Problem 7: Measuring the space of Metaplectic Whittaker functions

UMN REU
June 2022

Contents

1 Introduction .................................................. 2
  1.1 Motivation ................................................. 2
  1.2 Introducing the cocharacter equations ..................... 3
  1.3 Diagonal numbers .......................................... 4
  1.4 Outline and main results .................................. 5

2 Background on modular arithmetic techniques .................. 6

3 Cocharacter solutions and corollaries .......................... 8
  3.1 Equivalence classes of solutions ......................... 9
  3.2 Characterizing solutions and finding $a$ .................. 10
  3.3 Corollaries of cocharacter solutions formula .............. 12

4 Counting solutions to coroot equations ....................... 14

5 Relating the cocharacter equation to the coroot equations ... 17
  5.1 From coroot to cocharacter ............................... 18
  5.2 Strategy for identifying $\kappa$ and $M$ .................... 21
  5.3 Proof of Lemma 5.3 ..................................... 23
    5.3.1 Case 1: If $\ell \leq m - t$ ......................... 23
    5.3.2 Case 2: If $\ell \geq m - t$ ......................... 24
  5.4 Proof of Lemma 5.4 ..................................... 25
  5.5 Case when $r$ is a product of distinct primes .............. 26

6 Future Work ................................................. 30
1 Introduction

1.1 Motivation

Whittaker functions are special functions that arise in $p$-adic number theory and representation theory, specifically in the study of automorphic forms over local fields and the study of principal series representations of reductive groups. They can be written as integrals over matrix groups, as generating functions over many different combinatorial objects, and in some cases as partition functions of lattice models. In particular, when this last interpretation is true, it gives a connection between the algebraic structures of the space of Whittaker functions and a quantum group module.

One type of Whittaker functions that have been particularly well-studied are metaplectic Whittaker functions, which are Whittaker functions on the principal series representations of metaplectic covering groups.

**Definition.** Given a group $G$ and a natural number $n \in \mathbb{N}$, a $n$-fold metaplectic cover or $n$-fold metaplectic covering group $\tilde{G}$ is a central extension of $G$ by the $n$-th roots of unity $\mu_n$. That is, $\tilde{G}$ is defined by the following short exact sequence:

$$1 \rightarrow \mu_n \rightarrow \tilde{G} \rightarrow G \rightarrow 1.$$  

As a set, $\tilde{G}$ is the set of tuples $(\zeta, g)$ where $\zeta \in \mu_n, g \in G$; however, the group structure has a more complicated multiplication rule than just component-wise multiplication.

These groups are named after the first “Metaplectic Group,” the unique double cover of the symplectic group $Sp_{2n}$ discovered by Weil [6]. In the study of that specific metaplectic cover, it was discovered that general covers of this type inherit much of the interesting representation theory and number theory of their base groups.

One reason for this phenomenon is that if $G$ is a group that is also a topological space, the metaplectic cover is a covering space in the topological sense as well. For example, one such group, which will be the focus of this report, is $G = GL_r(F)$, the general linear group of $r \times r$ matrices over a local field $F$ containing $\mu_{2n}$. In this case, which was first studied by Kazhdan-Patterson [4] and led to a general theory for reductive groups, metaplectic covers have a particularly nice description.

**Theorem 1.1** (Brylinski-Deligne [1], Frechette [3]). Every metaplectic cover of $GL_r(F)$ corresponds to a bilinear form $B_{c,d,r}$ for some $c, d \in \mathbb{Z}$ that acts on $(x, y) \in \mathbb{Z}^r \times \mathbb{Z}^r$ by

$$B_{c,d,r}(x, y) = x^T \cdot \begin{pmatrix} c & d & d & \ldots & d \\ d & c & d & \ldots & d \\ d & d & c & \ldots & d \\ \vdots & \vdots & \ddots & \vdots \\ d & d & d & \ldots & c \end{pmatrix} \cdot y.$$
Principal series representations are a particularly nice class of group representations that can be constructed analogously on both a base group and any of its metaplectic covers. Thus, functions incorporating information from these representations, such as Whittaker functions, which map from $G \to \mathbb{C}$ (or $\tilde{G} \to \mathbb{C}$ in the metaplectic case), behave very similarly in many respects.

However, on the base group $GL_r(F)$, the space of Whittaker functions for any principal series is one-dimensional [2], while on a metaplectic cover, this is no longer true!

**Theorem 1.2** (McNamara [5]). Fix a metaplectic cover $\tilde{G}$ and let $\mathcal{W}$ be the space of metaplectic Whittaker functions for a principal series representation on $\tilde{G}$. Then

$$\dim(\mathcal{W}) = \left| \tilde{T}/H \right|$$

where $\tilde{T}$ is the preimage in $\tilde{G}$ of the group of diagonal matrices $T(F)$ and $H$ is the maximal abelian subgroup of $\tilde{T}$.

Note: the group $T$ of diagonal matrices is denoted $T$ because it is a torus, that is, it is isomorphic to $(F^\times)^r$. It is thus abelian. While we will call $\tilde{T}$ the metaplectic torus, it is no longer abelian, nor is it technically a torus, as its elements look like $(\zeta, t)$ where $\zeta \in \mu_n$ (where $\mu_n \subseteq F$) and $t \in T$.

Examining the explicit structures of the groups $\tilde{T}$ and $H$ for a local field $F$, we can reduce this to a finite computation.

**Theorem 1.3** (McNamara [5], Frechette [3]). For a metaplectic cover $\tilde{G}$ corresponding to $B_{c,d}$

$$\left| \tilde{T}/H \right| = \left| \{ x \in \mathbb{Z}^r : B_{c,d}(x, y) \equiv 0 \pmod{n} \text{ for all } y \in \mathbb{Z}^r \} \right| = \frac{n^r}{|\Lambda_{\text{fin}}|},$$

where $\Lambda_{\text{fin}} = \{ x \in (\mathbb{Z}_n)^r : B_{c,d}(x, y) \equiv 0 \pmod{n} \text{ for all } y \in (\mathbb{Z}_n)^r \}$.

Our goal in this project is to count $|\Lambda_{\text{fin}}|$, which will tell us $\dim(\mathcal{W})$. Counting $|\Lambda_{\text{fin}}|$ is equivalent to counting the number of solutions to the cocharacter equations which we introduce in the following section.

1.2 Introducing the cocharacter equations

It is known that $|\Lambda_{\text{fin}}|$ is equivalent to the number of solutions to a set of equations called the cocharacter equations, which we now define. We let $1_r = (1,1,\ldots,1)^T$ be the $r \times 1$ column vector with all entries equal to 1, and let $0_r = (0,0,\ldots,0)^T$ be the $r \times 1$ column vector with all entries equal to 0. Let $B_{c,d,r}$ be the $r \times r$ matrix for the bilinear form given in Theorem 1.1.

**Definition** (Cocharacter equations). For natural numbers $r, n \geq 2$ and constants $c, d \in \mathbb{Z}_n$, we call the following system of equations the cocharacter equations:

$$B_{c,d,r} x = 0_r \pmod{n}.$$  

Let $S_{\text{cochar}}$ be the number of solutions to the cocharacter equations.
Using Theorem 1.3, we can express elements of $\Lambda_{\text{fin}}$ as solutions to the cocharacter equations. Then Lemma 1.4 follows.

**Lemma 1.4.** The number of solutions to the cocharacter equations is $S_{\text{cochar}} = |\Lambda_{\text{fin}}|$.

### 1.3 Diagonal numbers

Looking at the values of $S_{\text{cochar}}$ for a fixed $r$ and $n$ as we range over $c$ and $d$, certain patterns emerge which motivate defining constants which we call the diagonal numbers. These constants will appear in our formulas for $S_{\text{cochar}}$.

For a fixed $r$ and $n$, one can make a table of the value of $S_{\text{cochar}}(n, r, c, d)$ as we vary $c$ and $d$ in the following way:

<table>
<thead>
<tr>
<th>$d$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>⋮</th>
<th>$(n-1)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$c$</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

We can then assign a number to each diagonal of slope $-1$ based on where it intersects the first row, and each diagonal of slope $r-1$ based on where it intersects the first column. In particular, if a diagonal of slope $-1$ intersects the first row at $d$, assign it the value $d_1 = \gcd(d, n)$, and if a diagonal of slope $r-1$ intersects the first column at $c$, assign it the value $d_2 = \gcd(n, c)$.

