rewrite K as $K = \langle (dy, ey, fy) \rangle$ since every element is a generator because it has order p.

Then, by Claim 2.3.1.0.3, we have that H, K must be conjugate. □

Thus, in order to solve the HSCP one must find a basis for S_H.

Now, consider $H = \langle (a, b, c) \rangle, h = (ax + \binom{x}{2}bc, bx, cx) \in H, g = (u, y, z) \in W_p, a, u \in \mathbb{Z}_p, b, c \in \mathbb{Z}_p^n$. Then,

$$(u, y, z)(ax + \binom{x}{2}bc, bx, cx)(-u + yz, -y, -z) = ((a - yc + bz)x + \binom{x}{2}cb, bx, cx)$$

and so $gHg^{-1} = H \Rightarrow b \cdot z - y \cdot c = 0$. We wish to determine when this is the case.

To do this, let us define the operation on the vector space V where $\forall (x, y), (x', y') \in V, S((x, y), (x', y')) = x \cdot y' - y \cdot x'$.

Next, let $(y, z) = \pi(g) \in V$ and $S_H = \{\pi(h) : h \in \langle (a, b, c) \rangle\} = \{(bx, cx) : x \in \mathbb{Z}_p\}$ from above. Also, define $S_H^{\perp} = \{(b, c) \in V : S((b, c), (x, y)) = 0 \forall (x, y) \in S_H\}$.

Thus, $\forall (bx, cx) \in S_H, S((bx, cx), (y, z)) = 0 \Rightarrow (y, z) \in S_H^{\perp}$.

On the other hand, suppose $(y, z) \in S_H^{\perp}$. Then, $S((y, z), (bx, cx)) = 0 = (bz - yc)x \forall (bx, cx) \in S_H$.

Now, let $G = \{g \in W_p : \pi(g) = (y, z)\} = \{(c, y, z) : c \in \mathbb{Z}_p\}$. Then, $gHg^{-1} = H \forall g \in G$.

This proves the following claim:

Claim 2.3.1.0.5. *Suppose $H = \langle (a, b, c) \rangle$. Then, $\forall g \in W_p,\ gHg^{-1} = H \Leftrightarrow \pi(g) \in S_H^{\perp}$*

Claim 2.3.1.0.6. *The subgroup $H = \langle (a, b, c) \rangle$ is abelian.*

Proof. While this follows from the fact that H is a cyclic subgroup generated by one element, we can alsso justify it by letting $h = (ax + \binom{x}{2}bc, bx, cx), g = (ay + \binom{y}{2}bc, by, cy) \in H$. Then,

$$(ax + \binom{x}{2}bc, bx, cx)(ay + \binom{y}{2}bc, by, cy) = (ax + \binom{x}{2}bc + ay + \binom{y}{2}bc + bcxy, bx + by, cx + cy)$$

$$= (ay + \binom{y}{2}bc, by, cy)(ax + \binom{x}{2}bc, bx, cx)$$

since the dot product and scalar multiplication commute. □

Claim 2.3.1.0.7. *If a subgroup $H \leqslant W_p$ is abelian then $\forall (b,c),(b',c') \in S_H, bc'-b'c=0$ and thus $S_H \subset S_H^{\perp}$. In fact, forall one-dimensional subspaces S of V, $S \subset S^{\perp}$.*

Proof. Let $h=(a,b,c) \in H$ and suppose H is abelian. Then, for all $g=(x,y,z) \in H$,

$$ghg^{-1} = (a-yc+bz, b, c) = (a,b,c) \Rightarrow bz-yc=0$$

Since $h, g \in H$ we know that $\pi(h)=(b,c), \pi(g)=(y,z) \in S_H$. Recall the inner product defined above. Then, $\forall \pi(g) \in S_H$,

$$(b,c)\cdot(y,z)=0 \implies (b,c) \in S_H^{\perp} \implies S_H \subset S_H^{\perp}$$

□

2.3.2 Representation theory

The representation theory for this group is analogous to that given in 2.2. We have p^{2n} one-dimensional representations

$$\chi_{a,b}(x,y,z) = \omega^{a\cdot y+b\cdot z},\ \omega = e^{\frac{2\pi i}{p}}, a,b,y,z \in \mathbb{Z}_p^n, x \in \mathbb{Z}_p$$

as well as $p-1$ p^n-dimensional irreps

$$\sigma_k(a,b,c) = \omega^{ak} \sum_{i \in \mathbb{Z}_p^n} \omega^{ibk} |i+c\rangle\langle i|,\ k \in \mathbb{Z}_p^*$$

with character

$$\chi_k(a,b,c) = \begin{cases} p^n\omega^{ak}, (a,b,c)=(a,0,0) \\ 0, \textbf{ else} \end{cases}$$

We will need to consider these as a normalized sum over all of $H=\langle (a,b,c)\rangle$:

$$\begin{aligned} \chi_{e,d}(H) &= \frac{1}{|H|}\sum_{x\in\mathbb{Z}_p^n} \chi_{e,d}(ax+\binom{x}{2}bc, xb, cx) = \frac{1}{p^n}\sum_{x\in\mathbb{Z}_p^n}\omega^{dxb+cex} \\ &= \begin{cases} 1,\ db+ce=0\ mod\ p \quad \Rightarrow \quad (e,d) \in S_H^{\perp} \\ 0,\ \textbf{else} \end{cases} \end{aligned}$$

$$\sigma_k(H) = \frac{1}{|H|}\sum_{x\in\mathbb{Z}_p^2}\sigma_k(ax+\binom{x}{2}bc, xb, cx) = \frac{1}{p^n}\sum_{x\in\mathbb{Z}_p^n}\omega^{(ax+\binom{x}{2}bc)k}\sum_{i\in\mathbb{Z}_p^n}\omega^{ibxk}|i+cx\rangle\langle i| \tag{2.6}$$

Since S_H is a one-dimensional subspace of V, and $dim V = 2n$, we know that $dim(S_H^{\perp}) = 2n-1$.

2.3.3 HSP

We are now ready to describe how [17] solved the HSP in this class of groups.

As before, we want to prepare two coset states, perform a QFT over both states, and measure the irrep label and index for each state. The probability of measuring a certain representation μ is given by the formula

$$P(\mu) = \frac{d_\mu |H|}{|W_p|} trace(\mu(H))$$

where in general $P(\chi)$ and $P(\sigma)$ refers to the probability of measuring *any* 1- and p-dimensional representations, respectively. Thus we have that

$$P(\chi_{(c,d)}) = \frac{|H|}{|W_p|}\chi_{(c,d)}(H) = \begin{cases} \frac{1}{p^{n+1}}, (c,d) \in S_H^\perp \\ 0, \textbf{ else} \end{cases} \Rightarrow P(\chi) = \frac{|S_H^\perp|}{p^{n+1}} = \frac{1}{p}$$

$$P(\sigma_k) = \frac{1}{p^{n+1}}\chi_k(H) = \frac{1}{p} \Rightarrow P(\sigma) = \frac{p-1}{p}$$

There are four possible outcomes, which occur with probabilities:

$$P(\chi \otimes \chi) = \frac{1}{p^2}, P(\chi \otimes \sigma) = 2\frac{p-1}{p^2}, P(\sigma \otimes \sigma) = \frac{(p-1)^2}{p^2}$$

This will result in measuring σ_{k_1} and σ_{k_2} with high probability.

Now, after Fourier sampling we have a state proportional to $\sigma_k(H) \otimes \sigma_l(H)$. If $k+l=0$ then after performing a CG transform ([17, Eq.13]) we obtain

$$\sum_{(a,b,c),(a',b',c') \in H, u,w \in \mathbb{Z}_p^n} \omega^{\frac{k}{2}(2(a'-a)+w(b'+b)-u(c'+c))} |u+b-b', w\rangle\langle u, w+c'-c| \tag{2.7}$$

Consider the entries on the diagonal of this matrix. These occur when $u+b-b'=u \Rightarrow b=b'$ and when $w+c'-c=w \Rightarrow c=c'$. Since our subgroup is $H = \rangle(a,b,c)\langle$, we also have that $a=a'$, since the elements in H correspond to $(ax+\binom{x}{2}, bx, cx)$ and $(ay+\binom{y}{2}, by, cy)$ so $by=bx \Rightarrow y=x \Rightarrow a=a'$. Thus, we have one-dimensional entries along the diagonal; these are

$$\frac{1}{p^n} \sum_{(a,b,c) \in H, u,w \in \mathbb{Z}_p^n} \omega^{k(wb-uc)} = \chi_{-u,w}(H) \tag{2.8}$$

While our goal would be to obtain such a state, with high probability we will instead obtain the state

$$\sigma_k(H) \otimes \sigma_l(H) = \frac{|H|^2}{p^{2n}} \sum_{(a,b,c),(a',b',c') \in H, u,v \in \mathbb{Z}_p^n} \omega^{k(a+bu)+l(a'+b'v)} |u+c, v+c'\rangle\langle u, v| \tag{2.9}$$

We wish to relabel the irreps so that $k=-l$. As such, consider the equation $x^2 l + k = 0$ which has a solution with probability $\frac{1}{2}$ (see below for a discussion). We then require a unitary transform V which returns the square root of a register.

Claim 2.3.3.0.1. *There exists a unitary transform U which which acts as follows:*

$$U : \frac{1}{\sqrt{2}}(|\sqrt{x}\rangle + |-\sqrt{x}\rangle) \to |x\rangle$$

$$U : \frac{1}{\sqrt{2}}(|\sqrt{x}\rangle - |-\sqrt{x}\rangle) \to |\epsilon x\rangle$$

$$U : |0\rangle \to |0\rangle$$

Where $\epsilon x = y^2$ for some $y \in \mathbb{Z}_p$.

Consider the unitary U defined above. Then, if we apply $U^\dagger$ instead, we obtain a superposition of two square roots of x. Measurement will allow us to obtain one of the two solutions with equal probability.

Specifically, since we wish to find $\sqrt{\frac{-k}{l}}$, consider

$$V|\frac{-k}{l}\rangle|\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\rangle = \frac{1}{\sqrt{2}}(|\sqrt{\frac{-k}{l}}, 0\rangle + |-\sqrt{\frac{-k}{l}}, 1\rangle)$$

Measuring the second register will yield the desired $\sqrt{\frac{-k}{l}}$ with probability $\frac{1}{2}$. Set $\alpha = \sqrt{\frac{-k}{l}}$ and let $U_\alpha : |u\rangle \to |\alpha u\rangle$ be a unitary transform. If we apply this to the first register of the above state; that is, to $\sigma_k(H)$, then we obtain

$$\begin{aligned}
U_\alpha \sigma_k(H) U_\alpha^\dagger &= \sum_{(a,b,c)\in H, u\in\mathbb{Z}_p^n} \omega^{k(a+bu)} |\alpha(u+c)\rangle\langle\alpha u| \\
&= \sum_{(a',b',c')\in H, u'\in\mathbb{Z}_p^n} \omega^{k(\alpha^{-2}a' + (\alpha^{-1}b')(\alpha^{-1}u'))} |u'+c'\rangle\langle u| \\
&= \sum_{(a',b',c')\in H, u'\in\mathbb{Z}_p^n} \omega^{k\alpha^{-2}(a'+b'u')} |u'+c'\rangle\langle u| \\
&= \sigma_{k\alpha^{-2}}(\psi_\alpha(H))
\end{aligned}$$

where we have defined $\psi_\alpha(a,b,c) = (\alpha^2 a, \alpha b, \alpha c)$, and $u' = \alpha u$.

Since we specifically chose $\alpha = \sqrt{\frac{-k}{l}}$ and $\alpha^{-2}k = (\frac{-l}{k})k = -l$ we have successfully relabeled $\sigma_k(H)$ as $\sigma_l(\psi_\alpha(H))$.

Claim 2.3.3.0.2. *$\psi_\alpha : W_p \to W_p$ is an isomorphism whenever $\alpha \neq 0$.*

Proof. Suppose $\alpha \neq 0$. Then, consider $ker\psi_\alpha$:

$$(a,b,c) \in ker\psi_\alpha \Leftrightarrow \psi_\alpha(a,b,c) = (0,0,0) \Leftrightarrow (\alpha^2 a, \alpha b, \alpha c) = (0,0,0) \Leftrightarrow a = b = c = 0$$

Thus ψ_α is injective. It is easy to see that it is also surjective: consider $(a,b,c) \in W_p$. Then, the element $(a',b',c') = (\alpha^{-2}a, \alpha^{-1}b, \alpha^{-1}c)$ must exist in W_p and $\psi_\alpha(a',b',c') = (a,b,c)$. □

Claim 2.3.3.0.3. *$\psi_\alpha(H)$ is a conjugate of H.*

Proof. Since ψ_α is an isomorphism we know that $|\psi_\alpha(H)| = |H|$. It suffices to show that $S_H = S_{\psi_\alpha(H)}$

$$S_H = \{\pi(h) : h \in H\} = \{(bx, cx) : x \in \mathbb{Z}_p\}$$
$$S_{\psi_\alpha(H)} = \{(\alpha bx, \alpha cx) : x \in \mathbb{Z}_p\}$$

Since $\alpha \in \mathbb{Z}_p$ we must have that $\alpha x \in \mathbb{Z}_p$ and thus if we let $y = \alpha x$ we can rewrite $S_{\psi_\alpha(H)}$ as

$$S_{\psi_\alpha(H)} = \{(by, cy) : y \in \mathbb{Z}_p\}$$

Clearly, $S_H = S_{\psi_\alpha(H)}$ and thus by Claim 2.3.1.0.4 $H, \psi_\alpha(H)$ are conjugate.

□

Claim 2.3.3.0.4. *Let $A_{a,b,c} = \langle (a, b, c) \rangle$. Then, $\psi_\alpha(A_{a,b,c}) = A_{\alpha a,b,c}$*

Proof. Note that by Claim 2.3.3.0.3 we immediately get that $\psi_\alpha(A_{a,b,c})$ must be a conjugate of $A_{a,b,c}$ and thus it must be of the form $A_{a',b,c}$.

Specifically, since $\psi_\alpha((ax + \binom{x}{2}bc, bx, cx)) = (\alpha^2(ax + \binom{x}{2}bc), \alpha bx, \alpha cx)$ we get that

$$\psi_\alpha(A_{a,b,c}) = \langle (\alpha^2 a, \alpha b, \alpha c) \rangle = \{(\alpha^2(ax + \binom{x}{2}bc), \alpha bx, \alpha cx) : x \in \mathbb{Z}_p\}$$

$$A_{\alpha a,b,c} = \langle (\alpha a, b, c) \rangle = \{(\alpha ax + \binom{x}{2}bc, bx, cx) : x \in \mathbb{Z}_p\}$$

Let $(\alpha^2 a, \alpha b, \alpha c)^x = (\alpha^2(ax + \binom{x}{2}bc), \alpha bx, \alpha cx) \in \psi_\alpha(A_{a,b,c}), x \in \mathbb{Z}_p$. Then, since $\alpha^{-1} \in \mathbb{Z}_p$ we have that $x = \alpha^{-1}x'$ for some $x' \in \mathbb{Z}_p$. Thus,

$$(\alpha^2 a, \alpha b, \alpha c)^x = (\alpha^2 a, \alpha b, \alpha c)^{\alpha^{-1}x'} = (\alpha ax' + \binom{x'}{2}bc, bx', cx') \in A_{\alpha a,b,c}$$

Similarly, let $(\alpha a, b, c)^y = (\alpha(ay + \binom{y}{2}bc), by, cy) \in A_{\alpha a,b,c}, y \in \mathbb{Z}_p$. As before, since $\alpha, y \in \mathbb{Z}_p$, let $y = \alpha y'$. Then,

$$(\alpha a, b, c)^y = (\alpha a, b, c)^{\alpha y'} = (\alpha^2(ay' + \binom{y'}{2}bc), \alpha by', \alpha cy') \in \psi_\alpha(A_{a,b,c})$$

Thus, $A_{\alpha a,b} = \langle \alpha a, b, c \rangle = \langle (\alpha^2 a, \alpha b, \alpha c) \rangle = \psi_\alpha(A_{a,b,c})$ as required.

□

Consider the state in Eq 2.9, and suppose we have relabeled $\sigma_k(H)$ as $\sigma_{-l}(\psi_\alpha(H))$. Then, we get

$$\sigma_{-l}(\psi_\alpha(H)) \otimes \sigma_l(H) = \frac{|H|^2}{p^{2n}} \sum_{\substack{(A,B,C)\in\psi_\alpha(H)\\(a',b',c')\in H,\\u,v\in\mathbb{Z}_p^{2n-2}}} \omega^{-l(A+Bu)+l(a'+b'v)} |u+C, v+c'\rangle\langle u, v|$$

$$= \frac{1}{p^{2n-2}} \sum_{x,y\in\mathbb{Z}_p, u,v\in\mathbb{Z}_p^n} \omega^{l(a(x-\alpha y)+bc(\binom{x}{2}-\alpha\binom{y}{2})+b(vx-yu))} |u+cx, v+cy\rangle\langle u, v|$$

To this we can apply the CG transform given in [17, Eq.21] to obtain

$$\frac{1}{p^{2n-2}} \sum_{x,y\in\mathbb{Z}_p, u,v,w_1,w_2\in\mathbb{Z}_p^n} \omega^{l(a(x-\alpha y)+bc(\binom{x}{2}-\alpha\binom{y}{2})+b(vx-yu))+\frac{l}{2}(u+cx+v+cy)w_1-\frac{l}{2}(u+v)w_2}$$
$$|u+cx-v-cy, w_1\rangle\langle u-v, w_2|$$

$$= \frac{1}{p^{2n-2}} \sum_{x,y\in\mathbb{Z}_p, u,v,w_1,w_2\in\mathbb{Z}_p^n} \omega^{l(a(x-\alpha y)+bc(\binom{x}{2}-\alpha\binom{y}{2})+b(vx-yu))+\frac{l}{2}((u+v)(w_1-w_2)+(cx+cy)w_1}$$
$$|u+cx-v-cy, w_1\rangle\langle u-v, w_2|$$

Now, to simplify, we can substitute $u' = u - v, v' = u + v$ and note that $v = \frac{v+-u+v}{2} = \frac{v'-u'}{2}$ and $u = \frac{u+v-v+u}{2} = \frac{u'+v'}{2}$. Then, we get

$$\frac{1}{p^{2n-2}} \sum_{x,y\in\mathbb{Z}_p, u',v',w_1,w_2\in\mathbb{Z}_p^n} \omega^{l(a(x-\alpha y)+bc(\binom{x}{2}-\alpha\binom{y}{2})+b(\frac{v'-u'}{2}x-y\frac{v'+u'}{2}))+\frac{l}{2}(v'(w_1-w_2)+(cx+cy)w_1}$$
$$|u'+cx-cy, w_1\rangle\langle u', w_2|$$

$$= \frac{1}{p^{2n-2}} \sum_{x,y\in\mathbb{Z}_p, u',v',w_1,w_2\in\mathbb{Z}_p^n} \omega^{l(a(x-\alpha y)+bc(\binom{x}{2}-\alpha\binom{y}{2}))+\frac{-u'b}{2}(x+y)+w_1c(x+y)+\frac{v'l}{2}((w_1-w_2)+(x-y)b)} \tag{2.10}$$
$$|u'+cx-cy, w_1\rangle\langle u', w_2|$$

Ideally we would like to simplify this. Since ω is a root of unity, we know that summing over, say, ω^k for all of $k \in \mathbb{Z}_p^n,\ k \neq 0$ will yield 0. Thus, as seen in [17], since v' only appears as an exponent of ω in Eq. 2.10 it can be factored out. Thus, consider the portion of the above equation that is a sum over v':

$$\sum_{v'\in\mathbb{Z}_p^n} \omega^{\frac{v'l}{2}((w_1-w_2)l+(x-y)b)} \begin{cases} p^n,\ (w_1-w_2)+(x-y)b = 0 \\ 0 \textbf{ else} \end{cases}$$

Thus, we only need to consider when $(w_1 - w_2) + (x - y)b = 0 \Rightarrow b(x-y) + w_1 = w_2$. With this substitution and then relabelling by $w = w_1 + b(x - y)$ Eq. 2.10 becomes

$$\frac{1}{p^{n-2}} \sum_{x,y\in\mathbb{Z}_p, u',w\in\mathbb{Z}_p^n} \omega^{l(a(x-\alpha y)+bc(\binom{x}{2}-\alpha\binom{y}{2})+b\frac{u'}{2}(x-y))+\frac{lc}{2}((x+y)(w-bx+by)} |u'+cx-cy, w-b(x-y)\rangle\langle u', w| \tag{2.11}$$

Now, recall that the conjugate subgroups of $A_{a,b,c}$ are determined by b, c. Suppose c is the zero vector; then b in its "standard form" is one of $\sum_{i=1}^{p} \binom{p}{i}$ possible vectors with only ones and zeroes as entries. Then Eq 2.11 is

$$\frac{1}{p^{n-2}} \sum_{x,y\in\mathbb{Z}_p,u',w\in\mathbb{Z}_p^n} \omega^{l(a(x-\alpha y)+b\frac{u'}{2}(x-y))}|u', w-b(x-y)\rangle\langle u', w|$$

If we then let $x' = x - y$ then we obtain

$$\frac{1}{p^{n-2}} \sum_{x',y\in\mathbb{Z}_p,u',w\in\mathbb{Z}_p^n} \omega^{l(a(x'+y(1-\alpha))+b\frac{u'}{2}x')}|u', w-bx'\rangle\langle u', w|$$

After measurement we obtain a $|w-bx'\rangle$ and $|u'\rangle$, both with probability $\frac{1}{p^n}$, collapsing the state to a multiple of

$$\sum_{y'\in\mathbb{Z}_p} \omega^{l(a(x'+y(1-\alpha))+b\frac{u'}{2}x')}$$

which is only nonzero if $x' + y(1-\alpha) = 0$.

On the other hand, consider $H = A_{a,b,c}$, c nonzero, for which the value of b, c determines the conjugate subgroups. As such, we do not care about the value of a for the HSCP. Thus, we want to remove in from our sum. To do this we can use the trick in [17], in which it is observed that for a subgroup H there is a conjugate subgroup of the form $H_0 = \{(\frac{xy}{2}, x, y) : (x, y) \in S_H\}$. If $H = A_{a,b,c}$ this subgroup would be $A_{0,b,c} = \{(\frac{bcx^2}{2}, bx, cx) : x \in \mathbb{Z}_p\}$.

To obtain this conjugate subgroup, let $g = (\hat{x}, \hat{y}, \hat{z}) \in W_p$ be an element such that $H^g = gHg^{-1} = H_0$. Then, we must have that for any $(x, y, z) \in H$,

$$g(x, y, z)g^{-1} = (x + y\hat{z} - \hat{y}z, y, z) = (\frac{yz}{2}, y, z)$$

Once again, if $H = A_{a,b,c}$ then this would correspond to

$$g(ax + \binom{x}{2}cb, bx, cx)g^{-1} = (ax + \binom{x}{2}cb + bx\hat{z} - \hat{y}x, bx, cx) = (\frac{bcx^2}{2}, bx, cx)$$

In addition, for $\psi_\alpha(A_{a,b,c})$ we want $\psi_\alpha(g) = (\alpha^2\hat{x}, \alpha\hat{y}, \alpha\hat{z})$ so that

$$\begin{aligned}\psi_\alpha(g)(\alpha^2(ax + \binom{x}{2}bc), \alpha bx, \alpha cx)\psi_\alpha(g)^{-1} &= (\alpha^2(ax + \binom{x}{2}bc) + \alpha^2 bx\hat{z} - \alpha^2\hat{y}cx, \alpha bx, \alpha cx) \\ &= (\frac{\alpha^2 bcx^2}{2}, \alpha bx, \alpha cx)\end{aligned}$$

However, since $\psi_\alpha(A_{a,b,c}) = A_{\alpha a,b,c}$ we could instead consider some $g' = (\hat{x}', \hat{y}', \hat{z}')$ so that

$$g'(\alpha ay + \binom{y}{2}bc, by, cy)g'^{-1} = (\alpha ay + \binom{y}{2}bc + by\hat{z}' - \hat{y}'cy, by, cy) = (\frac{bcy^2}{2}, by, cy)$$

However, it is easy to see that the $H_0 = A_{0,b,c}$ for both $A_{a,b,c}$ and $A_{\alpha a,b,c}$ and thus $g = g'$. Now, consider Eq. 2.11, with the normalization omitted, and make the required substitutions with g defined above:

$$\sum_{x,y\in\mathbb{Z}_p,u',w\in\mathbb{Z}_p^n} \omega^{l(\frac{bc}{2}(x^2-y^2)+\hat{y}c(x-y)-b\hat{z}(x-y)+b\frac{u'}{2}(x-y))+\frac{lc}{2}((x+y)(w-xb+by)} |u'+c(x-y), w-b(x-y)\rangle\langle u', w| \quad (2.12)$$

Consider the substitution $x' = x - y, y' = x + y$. Then Eq 2.12 becomes

$$\sum_{x',y'\in\mathbb{Z}_p,u',w\in\mathbb{Z}_p^n} \omega^{l(\frac{bc}{2}(x'y')+\hat{y}cx'-b\hat{z}x'+b\frac{u'}{2}x')+\frac{lc}{2}y'(w-bx')} |u'+cx', w-bx'\rangle\langle u', w|$$

After measuring to obtain $u' + cx', w' = w - bx'$, we are left with a multiple of

$$\sum_{y'\in\mathbb{Z}_p} \omega^{l(\frac{bc}{2}(x'y')+\hat{y}cx'-b\hat{z}x'+b\frac{u'}{2}x')+\frac{lc}{2}y'w'}$$

If we modify Eq 2.12 somewhat this may yield better results. First, do not simplify $\psi_\alpha(H)$. Second, consider $g = (\hat{x}, \hat{y}, \hat{z})$ where

$$g(ax + \binom{x}{2}bc, bx, cx)g^{-1} = (a + \binom{x}{2}bc + b\hat{z} - \hat{y}c, b, c) = (\frac{bc}{2}, b, c)$$

Make this substitution and $\phi_\alpha(g)$ instead and relabel so that our sum runs over elements in S_H; this is allowed as the substitution will remove the "a" term from the equation. That is, let $b := bx, c := x, b' := by, c' := y$. Then,

$$\frac{1}{p^n} \sum_{(b,c),(b',c')\in S_H,u',w\in\mathbb{Z}_p^n} \omega^{\frac{l}{2}(2(\hat{y}c-b\hat{z})-2\alpha(\hat{y}c'-\hat{z}b')+u'(b+b')+w(c+c')} |u'+c-c', w+b'-b\rangle\langle u', w|$$

Here we have used Claim 2.3.1.0.6 and Claim 2.3.1.0.7 in order to simplify, as these claims imply that $b'c - c'b = 0$ since $(b', c'), (b, c) \in S_H$

Now, let us try to simplify by setting $c_1 := c - c', b_1 := b - b'$; since S_H is a linear vector space this is allowed. Then,

$$\frac{1}{p^n} \sum_{(b,c),(b',c')\in S_H,u',w\in\mathbb{Z}_p^n} \omega^{\frac{l}{2}(2(\hat{y}(c_1+c')-(b_1+b')\hat{z})-2\alpha(\hat{y}c'-\hat{z}b')+u'(b_1+2b')+w((c_1+c')+c')} |u'+c_1, w-b_1\rangle\langle u', w| \quad (2.13)$$

Finally, this becomes:

$$\frac{1}{p^n}\sum_{(b_1,c_1),(b',c')\in S_H,u',w\in\mathbb{Z}_p^n}\omega^{l(b'(u'+\hat{z}(\alpha-1))+c'(\hat{y}(1-\alpha)+w))+\frac{l}{2}(b_1(u'-2\hat{z})+c_1(w+2\hat{y}))}|u'+c_1,w-b_1\rangle\langle u',w|$$

Measuring yields pairs $|u'+c_1\rangle, |w-b_1\rangle$ with the result

$$\sum_{(b',c')\in S_H}\omega^{l(b'(u'+\hat{z}(\alpha-1))+c'(\hat{y}(1-\alpha)+w))+\frac{l}{2}(b_1(u'-2\hat{z})+c_1(w+2\hat{y}))}|u'+c_1,w-b_1\rangle\langle u',w|$$

This is only nonzero when $b'(u'+\hat{z}(\alpha-1))+c'(\hat{y}(1-\alpha)+w)=0$ since the values of (b',c') go through all of S_H. Recall the symplectic inner product we defined previously. Then, this is nonzero when

$$(b',c')\cdot(\hat{y}(1-\alpha)+w,u'+\hat{z}(1-\alpha))=0\Rightarrow(\hat{y}(1-\alpha)+w,u'+\hat{z}(1-\alpha))\in S_H^\perp$$

Thus, measurement yields the vector $(\hat{y}(1-\alpha)+w,u'+\hat{z}(1-\alpha))\in S_H^\perp$.