**Example.** The table for $S_{\text{cochar}}$ where $n = 10, r = 3$ is shown in Figure 1.3 with diagonal numbers marked.

In this matrix, the value of every entry is determined by the numbers assigned to the two diagonal on which it falls. In particular we get that $S_{\text{cochar}}(10, 3, c, d) = d_1^{r-1}d_2 = d_1^2d_2$.

In general, given a random $n$ and $r$, the value of $S_{\text{cochar}}$ will not depend nearly so simply on $d_1$ and $d_2$, but they still play an important determining role. This motivates the following definition.

**Definition.** Let $d_1 = \gcd(c-d, n)$ be the first diagonal number and define $d_2 = \gcd(c + (r-1)d, n)$ to be the second diagonal number.
\[ d_1 = 10 \]

\[ d_2 = 10 \]

\[
\begin{array}{cccccccc}
1000 & 2 & 8 & 2 & 250 & 8 & 2 & 2 \\
1 & 100 & 5 & 4 & 1 & 4 & 25 & 20 & 1 & 4 \\
8 & 2 & 200 & 2 & 40 & 8 & 50 & 8 & 10 \\
1 & 20 & 1 & 100 & 1 & 4 & 5 & 4 & 25 & 4 \\
8 & 2 & 8 & 10 & 200 & 2 & 8 & 2 & 200 & 2 \\
125 & 4 & 1 & 4 & 1 & 500 & 1 & 4 & 1 & 4 \\
8 & 50 & 40 & 2 & 8 & 2 & 200 & 10 & 8 & 2 \\
1 & 4 & 25 & 4 & 5 & 4 & 1 & 100 & 1 & 20 \\
8 & 10 & 8 & 50 & 8 & 2 & 40 & 2 & 200 & 2 \\
1 & 4 & 1 & 20 & 25 & 4 & 1 & 4 & 5 & 100 \\
\end{array}
\]

\[ d_1 = 2, d_2 = 10 \]
\[ 40 = 2^2 \cdot 10 \]

Figure 1: A table showing \( S_{\text{cochar}}(10, 3, c, d) \) for all \((c, d) \in \mathbb{Z}_{10} \times \mathbb{Z}_{10}\)

### 1.4 Outline and main results

In Section 2 we will review properties of modular arithmetic that we use for later proofs in the paper. In Section 3 we find the total number of solutions to the inhomogenous cocharacter equations, defined as follows:

**Definition.** Let \( A \in \mathbb{Z}_n \), and \( x \in (\mathbb{Z}_n)^r \). Then the following are the inhomogeneous cocharacter equations:

\[
B_{c,d,r}x = A1_r \pmod{n}. \tag{2}
\]

We define \( S_{\text{inhom}} \), the number of solutions to the inhomogenous cocharacter equations, to be the number of choices of \( x \) which satisfy Equation (2) for some value of \( A \).

In Section 3 we also relate \( S_{\text{inhom}} \) to \( S_{\text{cochar}} \) to find the total number of solutions to the cocharacter equations:

**Theorem 1.5.** The number of solutions to the cocharacter equations is

\[
S_{\text{cochar}}(n, r, c, d) = d_1^{r-1} \gcd \left( d_2, \frac{n}{d_1} \gcd(c, d, n) \right). \tag{3}
\]

In Section 4 we find the total number of solutions to the coroot equations, defined as follows.

**Definition.** The following are the coroot equations:

\[
(c + (r - 1)d)(x_1 + \cdots + x_r) \equiv 0 \pmod{n} \quad \text{for all } 1 \leq i \leq r - 1 \tag{3}
\]
\[
(c - d)(x_i - x_r) \equiv 0 \pmod{n}. \tag{4}
\]
The coroot equations describe the metaplectic covers of $SL_r(F)$, whereas cocharacter equations describe metaplectic covers of $GL_r(F)$. In some cases, the coroot and cocharacter equations are equivalent, and in other cases they are closely related. This motivates us to count the solutions to the coroot equations and relate this number to $S_{\text{cochar}}$.

**Theorem 1.6.** The number of solutions to the coroot equations is

$$S_{\text{coroot}}(n, r, c, d) = d^{-1} r \gcd\left(\frac{n}{d}, \frac{n}{r}, r\right).$$

In Section 5, we relate $S_{\text{cochar}}$ to $S_{\text{coroot}}$ by proving the following:

**Theorem 1.7.** The number of solutions to the cocharacter equations can also be defined as

$$S_{\text{cochar}} = S_{\text{coroot}} \cdot \frac{M}{n}$$

where $M = \text{lcm}\left(\gcd(d_2, \frac{dn}{r_1}), \frac{n}{\gcd(n, r)}\right)$ is a factor of $n$ that is described in Section 2.

We will further prove the following formula for $M$.

**Proposition 1.8.** Let $r = p_1^{t_1} p_2^{t_2} \cdots p_j^{t_j}$ and $n = p_1^{m_1} p_2^{m_2} \cdots p_j^{m_j}$. For every $1 \leq i \leq j$, let

$$(c - d) \equiv c_i p_i^{s_i} \pmod{p_i^{m_i}} \quad \text{and} \quad d \equiv d_i p_i^{t_i} \pmod{p_i^{m_i}} \quad \text{for each } 1 \leq i \leq j$$

so that $0 \leq s_i, t_i \leq m_i$. Let $\mu_i = \min(m_i, t_i)$ and $c_i, d_i$ are relatively prime to $p_i$. Then

$$M = \prod_{i=1}^{j} p_i^{\max(m_i - \mu_i, \min(t_i, s_i + m_i - t_i))}.$$

2 Background on modular arithmetic techniques

Here we provide several lemmas that we will use to solve modular equations throughout this document.

**Lemma 2.1.** Suppose $f$ divides $n$ and

$$f\ell = fk \pmod{n}.$$ \hspace{1cm} (5)

Then it is equivalent to state that

$$\ell = k \pmod{\frac{n}{f}}.$$ \hspace{1cm} (6)

If we fix $k$, then Equation (6) has one solution, while Equation (5) has $f$ solutions. In particular, if $\ell = \ell_1$ is a solution to Equation (6), then $\ell = \ell_1 + j \frac{n}{f}$ is a solution to Equation (5) for any $0 \leq j < f$. 

6
The top line of Figure 2 illustrates an example of Equation (5) for some $l$ and $k$, where we have grouped all our numbers into blocks of size $f$. We get the bottom line of Figure 2 by dividing everything in the top line by $f$. This is now an example of Equation (6).

Figure 2: An illustrated example of Lemma 2.1.

Lemma 2.2. Let $b = \gcd(r, n)$. The equation $rx \equiv a \pmod{n}$ has $b$ solutions if $b$ divides $a$, and no solutions otherwise.

Proof. Let $r = sb$. We are counting the solutions to

$$sbx \equiv a \pmod{n}$$

where $s$ and $n$ are relatively prime and $b$ divides $n$.

If $b$ does not divide $a$, then taking Equation (7) modulo $b$ gives us

$$sbx \equiv 0 \not\equiv a \pmod{b}$$

which has no solutions. Therefore, Equation (7) can have no solutions in this case.

Suppose $b$ divides $a$, so that $a = kb$. Then we have

$$sbx \equiv kb \pmod{n}.$$  

By Lemma 2.1, Equation (9) is equivalent to

$$sx \equiv k \pmod{n/b}.$$
The numbers \( s = \frac{r}{b} \) and \( \frac{n}{b} \) must be relatively prime because \( b = \gcd(n, r) \). Therefore, \( s \) is invertible in \( \mathbb{Z}_{\frac{n}{b}} \). We can now rewrite Equation (10) as

\[
\begin{align*}
s^{-1}sx & \equiv s^{-1}k \pmod{\frac{n}{b}} \quad (11) \\
x & \equiv s^{-1}k \pmod{\frac{n}{b}}. \quad (12)
\end{align*}
\]

By Lemma 2.1, Equation (9) therefore has solutions \( x = s^{-1}k + j \frac{n}{b} \) for \( 0 \leq j < b \). This concludes the proof that Equation (7) has \( b \) solutions when \( b \) divides \( a \), and no solutions otherwise.

**Corollary 2.3.** If \( f = \gcd(h, n) \), then the equation \( hx \equiv 0 \pmod{n} \) has the same solutions as \( fx \equiv 0 \pmod{n} \), which is equivalent to \( x \equiv 0 \pmod{\frac{n}{f}} \) and has solutions \( x = j \frac{n}{f} \) for some \( 0 \leq j < f \).

**Proof.** This follows from the special case of the proof of Lemma 2.2 where \( a = 0 \).

**Lemma 2.4.** Let \( s_1, s_2 \in \mathbb{Z}_n \). Then for any \( x_1, x_2 \in \mathbb{Z}_n \), the minimum possible value that \( s_1x_1 + s_2x_2 \pmod{n} \) can have is \( \gcd(s_1, s_2, n) \).

### 3 Cocharacter solutions and corollaries

In this section we will solve for \( S_{\text{cochar}}(n, r, c, d) \). We do so by characterizing the set of solutions to the inhomogenous cocharacter equations and identifying the proportion of solutions with \( A \equiv 0 \). To do this, we will need to identify the smallest nonzero value of \( A \), for which Equation (2) has a solution.

**Definition.** Let \( a(n, r, c, d) \) be the smallest positive integer value for \( A \) such that there is a solution to the inhomogenous cocharacter equations. Note that in most cases a fixed \( n, r, c, d \) are implied from context, and we shorten to write \( a \) instead of \( a(n, r, c, d) \).

In Section 3.1 we show that the solutions to the inhomogenous cocharacter equations fall into \( \frac{n}{a} \) equivalence classes, each defined by \( A = ka \) for some \( 1 \leq k \leq \frac{n}{a} \), and that each equivalence class contains the same number of solutions. The solutions to the cocharacter equations are those in the class defined by \( A = a \frac{n}{a} = n \). Then

\[
S_{\text{cochar}}(n, r, c, d) = \frac{S_{\text{inhom}}(n, r, c, d)}{n/a} = \frac{a}{n} S_{\text{inhom}}(n, r, c, d) \quad (13)
\]

because all equivalence classes are of equal size. In Section 3.2 we characterize the solutions to the inhomogenous cocharacter equations, which provides an expression for \( S_{\text{inhom}}(n, r, c, d) \). We then find \( a \) by identifying the solution which minimizes \( A \). This will complete the proof of Theorem 1.5.

In Section 3.3 we state corollaries that provide simpler expressions for \( S_{\text{cochar}} \) when \( c \equiv d \equiv 0 \), when \( d_1 \equiv d_2 \equiv 1 \), when \( d \equiv 0 \), and when \( n \) and \( r \) are relatively prime.
3.1 Equivalence classes of solutions

First, we characterize the set of $A$ for which the inhomogeneous cocharacter equations have a solution.

**Lemma 3.1.** The equation $B_{c,d,r}x \equiv A1_r \pmod{n}$ has a solution if and only if $A$ is a multiple of $a$.

**Proof.** Let $x_a$ be a solution to

$$B_{c,d,r}x_a \equiv a1_r \pmod{n}.$$  

Suppose there exist some positive integer $g$ which is not a multiple of $a$ and a vector $x_g$ so that

$$B_{c,d,r}x_g \equiv g1_r \pmod{n}.$$  

Then $ja < g < (j + 1)a$ for some positive integer $j$. Therefore,

$$B_{c,d,r}(x_g - jx_a) \equiv B_{c,d,r}x_g - jB_{c,d,r}x_a \equiv (g - ja)1_r.$$  

This is a contradiction because $0 < g - ja < a$. \hfill \Box

**Corollary 3.2.** The value of $a(n, r, c, d)$ divides $n$.

This follows from Lemma 3.1 because the equation $B_{c,d,r}x \equiv n1_r \equiv 0_r \pmod{n}$ has the solution $x = 0_r$.

We now show that solutions to Equation (2) fall into equivalence based on the value of $A$, and that these equivalences classes are all of the same size.

**Proposition 3.3.** Let $W_k$ be the set of solutions to $B_{c,d,r}x \equiv ka1_r \pmod{n}$ for $1 \leq k \leq \frac{n}{a}$. Then $|W_k| = |W_1|$ for each $1 \leq k \leq \frac{n}{a}$.

**Proof.** Let $1 \leq k \leq \frac{n}{a}$ and let $(x_1, x_2, \ldots, x_r)^T \in W_1$. Consider the function

$$\phi : W_1 \rightarrow W_k;$$

$$(x_1, x_2, \ldots, x_r)^T \mapsto (x_1, x_2, \ldots, x_r)^T + (k - 1)(x_1', x_2', \ldots, x_r')^T.$$  

By the linearity of matrices, $\phi((x_1, x_2, \ldots, x_r)^T) \in W_{1+(k-1)} = W_k$. To show that $\phi$ is a bijection, consider its inverse:

$$\phi^{-1} : W_k \rightarrow W_1;$$

$$(x_1, x_2, \ldots, x_r)^T \mapsto (x_1, x_2, \ldots, x_r)^T - (k - 1)(x_1', x_2', \ldots, x_r')^T.$$  

It follows from the linearity of matrices that if $(x_1, x_2, \ldots, x_r)^T \in W_k$, then $\phi^{-1}((x_1, x_2, \ldots, x_r)^T)$ is in $W_{k-(k-1)} = W_1$. The proof that $\phi$ and $\phi^{-1}$ are inverses follows directly from the definitions of the functions. \hfill \Box
3.2 Characterizing solutions and finding \( a \)

We now understand how to find \( S_{cochar} \) in terms of \( S_{inhom} \) and \( a \), so it remains to find these values. In order to do so, we begin by characterizing the set of solutions to Equation (2), so that we may then count them.

**Proposition 3.4.** A vector \( \mathbf{x} = (x_1, x_2, \ldots, x_r)^T \) solves the inhomogenous cocharacter equations if and only if for each \( 2 \leq j \leq r \) we have \( x_j = x_1 + v_j \frac{n}{d_1} \) for some \( 1 \leq v_j \leq d_1 \).

To prove this we will use the following lemma.

**Lemma 3.5.** Let \( \mathbf{x} = (x_1, x_2, \ldots, x_r)^T \). Then \( \mathbf{x} \) solves the inhomogenous cocharacter equations if and only if \( cx_1 + dx_j \equiv dx_1 + cx_j \pmod{n} \) for every \( 2 \leq j \leq r \).

**Proof.** Let \( 2 \leq j \leq r \). The first row of the equation \( B_{c,d,r} \mathbf{x} \equiv A1_r \pmod{n} \) tells us that

\[
 cx_1 + dx_j + \sum_{\substack{2 \leq k \leq r \\ k \neq j}} dx_k \equiv m \pmod{n}
\]

while row \( j \) tells us that

\[
 dx_1 + cx_j + \sum_{\substack{2 \leq k \leq r \\ k \neq j}} dx_k \equiv m \pmod{n}.
\]

Setting the left-hand sides of these equations equal to each other and then subtracting \( \sum_{\substack{2 \leq k \leq r \\ k \neq j}} dx_k \) from both, observe that

\[
 cx_1 + dx_j \equiv dx_1 + cx_j \pmod{n}.
\]

To see the implication in the other direction, let

\[
 A \equiv cx_1 + dx_j + \sum_{\substack{2 \leq k \leq r \\ k \neq j}} dx_k \pmod{n}
\]

and suppose that \( cx_1 + dx_j \equiv dx_1 + cx_j \pmod{n} \) for every \( 2 \leq j \leq r \). Then

\[
 dx_1 + cx_j + \sum_{\substack{2 \leq k \leq r \\ k \neq j}} \equiv cx_1 + dx_j + \sum_{\substack{2 \leq k \leq r \\ k \neq j}} \equiv A
\]

for every \( 2 \leq j \leq r \). Thus, every line of \( B_{c,d,r} \mathbf{x} \) gives an expression equal to \( A \), which implies that \( B_{c,d,r} \mathbf{x} \equiv A1_r \pmod{n} \) as desired. \( \square \)

We now return to the proof of Proposition 3.4.
Proof. To characterize which \( \mathbf{x} \) solve the inhomogeneous cocharacter equations, it remains to characterize the solutions to the system of equations given by

\[
\begin{align*}
    cx_1 + dx_j &\equiv dx_1 + cx_j \pmod{n} 
\end{align*}
\]  \quad (14)

for every \( 2 \leq j \leq r \). If we subtract \( dx_1 + cx_j \) from both sides of Equation (14), we obtain

\[
(c - d)(x_1 - x_j) \equiv 0 \pmod{n}.
\]

Recalling that \( d_1 = \gcd(c - d, n) \), Lemma 2.3 tells us that this is equivalent to

\[
d_1(x_1 - x_j) \equiv 0 \pmod{n} \quad (15)
\]

This is true if and only if \( x_1 - x_j \) is a multiple of \( n d_1 \). Letting \( x_1 - x_j \equiv v_j n d_1 \) for some \( 1 \leq v_j \leq d_1 \), we obtain \( x_j \equiv x_1 + v_j n d_1 \). Thus, the solutions to \( B_{c,d,r} \mathbf{x} \equiv m1_r \pmod{n} \) are precisely the vectors of the form

\[
\begin{pmatrix}
1 \\
1 \\
\vdots \\
1
\end{pmatrix} + \frac{n}{d_1} \begin{pmatrix}
0 \\
v_2 \\
v_3 \\
v_r
\end{pmatrix}
\]

for \( 0 \leq x_1 < n \) and \( 1 \leq v_j \leq d_1 \). Let \( \mathbf{v} = (0, v_2, v_3, \ldots, v_r)^T \). This is equivalent to the statement of Proposition 3.4. \( \square \)

Now that we have precisely characterized the set of \( \mathbf{x} \) which solve the inhomogeneous cocharacteristic equations, we can count the size of this set.