If the above procedure is repeated n times we obtain a series of elements $(u_i,v_i)\in S_H$ and thus

$$(u_i+(1-\alpha_i)\hat{y},v_i+(1-\alpha_i)\hat{z})\in S_H^\perp,\ 1\leqslant i\leqslant n+1$$

After a division by $(1-\alpha_i)$ and taking differences one can obtain vectors

$$(u_i',v_i')=(\frac{u_i}{(1-\alpha_i)}-\frac{u_{n+1}}{(1-\alpha_{n+1})},\frac{v_i}{(1-\alpha_i)}-\frac{v_{n+1}}{(1-\alpha_{n+1})})\in S_H^\perp$$

which form a basis for $S_H^\perp$ with high probability. From this one can obtain S_H, H_0, and H, by setting $(\hat{y},\hat{z})=\frac{1}{1-\alpha_1}(u_1-u_1',v_1-v_1')$.

2.4 General Conclusions

A natural question to ask is what made the CG transform useful in the regular and generalized Heisenberg groups. While investigating other groups may be useful to determine when this transform is helpful, the observations listed below may help shed some light.

Firstly, the hidden subgroup in the above groups were normal in a normal subgroup of the overall group. Furthermore, due to the nature of the conjugacy classes, solving the HSP could be reduced to solving the HSCP, followed by some post-processing and the algorithm for solving the HSP in normal groups. Thus, groups in which conjugacy classes have a useful characterization may benefit from the CG transform, or have some reduction from the HSP to the potentially simpler HSCP.

Next, these groups are extraspecial p-groups. Thus, they have some useful properties, which makes them almost abelian. Firstly, they are two-step nilpotent and solvable. Further, the group mod the center is an elementary abelian p-group, and this is exploited in the solution.

The fact that the hidden subgroup is abelian was exploited in the procedure for the Weyl-Heisenberg group, and the fact that all subgroups are either normal or abelian may be of assistance, as well.

In the paper by [21] a proof is given in Theorem 1 for why the hidden conjugates of a subgroup $H_a = \langle (a, 0) \rangle, |H_a| = q, a \in Z_p^*$ are fully reconstructive in $A_p = Z_p^* \ltimes Z_p$, partially because of the high probability of observing a $p - 1$ dimensional representation, and because of a reduction, for $Z_q \ltimes Z_p$ as well. This is similar to the fact that for the regular- and generalized Weyl-Heisenberg groups, one observes a p dimensional irrep with high probablity; otherwise the irrep has dimension one. Not only does this allow the consideration of only two kinds of irreps, it indicates which one will most likely be measured. Further, the fact that the tensor product of such irreps decomposes in a useful manner is also of interest.

Chapter 3

Wreath Product Groups

3.1 Wreath Product Overview

This chapter will discuss the HSP in wreath product groups. It will begin with an overview of these groups: a definition, some general results, and so on, followed by some important background on the representation theory of such groups. Finally, a specific group, $\mathbb{Z}_p^n \wr \mathbb{Z}_p^d$ will be examined in its relation to the HSP.

There are a number of reasons why this class of groups was chosen to be analyzed. First, wreath product groups, in general, have a fascinating subgroup structure and interesting representation theory, with limited discussion in existing papers. Next, under certain conditions, as will be discussed later, these are nilpotent groups, which may have been one of the beneficial characteristics of the Weyl-Heisenberg group which allowed for the HSP to be solved. Additionally, for $\mathbb{Z}_p^n \wr \mathbb{Z}_p^d$, as will be shown, the representations are all of dimension a power of the prime p, which may indicate that the tensor product of two representations may decompose nicely.

Definition 15 (Wreath Product)**.** Let G, H be groups, where H acts on a set X with $|X| = n$, and let $B = \prod_{s \in X} G_s$, where "product" is the direct product. Then the *wreath product* of G, H is

$$G \wr H = B \rtimes_\psi H = \{(b, h) : b \in B, h \in H\}$$

where B is called the *base group*, and ψ is a homomorphism $\psi : H \to S_n$.

The group operation can be defined by

$$(b; h)(c; g) = (\psi_g(b)c; hg), \qquad \text{and} \quad (b; h)^{-1} = (\psi_{h^{-1}}(b^{-1}); h^{-1})$$

An alternate way of viewing this group is according to the definition in [5]. Let G, F be two groups where G acts on a finite set X. Let $F^X = \{f : X \to F\}$ be the set of maps, and define the operation on F^X as

$$(f \cdot h)(x) = f(x)h(x) \ \forall h, f \in F^X, x \in X$$

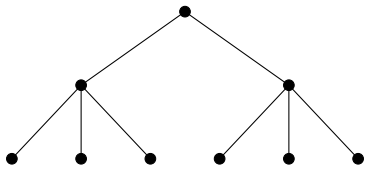

Figure 3.1: $Z_3 \wr Z_2$ Tree

In this case, G can be considered to act on F^X as

$$(gf)(x) = f(g^{-1}x) \text{ and } g(f \cdot f') = gf \cdot gf' \text{ and } (gf)^{-1} = gf^{-1}$$

Finally, the group operation can be defined as

$$(f, g)(f', g') = (g'f \cdot f', gg'), \text{ where } (gf' \cdot f)(x) = f'(g^{-1}x)f(x)$$

The similarities of this definition with the above one is clear. For the most part, this definition will not be employed.

Finally, one can view H as a subgroup of S_n when $|H| = n$, so that $X = \{1, 2, ..., n\}$, and so H acts by permutation on X, so that the end result is permuting the elements in B. That is, let $(g_1, .., g_n; \tau), (h_1, ..., h_n; \sigma) \in G \wr H$ where $g_i, h_i \in G, \tau, \sigma \in H$. Then the group operation is

$$(g_1, ..., g_n; \tau)(h_1, ..., h_n; \sigma) = (g_{\sigma(1)}h_1, ..., g_{\sigma(n)}h_n; \tau\sigma)$$

Clearly, if $|G| = m, |H| = n$, then $|G \wr H| = m^n n$. Unfortunately, in [4] it is shown that $G \wr H$ is nilpotent if, and only if, G, H are p groups. However, if G, H are solvable then $G \wr H$ will also be solvable.

Visually, one could picture this as a tree with height 2, where the first layer of nodes represent the base group, and the roots are the elements in G. As an example, consider $G = Z_3$, $H = Z_2$. Clearly, we have two "layers" of actions then: H permutes elements in the base group B by its action on X, and each element of this base group is the group G which acts on a set Y. That is, the automorphism group of the above tree is, in fact, isomorphic to the wreath product $G \wr H$.

Figure 3.1 helps visualize iterated wreath products, which can be thought of as increasing the height of the tree by appending additional nodes to the current root. This helps justify that the wreath product is an associative operation. That is, given three groups G, H, K,

$$(G \wr H) \wr K \cong G \wr (H \wr K)$$

Lemma 3.1.0.0.1. *Let G, H, K be three groups, where H acts on a set X and K on a set Y, where $|X| = x, |Y| = y$. Then, there is an isomorphism $\Psi : G \wr (H \wr K) \to (G \wr H) \wr K$.*

Proof. First, let

$$G \wr H = \{(g, h) : g \in G^X, h \in H\}$$
$$(G \wr H) \wr K = \{((g, h), k) : (g, h) \in (G \wr H)^Y, k \in K\}$$

Since $(G \wr H)^Y = ((G \wr H), ..., (G \wr H)) = (G^X \rtimes H, ..., G^X \rtimes H)$ we obtain $|XY|$ copies of G and $|Y|$ copies of H.

For brevity, denote the action of a group on the base group as a dot product; that is, for $(g,h),(g',h') \in (G \wr H)^Y$, let $(g,h) = ((g_1^1, ..., g_x^1; h_1), ..., (g_1^y, ..., g_x^y; h_y)), (g',h') = ((g_1^{'1}, ..., g_x^{'1}; h_1'), ..., (g_1^{'y}, ..., g_x^{'y}; h_y'))$, so that g, h are $y-$dimensional vectors with entries $(g_1^i, ..., g_x^i), h_i, 1 \leqslant i \leqslant y$ respectively. Then, for $((g,h);k),((g',h');k') \in (G \wr H) \wr K$ we get

$$\begin{aligned}
((g,h),k)((g',h'),k') &= ((k' \cdot (g,h))(g',h'), kk') \\
&= ((g_1^1, ..., g_x^1; h_1), ..., (g_1^y, ..., g_x^y; h_y); k)((g_1^{'1}, ..., g_x^{'1}; h_1'), ..., (g_1^{'y}, ..., g_x^{'y}; h_y'); k') \\
&= ((k' \cdot (g_1^1, ..., g_x^1; h_1))(g_1^{'1}, ..., g_x^{'1}; h_1'), ..., (k' \cdot (g_1^y, ..., g_x^y; h_y))(g_1^{'y}, ..., g_x^{'y}; h_y'); kk') \\
&= ((g_1^{k'(1)}, ..., g_x^{k'(1)}; h_{k'(1)})(g_1^{'1}, ..., g_x^{'1}; h_1'), ..., (g_1^{k'(y)}, ..., g_x^{k'(y)}; h_{k'(y)})(g_1^{'y}, ..., g_x^{'y}; h_y'); kk') \\
&= ((g_1^{h_1'(k'(1))} g_1^{'1}, ..., g_x^{h_1'(k'(1))} g_x^{'1}; h_{k'(1)} h_1'), ..., \\
&\quad (g_1^{h_y'(k'(y))} g_1^{'y}, ..., g_x^{h_y'(k'(y))} g_x^{'y}; h_{k'(y)} h_y'); kk') \\
&= (((h' \cdot (k' \cdot g))g', (k' \cdot h)h'), kk')
\end{aligned}$$

On the other hand, let

$$H \wr K = \{(h,k) : h \in H^Y, k \in K\}$$
$$G \wr (H \wr K) = \{(g,(h,k)) : g \in G^{XY}, (h,k) \in H \wr K\}$$

where, $(h,k) = (h_1, ..., h_y; k)$ and thus $(g,(h,k)) = (g_1, ..., g_{xy}; (h_1, ..., h_y; k))$ with the group operation, for $(g,(h,k)),(g',(h',k')) \in G \wr (H \wr K)$, defined by

$$\begin{aligned}
(g,(h,k))(g',(h',k')) &= (((h',k') \cdot g)g', (h,k)(h',k')) \\
&= (((h',k') \cdot g)g', ((k' \cdot h)h', kk'))
\end{aligned}$$

Consider an element $g = (g_1, ..., g_{xy}) \in G^{XY}$ and partition it to obtain $\hat{g_1} = (g_1, ..., g_x), \hat{g_y} = (g_{xy-x}, ..., g_{xy})$, so that $g = (\hat{g_1}, ..., \hat{g_y})$.

Next, consider the action of $(h,k) = (h_1, ..., h_y; k)$ on G^{XY}. We wish to map this action; that is, the action of $H \wr K$ on G^{XY} in $G \wr (H \wr K)$ to an action by $k \in K$ on the base group $(G \wr H)^Y$ in $(G \wr H) \wr K$.

Then, one can define $\Psi : (G \wr (H \wr K)) \to (G \wr H) \wr K$ by

$$\begin{aligned}
\Psi(((h',k') \cdot g)g', (k' \cdot h)h', kk') &= \Psi((h_1', ..., h_y'; k') \cdot (\hat{g_1}, ..., \hat{g_y})((\hat{g_1'}, ..., \hat{g_y'})), (k' \cdot (h_1, ..., h_y))(h_1', ..., h_y'); kk') \\
&= (((h_1' \cdot (k' \cdot \hat{g_1}))\hat{g_1'}; h_{k'(1)} h_1'), ..., ((h_y' \cdot (k' \cdot \hat{g_y}))\hat{g_y'}; h_{k'(y)} h_y')) \\
&= (((\hat{h'} \cdot (\hat{k'} \cdot \hat{g}))\hat{g'}, (\hat{k'} \cdot \hat{h})\hat{h'}), k\hat{k'})
\end{aligned}$$

where $\hat{g}$ is a y-dimensional vector with entries $\hat{g_i}, 1 \leqslant i \leqslant y$, $\hat{h}$ is simply a y-dimensional vector with values $h_i, 1 \leqslant i \leqslant y$, and $\hat{k} = k$.

If the input to Ψ is simply $(g,(h,k)) = (g_1,...,g_{xy},(h_1,...,h_y;k)))$, then

$$\Psi((g,(h,k)) = (((g_1,...,g_x;h_1),...,(g_{xy-x},...,g_{xy};h_y));k)$$

□

This idea allows for the definition of an iterated wreath product, given in [23]:

Definition 16 (Iterated wreath product)**.** Let r be a positive nonzero integers. Then the *iterated wreath product* of a group G can be defined recursively as

$$W_1 = G$$

$$W_r = W_{r-1} \wr G$$

So that $W_r \cong G \wr ... \wr G$ where G appears r times.

When $G = Z_n$ for a nonzero integer n this group will be denoted $W_{n,r}$.

3.1.1 Group structure

In this subsection we will consider the general subgroup structure of a wreath group, and also discuss conjugacy classes in such a group.

Let $G \wr H$ be a group with base group G^X as defined above. Recall that if $(b;h) \in G \wr H, b = (g_1,...,g_x)$ where $g_i \in G, x = |H|$ and where ψ denotes the action of H on base group G^X, then

$$(b;h)^{-1} = (\psi_{h^{-1}}(b^{-1});h^{-1}) = (g^{-1}_{h^{-1}(1)},...,g^{-1}_{h^{-1}(x)};h^{-1})$$

Then, let $x = (b;h), y = (a;k) \in G \wr H$. Then,

$$\begin{aligned} x^{-1}yx &= (\psi_{h^{-1}}(b^{-1});h^{-1})(a;k)(b;h) = (\psi_{h^{-1}}(b^{-1});h^{-1})(\psi_h(a)b;kh) \\ &= (\psi_{kh}(\psi_{h^{-1}}(b^{-1}))\psi_h(a)b;h^{-1}kh) \\ &= (\psi_k(b^{-1})\psi_h(a)b;h^{-1}kh) \end{aligned}$$

which gives us a formula for determining conjugates of an element. In general, if K is a subgroup of $G \wr H$, and $g \in G \wr H$, then let

$$K^g = \{g^{-1}kg : k \in K\}$$

denote the conjugate of K by g. Two subgroups K, K' of $G \wr H$ are then considered conjugate if $K' = K^g$ for some element $g \in G$.

Notice that the subgroup $B_w = \{(b;e_h) : b \in B\}$ is normal in $G \wr H$.

Now, let us determine the commutator and center subgroups of $G \wr H$. Let x, y be as defined above. Recall that $x \in Z(G \wr H) \Leftrightarrow x^{-1}yx = y \forall y \in G \wr H$. Thus, we wish to determine the form that $x \in Z(G \wr H)$ takes by solving this equality. Then,

$$x^{-1}yx = (\psi_k(b^{-1})\psi_h(a)b;h^{-1}kh) = (a;k) \text{ if } \psi_k(b^{-1})\psi_h(a)b = a, h^{-1}kh = k$$

Of course, $h^{-1}kh = k$ holds for $h \in Z(H)$. In addition, b must be of the form $b = (g, ..., g), g \in G$ so that $\psi_k(b) = b \forall k \in H$. In general, the subgroup

$$\Delta(G) = \{b : b \in G^X, h(b) = b \forall h \in H\} = \{(g, ..., g) : g \in G\} \cong G$$

is called the *diagonal subgroup* of G^X. Thus we require that $b \in \Delta(G)$ so that any action on it by h leaves it unchanged. Using such a b then the expression above becomes $b^{-1}\psi_h(a)b = a$; that is,

$$(g^{-1}, ..., g^{-1})(a_{h(1)}, ..., a_{h(n)})(g, ..., g) = (g^{-1}a_{h(1)}g, ..., g^{-1}a_{h(n)}g)$$

Thus, we require that $g \in Z(G)$ and that $\psi_h(a) = a$. Since this must hold for all $a \in G^X$, if $|X| > 1$ we additionally require that $h = e_H$. If $|X| = 1$ then h acts trivially on a and so h can be any element in H. Finally, we obtain the following set for the center, provided that $|X| > 1$:

$$Z(G \wr H) = \{(b; e_h) : b = (g, ..., g) \in \Delta(G), g \in Z(G)\}$$

If $|X| = 1$ then $Z(G \wr H) = \{(b; h) : b \in Z(G), h \in Z(H)\}$

Next, the commutator subgroup is generated by

$$\begin{aligned} y^{-1}x^{-1}yx &= (\psi_{k^{-1}}(a^{-1}), k^{-1})(\psi_k(b^{-1})\psi_h(a)b; h^{-1}kh) \\ &= (\psi_{h^{-1}kh}(\psi_{k^{-1}}(a^{-1}))\psi_k(b^{-1})\psi_h(a)b; k^{-1}h^{-1}kh) \\ &= (\psi_{[h,k^{-1}]}(a^{-1})\psi_k(b^{-1})\psi_h(a)b; k^{-1}h^{-1}kh) \end{aligned}$$

When H is abelian this expression becomes

$$y^{-1}x^{-1}yx = (a^{-1}\psi_k(b^{-1})\psi_h(a)b; e_H)$$

3.1.2 $Z_p^n \wr Z_q$

As a specific subset of wreath product groups, consider $G = Z_p^n, H = Z_q, B = G_0 \times ... \times G_{q-1}$, where p, q are prime powers. Then,

$$Z_p^n \wr Z_q = \{(g_0, ..., g_{q-1}; h) : g_i \in Z_p^n, h \in Z_q\} = \{(b; h) : b \in B, h \in H\}$$

We can then consider the action of Z_q on B as addition mod q: let $(g_0, .., g_{q-1}; a),, (h_0, ..., h_{q-1}; b) \in G \wr H$ where $g_i, h_i \in G, a, b \in H$. Then,

$$(g_0, .., g_{q-1}; a)(h_0, ..., h_{q-1}; b) = (g_{b \ mod \ q} + h_0, ..., g_{-1+b \ mod \ q} + h_{q-1}; a + b \ mod \ q)$$

Claim 3.1.2.0.1. *Let $P = \mathbb{Z}_p^n \wr \mathbb{Z}_q^d$, and Write any $h \in \mathbb{Z}_q^d$ as a unique string $k = (k_{d-1}...k_0) = (k_i)_{0 \leqslant i < d} \in \mathbb{Z}_q^d$ where each $k_i \in \mathbb{Z}_q$. Let $g = ((g_v)_{v \in \mathbb{Z}_q^d}; h) \in P$, where $h = (h_i)_{0 \leqslant i < d}, v = (v_i)_{0 \leqslant i < d} \in \mathbb{Z}_q^d$. Then, for $x \geqslant 1$,*

$$g^x = (\sum_{j=0}^{x-1} (g_{v+jh})_{v \in \mathbb{Z}_q^d}; xh)$$

where $v + jh = (v_i + jh_i)_{0 \leqslant i < d}, xh = (xh_i)_{0 \leqslant i < d}$.

Proof. Suppose $g = ((g_v)_{v\in\mathbb{Z}_q^d}; h) \in P$, where $h = (h_i)_{0\leqslant i<d}, v = (v_i)_{0\leqslant i<d} \in \mathbb{Z}_q^d$. Let us prove the result using induction on x. When $x = 1$ this is trivial. If $x = 2$ then

$$\begin{aligned} g^2 &= ((g_v)_{v\in\mathbb{Z}_q^d}; h)((g_v)_{v\in\mathbb{Z}_q^d}; h) = (\phi_h((g_v)_{v\in\mathbb{Z}_q^d})(g_v)_{v\in\mathbb{Z}_q^d}; 2h) \\ &= ((g_{v+h})_{v\in\mathbb{Z}_q^d}(g_v)_{v\in\mathbb{Z}_q^d}; 2h) = (\sum_{j=0}^{1}(g_{v+jh})_{v\in\mathbb{Z}_q^d}; 2h) \end{aligned}$$

Suppose this holds for all $x < k$ and consider $x = k$. Then, since $g^k = g^{k-1}g$,

$$\begin{aligned} g^k &= (\sum_{j=0}^{k-2}(g_{v+jh})_{v\in\mathbb{Z}_q^d}; (k-1)h)((g_v)_{v\in\mathbb{Z}_q^d}; h) \\ &= (\sum_{j=0}^{k-2}(g_{v+jh+h})_{v\in\mathbb{Z}_q^d}(g_v)_{v\in\mathbb{Z}_q^d}; kh) \\ &= (\sum_{j=0}^{k-1}(g_{v+jh})_{v\in\mathbb{Z}_q^d}; kh) \end{aligned}$$

which proves the claim. □

Lemma 3.1.2.0.1. *Let $P = Z_p^n \wr Z_q$, where p, q are powers of distinct primes. Then there is an element $g \in P$ of order pq.*

Proof. Let $k = (e_1, 0, ..., 0; 1) \in P$ where $e_1 = (1, 0, ..., 0) \in Z_p^n$,. Also, suppose $g = (((g_v)_{v\in\mathbb{Z}_q}; h)$. Then, using the previous lemma,

$$k^q = (e_1, ..., e_1; 0), k^{pq} = (k^q)^p = (pe_1, ..., pe_1; 0) = (0, ..., 0; 0)$$

Suppose $0 < x < pq$ and $k^x = (0, ..., 0; 0)$. Then, $g^x = (\sum_{i=0}^{x} g_i, ..., \sum_{i=0}^{x} g_{i-1}; xh) \Rightarrow xh = 0 \Rightarrow x = aq$ for some nonzero integer a.

Then,

$$g^x = (g^q)^a = (e_1, ..., e_1; 0)^a = (ae_1, ..., ae_1; 0) \Rightarrow a = p$$

But this would indicate that $x = pq$ which contradicts our assumption. That is, pq is the order of k. □

3.1.2.1 Nilpotency

This subsection will aim to determine the nilpotency class of $P = G \wr Z_q$ where G is an abelian group.

Recall that a group P is nil-k-potent if its upper central series terminates with P after k iterations; that is,

$$\{1\} = Z_0 \lhd Z_1 ... \lhd Z_k = P$$

where $Z_{i+1} = \{x \in P : [x, g] \in Z_i \ \forall g \in P\}$, and since $Z_1 = Z(P)$ so one can define Z_{i+1} instead according to the relation $Z_{i+1}/Z_i = Z(P/Z_i)$.

First, let us determine what $Z(P)$ is. Suppose $z = (z_0, ..., z_{q-1}; z_q) \in Z(P)$ so that $z^{-1} = (-z_{-z_q}, ..., -z_{-1-z_q}; -z_q)$ and let $g = (g_0, ..., g_{q-1}; h) \in P$. Then,

$$z^{-1}gz = (-z_h + g_{z_q} + z_0, ..., -z_{h-1} + g_{z_q-1} + z_{q-1}; h) = (g_0, ..., g_{q-1}; h)$$

This occurs if for each i we have $z_i = z_{h+i}$ and $z_q = 0$. Since this must hold $\forall h \in Z_q$ we must that each z_i is equal; that is, $z = (z_0, ..., z_0; 0)$.

Concretely, consider the case when $h = 1$ and $g_i = 0 \forall i \in Z_q$. Then,

$$z^{-1}gz = (-z_1 + z_0, ..., z_{q-1} - z_0; 1) = (0, ..., 0; 1)$$

The last equality holds if $z_i = z_{i+1} \forall i \in Z_q$ which forces all the z_i to be equal.

Similarly, consider when $g = (1, 0, ..., 0; 0)$ and then

$$z^{-1}gz = (g_{z_q}, ..., g_{z_q-1}; 0) = (1, 0, ..., 0; 0)$$

The final equality requires that $g_{z_q} = g_0 = 1 \Rightarrow z_q = 0$.

Then, $Z(P) = \{(z, z, ..., z; 0) : z \in G\} \cong G$.

This gives us Z_1 in the upper central series of P. Next, let us find $Z(P/Z_1)$. First,

$$P/Z_1 = \{gZ_1 : g \in P\}$$

and our goal is to find

$$Z(P/Z_1) = \{gZ_1 \in P/Z_1 : [gZ_1, hZ_1] = [g, h]Z_1 = Z_1 \forall h \in P\}$$

Now, if $zZ_1 \in Z(P/Z_1)$ then

$$[g, z]Z_1 = Z_1 \Rightarrow z^{-1}gzZ_1 = gZ_1 \Rightarrow z^{-1}gz \in gZ_1$$

for all $g \in P$.

Let $z = (z_0, ..., z_{q-1}; z_q) \in Z(P/Z_1), g = (g_0, ..., g_{q-1}; h) \in P$. Then, to find $Z(P/Z_1)$ we must solve for z in the equation

$$z^{-1}gz = (-z_h + g_{z_q} + z_0, ..., -z_{h-1} + g_{z_q-1} + z_{q-1}; h) = (g_0, ..., g_{q-1}; h)Z_1$$

Recall that $Z_1 = \{(a, ..., a; 0) : a \in G\}$ and thus

$$gZ_1 = \{(g_0 + a, ..., g_{q-1} + a; h) : a \in G\}$$

Thus, the above equation becomes, for some $a \in G$,

$$(-z_h + g_{z_q} + z_0, ..., -z_{h-1} + g_{z_q-1} + z_{q-1}; h) = (g_0 + a, ..., g_{q-1} + a; h)$$

Using the same process as before, first consider the case when $g = (0, ..., 0; 1)$. Then,

$$z^{-1}gz = (z_0 - z_1, ..., z_{q-1} - z_0; 1) = (a, ..., a; 1)$$

Since $z_i = z_{i+1} + a$ for all $i \in \mathbb{Z}_q$, we can make a series of substitutions; that is, we have that

$$z_0 = z_1 + a, z_1 = z_2 + a \Rightarrow z_0 = z_2 + 2a, z_2 = z_3 + a \Rightarrow z_0 = z_3 + 3a$$

That is, in general, for $x \in \mathbb{Z}_q$,

$$z_0 = z_x + xa \Rightarrow z_x = z_0 - xa$$

and thus we can write the center element as

$$z = (z_0, z_0 - a, ..., z_0 + a - qa; z_q)$$

On the other hand, consider $g = (1, 0, ..., 0; 0)$. Then,

$$z^{-1}gz = (-z_0 + g_{z_q} + z_0, ..., -z_{q-1} + g_{z_q-1} - z_{q-1}; 0) = (g_{z_q}, ..., g_{z_q-1}; 0) = (1 + b, b, .., b; 0)$$

for some $b \in G$. As before, this forces z_q to be equal to 0. Thus,

$$Z(P/Z_1) = \{(0, -a, ..., a - qa; 0)Z_1 : a \in G\}$$

and so

$$Z_2 = \{(z, z - a, ..., z + a - qa; 0) : z, a \in G\}$$

This method described above for determining Z_2 holds in general for subsequent Z_k. It will by referred to as the "upper central series algorithm" moving forward.

However, note that the final element can be written in two ways: $z_{q-1} = z_0 - (q-1)a$ and $z_{q-1} = z_0 + a$. Equating the two we get

$$z_0 - (q-1)a = z_0 + a \Rightarrow (1-q)a = a \Rightarrow a = 0 \text{ or } q = 0 \in G$$

Clearly, if $a = 0$ then $Z_1 = Z_2$, otherwise $Z_1 \leqslant Z_2$. This motivates the following proposition:

Proposition 3.1.2.1.1. *Suppose $P = Z_n^m \wr Z_q^d, m, d \geqslant 1$, where q, n are not powers of a prime p. Then, P is not nilpotent.*

Proof. Recall that the center of P is

$$Z_1 = \{(g, ..., g; 0) : g \in Z_n^m\}$$

Let $q = bn^j + k, -n < k < n, k \neq 0, 0 < b < n, 0 < j$. As discussed in "upper central series algorithm" above, when trying to calculate Z_2 we obtain, for $z = (z_0, ..., z_{q^d-1}; 0) \in Z_2$ and $g = (0, ..., 0; \mathbf{1}) \in P$, where $\mathbf{1} = (0, ..., 0, 1)$.

$$z^{-1}gz = (z_0 - z_1, ..., z_{q^d-1} - z_0; \mathbf{1}) = gZ = (a, ..., a; \mathbf{1})$$

for $a \in Z_n^m$. After a series of substitutions one obtains two equations relating z_{q^d-1} and z_0:

$$z_{q^d-1} = z_0 + a \text{ and } z_{q^d-1} = z_0 - (q^d - 1)a = z_0 - (k-1)a$$

Equating the two equations we get

$$a = -(k-1)a \Rightarrow a = 0 \ mod \ n \text{ or } k = 0 \ mod \ n$$

By our choice of k we know that $k \neq 0 \ mod \ n$ and so that leaves $a = 0 \ mod \ n$. Thus, since an element in Z_2 is of the form $(z, z-a, ..., z-(q^d-1)a; 0)$ we get that

$$Z_2 = \{(z, ..., z; 0) : z \in Z_n^m\} = Z_1$$

Thus, since $Z_2 = Z_1$ we can conclude that P is not nilpotent. □

Now it remains to consider the case when p, q are both p-groups. The following lemma describes the form of an element in the upper central series.

Lemma 3.1.2.1.1. *Suppose $P = Z_{p^d}^n \wr Z_q, q = p^m, m \geqslant n, p$ prime, with the upper central series given by $\{(0, ..., 0; 0)\} = Z_0 \lhd Z_1 \lhd ....$ Then, for $0 \leqslant j < q$, and any $z \in Z_{p^d}, a = (a_x) \in B = \prod_{x \in Z_q}(Z_{p^d}^n)$, let*

$$z_j = z + \sum_{x=1}^{i} (-1)^x \binom{j}{x} a_x$$

then, the $(i+1)^{th}$ group in the series is given by

$$Z_{i+1} = \{(z_0, z_1, ..., z_{q-1}; 0) : z, a_x \in Z_{p^d}^n\}$$

while $i+1$ is less than the nilpotency class of P. For example, if $i = 2$ then we have

$$Z_3 = \{(z, z-a, z-2a+b, z-3a+3b, ..., z-(q-1)a + \binom{q-1}{2} b)\}$$

Proof. Use induction on $i' = i + 1$ to prove. In the "upper central series algorithm" above we have already shown that this holds when $0 \leqslant i \leqslant 1$. Suppose, then, that it holds for all $i' \leqslant k$ and consider when $i' = k+1$. Then,

$$Z_{k+1}/Z_k = Z(P/Z_k) = \{gZ_k \in P/Z_k : [g, h]Z_k = Z_k \forall h \in P\}$$

Let $z = (z_0, ..., z_{q-1}; z_q) \in Z(P/Z_k), g = (g_0, .., g_{q-1}; h) \in P$.

Since the claim holds for all $i' \leqslant k$ we know that

$$Z_k = \{(z, z+a_1, z+2a_1+a_2, ..., z + \sum_{x=1}^{k-1} (-1)^x \binom{q-1}{x} a_x; 0) : z, a_j \in G\}$$

Thus, we need to solve for z when

$$z^{-1}gz = (-z_h+g_{z_q}+z_0,...,-z_{h-1}+g_{z_q-1}+z_{q-1};h)Z_k = (g_0+\zeta, g_1+\zeta-a_1,...,g_{q-1}+\zeta-\sum_{x=1}^{k-1}(-1)^x\binom{q-1}{x}a_x;h)$$

That is, when $z^{-1}gz \in gZ_k$ and thus $z^{-1}gz = gy$ for some $y \in Z_k$, which in the equation above is given by $y = (\zeta, \zeta - a_1, ..., \zeta - \sum_{x=0}^{k-1}(-1)^x\binom{q-1}{x}a_x; 0)$.

Consider the case when $g = (0,...,0;1)$. Then,

$$(z_0 - z_1, ..., z_{q-1} - z_0; 1) = (\zeta, \zeta - a_1, ..., \zeta + \sum_{x=1}^{k-1}(-1)^x\binom{q-1}{x}a_x; 1)$$

Using the "upper central series algorithm", we can see that, in general, we have that

$$z_{j-1} = \zeta + \sum_{x=1}^{k-1}(-1)^x\binom{j}{x}a_x + z_j$$

$$\begin{aligned} z_0 &= j\zeta + \sum_{x=1}^{k-1}(-1)^x(\sum_{i=x}^{j}\binom{i}{x}a_x) + z_j \\ &= j\zeta + \sum_{x=1}^{k-1}(-1)^x\binom{j+1}{x+1}a_x + z_j \end{aligned}$$

Using this relation, and the fact that if one considers $g = (1,0,...,0;0)$ then this forces the center to have $z_q = 0$, we obtain that an element in the center of P/Z_k must have the form

$$zZ_k = (z_0, z_0 - \zeta, ..., z_0 - (q-1)\zeta - \sum_{x=1}^{k-1}(-1)^x\binom{j+1}{x+1}a_x; 0)Z_k$$

Notice that for $0 \leqslant j \leqslant q-1$, if $z = (z_0, ..., z_{q-1}; 0)$ then

$$\begin{aligned} z_j &= z_0 - j\zeta - \sum_{x=1}^{k-1}(-1)^x\binom{j+1}{x+1}a_x \\ &= z_0 + (-1)\binom{j}{1}\zeta - \sum_{x=2}^{k-1}(-1)^{x-1}\binom{j+1}{x}a_{x-1} \\ &= z_0 + \sum_{x=1}^{k}(-1)^x\binom{j}{x}a_x \end{aligned}$$

where we reindex and let $a_1 = \zeta$.

Then, the group Z_{k+1} is

$$Z_{k+1} = \{(z_0, z_1, ..., z_{q-1}; 0) : z_j = z_0 + \sum_{x=1}^{k}(-1)^x\binom{j}{x}a_x, z_0 \in Z_{p^d}^n\}$$

Of course, $(q-1) = -1 \ mod\ p$ and $\binom{q-1}{2} = 1 \ mod\ p$.

This proves the lemma. □

Proposition 3.1.2.1.2. *Suppose $P = Z_p \wr Z_{p^d}$ where p is prime. Then, P is nilpotent of class p^d.*

Consider the $p^d - 1^{th}$ group in the upper central series of P. By Lemma 3.1.2.1.1, this will be

$$Z_{p^d-1} = \{(z_0, z_1, ..., z_{p^d-1}; 0) : z_j = z_0 + \sum_{x=0}^{p^d-1} (-1)^x \binom{j}{x} a_x, a_x, z_0 \in \mathbb{Z}_p\}$$

Before proving this proposition consider the following claim:

Claim 3.1.2.1.1. *Z_{p^d-1} is the base group of P; that is, $Z_{p^d-1} \cong \mathbb{Z}_p^{p^d}$*

Proof. Of course, $Z_{p^d-1} \leqslant \mathbb{Z}_p^{p^d} \times 0$ by the way it is defined. It remains to show that $|Z_{p^d-1}| = p^{p^d}$.

Each $a_x, z_0 \in \mathbb{Z}_p, 0 \leqslant x \leqslant p^d - 1$, and there are p^d choices from $\mathbb{Z}_p$; that is, p^{p^d} possible choices for elements and so $|Z_{p^d-1}| = p^{p^d}$. □

Proof of Prop. 3.1.2.1.2. Denote the base group by $B = \mathbb{Z}_p^{p^d} \times 0$. Then, since $Z_{p^d-1} = B = \{(b; 0) : b \in \mathbb{Z}_p^{p^d}\}$, we get that

$$Z_{p^d} = \{x \in P : [x, g] \in B \forall g \in P\}$$

To determine the value of x, let $x = (x_0, ..., x_{p^d-1}; a), g = (g_0, ..., g_{p^d-1}; b) \in P$. Then,

$$[x, g] = (-x_0 - g_a + x_b + g_0, ..., -x_{p^d-1} - g_{a-1} + g_{p^d-1} + x_{b-1}; 0) \in B$$

Thus, x can be any element in P; that is, we get that $Z_{p^d} = P$ and thus P is nilpotent of class p^d.

Note that since the order of the k^{th} group in the series, for $k < p^d$, isp^{k+1} since there are k variables a_x and one z, all from $\mathbb{Z}_p$, if $k < p^d - 1$ then $|Z_k| < B$. Thus we could use Lemma 3.1.2.1.1 since Z_{p^d-1} could not have been the whole group. □

When $P = Z_{p^n} \wr Z_p, n > 1$, while the general form for a group in the upper central series of P is similar to that given in Lemma 3.1.2.1.1, since $p < p^n$ there must be some modification.

Recall the "upper central series algorithm"; these apply to this group, as well, in that we obtain, for $z = (z_0, ..., z_{p-1}; 0) \in Z_2$,

$$(z_0 - z_1, ..., z_{p-1} - z_0; 0) = (a, .., a; 0)$$

for some $a \in Z_{p^n}$. Then, since $z_i - z_{i+1} = a$, after a series of substitutions we obtain two equations for the value of z_{p-1} in terms of z_0, namely $z_{p-1} = z_0 + a$ and $z_{p-1} = z_0 - (p-1)a$.

While in the case when $Z_p \wr Z_{p^n}$, $-(p^n - 1)a = a$ and thus this was the same equation, since $p < p^n$ this is no longer true. That is,

$$z_0 + a = z_0 - (p-1)a \Rightarrow a = p^{n-1}x, 0 \leqslant x < p$$

and thus an element Z_2 is

$$Z_2 = \{(z_0, z_0 - a, ..., z_0 - (p-1)a; 0) : a = p^{n-1}x, z_0 \in Z_{p^n}\}$$

This will be true in general; each additional value will be of the form $p^{n-1}a_x$ for some $0 \leqslant a_x < p$.

In addition, we will require that there are more variables than p; thus the binomial sum given in the lemma must be modified to account for this. That is, consider $Z_k, k > p$ in the upper central series. Suppose $z \in Z_k, z = (z_0, ..., z_{p-1}; 0)$. Then,

$$z_i = z_0 + \sum_{x=0}^{i} (-1)^x \binom{i}{x} a_x, \text{ where } a_i = p^{n-1}y, i < p-1$$

and so a general element z is of the form

$$z = (z_0, z_1, ..., z_{p-2}, z_0 + \sum_{x=0}^{p-1} (-1)^x \binom{p-1}{x} a_x + \sum_{x=p}^{k} a_x; 0)$$

Then, for Z_k we have k variables $p^{n-1}a_x, a_x \in \mathbb{Z}_p$, with p choices for each variable, and an additional value $z_0 \in Z_{p^n}$. This means that

$$|Z_k| = p^{n+k}$$

Now, since the base group of $P = \mathbb{Z}_{p^n} \wr \mathbb{Z}_p$ has size p^n, we require that, if P is nil-k potent, then $|Z_{k-1}| = p^{n+(k-1)} = p^{np}$. Thus, $n(1-p) = -(k-1) \Rightarrow k = 1 + n(p-1)$.

This discussion supports the following claim:

Claim 3.1.2.1.2. *Suppose $P = Z_{p^n} \wr Z_p, n \geqslant 1$. Then, P has nilpotency class of $1 + n(p-1)$.*

3.1.2.2 Subgroup structure

Now that we understand the nilpotency class of this subset of wreath products, let us examine its subgroup structure.

First, let us determine a generating set for $P = G \wr H = \mathbb{Z}_n^m \wr \mathbb{Z}_q^d$. Let $F = \{f_i : f_i \in H\}$ be a generating set for H. For simplicity take it to be the set of d standard basis vectors in $\mathbb{Z}_q^d$.

Let $E = \{e_i : e_i \in G\}$ be a generating set for G. For simplicity suppose each e_i is the i^{th} standard basis vector of G. Then G^X has a generating set which can be found in a similar manner; namely the set $A = \{(a_{i,j}; 0) : a_{i,j} \in \mathbb{Z}_n^m\}$ where $a_{i,j}$ contains the i^{th} standard basis vector of $\mathbb{Z}_n^m$ in the j^{th} position, $0 \leqslant j < q^d - 1$.

However, A contains "redundant" elements when considering H, since all elements of the form $a_{i,j_k}, 0 \leqslant k \leqslant q^d - 1$ will be in the same H-orbit; thus only the subset $B = \{a_{i,0} : a_{i,0} \in A\}$ should be considered.

Note that if we are looking at a more general group then B is a set of representatives for the orbit of H on elements in A.

Thus we can draw the following conclusion:

Claim 3.1.2.2.1. *Suppose $P = G \wr H = \mathbb{Z}_n^m \wr \mathbb{Z}_q^d$ with the sets B, F described above. Then,*

$$C = B \cup \{(0; f) : 0 \in G, f \in F\}$$

is a generating set for P.

Now, let us find the commutator subgroups of P. Recall that the commutator subgroup is the group

$$P' = \langle \{[g, h] : g, h \in P\} \rangle$$

and if $g = (g_0, ..., g_{q-1}; a), g^{-1} = (-g_{-a}, ..., -g_{-1-a}; -a), h = (h_0, ..., h_{q-1}; b), h^{-1} = (-h_{-b}, ..., -h_{-1-b}; -b) \in P$ then

$$\begin{aligned}
[g, h] &= (-g_{-a}, ..., -g_{-1-a}; -a)(-h_{-b}, ..., -h_{-1-b}; -b)(g_b + h_0, ..., g_{b-1} + h_{-1}; a + b) \\
&= (-g_0 - h_a + g_b + h_0, ..., -g_{-1} - h_{a-1} + g_{b-1} + h_{-1}; 0) \\
&= (-g_{-a}, ..., -g_{-1-a}; -a)(-h_a + g_b + h_0, ..., -h_{a-1} + h_{-1} + g_{b-1}; a) \\
&= (-g_0 - h_a + g_b + h_0, ..., -g_{q-1} - h_{a-1} + h_{q-1} + g_{b-1}; 0)
\end{aligned}$$

Notice specifically when $p = 2$ then

$$z = [g, h] = (g_0 + h_a + g_b + h_0, g_1 + h_{a+1} + h_1 + g_{b+1}; 0)$$

. Let $k = (k_0, k_1; c) \in P$. Then,

$$\begin{aligned}
z^{-1}kz &= (g_0 + h_a + g_b + h_0, g_1 + h_{a+1} + h_1 + g_{b+1}; 0)(k_0 + g_0 + h_a + g_b + h_0, k_1 + g_1 + h_{a+1} + h_1 + g_{b+1}; c) \\
&= \begin{cases} (k_0 + 2g_0 + 2h_a 2 + g_b + 2h_0, k_1 + 2g_1 + 2h_{a+1} + 2h_1 + 2g_{b+1}; 0) = k \text{ if } c = 0 \\ (k_0 + g_0 + h_a + g_b + h_0 + g_1 + h_{a+1} + g_{b+1} + h_1, k_1 + g_1 + h_{a+1} + h_1 + g_{b+1} + g_0 + h_a + h_0 + g_b; 1) \end{cases} \\
&= k
\end{aligned}$$

That is, $P' = Z(P)$ when $p = 2$.

Now, let us look at some of the subgroups of $P = Z_{p^n}^m \wr Z_q$.

Claim 3.1.2.2.2. *Let $P = Z_{p^n}^m \wr Z_q$ and let K be a subgroup of $B = Z_{p^n}^{mq}$. Then, $A = \{(k; 0) : k \in K\}$ is a subgroup of P.*

Proof. Clearly, $A \subset P$. Suppose $(k_1; 0), (k_2; 0) \in A$. Then,

$$(k_1; 0)(k_2; 0) = (k_1 k_2; 0) \in A, \text{ and } (-k_1; 0) \in A$$

Since K is a group. Thus, A is also a group, and $|A| = |K|$. □

Claim 3.1.2.2.3. *Let $P = Z_{p^d}^n \wr Z_q$ and suppose $g = (g_0, ..., g_{p-1}; a) \in P$. Then, if the order of a is b in Z_q and the order of $\sum_{i=0}^{q-1} g_{ia}$ is c in Z_{p^d} then the order of g is bc.*

Proof. First, recall that

$$g^x = (\sum_{i=0}^{x-1} g_{ia}, ..., \sum_{i=0}^{x-1} g_{ia+(q-1)}; xa)$$

If $a = 0$ then the order of $g \in P$ is the order of $(g_0, ..., g_{p-1}) \in Z_{p^d}^{nq}$, which is c, a divisor of p^d. Thus the order is $bc = 1c$.

Otherwise, the order must be at least q, since $o(a) = q$. Then,

$$g^q = (\sum_{i=0}^{q-1} g_i, ..., \sum_{i=0}^{q-1} g_i; 0)$$

and so the order of g^q must be the order of $(\sum_{i=0}^{q-1} g_i, ..., \sum_{i=0}^{q-1} g_i) \in Z_{p^d}^{nq}$, which is simply the order of $\sum_{i=0}^{q-1} g_i \in Z_{p^d}^n$; once again this is a divisor of p^d. Thus, the order of g is $q^a p^b$ where $a = 0$ or 1 and $0 \leqslant b \leqslant d$. Specifically, it is bc as required. □

Claim 3.1.2.2.4. *Suppose $P = Z_{p^n}^m \wr Z_q$, p, q prime, and let $B = Z_{p^n}^{mq}$ be the base group of B. Let $b \in B' \leqslant B$, where and $B' = \langle b \rangle$. Then, $H_i = \langle (b; i) \rangle, i \in Z_q$ is a proper subgroup of P.*

Proof. Of course, if $i = 0$ then this is simply the case above.

Suppose $i \neq 0$ and let $b = (b_0, .., b_{q-1}) \in B'$. Then, the order of i is q since q is prime. Let d be the order of $\sum_{i=0}^{q-1} b_i \in Z_{p^n}^m$.

Then by Claim. 3.1.2.2.3 the order of $(b; i)$ is $dq \leqslant p^n q \neq |P| = p^{nmq} q$ and so H_i is a proper subset. It is a subgroup since b is also a subgroup. □

Now, let us consider subgroups of $P = \mathbb{Z}_n^m \wr \mathbb{Z}_q^d$ with multiple generators.

3.1.2.2.1 Subgroups generated by $g_{i,j,k}$

Recall the set $A = \{(a_{i,j}; 0) : a_{i,j} \in \mathbb{Z}_n^m\}$ where $a_{i,j}$ contains the i^{th} standard basis vector of $\mathbb{Z}_n^m$ in the j^{th} position, $0 \leqslant j < q^d - 1$ and the set of standard basis vectors in $\mathbb{Z}_q^d$: $F = \{f_k : f_k \in \mathbb{Z}_q^d\}$. Finally, let $g_{i,j,k} = (a_{i,j}; f_k) \in P$.

Claim 3.1.2.2.5. *Any element of the form $g_{i,j,k}$ will generate a subgroup of order nq.*

Proof. The order of f_k in H is q, and $a_{i,j}$ in G is n. Then, $g^q_{i,j,k} = (\sum_{l=j}^{j+l} a_{i,j+lf_k}; 0)$. Since the order of any element in $\mathbb{Z}_n^m$ is n we have that

$$(g^q_{i,j,k})^n = (n\sum_{l=j}^{j+l} a_{i,j+lf_k}; 0) = (0; 0)$$

and thus $o(g_{i,j,k}) = |\langle g_{i,j,k}\rangle| = nq$ as required. □

Claim 3.1.2.2.6. *Suppose H is a cyclic group, so that $H = \mathbb{Z}_q$. Then, the groups generated by elements of the form $g_{i,j,k}$, so that $f_k = f \in \mathbb{Z}_q$ is a generator, intersect trivially if the i values are not the same and as a subgroup of the center otherwise.*

Proof. Recall that the center of P is

$$Z = \{(a, ..., a; 0) : a \in G\}$$

and we know that $g^q_{i,j,k} = (\sum_{l=0}^{q-1} a_{i,l}; 0)$ is in the center.

Then, since $|Z| = |G| = n^m$ and $o(g^q_{i,j,k}) = n$ we get that $\langle g^q_{i,j,k}\rangle = \{(a_i, ..., a_i; 0) : a_i \in G\} \leqslant Z$ with equality if $m = 1$.

Thus clearly, a group with one generator is contained in the center. Notice that these rely on the value of i; that is, since $g_{i,j,k} \neq \phi_h(g_{i',j',k'}$ for any $h \in \mathbb{Z}_q, i' \neq i$, they do not contain the same subgroup of $Z(P)$. Then, $\langle g_{i,j,k}\rangle \cap \langle g_{i',j',k'}\rangle = (0; 0)$

The claim follows quite easily. □

For simplicity let us consider the case when $d = 1$, so $F = \{1\}$. For brevity let $g_{i,j} := g_{i,j,k}$.

Let $g = (b; h) \in P$ and consider conjugating $g_{i,j}$ by it. Then,

$$\begin{aligned}(\phi_{-h}(b^{-1}); -h)(a_{i,j}; 1)(b; h) &= (b^{-1}\phi_h(a_{i,j})b; 1)\\ &= (b^{-1}a_{i,j+h}b; 1)\\ &= (a_{i,j+h}; 1)\\ &= g_{i,j+h}\end{aligned}$$

Of course, this shows that subgroups generated by $g_{i,j}$ are not normal in P; in fact, they are only normal in the base group G^X.

As well, this gives a characterization for conjugation classes; that is:

Claim 3.1.2.2.7. *A group generated by $g_{i,j}$ is conjugate to a group generated by $g_{i,k}, k \in Z_q$ under conjugation by $(b; h) \in P$ where $h = k - j$ mod q.*

Thus the conjugacy classes depend only on the value of i. In fact, this is true in general:

Claim 3.1.2.2.8. *Let $h = (g; f) = (\sum_{j=0}^{q} \alpha_j; f)$. Then, $\langle h \rangle$ is conjugate to any group which is generated by a cyclic permutation and shift of the elements α_j; that is,*

$$\{\langle (\sum_{j=0}^{q} (\beta_j + \alpha_{j+k}); f) \rangle : k \in H, \beta_j \in G\}$$

is the conjugacy class of $\langle h \rangle$.

Proof. Consider h above and conjugate by $(b; k)$. Then,

$$\begin{aligned}(\phi_{-k}(b^{-1}); -k)(g; f)(b; k) &= (\phi_f(b^{-1})\phi_k(\sum_{j=0}^{q} \alpha_j)b; f) \\ &= (\sum_{j=0}^{q} (\beta_j + \alpha_{j+k}); f) \text{ where } \beta_j = b_j - b_{j+f}\end{aligned}$$

The result follows closely. □

Because of this, when considering a subgroup generated by two generators with the same i-value, that is, $\langle g_{i,j}, g_{i,l} \rangle$, one could simply set $j = 0$. Then, $g_{i,0}g_{i,l}$ is in the same conjugacy class as $g_{i,j}g_{i,l+j}, j \in \mathbb{Z}_q$.

Consider a group generated by $g_{i,0}, g_{i,j}, j \neq 0$. Consider the group generated by combining the two generators, $g_{i,0}g_{i,j} = (a_{i,1} + a_{i,j}; 2), g_{i,j}g_{i,0} = (a_{i,j+1} + a_{i,0}; 2)$.

Instead, let us look at what happens if we conjugate one element by the other. That is, consider

$$\begin{aligned}g_{i,0}g_{i,j}^{y}g_{i,0} &= (-a_{i,-1}); -1)(\sum_{k=0}^{y} a_{i,j+k}; y)(a_{i,0}; 1) \\ &= (-a_{i,-1}); -1)(\sum_{k=0}^{y} a_{i,j+k+1} + a_{i,0}; y + 1) \\ &= (-a_{i,y} + \sum_{k=0}^{y} a_{i,j+k+1} + a_{i,0}; y) \\ &= (-a_{i,y} + \sum_{k=1}^{y+1} a_{i,j+k} + a_{i,0}; y)\end{aligned}$$

The first generates elements of the form

$$(g_{i,0}g_{i,j})^x = (\sum_{k=0}^{x-1} (a_{i,1+k} + a_{i,j+k}); 2x)$$

and the second generates elements

$$(g_{i,j}g_{i,0})^{y-1} = (\sum_{k=0}^{y} (a_{i,j+1+k} + a_{i,k}); 2y)$$

Claim 3.1.2.2.9. *Suppose $j = 1$. Then, $\langle (g_{i,0}g_{i,1})\rangle = \langle g_{i,2}\rangle$ if and only if $P = \mathbb{Z}_3^n \wr \mathbb{Z}_3$.*

Proof. Suppose $P = \mathbb{Z}_3^n \wr \mathbb{Z}_3$. Then

$$(g_{i,0}g_{i,1}) = (2a_{i,1}; 2) = (a_{i,2}; 1)^{-1}$$

and since $o((g_{i,0}g_{i,1})) = o((a_{i,2}; 1)^{-1})$ we get that $\langle (g_{i,0}g_{i,1})\rangle = \langle g_{i,2}\rangle$.