**Corollary 3.6.** The number of solutions to the inhomogenous cocharacter equations is

\[
S_{\text{inhom}}(n, r, c, d) = nd_1^{r-1}.
\]

**Proof.** We have \( n \) choices of \( x_1 \) and \( d_1 \) choices for each of \( v_2, v_3, \ldots, v_r \). Each distinct \( (x_1, v_2, \ldots, v_r) \) tuple yields a distinct solution to the inhomogenous cocharacter equations, so there are \( nd_1^{r-1} \) solutions in total. \( \square \)

We are now prepared to identify \( a \) in terms of \( n, r, c, \) and \( d \):

**Proposition 3.7.** The minimum positive integer \( a \) such that the inhomogenous cocharacter equations have a solution for \( A = a \) is \( a = \gcd \left( \frac{d_2}{d_1}, \frac{cn}{d_1} \right) \).

Note that we can equivalently write \( a \) as \( a = \gcd \left( \frac{d_2}{d_1}, \frac{cm}{d_1} \right) \). This follows from \( \frac{cm}{d_1} (c - d) \equiv 0 \pmod{n} \) which is true because \( d_1 \) divides \( c - d \). Therefore, \( \frac{dn}{d_1} \equiv \frac{cm}{d_1} \equiv \frac{c}{d_1} \gcd(c, d, n) \pmod{n} \).
Proof. We want to identify the minimum $A$ for which a solution to the inhomogeneous cocharacter equations exists. We have already characterized solutions to the inhomogenous cocharacter equations as vectors of the form $x = x_1 \mathbf{1}_r + \frac{n}{d_1} v$. Substituting this into Equation (2), we see that the right-hand side can equal

$$
\begin{pmatrix}
c & d & d & \cdots & d \\
d & c & d & \cdots & d \\
d & d & c & \cdots & d \\
\vdots & \vdots & \ddots & \ddots & \vdots \\
d & d & d & \cdots & c
\end{pmatrix}
\begin{pmatrix}
x_1 \\
1 \\
\vdots \\
1 \\
1
\end{pmatrix}
\begin{pmatrix}
0 \\
v_1 \\
v_2 \\
\vdots \\
v_r
\end{pmatrix}
\equiv
\begin{pmatrix}
dv_2 + dv_3 + \cdots + dv_r \\
cv_2 + dv_3 + \cdots + dv_r \\
v_2 + cv_3 + \cdots + dv_r \\
\vdots \\
dv_2 + dv_3 + \cdots + dv_{r-1} + cv_r
\end{pmatrix}.
$$

Every row of this expression must must equal a constant $A$. Therefore, looking at the first row,

$$A \equiv x_1(c + (r-1)d) + \frac{n}{d_1} (dv_2 + dv_3 + \cdots + dv_r) \pmod{n}
\equiv x_1(c + (r-1)d) + \frac{dn}{d_1} (v_2 + v_3 + \cdots + v_r) \pmod{n}.
$$

Observe that $x_1$ and $v_2 + v_3 + \cdots + v_r$ are both arbitrary constants. Thus, the minimum value $A$ can have is $\gcd\left(c + (r-1)d, \frac{dn}{d_1}, n\right)$ which equals $\gcd\left(d_2, \frac{dn}{d_1}\right)$ because $d_2 = \gcd(c + (r-1), n)$.

Finally, we substitute our values obtained for $S_{\text{inhom}}$ and $a$ into Equation (13) to prove Theorem 1.5. We have

$$S_{\text{cochar}}(n, r, c, d) = \frac{a}{n} S_{\text{inhom}}(n, r, c, d)
= \frac{1}{n} \cdot \gcd\left(d_2, \frac{dn}{d_1}\right) \cdot n d_1^{r-1}
= d_1^{r-1} \gcd\left(d_2, \frac{dn}{d_1}\right).
$$

3.3 Corollaries of cocharacter solutions formula

Many properties follow from Theorem 1.5.

**Corollary 3.8.** If $d = 0$, then $S_{\text{cochar}} = \gcd(c, n)^r$. 

12
Proof. If \( d \equiv 0 \equiv n \), then

\[
S_{\text{cochar}}(n, r, c, d) = \gcd(c - d, n)^r \gcd\left(c + (r - 1)d, n, \frac{dn}{\gcd(c - d, n)}\right)
\]

\[
= \gcd(c, n)^r \gcd\left(c, n, \frac{n^2}{\gcd(c, n)}\right)
\]

\[
= \gcd(c, n)^r.
\]

\[\square\]

**Corollary 3.9.** We have \( \dim(\mathfrak{W}) = 1 \) if and only if \( c = d = 0 \).

**Proof.** By Theorem 1.3, this statement is equivalent to saying that \( S_{\text{cochar}} = n^r \) if and only if \( c = d = 0 \). The forward direction follows from Corollary 3.8. Now assume \( S_{\text{cochar}} = n^r \). Then we must have \( d_1 = n \), so

\[
S_{\text{cochar}} = n^{r-1} \gcd\left(d_2, \frac{n}{n} \gcd(c, d, n)\right).
\]

This requires that \( c, d \equiv n \pmod{n} \).

\[\square\]

Note that both Corollary 3.8 and Corollary 3.9 are directly verifiable from looking at the cocharacter equations for \( d = 0 \).

**Corollary 3.10.** We have \( \dim(\mathfrak{W}) = n^r \) if and only if \( d_1 = d_2 = 1 \).

**Proof.** We will show that \( S_{\text{cochar}} = 1 \) if and only if \( d_1 = d_2 = 1 \). To have \( S_{\text{cochar}} = 1 \), we should have \( d_1^{-1} = 1 \) (implying \( d_1 = 1 \)) and \( \gcd\left(d_2, \frac{dn}{d_1}\right) = 1 \).

Since \( d_1 = 1 \) we have \( \gcd(d_2, dn) = 1 \) which tells us that \( d_2 \) must be relatively prime to \( n \). But \( d_2 = \gcd(c + (r - 1)d, n) \) so the only value of \( d_2 \) which has no common factors except 1 with \( n \) is \( d_2 = 1 \).

\[\square\]

**Corollary 3.11.** If \( n \) and \( r \) are relatively prime, then \( a = d_2 \) which implies that \( S_{\text{cochar}} = d_1^{-1}d_2 \).

**Proof.** Let \( c - d = g_1d_1 \) and \( c + (r - 1)d = g_2d_2 \). Then observe that

\[
rd \equiv (c + (r - 1)d) - (c - d) \pmod{n}
\]

\[
\equiv g_1d_1 - g_2d_2 \pmod{n}.
\]

If \( r \) and \( n \) are relatively prime, then \( r \) is invertible in \( \mathbb{Z}_n \), so

\[
d \equiv r^{-1}(g_1d_1 - g_2d_2) \pmod{n}.
\]

Therefore,

\[
d\frac{n}{d_1} \equiv r^{-1}(g_1d_1 - g_2d_2)\frac{n}{d_1} \pmod{n}
\]

\[
\equiv (r^{-1}g_1)d_1\frac{n}{d_1} - \left(r^{-1}g_2\frac{n}{d_1}\right)d_2 \pmod{n}
\]

\[
\equiv \left(-r^{-1}g_2\frac{n}{d_1}\right)d_2 \pmod{n}.
\]
which is a multiple of $d_2$. Therefore,
\[ \gcd \left( d_2, \frac{n}{d_1} \right) = d_2 \]
as desired. \hfill \Box

## 4 Counting solutions to coroot equations

In this section we will count $S_{\text{coroot}}$, the number of solutions to the coroot equations. In doing so, we will prove properties about the form these solutions take on. This will allow us to relate $S_{\text{cochar}}$ to $S_{\text{coroot}}$ in Section 5.