Next, let $x = 0$ and suppose there is a y where $(g_{i,0}g_{i,1}) = (g_{i,1}g_{i,0})^y$. Then,

$$\begin{aligned}(2a_{i,1}; 2) &= (\sum_{k=0}^{y-1}(a_{i,2+k} + a_{i,k}); 2y)\\ &= (\sum_{k=0}^{bq}(a_{i,2+k} + a_{i,k}); 2), b \geqslant 0, \text{ since } y = 1 \ mod\ q\\ &= (a_{i,2} + a_{i,0} + 2bqa; 2)\end{aligned}$$

where $a = (e_i, ..., e_i) \in G^X$. Finally, we then require that $2a_{i,1} = a_{i,2} + a_{i,0} + 2bqa$. This is true when $2 = 0\ mod\ n$ so $n = 2$. Otherwise, it occurs when $a_{i,2} + 2ba_{i,2} = a_{i,0} + 2ba_{i,0} = 0$ and $a = (e_i, e_i, e_i)$ so that only $2ba_{i,1}$ remains. Thus $q = 3$ and $2b + 1 = 0\ mod\ n$, say $2b + 1 = xn$.

Finally, $2ba_{i,1} = 2a_{i,1}$ implies that $b = 1\ mod\ n$, say $b = 1 + mn$. Equating the two equations with b we get $2(1 + mn) + 1 = xn$; that is, $3 = n(x - 2m) = 0\ mod\ n$. This forces $n = 3$ and so only groups $\mathbb{Z}_3^n \wr \mathbb{Z}_3$ satisfy this. □

Otherwise, the two groups are not equal. Consider all the groups generated by

$$g_{i,0}^x g_{i,j} = (\sum_{k=0}^{x-1} a_{i,k}; x)g_{i,j} = (\sum_{k=1}^{x+1} a_{i,k} + a_{i,j}, x + 1), 0 \leqslant x < q$$

For simplicity let $\alpha_j \in G$ be the value in the j^{th} entry.

Suppose $x + 1$ is a generator of $\mathbb{Z}_q$. Then, let $\beta = \sum_{j=0}^{q-1} \alpha_j$. If β is not a generator of G then $g_{i,0}^x g_{i,j}$ will generate a subgroup of order $o(\beta)q$ which contains a subgroup of the center given by $\langle (\beta, ..., \beta; 0)\rangle = \{((\beta x, ..., \beta x; 0) : 0 \leqslant x < o(\beta)\}$.

On the other hand, if β does generate G then each $g_{i,0}^x g_{i,j}$ will generate a subgroup of order nq which contains a subgroup of the center of order n, namely $\{(\alpha e_i, ..., \alpha e_i; 0) : \alpha \in \mathbb{Z}_n\}$.

Suppose $x + 1$ is not a generator of $\mathbb{Z}_q$ with order $0 < b < q$. Then,

$$(g_{i,0}^x g_{i,j})^b = (\sum_{l=0}^{b-1}(\sum_{k=1}^{x+1} a_{i,k+l(x+1)} + a_{i,j+l(x+1)}); 0)$$

Since $b < q$ this will not be a sum over all entries and so the group generated by such an element does not contain the center. Let $v = o(\sum_{l=0}^{b-1}(\sum_{k=1}^{x+1} a_{i,k+l(x+1)} + a_{i,j+l(x+1)}))$ in G^X. Then the order of such a subgroup is bv.

Claim 3.1.2.2.10. *Let $P = \mathbb{Z}_{p^n}^m \wr \mathbb{Z}_{q^d}$, $g_{i,j} = (b_j; 1) \in \mathbb{Z}_{p^n}^m \wr \mathbb{Z}_{q^d}$, where b_j, a_i are the element described above. Let K be a vector of nonequivalent tuples, $K = ((i_0, j_0), ..., (i_{l-1}, j_{l-1})), i \in \mathbb{Z}_{p^n}^m, j \in \mathbb{Z}_{q^d}, l = |K|$. Then, the set*

$$A_K = \langle \{g_{i,j} : (i,j) \in K\} \rangle$$

is a subgroup of P containing a subgroups of the center generated by $\{g_{i,j}^q : g_{i,j} \in A_K\}$.

Let us examine groups of the form $A_K = \langle \{g_{i,j} : (i,j) \in K\} \rangle$ as described above. First, notice that

$$\bigcap_{(i,j_a) \in K} \langle g_{i,j_a} \rangle \leqslant Z(P)$$

where all $i's$ are equal and $j_a's$ distinct.

Now, consider what happens if we quotient out by an appropriate subgroup of the center. Let $I = (i_0, ..., i_{d-1}) \in \mathbb{Z}_n^d$ be a vector where $0 < d \leqslant m$ so that $Z_I(P) = \{z \in Z(P) : z = (z_i, ..., z_i; 0), i \in I\}$; that is, it is a subspace of $Z(P)$ generated by the $g_{i,j}$. Of course, when $m = 1$ then $Z_I(P) = Z(P)$.

Then, if $K = ((i_0, j_0), ..., (i_{l-1}, j_{l-1})), I = (i_0, ..., i_r)$ where each $i \in I$ is unique and is contained in a tuple in K, so $r \leqslant l - 1$, then $Z_I(P) \leqslant A_K$.

Consider the simplest case, when $m = 1$ so that $Z_I(P) = Z(P) \leqslant A_K, K = (j)$. Then, since $A_k = \langle g_j \rangle = \{(\sum_{i=0}^x a_{j+i}; x) : 0 \leqslant x < nq\}$, every q^{th} power is in the center. Thus, when one quotients out by the center, only the elements when $0 \leqslant x < q$ are important. That is,

$$A_K/Z(P) = \{(\sum_{i=0}^{x} a_{j+i}; x)Z(P) : 0 \leqslant x < q\}$$

This group has order $\frac{nq}{n} = q$ and, in fact, is isomorphic to $\mathbb{Z}_q$.

Now, consider when $K = (0, l), l \neq 0$. Since $g_0, g_l \in A_K$ we know automatically that $A_{(0)}/Z(P), A_{(l)}/Z(P) \leqslant A_K/Z(P)$. In addition, any $(g_0^x g_l)^a, (g_l^y g_0)^b$ is in the center when $a = o(x+1), b = o(y+1)$ in $\mathbb{Z}_q$. Thus only consider the values of a,b such that $0 \leqslant a \leqslant o(x+1), 0 \leqslant b \leqslant o(y+1)$. This gives elements of the form

$$(g_0^x g_l)^a = (\sum_{i=0}^{a-1} (\sum_{k=1}^{x+1} a_{k+i(x+1)} + a_{l+i(x+1)}); a(x+1))$$

$$(g_l^y g_0)^b = (\sum_{i=0}^{b-1} (\sum_{k=1}^{y+1} a_{l+k+i(y+1)} + a_{i(y+1)}); b(y+1))$$

That is, these give coset representatives. Of course, if $x, y = 0$ then these are the coset representatives of $A_{(j)}/Z(P), A_{(l)}/Z(P)$. Now, when $x, y \neq 0$, it is important to ask if there is any overlap between these representatives.

Suppose $(g_0^x g_l)^a Z(P) = (g_l^y g_0)^b Z(P)$; then we must have that $((g_l^y g_0)^b)^{-1} (g_0^x g_l)^a \in Z(P)$ for some value of

a, b, x, y. Since

$$\begin{aligned}((g_l^y g_0)^b)^{-1} = (g_l^y g_0)^{-b} &= (\sum_{i=0}^{q-b-1}(\sum_{k=1}^{y+1} a_{l+k+i(y+1)} + a_{i(y+1)}); -b(y+1)) \\ &= ((g_l^y g_0)^{-1})^b = (-\sum_{k=0}^{y+1} a_{l+k+-y} - a_{-(y+1)}; -(y+1))^b \\ &= (-\sum_{i=1}^{b}(\sum_{k=1}^{y+1} a_{l+k-i(y+1)} + a_{-i(y+1)}); -b(y+1))\end{aligned}$$

we require that

$$\begin{aligned}(g_l^y g_0)^{-b}(g_0^x g_l)^a = (-\sum_{i=1}^{b}(\sum_{k=1}^{y+1} a_{l+k-i(y+1)+a(x+1)} + a_{-i(y+1)+a(x+1)}) + \\ \sum_{i=0}^{a-1}(\sum_{k=1}^{x+1} a_{k+i(x+1)} + a_{l+i(x+1)}); -b(y+1)+a(x+1)) \in Z(P)\end{aligned}$$

so $a(x+1) - b(y+1) = 0 \ mod \ q$.

Suppose $b = 1$ so $a(x+1) = y+1 \ mod \ q$ and

$$\begin{aligned}(g_l^y g_0)^{-1}(g_0^x g_l)^a &= (-\sum_{k=1}^{y+1} a_{l+k-y-1+a(x+1)} - a_{-(y+1)+a(x+1)} + \sum_{i=0}^{a-1}(\sum_{k=1}^{x+1} a_{k+i(x+1)} + a_{l+i(x+1)}); 0) \\ &= (-\sum_{k=1}^{y+1} a_{l+k} - a_0 + \sum_{i=0}^{a-1}(\sum_{k=1}^{x+1} a_{k+i(x+1)} + a_{l+i(x+1)}); 0) \\ &= (-\sum_{k=0}^{a(x+1)} a_{l+k+1} + \sum_{i=0}^{a-1} a_{l+i(x+1)} - a_0 + \sum_{i=0}^{a-1}(\sum_{k=1}^{x+1} a_{k+i(x+1)}); 0) \\ &= (-\sum_{k=1,(x+1)|k}^{a(x+1)+1} a_{l+k} - \sum_{k=1,(x+1)\nmid k}^{a(x+1)+1} a_{l+k} + \sum_{i=0}^{a-1} a_{l+i(x+1)} - a_0 + \sum_{i=0}^{a-1}(\sum_{k=1}^{x+1} a_{k+i(x+1)}); 0) \\ &= (-\sum_{i=1}^{a} a_{l+i(x+1)} - \sum_{k=1,(x+1)\nmid k}^{a(x+1)+1} a_{l+k} + \sum_{i=0}^{a-1} a_{l+i(x+1)} - a_0 + \sum_{i=0}^{a-1}(\sum_{k=1}^{x+1} a_{k+i(x+1)}); 0) \\ &= (-a_{l+a(x+1)} + a_l - \sum_{k=0,(x+1)\nmid k}^{a(x+1)} a_{l+k+1} - a_0 + \sum_{i=0}^{a-1}(\sum_{k=1}^{x+1} a_{k+i(x+1)}); 0) \in Z(P)\end{aligned}$$

Clearly, analyzing such groups becomes increasingly difficult as the number of generators increases. The following section will look at groups generated by a slightly different "type" of element. For simplicity, in subsequent sections and when examining the HSP the focus will be on cyclic subgroups.

3.1.2.2.2 Subgroups from "non-generators"

Suppose $P = \mathbb{Z}_n^m \wr \mathbb{Z}_q^d$. Consider a class of smaller subgroups, generated by "non-generators."

That is, suppose either $b \in \mathbb{Z}_n$ or $c \in \mathbb{Z}_q$ is a non-generator, so that $b = 0 \ mod \ n$ or $c = 0 \ mod \ q$ and let $b_I = b\sum_{i\in I} e_i \in \mathbb{Z}_n^m$ and $c_K = c\sum_{k\in K} e_k \in \mathbb{Z}_q^d$ where I, K are nonempty sets of elements in $\mathbb{Z}_m, \mathbb{Z}_d$, respectively so that the resulting b_I, c_K is a vector of dimension m, d with either b, c or 0 in its entries. Then, $h_j = (0, .., b_I, 0, ..., 0; c_K)$, where b_I is in the j^{th} entry, will generate a smaller group.

If b is a non-generator with order $x, 1 \leqslant x < n$ and c is a generator, then,

$$h^q = (b_I, ..., b_I; 0), (h^q)^x = (0, ..., 0; 0)$$

and so $\langle h \rangle$ has order xq and contains a subset of $Z(P)$ generated by $(b_I, ..., b_I; 0)$ and of order x.

If c is a non-generator with order $y, 1 \leqslant y < q$ and the order of b is $x, 1 \leqslant x \leqslant n$, then the group generated by h has order xy. However, since $y < q$,

$$h_j^y = (\sum_{l=0}^{y-1} b_{I,j+lc_K}; c_K)$$

where $b_{I,j}$ denotes b_I in the j^{th} spot. That is, the value of b only appears in the slots which are multiples of c (shifted by j). For this reason, this will not contain a non-trivial subgroup of the center.

Finally, consider more generally $f = (b; c)$ where $b = (b_0, .., b_{q^d-1})$. Let $\sum_{x=0}^{q^d-1} b_x = \beta v$, where $v \in \mathbb{Z}_n^m$ has entries which are either 0 or 1. If β is a non-generator in $\mathbb{Z}_n$ then this will, yet again, generate a small subgroup which contains a subgroup of the center of order $o(\beta)$ generated by $(\beta v, ..., \beta v; 0)$.

Suppose $P = \mathbb{Z}_{p^n}^m \wr \mathbb{Z}_{q^d}^f$ where p, q are prime. Then any non-generator of $\mathbb{Z}_{p^n}$ is of the form $xp, 0 \leqslant x < p^{n-1}$, and for $\mathbb{Z}_{q^d}$ it is of the form $yq, 0 \leqslant y < q^{d-1}$, and so $p^x, 1 \leqslant x \leqslant n, q^y, 1 \leqslant y \leqslant d$ are the representative non-generators.

There are $a = \sum_{i=1}^m \binom{m}{i}$ vectors in $b = \mathbb{Z}_{p^n}^m$ with at least one, and at most m, 1's, with all other entries being zero, and $\sum_{k=1}^f \binom{f}{k}$ in $\mathbb{Z}_{q^d}^f$ of the same nature. Also, there are q^d spots in the base group. As such, there are $(na)q^d(bd)$ "non-generators" of P which generate unique cyclic subgroups, do not contain a nontrivial subgroup of the center, and where only one of the elements in the base group is non-zero is xd.

Claim 3.1.2.2.11. *Let $f = (b; c) \in P = \mathbb{Z}_n^m \wr \mathbb{Z}_q^d, b = (b_0, ..., b_{q^d-1})$ where either c or b is a "non-generator" as described above. Then, the conjugates of f are also non-generators.*

Proof. Let $(g; h)$ be an element in P, where $g = (g_0, ..., g_{q^d-1})$. Then,

$$\begin{aligned}(\phi_{-h}(-g); -h)(b; c)(g; h) &= (\phi_{-h}(-g); -h)(\phi_h(b)g; c + h) \\ &= (\phi_c(-g)\phi_h(b)g; c)\end{aligned}$$

If c is a non-generator then clearly $(\phi_c(-g)\phi_h(b)g; c)$ is a non-generator.

Otherwise, suppose c generates $\mathbb{Z}_q$ but $\sum_{x=0}^{q^d-1} b_x = \beta v$ and β is a non-generator of $\mathbb{Z}_n$. Then,

$$\sum_{x=0}^{q^d-1}(-g_{c+x} + b_{x+h} + g_x) = \beta v + \sum_{x=0}^{q^d-1} g_x - \sum_{x=0}^{q^d-1} g_x = \beta v$$

and so $(\phi_c(-g)\phi_h(b)g; c)$ is a non-generator containing the same subgroup of $Z(P)$ as f. □

Consider the simplest case: when $P = \mathbb{Z}_{p^n} \wr \mathbb{Z}_{q^m}, q^m \geqslant p^n$ for p, q prime. Then, if $b_j = (0, ..., b, 0, ..., 0)$; that is, $b \in \mathbb{Z}_{p^n}$ is in the j^th spot, $0 \leqslant j < q^m$, then let $B = \{(b_j; c) : b = p^i, 1 \leqslant i \leqslant n, c \neq 0 \ mod \ q\}$.

Recall that elements from B generate subgroups of order $o(b)q^d$ which contain a subgroup of the center generated by $Z_b(P) = (b, ..., b; 0)$ of order $o(b)$.

Consider modding out $\langle (b_j; c)\rangle, (b_j; c) \in B$ by this subgroup of the center. Since $(b_j; c)^x = (\sum_{i=0}^{x-1} b_{j+ic}; cx)$ one then obtains

$$\langle (b_j; c)\rangle / Z_b(P) = \{(0; 0)Z_b(P), (\sum_{i=0}^{x-1} b_{j+ic}; cx)Z_b(P) : 1 \leqslant x \leqslant q^d - 1\}$$

Notice that

$$\begin{aligned}(\sum_{i=0}^{x-1} b_{j+ic}; cx)Z_b(P)(\sum_{k=0}^{y-1} b_{j+kc}; cy)Z_b(P)) &= (\sum_{i=y}^{y+x-1} b_{j+ic} + \sum_{k=0}^{y-1} b_{j+kc}; c(x+y))Z_b(P) \\ &= (\sum_{i=0}^{y+x-1} b_{j+ic}; c(x+y))Z_b(P)\end{aligned}$$

so $\langle (b_j; c)\rangle / Z_b(P) \cong \mathbb{Z}_{q^d}$.

In the more general case, consider $S = \langle (b_{j_0}; c_0), ..., (b_{j_k}; c_k)\rangle$ where each generator is from B so that $b_{j_l} = p^{i_l}, 1 \leqslant i_l \leqslant n$. Assume it is ordered, so that if $l < h$ then $p^{i_l} < p^{i_h}$, and let $(\beta_l; \delta_l) = (\sum_{i=0}^{l} b_{j_i}; \sum_{i=0}^{l} c_l), 0 \leqslant l \leqslant k$.

We know that whenever $o(c_l) = q^d$; that is, it is a generator, then $\langle (b_{j_l}); c_l)\rangle$ generates a subgroup which contains a subgroup of $Z(P)$ of order $o(b_{j_l}) = p^{n-i_l}$. Thus there are $k+1$ subgroups of the form $\langle (p^{i_l}, ..., p^{i_l}; 0)\rangle \leqslant Z(P), 0 \leqslant l \leqslant k$ in S.

Suppose $(\beta_l; \delta_l)$ is such that δ_l is a generator (if it is not a generator then it won't generate a subgroup of $Z(P)$). If each β_l is a non-generator then S only contains subgroups of the center of the form $\langle (p^x, ..., p^x; 0)\rangle \leqslant Z(P), 1 \leqslant x \leqslant n$. Of course, $\langle (p^x, ..., p^x; 0)\rangle < \langle (p^y, ..., p^y; 0)\rangle$ whenever $x > y$. Otherwise, if any β_l is a generator then the whole group $Z(P)$ is contained in S.

Let $Z_x(P) = \langle (p^x, ..., p^x; 0)\rangle = \bigcap \langle (p^y, ..., p^y; 0)\rangle \leqslant Z(P), 0 \leqslant x \leqslant n$; that is, it is the intersection of all the subgroups of the center contained in S. Consider $S/Z_x(P)$.

For the smallest subgroup, generated by $(b_{j_k}; c_k)$ we know that

$$\langle (b_{j_k}; c_k) \rangle / Z_x(P) = \{(0;0)Z_x(P), (\sum_{i=0}^{y-1} b_{j_k+ic}; cy)Z_x(P) : 1 \leqslant y \leqslant q^d - 1\} \cong \mathbb{Z}_{q^d}$$

Then, the group generated by $(b_{j_{k-1}}; c_{k-1})$, where $b_{j_{k-1}}$ contains $p^{i_{k-1}} < p^{i_k}$ in the j^{th} position, contains the group generated by $(b_{j_k}; c_k)$, so

$$\begin{aligned}\langle (b_{j_{k-1}}; c_{k-1}) \rangle / Z_x(P) &= \langle (b_{j_k}; c_k) \rangle / Z_x(P) \cup \\ &\{((p^{i_{k-1}}, .., p^{i_{k-1}}; cy) + (\sum_{i=0}^{y-1} b_{j_k+ic}; 0))Z_x(P) : 0 \leqslant y \leqslant q^d - 1\} \\ &\cong \mathbb{Z}_{q^d} \times \mathbb{Z}_2\end{aligned}$$

where $\sum_{i=0}^{y-1} a = 0$ when $y = 0$. This continues inductively, so that

$$\begin{aligned}\langle (b_{j_0}; c_0) \rangle / Z_x(P) &= \langle (b_{j_1}; c_1) \rangle / Z_x(P) \cup \\ &\{((p^{i_0}, .., p^{i_0}; cy) + (\sum_{i=0}^{y-1} b_{j_k+ic}; 0))Z_x(P) : 0 \leqslant y \leqslant q^d - 1\} \\ &\cong \mathbb{Z}_{q^d} \times \mathbb{Z}_{k+1}\end{aligned}$$

Then, consider the set of all elements $\{(\beta_l; \delta_l)\}$ where δ_l is a generator and β_l is not. Let $\tilde{b}_l = \sum_{x=0}^{q^d-1} \beta_l = \sum_{x=0}^{q^d-1} \sum_{i=0}^{l} b_{j_l+x} = (p^{w_l}, ..., p^{w_l}), 1 \leqslant w_l \leqslant n$. Suppose the set has length r and is ordered so that $o(\tilde{b}_0) > o(\tilde{b}_1)$. Finally, let i_y be the exponent where $p^{w_r} \leqslant p^{i_y}$. Then, as before,

$$\begin{aligned}\langle (\beta_r; \delta_r) \rangle / Z_x(P) &= \langle (b_{j_y}; c_y) \rangle / Z_x(P) \cup \\ &\{((p^{w_r}, .., p^{w_r}; \delta_r) + (\sum_{i=0}^{x-1} \beta_{r_{ic}}; 0))Z_x(P) : 0 \leqslant x \leqslant q^d - 1\} \\ &\cong \mathbb{Z}_{q^d} \times \mathbb{Z}_{(k-y)+1}\end{aligned}$$

and, inductively,

$$\begin{aligned}\langle (\beta_0; \delta_0) \rangle / Z_x(P) &= \langle (\beta_r; \delta_r) \rangle / Z_x(P) \cup \\ &\{((p^{w_0}, .., p^{w_0}; \delta_r) + (\sum_{i=0}^{x-1} \beta_{0_{ic}}; 0))Z_x(P) : 0 \leqslant x \leqslant q^d - 1\} \\ &\cong \mathbb{Z}_{q^d} \times \mathbb{Z}_{(k-y)+r+2}\end{aligned}$$

On the other hand, elements from C generate subgroups of order $o(b)o(c)$ which do not contain a non-trivial subgroup of the center.

Let us now consider conjugacy classes. For any $g \in P = Z_{p^n}^m \wr Z_q, H \leqslant P$ denote

$$H^g = \{g^{-1}hg : h \in H\}$$

Let $g = (g_0, ..., g_{q-1}; a), g^{-1} = (-g_{-a}, ..., -g_{-1-a}; -a), h = (h_0, ..., h_{q-1}; b)$. Then,

$$\begin{aligned} g^{-1}hg &= (-g_{-a}, ..., -g_{-1-a}; -a)(h_a + g_0, ..., h_{a-1} + g_{-1}; a + b) \\ &= (-g_b + h_a + g_0, ..., -g_{b-1} + h_{a-1} + g_{-1}; b) \end{aligned}$$

Thus the value of b determines the conjugacy class.

3.2 Representation Theory

This section will examine the representation theory of a wreath prodcuct $G \wr H$ where H acts on a set $X, |X| = n$, B denotes the base group $G \times ... \times G$, with G appearing n times. The notation G_x will be used to refer to the x^{th} occurrence of G in the direct product.

Suppose $R = \{\rho^{(i)}\}$ is the set of irreps of G. Then, the irreps of the group $G^X = \{(g, ..., g; e_H) : g \in G\} \triangleleft G \wr H$ are of the form

$$\rho_I = \otimes_{x \in X} \rho_x^{(i_x)}$$

where $I = (i_1, ..., i_n)$, and where

$$\rho^{(I)}(g_1, ..., g_n; e_h) = \otimes_{x \in X} \rho_x^{(i_x)}(g_x)$$

Recall that G^X is normal in $G \wr H$. Then, as discussed in [11], $G \wr H$ acts on the set of equivalence classes of irreducible representations of G^X, as discussed below. In order to determine the irreps of all of $G \wr H$ one can use induction of irreps; that is, the "little group method". First, a few definitions must be presented.

3.2.1 Some Definitions

Definition 17 (g-conjugate)**.** Let G be a group with normal subgroup N and let σ be a representation of N. Let $g \in G$. Then, the *g conjugate of* σ, denoted σ^g, is defined by

$$\sigma^g(h) = \sigma(g^{-1}hg)$$

for any $h \in N$.

Note that σ^g is again a representation of N.

An equivalence relation between two irreps σ, ρ is given according to whether they are conjugates. That is, $\sigma \sim \rho$, if there is a $g \in G$ where $\sigma^g = \rho$. This construction will be used below.

Definition 18 (Inertia group)**.** Let G be a group, N a normal subgroup of G, and let σ be an irrep of N. Then, the *inertia group* of σ in G is

$$I_G(\sigma) = \{g \in G : \sigma^g \sim \sigma\}$$

This will be an important group when determining the irreps of $G \wr H$ using the irreps of G^X.

Definition 19 (Extension)**.** Let G be a group, $N \lhd G$, and let σ be an irrep of N, $\tilde{\sigma}$ an irrep of G. Then, $\tilde{\sigma}$ is an *extension* of σ if

$$Res_N^G \tilde{\sigma} = \sigma.$$

Definition 20 (Stabilizer group)**.** Let H be a group acting on a set X. Then, the *stabilizer group* of $x \in X$ is the subgroup of H which acts trivially on x; that is,

$$H_x = \{h \in H : h \cdot x = x\}$$

Definition 21 (Isotropy subgroup of σ)**.** Let H be a group acting on a set X and let G be a group with the set of irreps $\widehat{G}$. Consider the group G^X with the set of irreps $\widehat{G^X}$ so that every $\sigma \in \widehat{G^X}$ is given by $\sigma = \otimes_{x \in X} \sigma_x, \sigma_x \in \widehat{G^X}$.

Then, for such a σ, define the *isotropy subgroup* to be the subgroup of $h \in H$ which stabilizes σ, given by

$$T_H(\sigma) = \{h \in H : \sigma_{hx} \sim \sigma_x \forall x \in X\}$$

Definition 22 (Inflation)**.** Let G be a group, $N \lhd G$. Let η be an irrep of G/N. Then, define the *inflation* of η to $\bar{\eta}$, an irrep of G, by

$$\bar{\eta}(g) = \eta(gN)$$

for every $g \in G$.

Note that this defines a representation of G that is trivial on N, and all representations of G that are trivial on N occur in this way.

3.2.2 The "Little Group" method

For the remainder of this section, consider the group $G \wr H$ where H acts on a set X, $|X| = n$ and let $G^X = \{(b; e_H) : b \in B\}$. Use $\widehat{N}$ to denote the set of irreps of a group N.

Let $(b; h) \in G \wr H$, $\sigma_x \in \widehat{G}$ for each $x \in X$, and $\sigma = \otimes_{x \in X} \sigma_x \in \widehat{G^X}$.