Let
\[ y_i \equiv x_i - x_r \]
\[ z \equiv x_1 + \cdots + x_r. \]

We can then rewrite Equations (3) and (4) as follows:
\[ (c + (r - 1)d)z \equiv 0 \pmod{n} \]
\[ (c - d)y_i \equiv 0 \pmod{n} \quad \text{for all } 1 \leq i \leq r - 1. \]

Lemma 2.3 tells us that Equation (18) holds if and only if $z$ is a multiple of $\frac{n}{d_2}$. Similarly, Equation (19) has solutions $y_i$ such that $y_i$ is a multiple of $d_1$.

**Definition.** Given a fixed $c$ and $d$, let $Y_{d_1}$ be the set of integers $a$ in $\mathbb{Z}/n$ such that $y_i = a$ is a solution to Equation (19), and let $Z_{d_2}$ be the set of integers $a$ in $\mathbb{Z}/n$ such that $z = a$ is a solution to Equation (18).

Then $Y_{d_1}$ is the set of multiples of $\frac{n}{d_1}$, and $|Y_{d_1}| = d_1$. Similarly $Z_{d_2}$ is the set of multiples of $n/d_2$, and $|Z_{d_2}| = d_2$.

Each set of $y_i$- and $z$-values that solve Equations (18) and (19) is an ordered tuple $(y_1, y_2, \ldots, y_{r-1}, z) \in Y_{d_1}^{r-1} \times Z_{d_2}$, and there are $d_1^{r-1} \cdot d_2$ such tuples. Given one of these, we search for tuples $(x_1, x_2, \ldots, x_r) \in \mathbb{Z}_{n}^{r}$ that satisfy Equations (16) and (17).

Solving for $x_i$ from Equation (16) we get
\[ x_i = y_i + x_r. \]

Substituting into Equation (17) and rearranging terms, observe that
\[ rx_r = z - \sum_{i=1}^{r-1} y_i \pmod{n}. \]

Let $b = \gcd(n, r)$. Then Lemma 2.2 tells us that Equation (21) has $b$ solutions when $z - \sum_{i=1}^{r-1} y_i$ is a multiple of $b$ and no solutions otherwise.
Lemma 4.1. Let \((x_1, \ldots, x_r)\) be a solution to equations \((16)\) and \((17)\) for a tuple \((z, y_1, \ldots, y_r)\) and \((x'_1, \ldots, x'_r)\) be a solution to equations \((16)\) and \((17)\) for a different tuple \((z', y'_1, \ldots, y'_r)\) ≠ \((z, y_1, \ldots, y_r)\). Then \((x_1, \ldots, x_r) \neq (x'_1, \ldots, x'_r)\).

Proof. Suppose to the contrary that we had \((x_1, \ldots, x_r) = (x'_1, \ldots, x'_r)\). This would imply

\[
\begin{align*}
y_i &\equiv x_i - x_r = x'_i - x'_r \equiv y'_i & \text{for all } 1 \leq i \leq r - 1 \\
z &\equiv x_1 + \cdots + x_r = x'_1 + \cdots + x'_r \equiv z'
\end{align*}
\]

which implies that \((z', y'_1, \ldots, y'_r) = (z, y_1, \ldots, y_r)\), a contradiction. Therefore, \((x_1, \ldots, x_r) \neq (x'_1, \ldots, x'_r)\).

Now, with the definition of one more function, we can give a convenient way to count the number of solutions to the coroot equations.

**Definition.** Let \(F_{rb}(d_1, d_2, n)\) be the proportion of \((y_1, \ldots, y_r, z)\) tuples that will yield a valid solution to the coroot equations. In other words,

\[
F_{rb} = \frac{|\{(y_1, \ldots, y_r, z) \in Y^{r-1} \times Z : z - y_1 - \cdots - y_r \text{ is a multiple of } b\}|}{|\{(y_1, \ldots, y_r, z) \in Y^{r-1} \times Z\}|}.
\]

**Remark 4.2.** When \(n\) and \(r\) are relatively prime, \(b = 1\) and so any tuple we pick adds to a multiple of \(b\). Thus \(F_{rb}\) evaluates to 1, and so by Theorem 1.6 we have \(S_{\text{coroot}} = d_1^{-1}d_2\).

**Proposition 4.3.** The function \(F_{rb}\) evaluates to

\[
F_{rb}(d_1, d_2, n) = \frac{\gcd\left(\frac{n}{d_1}, \frac{n}{d_2}, b\right)}{b}.
\]

Proof. Let \(k_1 = \gcd\left(\frac{n}{d_1}, b\right)\) so that \(b = m_1k_1\). Then we can show that \(y_i \pmod{b}\) can be any multiple of \(k_1\) in \(Z_b\) with equal probability. Lemma 2.2 tells us that, letting \(y_i = j \frac{n}{d_1}\), the equation

\[
y_i \equiv j \frac{n}{d_1} \equiv g \pmod{b}
\]

has \(k_1 = \gcd\left(\frac{n}{d_1}, b\right)\) solutions if \(k_1|g\), and no solutions otherwise. Thus, the values of \(y_i \pmod{b}\) fall into the \(m_1\) equivalence classes \(k_1, 2k_1, \ldots, m_1k_1 = b\) with equal probability.

Let \(y = \sum_{i=1}^{r-1} y_i\) be the sum of the \(y_i\)'s, and let \(g\) be a multiple of \(k_1\). We will examine the probability that \(y\) will equal \(g\) modulo \(b\). If we pick any arbitrary \(y_1, y_2, \ldots, y_{r-2}\), we are left with

\[
y_{r-1} = g - \sum_{i=1}^{r-2} y_i \pmod{b}.
\]
Figure 3: A visualization of our factorization of $b$, where the overlap of any two circles contains their greatest common divisor.

The right-hand side of this equation defines some equivalence class $\ell k_1 \pmod{b}$ from which we must choose $y_{r-1}$ to ensure that $y \equiv g \pmod{b}$. Exactly $\frac{1}{m_1}$ of the possible values of $y_{r-1}$ place us in the correct equivalence class for a given $g$. Thus, $y$ falls into the equivalence classes $k_1, 2k_1, \ldots, mk_1$ with equal probability.

Similarly, let $k_2 = \gcd(\frac{n}{d_2}, b)$ so that $b = m_2k_2$. Then Lemma 2.2 tells us that

$$z \equiv j \frac{n}{d_2} \equiv g \pmod{b}$$

has $k_2$ solutions if $k_2$ divides $g$, and no solutions otherwise. Therefore, $z \pmod{b}$ can be any of the $m_2$ multiples of $k_2$ modulo $b$ with equal probability.

Now let $k_s = \gcd(k_1, k_2)$ so that $k_1 = s_1k_s$ and $k_2 = s_2k_s$. Then we have $b = m_1s_1k_s = m_2s_2k_s$. Letting $m = \gcd(m_1, m_2)$, we write $b = ms_1s_2k_s$. Figure 3 provides a visualization of how these factors relate to $b$, $\frac{n}{d_1}$, and $\frac{n}{d_2}$. We now want to identify the proportion of $y$- and $z$-values that satisfy

$$z - y \equiv 0 \pmod{b},$$

or equivalently,

$$z \equiv y \pmod{ms_1s_2k_s}.$$ 

Let $y = \alpha k_1 = \alpha s_1k_s$ and $z = \beta k_2 = \beta s_2k_s$. Then we want to find the proportion of $(\alpha, \beta)$ pairs that solve

$$\beta s_2k_s \equiv \alpha s_1k_s \pmod{ms_1s_2k_s}.$$ 

We can divide through by $k_s$:

$$\beta s_2 \equiv \alpha s_1 \pmod{ms_1s_2}.$$
By Lemma 2.2, the right-hand side must be a multiple of \( s_2 \). Since \( s_1 \) and \( s_2 \) are relatively prime, we must have \( \alpha = as_2 \) for some \( a \). Exactly \( \frac{1}{s_2} \) of the possible \( \alpha \)-values are multiples of \( s_2 \). Then

\[
\beta s_2 \equiv as_1s_2 \pmod{ms_1s_2}
\]

which has solutions only for \( \beta \equiv as_1 \pmod{b} \). Out of the \( m_2 = ms_1 \) equivalence classes that \( z \) can fall into, only the one defined by \( \beta = as_1 \) works. Therefore,

\[
\frac{1}{s_2} \left( \frac{1}{ms_1} \right) = \frac{1}{ms_1s_2} = \frac{k}{b} = \frac{\gcd \left( \frac{n}{d_1}, \frac{n}{d_2}, b \right)}{b}
\]

of the choices of \( y \) and \( z \) solve Equation (22).

There are \( d_1^{-1} d_2 \) ordered pairs in \( Y^{-1} \times Z \), and we have shown that exactly \( \frac{\gcd \left( \frac{n}{d_1}, \frac{n}{d_2}, b \right)}{b} \) of these yield solutions to the coroot equations. Any set of \( y \)- and \( z \)-values that solves \( rx_r \equiv z - y \pmod{n} \) will yield \( b \) solutions to the coroot equations because \( x_r \) can take on \( b \) possible values. Therefore, there are

\[
d_1^{-1} d_2 \cdot \frac{\gcd \left( \frac{n}{d_1}, \frac{n}{d_2}, b \right)}{b} \cdot b = d_1^{-1} d_2 \cdot \gcd \left( \frac{n}{d_1}, \frac{n}{d_2}, r \right)
\]

solutions to the coroot equations, as stated in Theorem 1.6.

5 Relating the cocharacter equation to the coroot equations

In this section, we show how the coroot equations are obtained from the cocharacter equations. We then find the relationship between \( S_{\text{coroot}} \) and \( S_{\text{cochar}} \). To obtain the coroot equations from the cocharacter equations, we can multiply the matrix \( B_{c,d,r} \) which defines the cocharacter equations by

\[
L_r = \begin{pmatrix}
1 & 0 & \ldots & 0 & -1 \\
0 & 1 & \ldots & 0 & -1 \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & 1 & -1 \\
1 & 1 & \ldots & 1 & 1
\end{pmatrix}
\]
to obtain
\[ L_{r}B_{c,d,r} x \equiv 0 \pmod{n} \] (23)

which gives us precisely the coroot equations.

5.1 From coroot to cocharacter

We can apply the following linear transformation to the coroot equations to obtain the cocharacter equations, multiplied by \( r \):
\[
\begin{pmatrix}
  r - 1 & -1 & \ldots & -1 & 1 \\
  -1 & r - 1 & \ldots & -1 & 1 \\
  \vdots & \vdots & \ddots & \vdots & \vdots \\
  -1 & -1 & \ldots & r - 1 & 1 \\
  -1 & -1 & \ldots & -1 & 1
\end{pmatrix}
\begin{pmatrix}
  (c - d) & 0 & \ldots & 0 & (d - c) \\
  0 & (c - d) & \ldots & 0 & (d - c) \\
  \vdots & \vdots & \ddots & \vdots & \vdots \\
  0 & 0 & \ldots & (c - d) & (d - c) \\
  c + (r - 1)d & c + (r - 1)d & \ldots & c + (r - 1)d & c + (r - 1)d
\end{pmatrix}
\begin{pmatrix}
  x_1 \\
  x_2 \\
  \vdots \\
  x_r
\end{pmatrix}
= r
\begin{pmatrix}
  c & d & d & \ldots & d \\
  \vdots & \vdots & \vdots & \ddots & \vdots \\
  d & d & d & \ldots & c
\end{pmatrix}
\begin{pmatrix}
  x_1 \\
  x_2 \\
  \vdots \\
  x_r
\end{pmatrix}
\equiv \begin{pmatrix}
  0 \\
  0 \\
  \vdots \\
  0
\end{pmatrix} \pmod{n}. \quad (24)

If \( r \) and \( n \) are relatively prime, then \( r \) has an inverse \( r^{-1} \) in \( \mathbb{Z}_n \). In that case, we can multiply Equation (24) by \( r^{-1} \) on both sides to obtain the cocharacter equations. Then the cocharacter and coroot equations are equivalent. The co-root solutions have \( d r^{-1} d_2 \) solutions in this case, which gives us an additional proof of Corollary 3.11.
More generally, let $b = \gcd(r, n)$. Then we have

$$b \begin{pmatrix} \frac{r}{b} \\ \frac{b}{b} \end{pmatrix} \begin{pmatrix} c & d & d & \ldots & d \\ d & c & d & \ldots & d \\ d & d & c & \ldots & d \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ d & d & d & \ldots & c \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_r \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \pmod{b \cdot \frac{n}{b}}.$$

If we divide everything by $b$, we obtain

$$\begin{pmatrix} \frac{r}{b} \end{pmatrix} B_{c,d,r} x = 0_r \pmod{\frac{n}{b}}.$$

The number $\frac{r}{b}$ is relatively prime to $\frac{n}{b}$ and therefore invertible in $\mathbb{Z}_{\frac{n}{b}}$. Multiplying both sides by the inverse of $\frac{r}{b}$, we see that

$$B_{c,d,r} x = 0_r \pmod{\frac{n}{b}}. \quad (25)$$

**Remark 5.1.** When $r$ and $n$ are relatively prime $n = b$ and therefore the coroot and cocharacter equations are equivalent.

Combining Remarks 4.2 and 5.1 gives us an alternative way to see why Corollary 3.11 holds.

If $b \neq 1$, then for any coroot solution $x$, we get

$$B_{c,d,r} x \equiv \frac{n}{b} v \pmod{n} \quad (26)$$

for some vector $v$. We now show that for all coroot solutions, we have $v = k1_r$ where $k$ is some constant.

Let the $i$th row of the right-hand side of Equation (25) be

$$w_i \equiv \left( \sum_{j=1}^{i-1} dx_j + cx_i + \sum_{j=i+1}^{r} dx_j \right).$$

Then Equation (25) states that $w_i \equiv 0 \pmod{\frac{n}{b}}$ for each $1 \leq i \leq r$, which implies that each $w_i$ must be a multiple of $\frac{n}{b}$.

**Lemma 5.2.** All solutions to the coroot equations have $w_1 = w_2 = \cdots = w_r$.

**Proof.** Observe that for any $1 \leq i < r$,

$$w_i - w_r = (c - d)(x_i - x_r).$$

This must equal zero, by Equation (4). Therefore, $w_i = w_r$ for all $1 \leq i < r$. \qed

We have shown that if $x$ solves the coroot equations, then $x$ solves

$$B_{c,d,r} x = k \frac{n}{b} (1_r) \pmod{n} \quad (27)$$
where \(1 \leq k \leq b\). To see that the converse is true, suppose that \(x\) solves Equation (27) and define \(w_i\) as above for all \(1 \leq i \leq r\). Then

\[
(c - d)(x_i - x_r) \equiv w_i - w_r \equiv k \frac{n}{b} - k \frac{n}{b} \equiv 0 \pmod{n}
\]

\[
(c + (r - 1)d)(x_1 + x_2 + \ldots x_r) \equiv w_1 + w_2 + \ldots + w_r \equiv r \left( k \frac{n}{b} \right) \equiv 0 \pmod{n}
\]

which gives us the coroot equations. Thus, Equation (27) provides an equivalent formulation of the coroot equations.

In Section 3.1 we showed that Equation (27) has solutions if and only if \(k \frac{n}{b}\) is a multiple of \(a\), and that each class of solutions (defined by having the same \(k\)) is of the same size. Again, we now want to find the smallest nonzero \(k\) for which (27) has a solution.

**Definition.** Let \(\kappa(n, r, c, d)\) be the smallest positive value of \(k\) such that there is a solution to Equation (27), and let \(M(n, r, c, d) = \kappa(n, r, c, d) \frac{n}{b}\).

Again, it will often be clear from context that we are working with a particular fixed \(n, r, c, d\) in which case we will write \(\kappa\) and \(M\) instead of \(\kappa(n, r, c, d)\) and \(M(n, r, c, d)\) for brevity.