To begin, let us determine the (b;h)-conjugates of σ. Fix $(a; e_H) \in G^X$. Then, since

$$(\psi_{h^{-1}}(b^{-1}); h^{-1})(a; e_H)(b; h) = (b^{-1}\psi_h(a)b; e_H)$$

if one lets $b = (g_1, ..., g_n)$, $a = (k_1, ..., k_n)$, and define the $\psi_h(a) = (k_{h(1)}, ..., k_{h(n)})$ then the above relation becomes

$$(b^{-1}\psi_h(a)b; e_H) = (g_1^{-1}k_{h(1)}g_1, ..., g_n^{-1}k_{h(n)}g_n; e_H)$$

One can then calculate the following:

$$\begin{aligned}
\sigma^{(b;h)}(a; e_h) &= \sigma((b^{-1}\psi_h(a)b; e_H)) \\
&= \otimes_{x \in X} \sigma_x(g_x^{-1}k_{h(x)}g_x) \\
&= \otimes_{y \in X} \sigma_{h^{-1}(y)}(g_{h^{-1}(y)}^{-1}k_y g_{h^{-1}(y)}) \\
&= \otimes_{y \in X} \sigma_{h^{-1}(y)}^{g_{h^{-1}(y)}}(k_y)
\end{aligned}$$

using the substitution $y = h(x)$. Then, since $g_x \in G$ so that $\sigma_x^{g_x}(e_G) = \sigma_x(e_G)$, we get that

$$\sigma_x^{g_x} \sim \sigma_x$$

and so one can obtain the following result:

Lemma 3.2.2.0.1. *Let $\sigma, \sigma_x, (b;h)$ be as defined above. Then,*

$$\sigma^{(b;h)} \sim \otimes_{x \in X} \sigma_{h^{-1}x}$$

Using this relation one can prove the following:

Lemma 3.2.2.0.2. *Let $\sigma = \otimes_{x \in X} \sigma_x \in \widehat{G^X}$. Then, the inertia group of σ in $G \wr H$, denoted $I_{G \wr H}(\sigma)$, is given by*

$$I_{G \wr H}(\sigma) = G \wr T_H(\sigma)$$

where $T_H(\sigma)$ is the isotropy group of σ in H.

Proof. Recall that $I_{G \wr H}(\sigma) = \{(b;h) \in G \wr H : \sigma^{(b;h)} \sim \sigma\}$ and $T_H(\sigma) = \{h \in H : \sigma_{h(x)} \sim \sigma_x \forall x \in X\}$. Then,

$$G \wr T_H(\sigma) = \{(b;h) : b \in B, h \in T_H(\sigma)\} = \{(b;h) : b \in B, h \in H, \sigma_{h(x)} \sim \sigma_x \forall x \in X\}$$

It follows from Lemma 3.2.2.0.1 that

$$I_G(\sigma) = \{(b;h) \in G \wr H : \sigma_{h(x)} \sim \sigma_x \forall x \in X\}$$

and thus $G \wr T_H(\sigma) = I_G(\sigma)$. □

Thus far we have been dealing with irreps σ of $G^X \leqslant G \wr H$ which are the tensor product of irreps of G. Before inducing these to the whole group, they must be extended to $I_G(\sigma)$, as this will allow one to use the "little group method" to find irreps of $G \wr H$, as described in [5].

First, these extensions must be found. Of course, $G^X \leqslant I_G(\sigma)$ (take $h = e_H$), on which σ is defined (see above). Then, it remains to determine how σ acts on $(e_B; h)$ for $h \in H$ which satisfy $\sigma_{h(x)} \sim \sigma_x$. That is, if this relation is satisfied, choose the two representations to be equal by being of the same basis.

Lemma 3.2.2.0.3 (Lemma 2.4.3,[5])**.** *The extension of each $\sigma \in \widehat{G^X}$ to $\tilde{\sigma} \in \widehat{I_G(\sigma)}$ is defined by*

$$\tilde{\sigma}(b;h)(\otimes_{x \in X} v_x) = \otimes_{x \in X} \sigma_{h^{-1}x}(g_x) v_{h^{-1}x}$$

for every $(b;h) = (g_1, ..., g_n; h) \in G \wr T_H(\sigma)$ and $v_x \in V_x$, where σ_x acts on the vector space V_x.

Now that the extension to the inertia group has been determined, the "little group" method may be employed, summarized in the theorem below. Note that the term "$G \wr H$-conjugacy class" refers to the conjugacy classes of the representations of $\widehat{G^X}$ in $G \wr H$, where $\sigma, \rho \in \widehat{G^X}$ are equivalent if $\sigma^{(g;h)} = \rho$ for some $(g;h) \in G \wr H$. Note that since $\sigma^{(g;e_H)} = \sigma$ the conjugacy classes depend on the value of $h \in H$. This is important to avoid "double counting" when one induces the extended representation. The set of representatives for these conjugacy classes will be denoted Γ.

Recall, as well, that $G^X \lhd I_{G \wr H}$ and so $T_H(\sigma) \cong I_{G \wr H}(\sigma)/G^X$ and so one can inflate its irreducible representations to irreps of $I_{G \wr H}(\sigma)$ by making it act trivially on G^X.

Theorem 3.2.2.0.1 (Little Group Method, Thm. 1.3.11 [5]). *Use the notation from above. In addition, for irreps $\eta \in \widehat{T_H(\sigma)}$, denote the inflation to $\widehat{I_{G\wr H}}(\sigma)$ by $\bar{\eta}$, defined so that $\bar{\eta}(b;h) = \eta(h)$. Then, the irreps of the wreath product group are given by the following set:*

$$\widehat{G \wr H} = \{Ind_{I_{G\wr H}(\sigma)}^{G\wr H}(\tilde{\sigma} \otimes \bar{\eta}) : \sigma \in \Gamma, \eta \in \widehat{T_H}(\sigma)\}$$

3.2.3 Small example: $Z_2 \wr Z_n$

Before looking at more general wreath products of cyclic groups, in order to better understand the representation theory of wreath products, this section will explore the representations of $Z_2 \wr Z_n$.

In order to synthesize this group with the notation and theory above, note that $G = Z_2, H = Z_n, X = \{0, ..., n-1\}, G^X = \{(g_0, ..., g_{n-1}; 0) : g_i \in Z_2\}$. As well, the action of H on the base group $B = G \times ... \times G$ is defined as

$$\phi_h(b) = \phi_h(g_0, ..., g_{n-1}) = (g_h, ..., g_{h+n-1})$$

for $b = (g_0, ..., g_{n-1}) \in B, h \in Z_n$.

Since Z_2, Z_n are abelian groups, their irreps are all one dimensional. Specifically, we have

$$\widehat{Z_2} = \{1, -1\} = \{(e^{\pi i})^k : k \in Z_2\}$$

$$\widehat{Z_n} = \{(e^{\frac{2\pi i}{n}})^k : k \in Z_n\}$$

for simplicity let $\omega_m = e^{\frac{2\pi i}{m}}$ for any nonzero m.

Since the tensor of one-dimensional irreps is also one dimensional, the following set of irreps of $\widehat{G^X}$:

$$\widehat{G^X} = \{\otimes_{x \in Z_n} \omega_2^{k_x} : k_x \in Z_2\}$$

will result in a value of 1 or -1 when applied to a vector in Z_2^n. More precisely, let $v, k \in Z_2^n$, and let $\chi_k \in \widehat{G^X}, \chi_k = \otimes_{i \in Z_n} \omega_2^{k_i}$. Then, $\chi_k(v) = (-1)^{k \cdot v}$.

Next, consider $h \in Z_n$ which acts by permuting the base group. Then, $h\chi_k = \chi_{h+k}$, where addition occurs component-wise, and so Z_n simply permutes the representations of Z_2^n.

Let $\chi_k \in \widehat{G^X}$, $\omega_{2;x}^{k_x} \in G_x$, where $k \in Z_2^n$. Then, χ_k has the stabilizer group

$$T_{Z_n}(\chi_k) = \{y \in Z_n : \omega_{2;y+x}^{k_x} = \omega_{2;x}^{k_x} \forall x \in Z_n\}$$

Note that the $k_i's$ denote the label of the irrep, whereas the x subscript denotes which entry in the direct product it belongs to.

Example 3.2.3.0.1. If $n = 3, k = (1, 0, 1)$, then the irrep $\chi_k = \omega_{2;0} \otimes 1_1 \otimes \omega_{2;2}$. While $\omega_{2;0} = \omega_{2;2}$ the stabilizer is still only the trivial group, $T_{Z_n}(\chi_k) = \{0\}$, since Z_3 acts by addition. If instead we had $H = S_3$ then the elements $(), (13)$ would stabilize the above expression.

In general, since the stabilizer group must be a subgroup of Z_n, its order must divide n. Consider the stabilizer of a $\chi_k \in \widehat{G^X}$, where $h \in H$ acts by $h\chi_k = \chi_{h+k}$ where h is added to each k_i so that $h+k = (k_0+h, ..., k_{n-1}+h)$, since

$$h\chi_k = \otimes_{x\in X}\chi_{h+x}^{k_x} = \otimes_{x\in X}\chi_x^{h+k_x} = \chi_{h+k}$$

In this case, the stabilizer is analogous to the period of k viewed as a function; that is, if $k(h) = (k_0 + h, ..., k_{n-1} + h)$ then the smallest integer t such that $k(h + t) = k(t)$ for all integers h is the "period" of k and will be in the stabilizer; in fact, it will generate the stabilizer.

Since addition is being done modulo n, $1 \leqslant t \leqslant n$ and $k(h + n) = k(h)$ as well. Thus, $n = tm$ for some $1 \leqslant m \leqslant n$, and so t must divide the order of Z_n, and actually generates the stabilizer. Thus, we obtain the following claim describing the stabilizer subgroup:

Claim 3.2.3.0.1. *Suppose $P = Z_2 \wr Z_n$, and let $H = Z_n$. If $\chi_k = \otimes_{x\in X}\chi_x^{k_x}$ is an irrep of Z_2^n and t is the smallest integer such that $k(h+t) = (k_0 + h + t, ..., k_{n-1} + h + t) = k(h)$ then the stabilizer subgroup of χ_k is*

$$T_H(\chi_k) = \{h \in H : h\chi_k = \chi_{h+k} = \chi_k\} = \langle t\rangle \cong Z_m$$

where $m = \frac{n}{t}$.

Example 3.2.3.0.2. If $n = 4, k = (1, 0, 1, 0), k' = (1, 1, 1, 0)$ then $T_H(\chi_k) = \{0, 2\} = \langle 2\rangle \cong Z_2$ and $T_H(\chi_{k'}) = \{0\}$.

Let $m = |T_H(\chi_k)| = |Z_m|$. Note that while $m \leqslant n$, the elements in this stabilizer group are still acting on the full set X, and thus the action of Z_m is not transitive on X. For this reason, the wreath product is still a semidirect product with $G^X = Z_2^n$. Then, the inertia group is

$$I_{Z_2\wr Z_n}(\chi_k) = \{(b; h) : b \in Z_2^n, h \in \langle t\rangle\}$$

Next, an extension of χ_k to the inertia group, denoted $\tilde{\chi_k}$, must be found. This definition is quite straightforward: for $h \in T_H(\chi_k), b \in Z_2^n$,

$$\tilde{\chi_k}(b; h) = \chi_k(b) = \omega_2^{k\cdot b}$$

This is because every $h \in \langle t\rangle$ is of the form $h = ty$ and so $h^{-1} \in \langle t\rangle$. Then, $h^{-1}(x) = x$ since it is a multiple of the period of k. Thus, using Lemma 3.2.2.0.3,

$$\tilde{\chi_k}(b; h)(\otimes_{x\in X} v_x) = \otimes_{x\in X}\chi_{h^{-1}x}(g_x)v_{h^{-1}x} = \otimes_{x\in X}\chi_x(g_x)v_x$$

Since $\widehat{Z_n} = \{\omega_n^k : k \in Z_n\}$, the irreps of the stabilizer group, which is isomorphic to Z_m for $m \leqslant n$, will be a subset of this.

The irreps of a group Z_m are the m-roots of unity; that is, the set $\widehat{Z_m} = \{\omega_m^k : k \in Z_m\}$. Consider $\omega_n^j \in \widehat{Z_n}$. Then, when restricted to the stabilizer group it only acts on elements of the form tb where b is an integer. Then, since $n = tm$,

$$\omega_n^j(tb) = (e^{\frac{2\pi i}{n}})^{j(tb)} = e^{\frac{2\pi ij}{tm}tb} = \omega_m^j(b)$$

To avoid confusion with the larger group define the irreps of the stabilizer group in terms of the m^{th}-roots of unity; that is, as

$$\widehat{T_H(\chi_k)} = \{\omega_m^j : j \in Z_m\}$$

where $\omega_m^j(bt) = \omega_m^{jb}$, and, of course, the particular choice of m, t depends on the value of k (it can be thought of as a function of k since it is dependent on its value. For brevity, though, this dependence will be omitted from notation).

Let $\eta_j \in \widehat{T_H(\chi_k)}$ and define its inflation to the inertia group as

$$\bar{\eta_j}(b; h) = \eta_j(h) = \omega_m^{jl}$$

where $h = tl \in \langle t \rangle$.

Since $\bar{\eta_j}, \tilde{\chi_k}$ are both one dimensional representations, their tensor product is also one-dimensional, given by

$$\tilde{\chi_k} \otimes \bar{\eta_j}(b; tl) = \chi_k(b)\eta_j(tl) = \omega_2^{k \cdot b}\omega_m^{jl}$$

This tensor is now defined on the inertia group and thus can be induced to the whole group. First, however, the set Γ of the irreps of representatives of the $Z_2 \wr Z_n$-conjugacy classes of Z_2^n must be determined. That is, not all $\chi_k \in \widehat{Z_2^n}$ will give distinct representations. Since conjugate representations under Z_n will induce to the same representation, one only needs to consider representatives for these representations.

To determine the orbit of Z_n on Z_2^n one can use Pólya-Redfield theory, as discussed in [8]. Let $|Fix(h)|$ denote the number of elements in Z_2^n which are fixed by h. For example, if $h = 0$ then all elements in Z_2^n are fixed by h, so that $|Fix(b)| = 2^n$.

Then, the number of elements in Γ is given by a variation of Burnside's lemma, so that

$$|\Gamma| = \frac{1}{|Z_n|} \sum_{h \in Z_n} |Fix(h)|$$

Example 3.2.3.0.3. Suppose $n = 2$, and so $Z_2^2 = \{(0,0), (0,1), (1,0), (1,1)\}$. Then, the sum is

$$|\Gamma| = \frac{1}{2}(|Fix(0)| + |Fix(1)|) = \frac{1}{2}(|Z_2^2| + |\{(0,0), (1,1)\}|) = 3$$

Next, since

$$Z_2 \cdot (0,0) = \{(0,0)\}, Z_2 \cdot (1,1) = \{(1,1)\}$$
$$Z_2 \cdot (1,0) = Z_2 \cdot (0,1) = \{(1,0), (0,1)\}$$

there are three distinct orbits, and so the set $\{(0,0), (0,1), (1,1)\}$ holds representatives of the orbits. Note that we could have chosen $(1,0)$ instead of $(0,1)$. Then,

$$\Gamma = \{\chi_{(0,0)}, \chi_{(0,1)}, \chi_{(1,1)}\}$$

Returning to the general case, since $T_H(\chi_k) = \langle t \rangle \cong Z_m$ stabilizes χ_k, the orbit of χ_k is

$$Z_n \cdot \chi_k = \{\chi_{k+c} : c \in Z_n\}$$

Since $\chi_{tb+k} \sim \chi_k$ the above definition restricts c so that it is not a multiple of t. That is, it gives representatives for the orbits of χ_k. Thus, Γ, which is a set of representations of the *representatives* of the orbits should given by

$$\Gamma = \{\chi_{k+c} : c \in Z_n, c \notin \langle t \rangle\}.$$

Finally, it remains to employ the "Little Group" method, given as Theorem 3.2.2.0.1. Use the notation above. Then, the irreps of $Z_2 \wr Z_n$ are given by

$$\widehat{Z_2 \wr Z_n} = \{Ind_{I_{Z_2 \wr Z_n}(\chi_k)}^{Z_2 \wr Z_n}(\tilde{\chi_k} \otimes \bar{\eta}) : \chi_k \in \Gamma, \eta \in \widehat{T_H}(\sigma)\}.$$

Since the inertia group is

$$I_{Z_2 \wr Z_n}(\chi_k) = \{(b; h) : b \in Z_2^n, h \in \langle t \rangle\}$$

and is normal in $Z_2 \wr Z_n$ its quotient with this group is given by

$$Z_2 \wr Z_n / I_{Z_2 \wr Z_n}(\sigma) = \{(0; c) I_{Z_2 \wr Z_n} : c \in Z_n, c \notin \langle t \rangle\} \cong Z_t$$

In fact, more generally, we have the relation

$$(G \wr H)/I_{G \wr H}(\sigma) \cong H/T_H(\sigma).$$

Because of the isomorphism above, instead of considering $(G \wr H)/I_{G \wr H}(\sigma)$ we can consider $H/T_H(\sigma)$; that is, use the set of coset representatives for this quotient. This is simply $\{0, h : h \notin \langle t \rangle\}$.

We can thus specify the irreps of $\widehat{Z_2 \wr Z_n}$. Suppose we are inducing the irrep $\tilde{\chi_k} \otimes \bar{\eta_j}$ which acts on the vector space $V = \mathbb{C}$ since it is one-dimensional.

Then, let $(b; h) \in Z_2 \wr Z_n$. To determine its action on $v \in V$, note the following:

$$\begin{aligned}
(b; h) \sum_{c \in Z_t} (0; c) \otimes v &= \sum_{c \in Z_t} (\psi_c(b); h + c) \otimes v \\
&= \sum_{c \in Z_t} (0; c)(\psi_c(b); h) \otimes v \\
&= \sum_{c \in Z_t} (0; c) \otimes (\tilde{\chi_k} \otimes \bar{\eta_j})((\psi_c(b); h))v \\
&= \sum_{c \in Z_t} (0; c) \otimes (\chi_k(\psi_c(b)) \otimes \eta_j(h))v \\
&= \sum_{c \in Z_t} (0; c) \otimes \omega_2^{k \cdot \psi_c(b)} \omega_n^{jh} v
\end{aligned}$$

Thus, the final, induced representation, denoted $\sigma_{k,j}$ is given by

$$\sigma_{k,j}(b; h) = \sum_{c \in Z_t} \omega_2^{k \cdot \psi_c(b)} \omega_n^{jh} |c\rangle\langle c|.$$

3.2.4 Another example: $\mathbb{Z}_n^m \wr \mathbb{Z}_q$

Let us now consider the representation theory of a group $P = \mathbb{Z}_n^m \wr \mathbb{Z}_q$. For brevity let $G = \mathbb{Z}_n^m, H = \mathbb{Z}_q$, with base group G^X (of course, $X = \{0, 1, ..., q-1\}$).

First, consider the irreps of G; these are simply the n^m one-dimensional representations

$$\chi_k(a) = \omega_n^{k \cdot a}, \omega_n = e^{\frac{2\pi i}{n}}, a, k \in G$$

This gives rise to n^{mq} one-dimensional irreps of G^X:

$$\widehat{G^X} = \{\otimes_{x \in Z_q} \chi_{k_x} : k_x \in Z_{p^n}^m\}$$

where, for $\kappa_k = \otimes_{x \in Z_q} \chi_{k_x} \in \widehat{G^X}, v, k \in Z_n^{mq}, k = (k_0, ..., k_{q-1}), v = (v_0, ..., v_{q-1})$,

$$\begin{aligned}
\kappa(v) &= \otimes_{x \in Z_q} \chi_{k_x}(v_x) \\
&= \otimes_{x \in Z_q} \omega_n^{k_x \cdot v_x} \\
&= \omega_n^{\sum_{x \in Z_q} k_x \cdot v_x} \\
&= \omega_n^{k \cdot v}
\end{aligned}$$

Next, we need to find the isotropy group,

$$T_H(\kappa_k) = \{y \in \mathbb{Z}_q : \chi_{k_{x+y}} = \chi_{k_x} \forall x \in \mathbb{Z}_q\}$$

As before, this will be a function of k; that is, if $k(h) = (k_0 + h, ..., k_{q-1} + h)$ then the smallest integer t where $k(h + t) = k(h)$ for all integers h generates the isotropy group.

Since the order of t must divide q, if q is prime then

$$T_H(\kappa_k) = \begin{cases} \mathbb{Z}_q \text{ if } \chi_{k_x} = \chi_{k_y} \forall x, y \in Z_q \\ \{0\} \text{ else} \end{cases}$$

Since G is cyclic abelian, the irreps of G^X can be extended trivially to the inertia group.

Next, suppose $d = \frac{q}{t}$. Then, since the irreps of $\mathbb{Z}_q$ are of the form $\omega_q^j, j \in \mathbb{Z}_q$, the irreps of the isotropy group, with elements of the form $tb \in \langle t \rangle$, are given by

$$\omega_q^j(tb) = \omega_d^j(b)$$

where, of course, if q is prime then d is either 1 or q. That is, we get the set

$$\widehat{T_H(\kappa_k)} = \{\omega_d^j : j \in Z_d\}, \text{ where } \omega_d^j(bt) = \omega_d^{jb}$$

The inflation of any irrep $\eta_j \in \widehat{T_H(\kappa_k)}$ can be defined simply as

$$\bar{\eta_j}(b; h) = \eta_j(h) = \omega_m^{jl}, h = tl \in \langle t \rangle$$

Finally, the tensor product of an irrep $\bar{\kappa_k} \in \overline{G^X}, \bar{\eta_j} \in \overline{T_H(\kappa_k)}$ is given by

$$\bar{\kappa_k} \otimes \bar{\eta_j}(b;tl) = \kappa_k(b)\eta_j(tl) = \omega_n^{k\cdot b}\omega_d^{jl}$$

Now, consider inducing $\bar{\kappa_k} \otimes \bar{\eta_j}$ which acts on the vector space $V = \mathbb{C}$, since it is one-dimensional, to an irrep of $\widehat{G \wr H} = \widehat{\mathbb{Z}_n^m \wr \mathbb{Z}_q}$.

To determine the coset representatives, consider $(G \wr H)/I_{G\wr H}(\sigma) \cong H/T_H(\sigma) = \{0, h : h \notin \langle t \rangle\}$. Let T denote the set of coset representatives. Then, let $(b;h') \in G \wr H$ where $(b;h') = (b;h+d)$ for some $h \in \langle t \rangle, d \notin T_H(\kappa_k)$ and consider its action on $v \in V$. One can calculate the following:

$$\begin{aligned}
(b;h')\sum_{c\in T}(0;c)\otimes v &= \sum_{c\in T}(\psi_c(b);h'+c)\otimes v \\
&= \sum_{c\in T}(0;c+d)(\psi_c(b);h)\otimes v \\
&= \sum_{c\in T}(0;c+d)\otimes(\overline{\kappa_k}\otimes\bar{\eta_j})((\psi_c(b);h))v \\
&= \sum_{c\in T}(0;c+d)\otimes(\kappa_k(\psi_c(b))\otimes\eta_j(h))v \\
&= \sum_{c\in T}(0;c+d)\otimes\omega_n^{k\cdot\psi_c(b)}\omega_q^{jh}v
\end{aligned}$$

Thus, the final, induced representation, denoted $\sigma_{k,j}$ is given by

$$\sigma_{k,j}(b;h') = \sum_{c\in T}\omega_n^{k\cdot\psi_c(b)}\omega_q^{jh}|c+d\rangle\langle c|$$

with dimension $d = \frac{q}{t}$.

If q is prime then all irreps are either dimension 1 or q. In fact, for $G = \mathbb{Z}_n^m, H = \mathbb{Z}_{\text{ıı}}, q$ prime, there are n^m irreps κ_k of G^X which have $T_H(\kappa_k) = \mathbb{Z}_q$, occurring when $k = (i,i,...,i), i \in \mathbb{Z}_p^n$. These will induce to 1-dimensional irreps. The remaining irreps will induce to irreps of dimension q.

Since each element in Z_q when q is prime fixes elements in G^X which are in the diagonal subgroup, and $0 \in Z_q$ fixes every element in G^X,

$$|\Gamma| = \frac{1}{q}\sum_{h\in Z_q}|Fix(h)| = \frac{1}{q}(|G^X| + (q-1)|G|) = \frac{n^{mq}+(q-1)n^m}{q}$$

gives the total number of κ_k one needs to induce.

That is, each element $g \in \mathbb{Z}_n^m$ has an orbit of size $\binom{q}{q-l}$ where l is the number of zeroes in g when acted on by Z_q. Then, the n^m elements in the diagonal subgroup have orbit of size 1 and thus are fixed by every $h \in T_H(\kappa)$ giving n^m 1-dimensional irreps and $\frac{n^{mq}+(q-1)n^m}{q} - n^m = \frac{n^{mq}-n^m}{q}$ q-dimensional irreps.

3.3 $\mathbb{Z}_p^n \wr \mathbb{Z}_p^d$

This section will specifically consider the group $P = \mathbb{Z}_p^n \wr \mathbb{Z}_p^d = G \wr H, n, d \geqslant 1$. Of course, this must be a nilpotent group, and has order $(p^n)^{p^d} p^d = p^{p^d n + d}$.

The set X being acted on by H has size p^d; it can be considered H itself where the action is addition as defined in H. Specifically, consider elements in H, G as uniquely encoded strings. Let $h \in H$ be the string $h = h_{d-1}...h_0 = (h_k)_{0 \leqslant k < d}$ where each $h_k \in \mathbb{Z}_p$. Similarly, let $a \in G$ be the string $a = a_{n-1}...a_0 = (a_i)_{0 \leqslant k < n}$ where each $a_k \in \mathbb{Z}_p$. Addition occurs component-wise, so that if $h, t \in H$ then $h + t = (h_k + t_k)_{0 \leqslant k < d}$, and similarly for addition in G.

In order to define an ordering, identify each $h = (h_k)_{0 \leqslant < d} \in H$ with a unique string so that each h_k is an integer, $0 \leqslant h_k < p$, and consider a map $\phi_H : H \to \mathbb{Z}_{p^d}$ and $\phi_G : G \to \mathbb{Z}_{p^n}$ given by

$$\phi_H(h_k)_{0 \leqslant k < d} = \sum_{k=0}^{d-1} h_k p^k$$

$$\phi_G(g_k)_{0 \leqslant k < n} = \sum_{k=0}^{n-1} g_k p^k$$

Then, we define the ordering as follows: for $h, t \in H, h < t \Leftrightarrow \phi_H(h) < \phi_H(t)$. An analogous relation holds in G.

Finally, since $G^X = \prod_{x \in X} G$, let $g \in G^X$ be defined as $g = (g_x)_{x \in \phi_H(X)} = (g_0, ..., g_{p^d - 1})$ where each $g_j = (a_i)_{0 \leqslant i < n}, a_i \in \mathbb{Z}_p$ as described above, and $\phi_H(X) = \{\phi_H(x) : x \in X\}$ is a set ordered in $\mathbb{Z}_{p^d}$. Of course, one could equivalently write $g' = (g'_x)_{x \in X} = (g_{(0_k)_{0 \leqslant k < d}}, g_{(0_k 1)_{1 \leqslant k < d}}, ..., g_{(12_k)_{0 \leqslant k < d-1}}, g_{(2_k)_{0 \leqslant k < d}})$.