We can relate the values of \(M(n, r, c, d)\) and \(a(n, r, c, d)\) as follows.

\[
M = \text{lcm} \left( a, \frac{n}{b} \right) = \text{lcm} \left( \frac{n}{b}, \gcd \left( d_2, \frac{dn}{d_1} \right) \right),
\]

Then there are \(\frac{n}{M} = \frac{b}{\kappa}\) equivalence classes of solutions to Equation (27). Exactly one of these equivalence classes—the one given by \(k = b\)—gives the solutions to the cocharacter equations. Therefore,

\[
S_{\text{cochar}} = \frac{S_{\text{coroot}}}{n/\kappa} = \frac{S_{\text{coroot}} \cdot M}{n} = S_{\text{coroot}} \cdot \frac{\kappa}{b}.
\]

Substituting in our earlier expressions for the values of \(S_{\text{coroot}}\) and \(M\), we obtain

\[
S_{\text{cochar}} = \frac{d_1^{-1} d_2}{n} \gcd \left( \frac{n}{d_1}, \frac{n}{d_2}, b \right) \text{lcm} \left( \frac{n}{b}, \gcd \left( d_2, \frac{dn}{d_1} \right) \right).
\]

Although it is not immediately clear from looking at this equation, we know that this formula is equivalent to the one given in Theorem 1.5. One area of future work would be to simplify this expression and more directly understand why it is equivalent to the statement of Theorem 1.5.

In the next section, we conjecture yet another equivalent formula for \(S_{\text{cochar}}\) by expressing the values of \(M\) and \(\kappa\) directly in terms of the prime factors of \(n, r, c\) and \(d\).
5.2 Strategy for identifying $\kappa$ and $M$

In the following subsections, we identify $M$ (and, equivalently, $\kappa$) for all possible values of $n$, $r$, $c$, and $d$. We identify $M$ in the following three cases:

1. When $r = p^\ell$ and $n = p^m$ for a prime $p$ (Theorem 5.3)

2. When $r = p^\ell$ and $n = n_0p^m$ for a prime $p$ and $n_0$ relatively prime (Lemma 5.4)

3. When $r = p_1^{\ell_1}p_2^{\ell_2} \ldots p_j^{\ell_j}$ and $n = n_0p_1^{m_1}p_2^{m_2} \ldots p_j^{m_j}$ (Conjecture ??)

In the case where $r = p^\ell$ and $n = p^m$, we prove the following theorem in Section 5.3:

Lemma 5.3. Fix a prime $p$ so that $r = p^\ell$, $n = p^m$, and $b = p^\mu$. Let $(c - d) = c_0p^t$ and $d = d_0p^s$ where $c_0$ and $d_0$ are relatively prime to $p$. Then

$$M = p^\max(m-\mu,\min(t,s+m-t)).$$

is the smallest positive integer such that there exists a solution $x$ to the coroot equations which satisfies

$$B_{c,d,r}x \equiv M1_r \pmod{n}.$$  \hspace{1cm} (32)

Note that all other solutions $v$ of the coroot equations satisfy $B_{c,d,r}v = C1_r$ for some $C$ a multiple of $M$.

Example. We can store $\kappa$ in tables using the same setup we earlier used to make tables of $S_{\text{cochar}}$. For $n = 8 = 2^3$ and $r = 2^\ell$, the following tables show how $\kappa$ changes as $\ell$ increases from 1 to 3. Because $M$ and $\kappa$ depend on $\mu = \min(\ell, m)$ rather than on $\ell$, any $\kappa$ table for $\ell > 3$ would be identical to the table for $\ell = 3$.

The entries in these tables are determined by the main diagonals they lie on, which are described by $s$, and the columns they lie in, which are described by $t$ and index how far down the main diagonal an entry is. In particular, to obtain the matrix for $\ell + 1$, we start with the matrix for $\ell$ and then multiply a specific fraction of the elements falling on highlighted diagonals of the $\ell + 1$ matrix by $p$.

To extend the result of Theorem 5.3 to the case where $n = n_0p^m$ and $r = p^\ell$, we prove the following lemma in Section 5.4

n = 8, r = 2

\begin{align*}
&\begin{pmatrix} 2 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
& 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
& 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
& 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
& 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
& 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
& 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
& 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
\end{pmatrix} \\
&\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
& 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
& 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
& 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
& 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
& 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
& 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
& 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
\end{pmatrix} \\
&\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
& 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
& 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
& 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
& 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
& 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
& 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
& 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
\end{pmatrix} \\
\end{align*}

21
**Lemma 5.4.** Let \( n = n_0p^m \) where \( n_0, p \) relatively prime and \( c \equiv c' \pmod{p^m} \), \( d \equiv d' \pmod{p^m} \) for \( 0 \leq c', d' < p^m \). Then

\[
\kappa(n, r, c, d) = \kappa(p^m, r, c', d') \quad \text{and} \quad M(n, r, c, d) = n_0M(p^m, r, c', d').
\]

**Example.** Below are the \( \kappa \) tables for \( r = 2^2 \) and \( n = 2^2 \) and \( 3 \cdot 2^2 \):

\[
\begin{align*}
\kappa(2^2, 2^2) &= \begin{pmatrix}
4 & 1 & 2 & 1 \\
1 & 1 & 1 & 2 \\
2 & 1 & 2 & 1 \\
1 & 2 & 1 & 1
\end{pmatrix} \\
\kappa(3 \cdot 2^2, 2^2, 6) &= \begin{pmatrix}
4 & 1 & 2 & 1 & 4 & 1 & 2 & 1 & 4 & 1 & 2 & 1 \\
1 & 1 & 1 & 2 & 1 & 1 & 1 & 2 & 1 & 1 & 1 & 2 \\
2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 \\
1 & 2 & 1 & 1 & 2 & 1 & 1 & 1 & 2 & 1 & 1 & 1
\end{pmatrix}
\end{align*}
\]

When \( n = 3 \cdot 2^2 \), we obtain the \( \kappa \) table for \( n = 2^2 \), tessellated in a \( 3 \times 3 \) grid. This happens because, as Lemma 5.4 tells us, increasing \( c \) or \( d \) by a multiple of \( p^m = 2^2 \) does not change \( \kappa \).

In Section 5.5 we prove the following lemma:

**Lemma 5.5.** Let \( r = p_1^{\ell_1}p_2^{\ell_2} \ldots p_j^{\ell_j} \), and let \( M_i = M(n, p_i^{\ell_i}, c, d) \). Let \( b_i = \gcd(n, p_i^{\ell_i}) \) and \( M_i = \kappa_i \frac{n}{b_i} \). Then

\[
M(n, r, c, d) = \gcd(M_1, M_2, \ldots, M_j) = \kappa_1 \kappa_2 \ldots \kappa_j \frac{n}{b}.
\]

We restate this lemma and combine it with our results from Sections 5.3 and 5.4 to obtain a formula for \( M \) in terms of the prime factors of \( n \) and \( r \).

**Example.** Below are the kappa tables for \( n = 2 \cdot 3 = 6 \) and \( r = 2, 3, 6 \):

\[
\begin{align*}
\kappa(2, 6) &= \begin{pmatrix}
2 & 1 & 2 & 1 & 2 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 \\
2 & 1 & 2 & 1 & 2 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 \\
2 & 1 & 2 & 1 & 2 & 1 \\
1 & 1 & 1 & 1 & 1 & 1
\end{pmatrix} \\
\kappa(3, 6) &= \begin{pmatrix}
3 & 1 & 1 & 3 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1
\end{pmatrix} \\
\kappa(6, 6) &= \begin{pmatrix}
6 & 1 & 2 & 3 & 2 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 \\
2 & 1 & 2 & 1 & 2 & 1 \\
3 & 1 & 1 & 3 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1
\end{pmatrix}
\end{align*}
\]

The table for \( r = 6 \) is obtained by multiplying the tables for \( r = 2 \) and \( r = 3 \) together elementwise.
5.3 Proof of Lemma 5.3

For a solution \( \mathbf{x} = (x_1, x_2, \ldots, x_r)^T \) to the coroot equations, let \( B_{c,d,r} \mathbf{x} = C \mathbf{1}_r \).

From the last line of the cocharacter equations, we know that
\[
\begin{align*}
d(x_1 + \cdots + x_{r-1}) + cx_r & \equiv C \pmod{n} \\
d(x_1 + \cdots + x_{r-1} + x_r) + (c-d)x_r & \equiv C \pmod{n}.
\end{align*}
\]

We can now substitute in \( z = x_1 + \cdots + x_r \):
\[
dz + (c-d)x_r \equiv C \pmod{n}.
\]

To find the minimum possible value for \( C \), we will first express Equation (33) in terms of the variables defined in the theorem statement. In particular, we need to express \( y, z \) and \( x_r \) in terms of these variables.

First we compute \( y \), which can be any multiple of \( \frac{n}{d_1} \). We have
\[
d_1 = \gcd(c - d, n) = \gcd(c_0 p^\ell, p^m) = p^\ell.
\]

Therefore,
\[
y = \frac{n}{d_1} = p^{m-t},
\]
for \( 0 \leq \frac{n}{d_1} < p^\ell \). We now get an expression for \( d_2 \) which we use to find \( z \).