Now, let us specify the action of H on G^X. This will simply be a permutation of G^X according to component-wise addition in the elements of X. That is, for $(g; h) = ((g_x)_{x \in X}; (h_k)_{0 \leqslant k < d}), (g'; h') = ((g'_x)_{x \in X}; (h'_k)_{0 \leqslant k < d})$, and where addition occurs component-wise as described previously,

$$(g; h)(g'; h') = ((g_{x+h'})_{x \in X} + (g'_x)_{x \in X}; (h_k + h'_k)_{0 \leqslant k < d})$$

and inverses are given by

$$(g; h)^{-1} = ((-g_{x-h})_{x \in X}; -h)$$

where $-h = (-h_k)_{0 \leqslant k < d}, -g_{x-h} = (-a_i)_{0 \leqslant i < n})$.

Consider conjugation in this group: let $(g; h), (g'; h') \in P$. Then,

$$\begin{aligned}((-g'_{x-h'})_{x \in X}; -h')(g; h)(g'; h') &= ((-g'_{x-h})_{x \in X}; -h')((g_{x+h'})_{x \in X} + (g'_x)_{x \in X}; (h_k + h'_k)_{0 \leqslant k < d}) \\ &= ((-g'_{x+h})_{x \in X} + (g_{x+h1})_{x \in X} + (g'_x)_{x \in X}; h) \\ &= ((-g'_{x+h} + g_{x+h'} + g'_x)_{x \in X}; h)\end{aligned}$$

Clearly, two elements $(g;h),(r;h')$ are conjugate only if $h=h'$. Let $(r;h)=((-g'_{x+h}+g_{x+h'}+g'_x)_{x\in X};h)$ and notice that

$$\begin{aligned}(r;h)^p &= ((\sum_{i=0}^{p-1} r_{x+ih})_{x\in X};0)\\ &= ((\sum_{i=0}^{p-1} g_{x+ih+h'})_{x\in X};0)\\ &= ((-g'_{x-h'})_{x\in X};-h')(g;h)^p(g';h')\end{aligned}$$

and thus if $(g;h),(r;h)$ then $\sum_{i=0}^{p-1} r_{x+ih}=\sum_{i=0}^{p-1} g_{x+ih+h'}$ for all $x\in X$ and some $h'\in H$.

Now, suppose $(g;h),(r;h)$ are conjugate, so that $(g;h)(g';h')=(g';h')(r;h)$ fore some $(g';h')\in P$. Then we get the equation

$$((g_{x+h'})_{x\in X}+(g'_x)_{x\in X};(h_k+h'_k)_{0\leqslant k<d})=((g'_{x+h})_{x\in X}+(r_x)_{x\in X};(h'_k+h_k)_{0\leqslant k<d})$$

That is, for each $x\in X$ we get the equation

$$g_{x+h'}+g'_x=g'_{x+h}+r_x$$

Claim 3.3.0.0.1. *Suppose $(g;h),(r;h')$ are two elements in P. Then, they are conjugate if and only if $h=h'$ and $g_{x+k}+g'_x=g'_{x+h}+r_x$ for all $x\in X$ and some $k\in H, g'=(g'_x)_{x\in X}\in G^X$. Note that this will imply that $(\sum_{i=0}^{p-1} g_{x+ih+k})_{x\in X}=(\sum_{i=0}^{p-1} r_{x+ih})_{x\in X}$.*

The center, as shown in a previous section, is given by

$$Z(P)=\{((g)_{x\in X};0):g\in\mathbb{Z}_p^n\},\ |Z(P)|=p^n$$

3.3.1 Subgroups with one generator

3.3.1.1 General theory

This section will examine the nature of single-generator subgroups. In order to better understand these, consider the orbit of a fixed element in H on each X. Of course, the action of H on X is transitive, however given a $(g;h)\in P$, repeated products will not permute all elements in g; that is, $\psi_h(g)$ is not transitive, where $(g;h)(g;h)=(\psi_h(g)g;h)$. Instead, the size of its orbit is p.

Specifically, fix $h=(h_k)_{0\leqslant k<d}\in H, x=(x_k)_{0\leqslant k<d}\in X$ and consider $h\cdot x$, where $\cdot$ denotes the action by component-wise addition. Then,

$$h\cdot x=(h_k+x_k)_{0\leqslant k<d}, h\cdot(h\cdot x)=(2h_k+x_k)_{0\leqslant k<d}, h\cdot(h\cdot(h\cdot x))=x$$

Consider a subgroup generated by any $(g;h)\in P$.

$$(g;h)^y=(\sum_{i=0}^{y-1}(g_{x+ih})_{x\in X};yh)$$

Of course, if $h \neq 0$ then $o(h) = p$ and so $(g;h)^p = (\sum_{i=0}^{2}(g_{x+ih})_{x\in X}; 0)$. Then, if $\sum_{i=0}^{2}(g_{x+ih})_{x\in X} \neq 0$ then $o(\sum_{i=0}^{2}(g_{x+ih})_{x\in X}) = p$ and so $(g;h)^{p^2} = (0;0)$. As well, note that if $y = pk + t, k \geqslant 0, p > t \geqslant 0, y > 0$, then

$$(g;h)^y = (k\sum_{i=0}^{p-1}(g_{x+ih})_{x\in X} + \sum_{i=0}^{t-1}(g_{x+ih})_{x\in X}; th)$$

For this reason, we obtain the following lemma:

Lemma 3.3.1.1.1. *Suppose a subgroup of P is generated by a single element $(g;h) = ((g_x)_{x\in X}; (h_k)_{0\leqslant k<d}), h \neq 0$, where each $g_j = (a_i)_{0\leqslant i<n}, a_i \in \mathbb{Z}_p$. Then, $\langle (g;h)\rangle$ will contain a nontrivial subgroup of the center if and only if $\sum_{i=0}^{p-1} g_{x+ih} = \sum_{i=0}^{p-1} g_{x'+ih} \neq 0$ for all $x, x' \in X$.*

Specifically, this subgroup will be generated by $((\sum_{i=0}^{p-1} g_{ih})_{x\in X}; 0)$.

This gives us the following brief corollary:

Corollary 3.3.1.1.1. *Suppose a subgroup of P is generated by a single element $(g;h)$ as defined in the lemma above. Then, the order of $\langle (g;h)\rangle$ is:*

1. *1, if $(g;h) = (0;0)$*
2. *p, if $\sum_{i=0}^{p-1} g_{x+ih} = 0$ for all $x \in X$*
3. *p^2 in all other cases.*

Let us try to determine the conjugate subgroups of $\langle (g;h)\rangle$. Before doing so, however, let us determine when two distinct elements $(g';h'), (g;h) \in P$ commute. This occurs if

$$(g';h')(g;h) = ((g'_{x+h} + g_x)_{x\in X}; h' + h) = ((g_{x+h'} + g'_x)_{x\in X}; h + h')$$

Since component-wise addition commutes, we require that $g'_{x+h} + g_x = g_{x+h'} + g'_x$ for all $x \in X$. This occurs if components in the same h, h' orbit are equal; that is, if $g_{x+h'} = g_{x+ih'}$ and $g'_x = g'_{x+ih}$ for all $0 \leqslant i < p$ and for all $x \in X$. To summarize, this indicates the following lemma:

Lemma 3.3.1.1.2. *Let $(g;h) = ((g_x)_{x\in X}; h) \in P$. Let $g' = (g'_x)_{x\in X} \in G^X$ be such that that $g'_x = g'_{x+ih}$ for all $0 \leqslant i < p$ and $x \in X$. Call this property the "h- orbit property ". Finally, suppose g has the h'-orbit property. Then, $(g;h)$ commutes with $(g';h')$.*

Note that any element must always have the 0-orbit property.

Recall that for an element $(g';h') \in P$, and where $-h' = (-h'_i)_{0\leqslant i<d}$,

$$(\psi_{-h'}(-g'); -h')(g;h)(g';h') = ((-g'_{x+h} + g'_x + g_{x+h'})_{x\in X}; h)$$

Of course, if $(g';h'), (g;h)$ commute, as per Lemma 3.3.1.1.2, then the final value is simply $(g;h)$.

Otherwise, we know by Claim 3.3.0.0.1 that two elements $(r;h), (g;h)$ are conjugate if $g_{x+k} + g'_x = g'_{x+h} + r_x$ for all $x \in X$ and some $k \in H$.

Additionally,

$$((-g'_{x+h}+g'_x+g_{x+h'})_{x\in X};h)^p=(\sum_{i=0}^{p-1}(g_{x+ih+h'})_{x\in X};0)$$

which is just a permutation of G^X in $(g;h)^p$ by h' and so if $(g;h)$ is conjugate to $(r;h)$ then $\sum_{i=0}^{p-1}r_{x+ih}=\sum_{i=0}^{p-1}g_{x'+ih}$ for some $x,x'\in X$. Of course, this implies that $\langle(r;h)\rangle$ will generate the same subgroup of the base group as $(g;h)$.

Suppose $(g';h')$ stabilizes $\langle(g;h)\rangle$. Then, one obtains a series of p equations which must be satisfied for each $0\leqslant t<p$, where $\sum_{i=0}^{-1}g=0$, and for any $0\leqslant k\leqslant p$:

$$\begin{aligned}(\phi_{-h'}(-g');-h')(g;h)^{pk+t}(g';h')&=(\phi_{-h'}(-g');-h')((k\sum_{i=0}^{p-1}g_{x+ih}+\sum_{i=0}^{t-1}g_{x+ih})_{x\in X};th)(g';h')\\&=(\phi_h(-g')+\phi_{h'}(k\sum_{i=0}^{p-1}g_{x+ih}+\sum_{i=0}^{t-1}g_{x+ih})_{x\in X}+g';th)\\&=((-g'_{x+th}+k\sum_{i=0}^{p-1}g_{x+ih+h'}+\sum_{i=0}^{t-1}g_{x+ih+h'}+g'_x)_{x\in X};th)\\&=((k'\sum_{i=0}^{p-1}g_{x+ih}+\sum_{i=0}^{t-1}g_{x+ih})_{x\in X};th)\end{aligned}$$

and thus the equality $-g'_{x+th}+k\sum_{i=0}^{p-1}g_{x+ih+h'}+\sum_{i=0}^{t-1}g_{x+ih+h'}+g'_x=k'\sum_{i=0}^{p-1}g_{x+ih}+\sum_{i=0}^{t-1}g_{x+ih}$ must be satisfied for all $x\in X$. Consider when $t=p-1$ and subtract from it the case when $t=p-2$ to obtain

$$-g'_{x-h}+g'_{x-2h}+g_{x-h+h'}-g_{x-2h}=\kappa\sum_{i=0}^{p-1}g_{x+ih}$$

Thus we can conclude with the following claim:

Claim 3.3.1.1.1. *Consider an element $(g;h)\in P$. Then, $(g;h)$ is conjugate to any $(r;h)$ if there exists some $k\in H$ where, for all $x\in X$, the relation $g_{x+k}+g'_x=g'_{x+h}+r_x$ is satisfied.*

If the above conditions hold then $\sum_{i=0}^{p-1}r_{x+ih}=\sum_{i=0}^{p-1}g_{x+k+ih}$ and thus $\langle(r;h)\rangle$ and $\langle(g;h)\rangle$ will contain the same subgroup $\langle((\sum_{i=0}^{p-1}r_{x+ih})_{x\in X};0)\rangle$ of the base group.

As well, the subgroup generated by $\langle(g;h)\rangle$ is stabilized by $(g';h')$ if there exists some $0\leqslant d<p$ so that the relation $g'_x-g'_{x+h}+g_{x+h'}-g_x=d\sum_{i=0}^{p-1}g_{x+ih+h'}$ is satisfied for all $x\in X$.

Example 3.3.1.1.1. Consider the case when $h'=0,p=3$, and $(g';0)$ stabilizes $\langle(g;h)\rangle$. Then, this implies that $g'_x-g'_{x+h}+g_x-g_x=d\sum_{i=0}^{2}g_{x+ih}$ and thus for a fixed x we get the equations

$$g'_x-g'_{x+h}=k,g'_{x+h}-g'_{x+2h}=k,g'_{x+2h}-g'_x=k$$

where $k=d\sum_{i=0}^{2}g_{x+ih}\in\mathbb{Z}_3^n$. Then,

$$2g'_x-g'_{x+h}=g'_{x+2h},2g'_{x+h}-2g'_x=k$$

which gives 3^n possible solutions for each value of k.

3.3.1.2 Specific generators

Let us now limit ourselves to subgroups generated by a specific subset of elements in G, H in order to obtain unique single-generator subgroups. Note that every non-zero element in $\mathbb{Z}_p$ is a generator, and G, H cannot be generated by a single element.

Let $c_K \in H, K \in \mathbb{Z}_2^d$ be an elements such that $c_K = (k_i)_{0 \leqslant i < d}$; that is, an element in H with only ones and zeroes as entries. Note that $H = \langle \{ c_K : K \text{ contains exactly one } 1 \} \rangle$.

Similarly, let $b_I = (i_x)_{0 \leqslant x < n} \in G$ where $I \in \mathbb{Z}_2^n$. Then, let $g_{I,K,j} = ((0)_{x \in X, x<j} (b_I)_{x \in X, x=j} (0)_{x \in X, x>j}; c_K)$. For brevity write this as $g_{I,K,j} = (b_{I,j}; c_K)$.

Consider a subgroup generated by a single $g_{I,K,j}$. Since

$$g_{I,K,j}^p = (\sum_{i=0}^{p-1} (b_{I,j+ic_K}); 0)$$

by Lemma 3.3.1.1.1 for this to contain a non-trivial subgroup of the center we must have that $\{ j + ic_K : i \in \mathbb{Z}_p \} = X$, which implies that $d = 1$.

To summarize this as a claim, we get that

Claim 3.3.1.2.1. *Let $g_{I,K,j}$ be as discussed above. Then, $\langle g_{I,K,j} \rangle$ contains a non-trivial subgroup of the center only if $d = 1$.*

As well, if either $b_K = (0)_{x \in X}$ or $c_K = (0)_{0 \leqslant v < d}$ then $\sum_{i=0}^{p-1} (b_{I,j+ic_K}) = 0$ and so the generated subgroup has order p. (Of course, if both are zero then this is simply the trivial subgroup).

Suppose $c_K = 0$. Then, by Claim 3.3.1.1.1, $g_{I,0,j} = (b_{I,j}; 0)$ is conjugate to any $(r; 0)$ where $g_{x+k} + g'_x = g'_x + r_x$ and thus $r_x = g_{x+k}$ for some $k \in H$ and for all $x \in X$. Note that such an element $(r; 0)$ will then satisfy $\sum_{i=0}^{p-1} r_x = 0$ for all $x \in X$.

Specifically, this equality must hold when $x = j - k$ so that $g_j = b_I$, and thus in this case we get that $r_{j-k} = g_j = b_I$. For all other values of x we get that $r_x = 0$.

Alternatively, one can suppose that $g_{I,0,j}$ and $(k; 0)$ are conjugate by $(g'; h') \in P$. Then, the equality is the following:

$$(b_{I,j+h'} + g'; h') = (g' + k; h') \Rightarrow b_{I,j+h'} = k$$

where h' is arbitrary. Thus $g_{I,0,j}, g_{I,0,j'}$ are conjugate for any $j, j' \in X$.

This holds in general; that is, $(a; 0), (b; 0) \in P$ are conjugate if and only if $(\phi_h(a)) = b$ for some $h \in H$ since for some $(g; h) \in P$,

$$\begin{aligned} (a; 0)(g; h) &= (\phi_h(a) + g; h) \\ &= (g; h)(b; 0) = (g + b; h) \end{aligned}$$

As well, it is normal in a subgroup generated by $(g';h')$ if $g'_x - g'_x + g_{x+h'} - g_x = g_{x+h'} - g_x = d\sum_{i=0}^{2} g_x = 0$. Thus, since $g_j = b_I$ and $g_x = 0$ when $x \neq j$ we get that $(g';h')$ stabilizes $\langle g_{I,0,j} \rangle$ iff $h' = 0$. Thus this group is normal in the base group.

Similarly, suppose $b_I = 0$. Then $g_{0,j,K}$ is conjugate to all elements in P and the subgroup it generates is normal in P.

In general, assume I, K are not all zeroes. Thus, we have a subgroup of order p^2 which does not contain a non-trivial subgroup of the center, since

$$\sum_{i=0}^{2} (b_{I,j+ic_K})_x = \begin{cases} b_I \text{ if } x = j + ic_K, 0 \leqslant i < p \\ 0 \text{ otherwise} \end{cases}$$

In other words, $g^p_{I,K,j}$ will contain the value of b_I in the $j, j + c_K, j + 2c_K$ spots and zeroes elsewhere. We can thus apply Claim 3.3.1.1.1 to see that $g_{I,K,j}$ is conjugate to some $(w; c_K)$ where $g_{x+h'} + g'_x = g'_{x+c_K} + w_x$. Specifically, since $g_j = b_I$ and $g_x = 0$ for all other $x \in X$, consider when $x = j - h'$:

$$g_j + g'_j = g'_{j-h'+c_K} + w_j \Rightarrow b_I - w_j = g'_{j-h'+c_K} - g'_j$$

for all other values of x we get that

$$g'_x - g'_{x+c_K} = w_x$$

In addition, $(w; c_K)$ must satisfy the relation that $\sum_{i=0}^{2} w_{x+ic_K+h'} = b_I$ for the $h' \in H$ given above.

Finally, the subgroup generated by $g_{I,K,j}$ is stabilized by $(g';h')$ if

$$g'_x - g'_{x+c_K} + g_{x+h'} - g_x = d\sum_{i=0}^{p-1} g_{x+h'+ic_K}$$

consider four cases: when $x = j$, when $x = j - h'$, when $x = j - h' - ac_K$, for $1 \leqslant a \leqslant p-1$, and all other choices for $x \in X$, which give the following equations, respectively:

$$1. \quad g'_j - g'_{j+c_K} + g_{j+h'} - b_I = d\sum_{i=0}^{p-1} g_{j+h'+ic_K} \Rightarrow \begin{cases} g'_j - g'_{j+c_K} = db_I \text{ if } h' = 0 \\ g'_j - g'_{j+c_K} = b_I \text{ else} \end{cases}$$

$$2. \quad g'_{j-h'} - g'_{j-h'+c_K} + b_I - g_{j-h'} = d\sum_{i=0}^{p-1} g_{j+ic_K} \Rightarrow \begin{cases} g'_j - g'_{j+c_K} = db_I \text{ if } h' = 0 \\ g'_{j-h'} - g'_{j-h'+c_K} = (d-1)b_I \text{ else} \end{cases}$$

$$p. \quad g'_{j-h'-ac_K} - g_{j-h'+(1-a)c_K} = d\sum_{i=0}^{p-1} g_{j+ic_K} = db_I$$

$$4. \quad g'_x - g'_{x+c_K} = 0$$

Thus, g' must have the c_K-orbit property.

The above discussion can be summarized in the following lemma:

Lemma 3.3.1.2.1. *Suppose $g_{I,K,j} \in P$ is as defined above. Then:*

1. *$g_{I,0,j}$ and $g_{I,0,j'}$ are conjugate for all $j, j' \in X$ and the subgroup $g_{I,0,j}$ generates is normal in the base group.*
2. *$g_{0,K,j}$ is conjugate to all elements in P and is normal in P.*
3. *$g_{I,K,j}, I, K \neq 0$ is conjugate to any element $(w; c_K)$ where $g_{x+h'} + g'_x = g'_{x+c_K} + w_x$ and which implies that $\sum_{i=0}^{2} w_{x+h'+ic_K} = b_I$ and the subgroup it generates is stabilized by $(g'; h')$ if $g'_x - g'_{x+c_K} + g_{x+h'} - g_x = d\sum_{i=0}^{p-1} g_{x+h'+ic_K}$ for all $x \in X$.*

3.3.2 Representation theory

This section will focus on the representation theory of P. It is essentially just a specification of the discussion in Section 3.2.4.

First, consider the irreps of G; these are simply the p^n one-dimensional representations

$$\chi_k(a) = \omega_p^{k \cdot a}, \omega_p = e^{\frac{2\pi i}{p}}, a, k \in G$$

This gives rise to p^{np^d} one-dimensional irreps of G^X:

$$\widehat{G^X} = \{\otimes_{x \in X} \chi_{k_x} : k_x \in G\}$$

where, for $\kappa_k = \otimes_{x \in X} \chi_{k_x} \in \widehat{G^X}, v, k \in G^X, k = (k_x)_{x \in X}, v = (v_x)_{x \in X}$,

$$\kappa(v) = \omega_p^{\sum_{x \in X} k_x \cdot v_x} = \omega_p^{k \cdot v}.$$

Next, we need to find the isotropy group, which will be a function of k and will have order dividing p^d. It is given by

$$\begin{aligned} T_H(\kappa_k) &= \{y \in \mathbb{Z}_p^d : \chi_{k_{x+y}} = \chi_{k_x} \forall x \in \mathbb{Z}_p^d\} \\ &= \{h \in H : k \text{ has the h-orbit property}\} \\ &\cong \mathbb{Z}_p^f, \quad \text{for some } 0 \leqslant f \leqslant d. \end{aligned}$$

Next, the inertia group is given by

$$I_{G \wr H}(\kappa_k) = \{(b; h) : b \in G^X, h \in T_H(\kappa_k)\}$$

and we must extend the irreps κ_k of $\widehat{G^X}$ to irreps $\tilde{\kappa_k}$ of this group. In order to do this, recall Lemma 3.2.2.0.3. Then, for $((g_x)_{x \in X}; h) \in I_{G \wr H}(\kappa_k)$,

$$\tilde{\kappa_k}((g_x)_{x \in X}; h)(\otimes_{x \in X} v_x) = \otimes_{x \in X} \chi_{h^{-1}x}(g_x) v_{h^{-1}x}$$

Then, if k has the h-orbit property then it immediately has the h^{-1}-h-orbit property, as well, and so $h^{-1}(x) = x$. Thus we can choose the trivial extension so that

$$\tilde{\kappa_k}((g_x)_{x\in X}; h) = \kappa_k((g_x)_{x\in X}) \quad \text{for all } h \in T_H(\kappa_k).$$

Next, the irreps of $H = \mathbb{Z}_p^d$ are of the form $\rho_\ell(a) = \omega_p^{\ell\cdot a}, a, \ell \in \mathbb{Z}_p^d$, and there are p^d such irreps.

To determine $\widehat{T_H(\kappa_k)}$ consider the set of generators $T = \{h^i : 0 \leqslant i < f, h \in T_H(\kappa_k)\}, |T| = f \leqslant d$ where $f = d$ implies that $T_H(\kappa_k) = H$. Then, any $b \in T_H(\kappa_k)$ can be written as $b = \sum_{i=0}^f a_i h^i$ where $0 \leqslant a_i < p$. Thus, for $\rho_\ell \in \widehat{H}$,

$$\begin{aligned}\rho_\ell(b) = \rho_\ell(\sum_{i=0}^f a_i h^i) &= \omega_p^{\ell\cdot\sum_{i=0}^f a_i h^i} \\ &= \prod_{i=0}^f (\omega_p^{\ell\cdot h^i})^{a_i} \\ &= \prod_{i=0}^f \rho_\ell(h^i)^{a_i}\end{aligned}$$

Notice the redundancy of ℓ when $T_H(\kappa_k) \neq H$, which occurs due to the dot product relying on multiplication. Thus, one can limit the choice of ℓ to the p^f elements in $T_H(\kappa_k)$. That is, $\widehat{T_H(\kappa_k)} = \{\rho_\ell : \ell \in \mathbb{Z}_p^f\}$. As an aside, note that the indices when $h_x^i = 0$ do not contribute to the sum and could be "removed"; this is what allows for the isomorphism to be stated (that is, that $T_H(\kappa_k) \cong \mathbb{Z}_p^f, f \leqslant d$).

Then, we get the set

$$\widehat{T_H(\kappa_k)} = \{\omega_p^j : j \in T_H(\kappa_k)\}$$

The inflation of any irrep $\eta_j \in \widehat{T_H(\kappa_k)}$ can be defined simply as

$$\bar{\eta_j}(b; h) = \eta_j(h)$$

Finally, the tensor product of an irrep $\bar{\kappa_k} \in \widehat{G^X}, \bar{\eta_j} \in \widehat{T_H(\kappa_k)}$ is given by

$$\bar{\kappa_k} \otimes \bar{\eta_j}(b; \sum_{i=0}^f a_i h^i) = \kappa_k(b)\eta_j(\sum_{i=0}^f a_i h^i) = \omega_p^{k\cdot b + \sum_{i=0}^f a_i j\cdot h^i)}$$

Now, consider inducing $\bar{\kappa_k} \otimes \bar{\eta_j}$ which acts on the vector space $V = \mathbb{C}$, since it is one-dimensional, to an irrep of $\widehat{G \wr H}$.

To determine the coset representatives, consider $(G \wr H)/I_{G\wr H}(\sigma) \cong H/T_H(\sigma)$ with coset representatives $D = \{0, h : h \notin \langle T\rangle\}$. That is, suppose $t \in T_H(\kappa_k)$ is of the form $t = (0_i)_{f\leqslant i<d}(h_i)_{0\leqslant i<f}$ so that one can write any $h \in H$ as $h = t + c$ for some $c = (c_i)_{f\leqslant i<d}(0)_{0\leqslant i<f} \in D$ and so the cosets of the quotient group are $c\langle T\rangle$ for $c \notin \langle T\rangle$.

Then, let $(g;h') = (g;h+b) \in G \wr H, h = \sum_{i=0}^{f}(a_i h^i), b \notin T_H(\kappa_k)$ and consider its action on $v \in V$. One can calculate the following:

$$\begin{aligned}
(g;h')\sum_{c\in D}(0;c)\otimes v &= \sum_{c\in D}(\psi_c(g);h'+c)\otimes v \\
&= \sum_{c\in D}(0;c+b)(\psi_c(g);h)\otimes v \\
&= \sum_{c\in D}(0;c+b)\otimes(\overline{\kappa_k}\otimes\overline{\eta_j})((\psi_c(g);h))v \\
&= \sum_{c\in D}(0;c+b)\otimes(\kappa_k(\psi_c(g))\otimes\eta_j(h))v \\
&= \sum_{c\in D}(0;c+b)\otimes\omega_p^{k\cdot\psi_c(g)+\sum_{i=0}^{f}a_i j\cdot h^i)}v
\end{aligned}$$

Thus, the final, induced representation, denoted $\sigma_{k,j}$ is given by

$$\sigma_{k,j}(g;h') = \sum_{c\in D}\omega_p^{k\cdot\psi_c(g)+\sum_{i=0}^{f}a_i j\cdot h^i)}|c+b\rangle\langle c|$$

with dimension p^{d-f}. We thus get the following corollary:

Corollary 3.3.2.0.1. *Suppose $k=(i,i,...,i), i\in G$ is a label of an irrep of G^X so that $\kappa_k \in \widehat{G^X}$. There are $|G|=p^n$ choices of such irreps, and each give $T_H(\kappa_k)=\mathbb{Z}_p^d$. Thus these irreps induce to the 1-dimensional irreps of P. Since the orbit of each such k is k there are p^n such labels. For each there are $|H|=p^d$ choices for the label of η_j and thus a total of p^{n+d} one dimensional irreps.*

Notice that for a given $k=(k_x)_{x\in X}, k_x \in G$, if we associate it to $\tilde{k}=(k;0)\in P$, then there is a direct correspondence between the values of $h\in H$ for which $\tilde{k}$ has the h-orbit property and the values of $h\in T_H(\kappa_k)$ since if $\tilde{k}$ has the h-orbit property then $k_x = k_{x+h}$ for all $x\in X$ and so h is in the isotropy group of κ_k.

Consider the elements of G^X which are fixed by a specific $h\in H$ and labels $k=(k_x)_{x\in X}, k_x\in G$ associated with $\tilde{k}=(k;0)\in P$. To determine each $T_H(\kappa_k)$ one must understand the values of $h\in H$ for which $(\psi_h(k);0)=(k;0)$; that is, values of $h\in H$ which fix an element in G^X. Similarly, Γ is the set of representatives of the orbits of elements in $\widehat{G^X}$ with unique orbits; that is, for each label k,k' such that $k'=(k_{x+h})_{x\in X}$ for some $h\in H$ one only requires a single representative k for the orbit.

Note the following observation:

1. If $h=(0)$ then it fixes all p^d elements in X and p^{np^d} elements in G^X.
2. If $h'\in\langle h\rangle$ then it fixes the same elements as h and thus elements being acted on by h,h' have the same orbit.
3. If an element is in the diagonal subgroup of G^X then it is fixed by every $h\in H$ and thus has an orbit of one.

4. Any $h \in H$ fixes at least $p^{np^{d-1}}$ elements.

Then, by Burnside's lemma we have that $|\Gamma| = \frac{1}{|H|}\sum_{h\in H}|Fix(h)|$ and so

$$\frac{1}{p^d}(p^{np^d} + (p^d - 1)p^{np^{d-1}}) \leqslant |\Gamma| \leqslant p^{np^d}$$

In order to understand Γ and understand the number of irreps of a certain dimension, one must understand the what elements k associated with $\tilde{k} \in G^X$ a given element $h \in H$ fixes.

Example 3.3.2.0.1. Suppose $p = 3$ and $h = (0)_{1\leqslant j<d}1$ so that it generates the subgroup $\langle h\rangle = (0)_{1\leqslant j<d}b \cong \mathbb{Z}_3, b \in \mathbb{Z}_p$. Then, $\langle h\rangle$ fixes all elements of the form $k = (k_a k_a k_a)_{0\leqslant a<3^{d-1}}, k_a \in G$.

For example, if $d = 2$ this corresponds to $k = (aaa, bbb, ccc)$ for $a, b, c \in G$.

There are $|G|^{3^{d-1}} = 3^{n3^{d-1}}$ such elements. 3^n of these elements are in the center and thus their isotropy group is all of H instead. There are additional elements of this form which are fixed by other elements $h \in H$ as well. This will be addressed more later.

Example 3.3.2.0.2. Consider when $p = 3$ and $h = (0)_{2\leqslant j<d}10$ so that $\langle h\rangle \cong \mathbb{Z}_3$. Then, this subgroup fixes all elements of the form $k = (k_A k_A k_A)_{0\leqslant A<3^{d-2}}, k_A \in G^3$. For example, if $d = 2$ this includes $k = (abc, abc, abc)$.

There are $|G|^{3^{d-2}} = 3^{n3^{d-2}}$ such elements, of which 3^n are in the center and will thus have a different isotropy group. As before, there are additional elements of this form which are fixed by other elements $h \in H$ as well.

As demonstrated in the examples above, if an element k is stabilized by a subgroup of H of order p^j, then there exists some smaller subgroup of order p^{j-1} by which it is is also stabilized, for $1 \leqslant j \leqslant d$. Thus, one must be careful to avoid double-counting, and thus it is beneficial to begin by considering the elements stabilized by the largest subgroups of H and decreasing. That is, begin with subgroups of size p^d of H which have d generators and examine what happens as the number of generators decreases. From before we already know that there are p^n elements k stabilized by all elements $h \in H$; thus these have an isotropy subgroup of order p^d.

Note that the number of subgroups of H of order p^j is given by the number of j-dimensional subspaces of a $d-$dimensional vector space over $\mathbb{Z}_p$. The group H can be associated with the vector space $\mathbb{Z}_p^d$. Then, the Gaussian binomial coefficient can be used to enumerate the j-dimensional subspaces of this vector space:

$$\binom{d}{j}_p = \prod_{f=0}^{j-1}\frac{p^{d-f}-1}{p^{j-f}-1}$$

Thus, if $j = d - 1$ then this gives $\binom{d}{j-1}_p$ subspaces in total. For each subgroup associated to a subspace of this dimension there are $p^{d-j} = p$ cosets in H on which a representation is constant, giving $|G|^p = p^{np}$ elements k fixed by such a subgroup. However, there are p^n elements which are fixed by a larger isotropy

group, namely the whole group. Thus there is a total of $\binom{d}{j-1}_p p^{pn} - p^n$ labels fixed by a subgroup of H associated with a $d-1$-dimensional subspace. Each label has an orbit of $p^{d-j} = p$ and isotropy group of order p^{d-1}. Thus there are a total of $\binom{d}{j-1}_p p^{pn-1} - p^{n-1}$ elements which will induce to a p-dimensional irrep in Γ.

For each irrep $\kappa_k \in \Gamma$ with a stabilizer of order p^{d-1} there are p^{d-1} choices for $\eta_\ell \in |T_H(\kappa_k)|$, resulting in a total of $\binom{d}{j-1}_p p^{pn+d-2} - p^{n+d-2}$ induced representations of dimension p.

This continues in general, as summarized in the following proposition:

Proposition 3.3.2.0.1. *Suppose $P = \mathbb{Z}_p^n \wr \mathbb{Z}_p^d = G \wr H$. Then, for $0 \leqslant j \leqslant d$ there are $\binom{d}{j}_p$ j-dimensional subspaces of $\mathbb{Z}_p^d$ corresponding to subgroups of H with order p^j, with each element having an orbit of size p^{d-j}.*

Then, for $0 \leqslant j \leqslant d$ there is a total of

$$p^{j-d}\left(\binom{d}{j}_p p^{np^{d-j}} - \binom{d}{j+1}_p p^{np^{d-j-1}}\right)$$

labels k which correspond to elements κ_k in Γ, where $\binom{d}{j}_p = 0$ if $j \geqslant d$. Associated to each is an isotropy group of size p^j and thus there is a total of

$$p^{2j-d}\left(\binom{d}{j}_p p^{np^{d-j}} - \binom{d}{j+1}_p p^{np^{d-j-1}}\right)$$

representations of P of dimension p^{d-j}.

Proof. Before proving the above inductively, consider two "sanity checks". First, we require that the total number of labels k sum to $|G^X| = p^{p^d n}$. That is,

$$\begin{aligned}\sum_{j=0}^{d}\left(\binom{d}{j}_p p^{np^{d-j}} - \binom{d}{j+1}_p p^{np^{d-j-1}}\right) &= \binom{d}{0}_p p^{np^d} - \sum_{j=1}^{d}\left(\binom{d}{j+1}_p p^{np^{d-j-1}} - \binom{d}{j+1}_p p^{np^{d-j-1}}\right)\\ &= p^{np^d}\end{aligned}$$

Similarly, the irreps must satisfy the equation $\sum_{\rho\in\widehat{P}} d_\rho^2 = |P|$ where d_ρ is the dimension of each irrep ρ. Then,

$$\begin{aligned}\sum_{j=0}^{d}((p^{d-j})^2(p^{2j-d}\left(\binom{d}{j}_p p^{np^{d-j}} - \binom{d}{j+1}_p p^{np^{d-j-1}}\right)) &= p^d \sum_{j=0}^{d}\left(\binom{d}{j}_p p^{np^{d-j}} - \binom{d}{j+1}_p p^{np^{d-j-1}}\right)\\ &= p^d(p^{np^d}) = p^{np^d+d}\end{aligned}$$

Now, use induction on j and thus the dimension of the irrep to formally proof the relation. In the discussion above the proposition, the relation has been shown to hold for the case when $j = d$ and $j = d-1$. Suppose it holds when $j = d-k$ and consider $i = j-1 = d-k-1$.

Then, we are considering a subgroup of H of order p^i with i generators. Consider $h \in H$, one of the n generators of this subgroup. Then, the label k is stabilized by h if k has the h-orbit property. There are thus $|G|$ choices for each triple above, and $d-1$ such triples. This means that any single generator stabilizes $|G|^{p^{d-1}}$ elements, and i generators result in p^{i-1} such triples to consider. More precisely, the $p^{d-i} = p^{k+1}$ cosets of H must be considered, which then results in $|G|^{p^{d-i}} = p^{np^{d-i}}$ elements k stabilized by such a subspace.

Since there are $\binom{d}{i}_p$ such subspaces there is a total of $\binom{d}{i}_p p^{np^{d-i}}$ elements fixed by such a subgroup.

Now, by the inductive hypothesis, we know that there are $\binom{d}{j}_p p^{np^{d-j}} - \binom{d}{j+1}_p p^{np^{d-j-1}}$ labels k which are stabilized by a subspace of size $j, d \geqslant j > i$, and thus $\binom{d}{j}_p p^{np^{d-j}}$ stabilized by a subspace of size greater than or equal to j. Thus, if we let $j = i+1$, this gives the number of elements stabilized by a subspace greater than i, and thus $\binom{d}{i}_p p^{np^{d-i}} - \binom{d}{i+1}_p p^{np^{d-i-1}}$ gives the number of elements stabilized by a subgroup with i generators.

However, prior to inducing any such representation, one must consider the size of the orbit of each label k. Since the order of its stabilizer is p^i it follows that its orbit is p^{d-i}. Thus, the number of labels of irreps in Γ is $p^{i-d}(\binom{d}{i}_p p^{np^{d-i}} - \binom{d}{i+1}_p p^{np^{d-i-1}})$.

Finally, there are p^i choices of irreps of the isotropy group for each choice of irrep of the base group. This results in a total of $p^{2i-d}(\binom{d}{i}_p p^{np^{d-i}} - \binom{d}{i+1}_p p^{np^{d-i-1}})$ irreps of dimension p^{d-i}, as expected. □

As a proof of concept consider the following example:

Example 3.3.2.0.3. Suppose $d = 3$ so that $|P| = p^{np^p+p}$. Then, there are p^n labels k which induce to a total of p^{n+p} one-dimensional representations of P. Clearly, $\binom{p}{p}_p = 1$ and $p^{p-p}(p^n) = p^n$ corresponds to the number of elements κ_k in Γ. As well, $p^d p^n = p^{n+d}$ and thus the equations in Prop. 3.3.2.0.1 are satisfied.

Then, for $j = d-1 = 2$, according to the proposition there are

$$\begin{aligned} p^{-1}(\frac{(p^3-1)(p^2-1)}{(p^2-1)(p-1)}p^{np} - p^n) &= p^{-1}(\frac{(p^3-1)}{(p-1)}p^{pn} - p^n) \\ &= p^{-1}((p^2+p+1)p^{pn} - p^n) \\ &= p^{pn+1} + p^{pn} + p^{pn-1} - p^{n-1} \end{aligned}$$

labels fixed by a two-dimensional subspace resulting in a total of

$$p^{pn+3} + p^{pn+2} + p^{pn+1} - p^{n+1}$$

irreps of dimension p.

For $j = d - 2 = 1$ there are

$$\begin{aligned} p^{-2}(\frac{(p^3-1)}{(p-1)}p^{np^2} - \frac{(p^3-1)}{(p-1)}p^{np}) &= \frac{(p^3-1)}{(p-1)}p^{-2}(p^{p^2n} - p^{np}) \\ &= p^{-2}(p^2+p+1)(p^{p^2n} - p^{np}) \\ &= p^{p^2n} + p^{p^2n-1} + p^{p^2n-2} - p^{np} - p^{np-1} - p^{np-2} \\ &= (1+p^{-1}+p^{-2})(p^{p^2n} - p^{np}) \geqslant p^{p^2n} - p^{np} \end{aligned}$$

labels resulting in a total of

$$(p + 1 + p^{-1})(p^{p^2n} - p^{np})$$

irreps of dimension p^2.

Finally, for $j = 0$ there are

$$\begin{aligned} p^{-3}(p^{np^3} - \frac{(p^3-1)}{(p-1)}p^{np^2}) &= p^{-3}(p^{np^3} - (p^2+p+1)p^{np^2}) \\ &= p^{np^3-3} - p^{np^2-1} - p^{np^2-2} - p^{np^2-3} \end{aligned}$$

labels and thus a total of

$$p^{np^3-3} - p^{np^2-1} - p^{np^2-2} - p^{np^2-3}$$

irreps of dimension p^3.

Notice that when p is very large the subtracted terms are almost negligible. That is, with high probability one will obtain a p^3-dimensional irrep.

Now, a Gaussian coefficient $\binom{d}{j}_p$ yields, in fact, a polynomial of degree $j(d-j)$ of the form $\sum_{i=0}^{j(d-j)} a_i p^i$ where $a_i = a_{j(d-j)-i}$ [**?**].

Then, there will be

$$\begin{aligned} p^{2j-d}(\mathcal{O}(p^{j(d-j)})p^{np^{d-j}} - \mathcal{O}(p^{(j+1)(d-j-1)})p^{np^{d-j-1}}) &= \mathcal{O}(p^{j(d-j)+np^{d-j}+2j-d} - p^{(j+1)(d-j-1)+np^{d-j-1}+2j-d}) \\ &= \mathcal{O}(p^{j(d-j+2)+np^{d-j}-d}) \end{aligned}$$

representations of dimension p^{d-j}. This proves the following corollary:

Corollary 3.3.2.0.2. *The number of irreps of dimension p^{d-j} is in $\mathcal{O}(p^{j(d-j+2)+np^{d-j}-d})$.*

Thus, as p tends to infinity the probability of observing a p^d is significantly greater than the probability of observing any other representation of dimension p^{d-i} where $i > 0$.

3.3.3 Introduction to the HSP in $\mathbb{Z}_p^n \wr \mathbb{Z}_p^d$

Recall the methodology of [2], as discussed in Section 2.2.3, as well as [17], discussed in Section 2.3. The goal of this section is to apply similar methodology to solving the HSP in $P = \mathbb{Z}_p^n \wr \mathbb{Z}_p^d$.

Begin by only considering the cyclic subgroups

$$A_{g,h} = \langle (g;h) \rangle = \{((k\sum_{i=0}^{p-1} g_{x+ih} + \sum_{i=0}^{c-1} g_{x+ih})_{x\in X}; th) : t = pk + c \in \mathbb{Z}_{p^2}\}$$

where $g = (g_x)_{x\in X}, g_x \in G, h = (h_k)_{0\leqslant k<d}$ and which has conjugate subgroups of the form

$$A_{g',h} = \langle (g';h) \rangle \text{ where } g_{x+k} - g'_x = \gamma_{x+h} - \gamma_x$$

for some $(\gamma; k) \in P$ and for all $x \in X$. Of course, this condition implies that $\sum_{i=0}^{p-1} g_{x+k+ih} = \sum_{i=0}^{p-1} g'_{x+ih}$ for all $x \in X$.

Claim 3.3.3.0.1. *Suppose $k = (i, ..., i), i \in G$ so that κ_k induces to a one-dimensional irrep $\chi_{k,j}$ for every $j \in H$. There are p^n choices for k and thus p^{n+d} for $\chi_{k,j}$. Then, for an element $(g; h) \in P$,*

$$\chi_{k,j}(g;h) = \omega_p^{i\cdot\sum_{x\in X} g_x + j\cdot h} = 1$$

if

1. *$i = 0$ and $j = 0$, giving p^d choices for h and p^{np^d} for g*
2. *$\sum_{x\in X} g_x = 0$ and $j = 0$, giving p^d choices for h and p^n for k*
3. *$\sum_{x\in X} g_x = 0$ and $h = 0$, giving p^d choices for j and for a fixed k*
4. *$\sum_{x\in X} g_x = 0$ and $h \neq 0$ and so is orthogonal to a $d-1$-dimensional subspace, giving $p^{d-1}+1$ choices for j for a fixed k*
5. *$\sum_{x\in X} g_x$ is one of the $p^{n-1}+1$ elements in G which are in the the $n-1$-dimensional orthogonal subspace of i and either $h = 0$, $j = 0$, or h is orthogonal to j, giving $p^{d-1}+1$ choices for j for a fixed h (or vice versa)*
6. *$j = ah$ for some $a = 1, 2$ and $i \cdot \sum_{x\in X} g_x \neq 0$ and thus $(i, j) \cdot (\sum_{x\in X} g_x, h) = 0$.*

Proof. Notice that $\sum_{x\in X} g_x \in \mathbb{Z}_p^n$. If this equals zero there are $|G| = p^n$ choices for i and $j \cdot h = 0$. If $h = 0$ then there are $|H| = p^d$ choices for j. Otherwise h generates a one-dimensional subspace and is thus orthogonal to a $d-1$-dimensional one. Thus, there are $p^{d-1}+1$ choices for j.

Otherwise, suppose $\sum_{x\in X} g_x \neq 0$. If $i = 0$ then there are yet again p^d choices for j if $h = 0$, otherwise there are $p^{d-1}+1$ choices for j. Otherwise, if $i\cdot\sum_{x\in X} g_x = \gamma \neq 0$ then $j \cdot h = -\gamma$ implies that $j = ah + h', h' \notin \langle h \rangle$. This gives p^d choices for j. □

Theorem 3.3.3.0.1. *Suppose $A_{g,h} = \langle (g;h) \rangle$ is the hidden subgroup. Then, the probability that one observes any p^{d-j}-dimensional irrep $\sigma^{(p^{d-j})}$ is*

$$P(\sigma^{(p^{d-j})}(A_{g,h})) \geqslant \frac{|A_{g,h}|}{p^{np^d+3d-2j}}(p^{j-p+2} + p^d - p^j)(\binom{d}{j}_p p^{np^{d-j}} - \binom{d}{j+1}_p p^{np^{d-j-1}})$$

where as p tends to infinity this tends to equality.

Proof. Note that when considering a cyclic subgroup it is sufficient to consider the behavior of the character on the generator. The following calculates the probability of measuring a one-dimensional irrep $\chi_{k,j}$:

$$\begin{aligned}
p(\chi_{k,j}) &= \frac{|A_{g,h}|}{|P|} \sum_{(a;b)\in A_{g,h}} \chi_{k,j}((a;b)) \\
&= \frac{|A_{g,h}|}{p^{np^d+d}} \sum_{0\leqslant pf+t<|A_{g,h}|} \omega_p^{it\sum_{x\in X} g_x + tj\cdot h} \\
&= \begin{cases} \frac{p^2}{p^{np^d+d}} \sum_{l=0}^{p-1} \omega_p^{li\sum_{x\in X} g_x + lj\cdot h} & \text{if } |A_{g,h}| = p^2 \\ \frac{p}{p^{np^d+d}} \sum_{l=0}^{p-1} \omega_p^{li\sum_{x\in X} g_x + lj\cdot h} & \text{if } |A_{g,h}| = p \end{cases} \\
&= \begin{cases} \frac{1}{p^{np^d-3+d}} \text{ if } |A_{g,h}| = p^2 \text{ and } i\cdot\sum_{x\in X} g_x + j\cdot h = 0 \\ \frac{1}{p^{np^d-2+d}} \text{ if } |A_{g,h}| = p \text{ and } i\cdot\sum_{x\in X} g_x + j\cdot h = 0 \\ 0 \text{ otherwise} \end{cases}
\end{aligned}$$

Thus, using the claim and calculations above, for a fixed g, h where $h, \sum_{x\in X} g_x \neq 0$ there are $p^{d-1} + p^{n+d}$ choices of k, j that result in 0. If $\sum_{x\in X} g_x = 0$ then there are $p^d(p^{d-1}+1)$ choices.

Note that if $|A_{g,h}| = p$ then we require that $\sum_{x\in X} g_x = 0$. If $h = 0$ then there are p^{n+d} choices for the labels k, j, otherwise there are $p^n(p^{d-1}+1)$ choices. Note that $h = 0$ if and only if $|A_{g,0}| = p$ and $\sum_{x\in X} g_x = 0$.

This gives that the probability of observing any one-dimensional irrep is

$$P(\chi) = \begin{cases} \frac{1+p^{n+1}}{p^{np^d-2}} \text{ if } |A_{g,h}| = p^2, \sum_{x\in X} g_x \neq 0 \\ \frac{1+p^{d-1}}{p^{np^d-p}} \text{ if } |A_{g,h}| = p^2, \sum_{x\in X} g_x = 0 \\ \frac{1}{p^{n(p^d-1)-2}} \text{ if } |A_{g,h}| = p, h \neq 0 \\ \frac{1+p^{d-1}}{p^{n(p^d-1)-2+d}} \text{ if } |A_{g,h}| = p, h = 0 \end{cases}$$

Let $\sigma_{k,j}^{(p^i)}$ denote a p^i-dimensional irrep and consider $\sigma_{k,j}^{(p)}$. There are $p^{d-2}(\binom{d}{d-1}_p p^{np} - \binom{d}{d}_p p^n) = p^{d-2}(\binom{d}{j}_p p^{np} - p^n)$ such irreps. Consider the probability of observing such an irrep. Suppose D is the set of coset representatives of $H/T_H(\kappa_k)$ with $|D| = p$ and let $h = \sum_{i=0}^{d-1} a_i t^i + r$ where $r \in D, t^i \in T_H(\kappa_k)$. Then:

$$\begin{aligned}
P(\sigma_{k,j}^{(p)}) &= \frac{|A_{g,h}|}{|P|} Tr\Big(\sum_{(a;b)\in A_{g,h}} \sigma_{k,j}^{(p)}((a;b))\Big) \\
&= \frac{|A_{g,h}|}{p^{np^d+d}} Tr\Big(\sum_{c\in D} \sum_{0<f\leqslant|A_{g,h}|} \omega_p^{k\cdot\psi_c(\sum_{u=0}^{f-1}\psi_{uh}(g)) + f\sum_{i=0}^{d-1} a_i j\cdot t^i} |c+fr\rangle\langle c|\Big)
\end{aligned}$$

The trace of the above matrix is given when $c + fr = c$ and so $fr = 0 \ mod\ p$. Thus, either $r = 0$ and thus $h = \sum_{i=0}^{d-1} a_i t^i \in T_H(\kappa_k)$ or $f = 0 \ mod\ p$.

Case 1: $r = 0$

$$
\begin{aligned}
P(\sigma^{(p)}_{k,j}(A_{g,h})) &= \frac{|A_{g,h}|}{p^{np^d+d}} Tr(\sum_{c\in D}\sum_{0<f\leqslant|A_{g,h}|} \omega_p^{k\cdot\psi_c(\sum_{u=0}^{f-1}\psi_{uh}(g))+f\sum_{i=0}^{d-1}a_ij\cdot t^i)}|c\rangle\langle c|) \\
&= \frac{|A_{g,h}|}{p^{np^d+d}} \sum_{c\in D}\sum_{0<f\leqslant|A_{g,h}|} \omega_p^{k\cdot\psi_c(\sum_{u=0}^{f-1}\psi_{uh}(g))+f\sum_{i=0}^{d-1}a_ij\cdot t^i)} \\
&= \frac{|A_{g,h}|}{p^{np^d+d}} \sum_{c\in D}(\sum_{l=0}^{p-1}\omega_p^{lk\cdot\sum_{i=0}^{p-1}\psi_{c+ih}(g)})(\sum_{l=0}^{p-1}\omega_p^{k\cdot\psi_c(\sum_{\ell=0}^{l}\psi_{\ell h}(g))+\sum_{i=0}^{d-1}a_ij\cdot t^i}) \\
&= \begin{cases} \frac{|A_{g,h}|}{p^{np^d+d-2}} \text{ if } \sum_{i=0}^{p-1}\psi_{c+ih}(g)=0, k\cdot\psi_c(\sum_{\ell=0}^{l}\psi_{\ell h}(g))+\sum_{i=0}^{d-1}a_ij\cdot t^i=0 \text{ for each } 0\leqslant l<p \\ 0 \text{ else} \end{cases}
\end{aligned}
$$

where at * the fact that f is of the form $pl+i$

We require that $k\cdot\sum_{i=0}^{p-1}\psi_{c+ih}(g)=0$. If $h\in T_H(\kappa_k)$ then this is always true, since $\sum_{i=0}^{p-1}\psi_{c+ih}(g) = p\psi_c(g)=0$. Otherwise, $\sum_{i=0}^{p-1}\psi_{c+ih}(g)$ must be orthogonal to k. Since $dim(span(k))=1$ there are $p^{n-1}+1$ such vectors. Thus, for a fixed k,j we have that

$$
\begin{aligned}
P(\sigma^{(p)}_{k,j}(A_{g,h})) &= (\frac{|A_{g,h}|}{p^{np^d+d-2}})(\frac{|T_H(\kappa_k)|}{|H|}+\frac{p^{n-1}+1}{p^n}) \\
&= |A_{g,h}|\frac{p^{d-1}(p^{n-1}+1)}{p^{n(p^d+1)+2d-2}}
\end{aligned}
$$

Finally, consider $\sigma^{(p^{d-j})}_{k,j}$; that is, a p^{d-j}-dimensional irrep corresponding to an isotropy group of order p^j which is associated to a j-dimensional vector space. There are $p^{2j-d}(\binom{d}{j}_p p^{np^{d-j}} - \binom{d}{j+1}_p p^{np^{d-j-1}})$ such irreps.

Let $((g;h)=(g;h'+b)\in P, h'=\sum_{i=0}^{j-1}(a_ih^i), b\notin T_H(\kappa_k)$.

Then, any $(a;b)\in A_{g,h}$ can be written as $(a;b)=(g;h)^{pf+t} = ((f\sum_{i=0}^{p-1}g_{x+ih}+\sum_{i=0}^{t-1}g_{x+ih})_{x\in X};th) = ((f\sum_{i=0}^{p-1}g_{x+ih'+ib}+\sum_{i=0}^{t-1}g_{x+ih'+ib})_{x\in X};th'+tb)$ for $0\leqslant t\leqslant p-1$.

Then, the probability of measuring such an irrep over $A_{g,h}$ and assuming $k\neq 0$ (if k = 0 this will be a one-dimensional irrep, discussed above) is given by

$$
\begin{aligned}
P(\sigma^{(p^{d-j})}_{k,\ell}(A_{g,h})) &= \frac{|A_{g,h}|}{|P|}\sum_{(a;b)\in A_{g,h}}\sigma_{k,\ell}((a;b)) \\
&= \frac{|A_{g,h}|}{p^{np^d+d}}\sum_{c\in D}(\sum_{l=0}^{p-1}\omega_p^{lk\cdot\sum_{i=0}^{p-1}\psi_{c+ih}(g)})(\sum_{l=0}^{p-1}\omega_p^{k\cdot\sum_{i=0}^{l-1}\psi_{c+lh}(g)+l\sum_{i=0}^{j-1}a_i\ell\cdot h^i})|c+tb\rangle\langle c| \\
&= \begin{cases} \frac{p^2|A_{g,h}|}{p^{np^d+d}} \text{ if } r=0, k\cdot\sum_{i=0}^{p-1}\psi_{c+ih}(g)=0, k\cdot\sum_{i=0}^{l-1}\psi_{c+ih}(g)+l\ell\cdot h=0\ \forall l\in\mathbb{Z}_p \\ \frac{p|A_{g,h}|}{p^{np^d+d}} \text{ if } r\neq 0 \text{ and } k\cdot\sum_{i=0}^{p-1}\psi_{c+ih}(g) \\ 0 \text{ else} \end{cases}
\end{aligned}
$$

$r = 0$ occurs if $h \in T_H(\kappa_k)$. For a fixed k, since $|T_H(\kappa_k)| = p^j$ this occurs with probability $\frac{p^j}{p^d} = p^{j-d}$. Since $h \in T_H(\kappa_k)$ we get that $\ell \cdot h = 0$ only if $\ell = 0$ or $h = 0$. For a fixed k $\ell = 0$ with probability $\frac{1}{p^j}$. As well, the probability that $h = 0$ given that $r = 0$ is also $\frac{1}{p^j}$; in general though it is $\frac{1}{p^d}$.

Then, $k \cdot \sum_{i=0}^{p-1} \psi_{c+ih}(g) = 0$ if $k, \sum_{i=0}^{p-1} \psi_{c+ih}(g)$ are orthogonal. Since $k \in \mathbb{Z}_p^{p^d n}$ it is orthogonal to $p^{p^d n - 1}$ elements. Thus, $k \cdot \sum_{i=0}^{p-1} \psi_{c+ih}(g) = 0$ with probability $\frac{p^{p^d n - 1}}{p^{p^d n}} = p^{-1}$.

Finally, suppose p_l gives the probabilities that $k \cdot \sum_{i=0}^{l-1} \psi_c(g) + l\ell \cdot h = 0$ for $1 \leqslant l < p$. This corresponds to the probability that $(k, l\ell) \cdot (\sum_{i=0}^{l-1} \psi_c(g), h) = 0$. Since $(k, l\ell)$ yields a one-dimensional vector space in a $p^d np^d n = p^{2d} n^2$-dimensional vector space it will be orthogonal to $p^{p^{2d} n^2 - 1}$ elements. Thus for each l it will be zero with probability $\frac{p^{p^{2d} n^2 - 1}}{p^{p^{2d} n^2}} = p^{-1}$.

Then the overall probability in this case is given by $p(r = 0) \wedge p(k \cdot \sum_{i=0}^{p-1} \psi_{c+ih}(g) = 0) \wedge (p((k \cdot \sum_{i=0}^{l-1} \psi_{c+ih}(g) = 0 \wedge \ell \cdot h = 0) \vee (k \cdot \sum_{i=0}^{p-1} \psi_{c+ih}(g) + l\ell h = 0)))$. That is,

$$\begin{aligned} p^{j-d} p^{-1} \prod_{l=1}^{p-1} (p^{-1} \frac{2}{p^j} + p^{-1}) &= p^{j-d} p^{-1} (\frac{2 + p^j}{p^{j+1}})^{p-1} \\ &= \frac{(2 + p^j)^{p-1}}{p^{p(j+1)+d-2j}} \\ &\geqslant p^{j-d-p} \end{aligned}$$

Case 2: $r \neq 0$ If $f = 0 \ mod \ p$ then we obtain the following equation:

$$\begin{aligned} P(\sigma_{k,j}^{(p)}) &= \frac{|A_{g,h}|}{p^{np^d + d}} (\sum_{c \in D} \omega_p^{k \cdot \psi_c(\sum_{u=0}^{f-1} \psi_{uh}(g))}) \\ &= \frac{|A_{g,h}|}{p^{np^d + d}} \sum_{c \in D} (1 + \omega_p^{k \cdot (\sum_{i=0}^{p-1} \psi_{c+ih}(g)} + \omega_p^{2k \cdot (\sum_{i=0}^{p-1} \psi_{c+ih}(g)} \\ &= \begin{cases} \frac{|A_{g,h}|}{p^{np^d + d - 1}} \text{ if } k \cdot \sum_{i=0}^{p-1} \psi_{c+ih}(g) = 0 \\ 0 \text{ else} \end{cases} \end{aligned}$$

Now, $r \neq 0$ if $h \notin T_H(\kappa_k)$. For a fixed k this occurs with probability $\frac{p^d - p^j}{p^d}$. As before, $k \cdot \sum_{i=0}^{p-1} \psi_{c+ih}(g) = 0$ occurs with probability p^{-1}. This gives an overall probability of $\frac{p^d - p^j}{p^{d+1}}$ for a fixed k.

Thus, for a fixed k, upon which all other terms depend, we get that

$$\begin{aligned} P(\sigma_{k,\ell}^{(p^{d-j})}(A_{g,h})) &= \frac{p^2 |A_{g,h}|}{p^{np^d + d}} \frac{(2 + p^j)^{p-1}}{p^{p(j+1)+d-2j}} + \frac{p|A_{g,h}|}{p^{np^d + d}} \frac{p^d - p^j}{p^{d+1}} \\ &\geqslant \frac{|A_{g,h}|}{p^{np^d + 2d}} (p^{j-p+2} + p^d - p^j) \end{aligned}$$

Since there are $p^{2j-d}(\binom{d}{j}_p p^{np^{d-j}} - \binom{d}{j+1}_p p^{np^{d-j-1}})$ irreps of dimension p^{d-j} we get an overall probability of

$$\begin{aligned} P(\sigma^{(p^{d-j})}(A_{g,h})) &\geqslant \frac{|A_{g,h}|}{p^{np^d+2d}}(p^{j-p+2}+p^d-p^j)p^{2j-d}(\binom{d}{j}_p p^{np^{d-j}} - \binom{d}{j+1}_p p^{np^{d-j-1}}) \\ &= \frac{|A_{g,h}|}{p^{np^d+3d-2j}}(p^{j-p+2}+p^d-p^j)(\binom{d}{j}_p p^{np^{d-j}} - \binom{d}{j+1}_p p^{np^{d-j-1}}) \end{aligned}$$

as required. □

Note that the character of a representation over the trivial group always yields zero and thus over the trivial group:

$$P(\chi) = \frac{1}{p^{np^d-1}}, P(\sigma^{(p^{d-j})}) = \frac{\binom{d}{j}_p p^{np^{d-j}} - \binom{d}{j+1}_p p^{np^{d-j-1}}}{p^{np^d+d-j}}$$

Now, consider the general algorithm in [17]: first, we need to set up two coset states, and perform the QFT over each. After relabelling, perform a CG-transform so that the irreps decompose into one-dimensional representations. After measuring and classical post-processing one can obtain the hidden subgroup.

In order to implement such an algorithm we must understand how the tensor product of two (or potentially more) irreps decompose.

Let $(g;h') = (g;h+b) \in P, h = \sum_{i=0}^{f_1}(a_i h^i), b \notin T_H(\kappa_k)$ and $(w;r') = (f;r+t) \in P, r = \sum_{i=0}^{f_2}(\alpha_i r^i), t \notin T_H(\kappa_\ell)$, with induced representations $\sigma_{k,j}$ with dimension p^{d-f_1} and $\sigma_{\ell,y}$ with dimension p^{d-f_2}, respectively, for $j \in T_H(\kappa_k), y \in T_H(\kappa_\ell)$, and with coset representatives given by the set D_1, D_2, respectively, given by

$$\sigma_{k,j}(g;h') = \sum_{c \in D_1} \omega_p^{k\cdot\psi_c(g)+\sum_{i=0}^{f_1} a_i j\cdot h^i)} |c+b\rangle\langle c|$$

$$\sigma_{\ell,y}(w;r') = \sum_{c' \in D_2} \omega_p^{\ell\cdot\psi_{c'}(w)+\sum_{i=0}^{f_2} a_i y\cdot r^i)} |c'+t\rangle\langle c'|$$

An entangled coset state after the QFT and measurement is given by

$$\begin{aligned} \frac{|A_{g,h}|}{|P|}\sigma_{k,j}(A_{g,h}) \otimes \sigma_{\ell,y}(A_{g,h}) &= \frac{|A_{g,h}|}{p^{np^d+d}} \sum_{(g;h') \in A_{g,h}} \sigma_{k,j}(g;h) \otimes \sum_{(w;r') \in A_{g,h}} \sigma_{\ell,y}(w;r') \\ &= \frac{|A_{g,h}|}{p^{np^d+d}} \sum_{(g;h'),(w;r') \in A_{g,h}} \sum_{c \in D_1} \omega_p^{k\cdot\psi_c(g)+\sum_{i=0}^{f_1} a_i j\cdot h^i)} |c+b\rangle\langle c| \\ &\quad \otimes \sum_{c' \in D_2} \omega_p^{\ell\cdot\psi_{c'}(w)+\sum_{i=0}^{f_2} a_i y\cdot r^i)} |c'+t\rangle\langle c'| \end{aligned}$$

With high probability, the measured irreps will both be p^d-dimensional, and thus $D_1 = D_2 = H$. As well, this implies that the isotropy groups has order 1 so that the only element stabilizing any label k is $0 \in H$.

Thus, denote this representation as $\rho_k := \sigma_{k,0}$ instead. Then,

$$\frac{|A_{g,h}|}{|P|}\rho_k(A_{g,h}) \otimes \rho_\ell(A_{g,h}) = \frac{|A_{g,h}|}{p^{np^d+d}} \sum_{(g;h'),(w;r')\in A_{g,h}} \sum_{c,c'\in H} \omega_p^{k\cdot\psi_c(g)} |c+h'\rangle\langle c| \otimes \omega_p^{\ell\cdot\psi_{c'}(w)} |c'+r'\rangle\langle c'| \tag{3.1}$$

$$= \frac{|A_{g,h}|}{p^{np^d+d}} \sum_{(g;h'),(w;r')\in A_{g,h}} \sum_{c,c'\in H} \omega_p^{k\cdot\psi_c(g)+\ell\cdot\psi_{c'}(w)} |c+h', c'+r'\rangle\langle c, c'| \tag{3.2}$$

and the resulting matrix will be p^{2d}-dimensional. Recall that with the Heisenberg groups, for a p^2-dimensional matrix, resulting from the tensor product of two p-dimensional representations with labels k_1, k_2, one could apply a CG transform to obtain the p^2 distinct one-dimensional irreps (that is, each with multiplicity one) when $k_1 = -k_2$ and p copies of the same p-dimensional irrep otherwise. This was motivated by the fact that if $k_1 = -k_2$ then $k_1 + k_2 = 0$ which was not a valid p-dimensional label, whereas for all other values the resulting sum is a valid label and thus the tensor reduces to the irrep corresponding to that label. Following this line of thought one obtains the following:

Theorem 3.3.3.0.2. *Consider $\rho_k \otimes \rho_\ell$; that is, the tensor product of two p^d-dimensional representations. Let $\gamma = k + \ell$ and suppose γ is a label of $\kappa_\gamma \in \widehat{G^X}$ which induces to a total of p^j representations of dimension p^{d-j} for $0 \leqslant j \leqslant d$.*

Then, each of the p^j irreps occur in the tensor product of the representation with multiplicity p^d.

Proof. Let $B = \{(g;0) : g \in G^X\} \leqslant P$ and begin by considering the restriction $Res_B \rho_k \otimes \rho_\ell$. Then, for any $(g;0) \in B$ we can see that

$$R = Res_B \rho_k \otimes \rho_\ell(g;0) = \sum_{c,c'\in H} \omega_p^{k\cdot\psi_c(g)+\ell\cdot\psi_{c'}(g)} |c, c'\rangle\langle c, c'|$$

With character

$$|H| \sum_{i\in H} \omega_p^{k\cdot\psi_i(g)+\ell\psi_i(g)} = p^d \sum_{i\in H} \omega_p^{(k+\ell)\cdot\psi_i(g)} = \begin{cases} p^{2d} \text{ if } \gamma\cdot\psi_i(g) = 0 \ \forall i \in H \\ 0 \text{ else} \end{cases}$$

Consider the inner product of the character of this restriction with κ_γ, and suppose $p^d \geqslant |T_H(\kappa_\gamma)| = p^f \geqslant 1$.

Then,

$$\begin{aligned}
\langle \kappa_\gamma, \chi(R) \rangle &= \frac{1}{|G^X|} \sum_{g \in G^X} \omega_p^{-\gamma \cdot g} p^d \sum_{i \in H} \omega_p^{\gamma \cdot \psi_i(g)} \\
&= p^{d-np^d} \sum_{g \in G^X} \sum_{i \in H} \omega_p^{-\gamma \cdot g + \gamma \cdot \psi_i(g)} \\
&= p^{d-np^d} \sum_{z \in Z(G^X)} \sum_{g \in G^X/Z(G^X)} \sum_{i \in T_H(\kappa_\gamma)} \sum_{c \in H/T_H(\kappa_\gamma)} \omega_p^{-\gamma \cdot (z+g) + \gamma \cdot \psi_{i+c}(z+g)} \\
&= p^{d-np^d} p^n \sum_{g \in G^X/Z(G^X)} \sum_{i \in T_H(\kappa_\gamma)} \sum_{c \in H/T_H(\kappa_\gamma)} \omega_p^{-\gamma \cdot (g) + \gamma \cdot \psi_{i+c}(g)} \\
&= p^{d+n-np^d} \sum_{g \in G^X/Z(G^X)} p^f \sum_{c \in H/T_H(\kappa_\gamma)} \omega_p^{-\gamma \cdot (g) + \gamma \cdot \psi_c(g)} \\
&= p^{d+n-np^d} p^{f+np^d-n} \sum_{g \in G^X/Z(G^X)} \sum_{c \in H/T_H(\kappa_\gamma)} \omega_p^{-\gamma \cdot (g) + \gamma \cdot \psi_c(g)} \\
&= p^{d+f} \sum_{g \in G^X/Z(G^X)} \sum_{c \in H/T_H(\kappa_\gamma)} \omega_p^{-\gamma \cdot (g) + \gamma \cdot \psi_c(g)} * \\
&= p^{d+f} p^{d-f} \\
&= p^{2d}
\end{aligned}$$

Where the line * is simplified by noting that $\sum_{c \in H/T_H(\kappa_\gamma)} \omega_p^{-\gamma \cdot (g) + \gamma \cdot \psi_c(g)} = p^{d-f}$ if $g = 0$ and 0 otherwise. This gives the multiplicity of κ_γ in R.

Now, we wish to determine the behavior of $\rho_k \otimes \rho_\ell$ when restricted to $I = G^X \rtimes T_H(\kappa_\gamma)$. Suppose $(g; h) \in I$. Then,

$$R' = Res_I \rho_k \otimes \rho_\ell(g; h) = \sum_{c, c' \in H} \omega_p^{k \cdot \psi_c(g) + \ell \cdot \psi_{c'}(g)} |c + h, c' + h\rangle\langle c, c'|$$

with character

$$\chi_{R'}(g; h) = \begin{cases} \chi_R(g; 0) \text{ if } h = 0 \\ 0 \text{ else} \end{cases}$$

Thus, consider any one-dimensional representation $\alpha_{\gamma,j} = \kappa_\gamma \otimes \eta_j$ where $\eta_j \in \widehat{T_H(\kappa_\gamma)}$. There are p^f such representations, and if κ_γ occurs in R with multiplicity m then each $\alpha_{\gamma,j}$ must occur in R' with multiplicity $\frac{m}{p^f}$. However, the size of the induced representation must be accounted for. Thus, by the calculations above, and since the irrep will have dimension p^{d-f}, we see that each $\alpha_{i,j}$ occurs in R' with multiplicity $p^{2d-f}/p^{d-f} = p^d$.

Since

$$\langle \alpha_{\gamma,j}, \chi(R') \rangle = \langle Ind_I^P \alpha_{\gamma,j}, \chi(\rho_k \otimes \rho_\ell) \rangle$$

we have that the multiplicity of each $Ind_I^P \alpha_{\gamma,j}$ in $\rho_k \otimes \rho_\ell$ is p^d.

As a check, notice that since there are p^f irreps of dimension p^{d-f} and each having multiplicity p^d, this has a total count of p^{2d} which is the dimension of $\rho_k \otimes \rho_\ell$. □

Conjecture 3.3.3.0.1. *Using the notation from Theorem 3.3.3.0.2, there is some unitary Clebsh-Gordan transform U_{CG} which transforms $\rho_k \otimes \rho_\ell$ into a tensor of the p^{d-j}-dimensional irreps of P which are obtained by inducing κ_γ. Each of the p^j irreps will occur with multiplicity p^d. More precisely,*

$$U_{CG}^\dagger(\rho_k \otimes \rho_\ell)U_{CG} = I_{p^d} \otimes \oplus_{l \in \widehat{T_H(\kappa_\gamma)}} \sigma_{\gamma,l}^{(p^{d-j})}$$

Remark 3.3.3.0.1. *With high probability the tensor product of two p^d-dimensional irreps will be a tensor product of one p^d-dimensional irrep with multiplicity p^d; that is, γ would correspond to the label of a p^d-dimensional representation. In this case, we begin with a state*

$$\rho_k((g;h)) \otimes \rho_\ell((g;h)) = \sum_{c,c' \in H} \omega_p^{k \cdot \psi_c(g) + \ell \cdot \psi_{c'}(g)} |c+h, c'+h\rangle\langle c, c'|$$

and wish to obtain something of the form

$$\sum_{u \in H} |u\rangle\langle u| \otimes \sum_{d \in H} \omega_p^{\gamma \cdot \psi_d(g)} |d+h\rangle\langle d| = I_{p^d} \otimes \rho_\gamma(g;h)$$

3.3.4 HSP for $\mathbb{Z}_p^n \wr \mathbb{Z}_p^d$: Next Steps

Now that we know that the tensor product of two p^d-dimensional representations decomposes quite nicely into irreps of certain kinds, there are two, similar proposed "next steps" for solving the HSP in this group.

In either case, the first step would be to obtain a correct unitary CG transform which can be *efficiently* implemented on quantum circuits.

Next, one could apply the CG transform to $\rho_k(A_{g,h}) \otimes \rho_\ell(A_{g,h})$ to decompose it into a direct sum of a single p^d-dimensional irrep, analogous to the methodology in [2]. One potential issue with this is that in [2] the group was lower dimensional; the additional orbits and non-transitive action of H on G^X may pose an issue.

Alternatively, one could attempt to utilize the methodology in [17], since perhaps this group is more similar to the one examined there. In this case, there may exist a transform which would allow for a clever "relabelling" of one of the irreps in the tensor product in order to force γ to be the label of an irrep which induces to an irrep of a smaller dimension. Ideally, it would induce to a one-dimensional irrep, so that $\gamma = (i, ..., i), i \in G$, however, any additional symmetry which can be "forced" onto γ would be beneficial. That is, the goal would be to *maximize* the size of $T_H(\kappa_\gamma)$.

Of course, after such a transform is applied, one must measure and post-process the results. In the case that the post-processing is inefficient, perhaps more entangled states would be beneficial.

Finally, it would be useful to better understand the conjugacy classes and subgroup structure of this group in order to better exploit such aspects when solving the HSP. This may help when selecting which subgroups are relevant, what information would be useful to obtain, and what simplifications one may apply. In [17], for example, the fact that there was a nice vector space associated to the group which helped characterize conjugacy classes was exploited heavily in the simplification and post-processing of the quantum state.

3.4 Conclusions and Further Research

Evidently, wreath product groups are quite fascination, and for the specific class of groups studied above, the representation theory seems to imply that the methodology used to solve the HSP in certain extraspecial groups may be exploited for this group as well.

It would be of interest to not only solve the HSP in the groups of the form $P = \mathbb{Z}_p^n \wr \mathbb{Z}_p^d$, but more generally, as well. While P is nilpotent, it is relevant to ask if this is a necessary condition: perhaps the HSP would be efficiently solvable even groups of the form $\mathbb{Z}_n^n \wr \mathbb{Z}_m^d$, which, in general, are not nilpotent.

More general groups would be useful to study as well: what happens in $G \wr H$ when G, H are non-abelian? What about infinite wreath product groups?

Since any Sylow p subgroup of S_{p^n} is isomorphic to an n-time iterated wreath product $\mathbb{Z}_p \wr .... \wr \mathbb{Z}_p$ understanding this group may provide insight into solving the elusive HSP for the symmetric group, and thus valuable information regarding the graph isomorphism problem.

Finally, wreath product groups become increasingly complex and further away from abelian as the chosen base groups become more intricate. There is a hope that if the CG transform successfully solves, or at least simplifies, the HSP in wreath product groups, then similar methodology would be useful for tackling the HSP in other non-abelian group.

Chapter 4

Conclusion

4.1 Summary and Concluding Remarks

Evidently, the HSP is a fascinating problem with many avenues still left to explore. It is a relevant area of research both for its theoretical properties – namely, the relationship between a group, its structure, and its representations – and due to its applications in post-quantum cryptography.

This report aimed to introduce readers to some of the relevant research conducted in this area, and attempt to understand how and in which groups one can utilize the Clebsch-Gordon transform to solve the HSP. This was done by exploring the methodology in [2] and [17] to understand why the techniques were successful in the Heisenberg and Weyl-Heisenberg groups, respectively. Ultimately, one of the main factors was the symmetry of the hidden coset states in these groups across conjugacy classes; that is, the HCSP lent itself to using a Clebsch-Gordon transform, and in these groups the HSP reduces to the HCSP. Furthermore, the nature of the representations of these groups also made this technique successful.

Wreath products of the form $\mathbb{Z}_p^n \wr \mathbb{Z}_p^d$ were then chosen to be analyzed due to their useful group structure: they are nilpotent, have many p^j-dimensional representations, where $0 \leqslant j \leqslant d$, and have a fascinating subgroup structure. In order to simplify the problem at hand, it was assumed that the hidden subgroup is a cyclic subgroup. Unfortunately, the conjugacy classes of such subgroups were not as easy to classify as for the Heisenberg groups, and the enumeration of the representations was also more complex. This means that utilizing the Clebsch-Gordon transform to solve the HSP proved to be more difficult.

Further research in the area includes attempting to solve the HSP using the CG transform in other wreath product groups, including iterated wreath products. Furthermore, better understanding when this transform is useful could aid in determining which groups to employ it in. A recommendation would be to examine other p-groups; nilpotent groups; and groups in which the HSP and HCSP are equivalent.

Bibliography

[1] M. Aschbacher. *Finite group theory*. Cambridge University Press, 2000.

[2] D. Bacon. How a clebsch-gordan transform helps to solve the heisenberg hidden subgroup problem. *arXiv preprint quant-ph/0612107*, 2006.

[3] D. Bacon, A. M. Childs, and W. van Dam. From optimal measurement to efficient quantum algorithms for the hidden subgroup problem over semidirect product groups. In *46th Annual IEEE Symposium on Foundations of Computer Science (FOCS'05)*, pages 469–478. IEEE, 2005.

[4] G. Baumslag. Wreath products and p–groups. *Mathematical Proceedings of the Cambridge Philosophical Society*, 55(3):224–231, 1959.

[5] T. Ceccherini-Silberstein, F. Scarabotti, and F. Tolli. *Representation Theory and Harmonic Analysis of Wreath Products of Finite Groups*. London Mathematical Society Lecture Note Series. Cambridge University Press, 2014.

[6] A. M. Childs and W. Van Dam. Quantum algorithms for algebraic problems. *Reviews of Modern Physics*, 82(1):1, 2010.

[7] D. A. Craven. The theory of p-groups.

[8] R. Curtis. A course in combinatorics (2nd edn), by j. h. van lint and r. m. wilson. pp. 602. £24.95. 2001. isbn 0 521 00601 5 (cambridge university press). *The Mathematical Gazette*, 87(509):399–400, 2003.

[9] J. M. Ettinger, P. Hoyer, and E. Knill. The quantum query complexity of the hidden subgroup problem is polynomial. *Information Processing Letters*, 91:43–48, 07 2004.

[10] S. Hallgren, A. Russell, and A. Ta-shma. The hidden subgroup problem and quantum computation using group representations. *SIAM Journal on Computing*, 32:2003, 2003.

[11] M. S. Im and A. Wu. Generalized iterated wreath products of symmetric groups and generalized rooted trees correspondence. In *Association for Women in Mathematics Research Symposium*, pages 29–46. Springer, 2017.

[12] Y. Inui and F. L. Gall. Efficient quantum algorithms for the hidden subgroup problem over a class of semi-direct product groups. *arXiv preprint quant-ph/0412033*, 2004.

[13] G. Ivanyos, L. Sanselme, and M. Santha. An efficient quantum algorithm for the hidden subgroup problem in extraspecial groups. In *Annual Symposium on Theoretical Aspects of Computer Science*, pages 586–597. Springer, 2007.

[14] G. Ivanyos, L. Sanselme, and M. Santha. An efficient quantum algorithm for the hidden subgroup problem in nil-2 groups. In *Latin American Symposium on Theoretical Informatics*, pages 759–771. Springer, 2008.

[15] D. Kaur. Classification of extraspecial p -groups using quadratic forms. 88:27–38, 06 2020.

[16] H. Kobayashi. Dihedral hidden subgroup problem: A survey. *IPSJ Digital Courier*, 1:470–477, 2005.

[17] H. Krovi and M. Rötteler. An efficient quantum algorithm for the hidden subgroup problem over weyl-heisenberg groups. In *Mathematical Methods in Computer Science*, pages 70–88. Springer, 2008.

[18] G. Kuperberg. A subexponential-time quantum algorithm for the dihedral hidden subgroup problem. *SIAM Journal on Computing*, 35(1):170–188, 2005.

[19] C. Lomont. The hidden subgroup problem – review and open problems. *Cybernet*, Nov 2004.

[20] C. Moore, D. Rockmore, A. Russell, and L. J. Schulman. The power of basis selection in fourier sampling: Hidden subgroup problems in affine groups. In *Proceedings of the Fifteenth Annual ACM-SIAM Symposium on Discrete Algorithms*, SODA '04, page 1113–1122, USA, 2004. Society for Industrial and Applied Mathematics.

[21] C. Moore and A. Russel. For distinguishing conjugate hidden subgroups, the pretty good measurement is as good as it gets. Jan 2005.

[22] C. Moore, A. Russell, and L. Schulman. The symmetric group defies strong fourier sampling. *46th Annual IEEE Symposium on Foundations of Computer Science (FOCS05)*.

[23] R. Orellana, M. Orrison, and D. Rockmore. Rooted trees and iterated wreath products of cyclic groups. *Advances in Applied Mathematics*, 33(3):531–547, 2004.

[24] T. Pham, M. Tait, L. A. Vinh, and R. Won. A structure theorem for product sets in extra special groups. *Journal of Number Theory*, 184:461–472, 2018.

[25] M. Roetteler and T. Beth. Polynomial-time solution to the hidden subgroup problem for a class of non-abelian groups. *arXiv preprint quant-ph/9812070*, 1998.

[26] P. W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pages 124–134, 1994.

[27] B. Steinberg. *Induced Representations*. Springer New York, New York, NY, 2012.