Observe that
\[
c + (r-1)d = c - d + rd = c_0 p^\ell + d_0 p^{\ell+s}.
\]

Let \( \nu = \min(t, s + \ell) \). Then
\[
\begin{align*}
d_2 &= \gcd(c + (r-1)d, n) = p^{\nu} \quad \text{and} \\
z &= \frac{n}{d_2} = p^{m-\nu},
\end{align*}
\]
where \( 0 \leq \frac{n}{d_2} < p^{\nu} \).

We can now solve for \( x_r \). We have that
\[
\begin{align*}
r x_r & \equiv z - y \pmod{n} \\
p^\ell x_r & \equiv p^{m-\nu} - p^{m-t} \pmod{p^m}.
\end{align*}
\]

We now consider two different cases.

5.3.1 Case 1: If \( \ell \leq m - t \)

When \( \ell \leq (m - t) \), then \( p^\ell \) divides both terms on the right side of Equation (37) because \( m - t \leq m - \nu \). Dividing everything (including \( n \) in the modulus) by
If \( p^\ell \), we get that \( x_r \) must satisfy the equation
\[
x_r \equiv \bigcirc p^{m-\nu-\ell} - p^{m-t-\ell}\pmod{ap^{m-t}}
\equiv p^{m-t-\ell}\left(p^{t-\nu} - \bigcirc\right)\pmod{p^{m-t}}
\]
because \( t \geq \nu \). Then \( x_r \) can be any multiple of \( p^{m-t-\ell} \). Let
\[
x_r \equiv \bigcirc p^{m-t-\ell}
\] (38)
where \( 0 \leq \bigcirc < p^{t+1} \). Given any choice of \( \bigcirc \) and any choice of \( \bigcirc \), we can always find some value of \( \bigcirc \) to make Equation (38) hold.

Substituting the possible values of \( z \) and \( x_r \) given in Equations (35) and (38) along with the values of \( d \) and \( c - d \) into Equation (33) and simplifying, we get
\[
dz + (c - d)x_r \equiv \kappa \frac{n}{b}\pmod{n}
\]
\[
d_0p^\nu \bigcirc p^{m-\nu} + c_0p^\ell \bigcirc p^{m-t-\ell} \equiv \kappa p^{m-\ell}\pmod{p^{m}}
\]
\[
\bigcirc \cdot d_0p^{m-\nu+s} + \bigcirc \cdot c_0p^{m-\ell} \equiv \kappa p^{m-\ell}\pmod{p^{m}}.
\]
Let \( \bigcirc = 0 \). We then have
\[
\bigcirc = c_0^{-1} p^{m-\ell} \equiv \kappa p^{m-\ell}\pmod{p^{m}}.
\]
Observe that \( c_0 \) is relatively prime to \( p^{m} \) and therefore invertible, so we can let \( \bigcirc = c_0^{-1} \) and obtain a solution for \( \kappa = 1 \) and \( M = p^{m-\ell} = p^{m-\mu} \).

**5.3.2 Case 2: If \( \ell \geq m - t \)**

In this case, \( p^{m-t} \) divides all terms in Equation (37), so we can divide all terms by \( p^{m-t} \) to yield
\[
p^{\ell-m+t}x_r \equiv \bigcirc p^{t-\nu} - \bigcirc\pmod{p^{\ell}}.
\]
Therefore, \( x_r \) can be any number in \( \mathbb{Z}_{p^m} \), and \( \bigcirc \) can vary simultaneously because we can always pick \( \bigcirc \) to obtain the desired \( x_r \). Let \( x_r = \bigcirc \).

Substituting the possible values of \( z \) given in Equation (35) and \( x_r = \bigcirc \) into the right-hand side Equation (33) and simplifying, we get
\[
dz + (c - d)x_r \equiv \kappa \frac{n}{b}\pmod{n}
\]
\[
d_0p^\nu \bigcirc p^{m-\nu} + c_0p^\ell \bigcirc \equiv \kappa p^{m-\mu}\pmod{p^{m}}
\]
\[
\bigcirc \cdot d_0p^{m-\nu+s} + \bigcirc \cdot c_0p^\ell \equiv \kappa p^{m-\mu}\pmod{p^{m}}.
\]
The numbers \(c_0\) and \(d_0\) are relatively prime to \(p^m\) and therefore invertible in \(\mathbb{Z}_{p^m}\). Then we can reparameterize \(\bigcirc\) and \(\bigotimes\) to obtain
\[
\bigcirc p^{s+m-\nu} + \bigotimes p^t \equiv \kappa p^{m-\mu} \pmod{p^m}.
\]
The minimum nonzero value that the right-hand side can have is \(p^{\min(s+m-\nu,t)}\), where \(\nu = \min(t, \ell + s)\). If \(\ell + s < t\), then \(p^{s+m-\nu} = p^{m-t} = p^{m-\mu}\) and we have a solution for \(\kappa = 1\). If \(\ell + s > t\), then \(p^{\min(s+m-\nu,t)} = p^{\min(s+m-t,t)}\). Then
\[
\kappa p^{m-\mu} = M = p^{\max(m-\mu, \min(t, s+m-t))}.
\]
Equivalently,
\[
\kappa = p^{\max(0, \min(s+\mu-t, t+\mu-m))},
\]
These formulas also account for case 1, since our assumption that \(\ell \leq m - t\) implies that \(\ell = \mu\) and \(t \leq m - \ell\). Therefore,
\[
\max(m - \mu, \min(t, s + m - t)) = m - \mu = m - \ell
\]
as desired if \(\ell \leq m - t\).

5.4 Proof of Lemma 5.4

Proof. Let \(r = p^\ell\) for a prime \(p\) and \(n = n_0 p^m\) for some \(n_0\) relatively prime to \(p\). To show that \(\kappa(n_0 p^m, r, c, d) = \kappa(p^m, r, c', d')\), we first prove that if
\[
B_{c',d',r} x \equiv k \frac{p^n}{\gcd(p^m, r)} 1_r \pmod{p^m}
\]
has a solution then
\[
B_{c,d,r} x' \equiv k \frac{n}{\gcd(n, r)} 1_r \pmod{a p^m}.
\]
does as well. We then show that if Equation (42) has a solution, then Equation (41) does as well.

To do this, we must first write \(B_{c,d,r}\) in terms of \(B_{c',d',r}\). Observe that \(\gcd(p^m, r) = \gcd(n, r) = b\). Now we first suppose that \(x' = n_0 x\) is a solution to Equation (41). We show that \(x' = n_0 x\) is a solution to Equation (42). By Lemma 2.1 we know that
\[
B_{c,d,s}(n_0 x) \equiv k \left( \frac{n}{b} \right) 1_r \pmod{n}.
\]
Observe that \(B_{c,d,r}\) differs from \(B_{c',d',r}\) in that we add some multiples of \(p^m\) to \(c'\) and \(d'\) to obtain \(c\) and \(d\), respectively. Then, for some constants \(0 \leq \alpha_c, \alpha_d < n_0\), we have
\[
B_{c,d,r} = B_{c',d',r} + \begin{pmatrix}
\alpha_c p^m & \alpha_d p^m & \cdots & \alpha_d p^m \\
\alpha_d p^m & \alpha_c p^m & \cdots & \alpha_d p^m \\
\vdots & \vdots & \ddots & \vdots \\
\alpha_d p^m & \alpha_d p^m & \cdots & \alpha_c p^m
\end{pmatrix}.
\]
Therefore,

\[ B_{c,d,r}(n_0x) \equiv B'_{c',d',r}(n_0x) + \begin{pmatrix} \alpha c p^m & \alpha d p^m & \cdots & \alpha d p^m \\ \alpha d p^m & \alpha c p^m & \cdots & \alpha d p^m \\ \vdots & \vdots & \ddots & \vdots \\ \alpha d p^m & \alpha d p^m & \cdots & \alpha c p^m \end{pmatrix} (n_0x) \pmod{n}. \]

Multiplying the matrix in the second term by \( n_0 \), all entries are now 0 \( \pmod{n_0p^m} \). Thus the entire second term on the right-hand side is 0 \( \pmod{n} \), and we obtain

\[ B_{c,d,r}(n_0x) \equiv B'_{c',d',r}(n_0x) \equiv n_0k \frac{p^m}{b} \pmod{n}. \]

Now suppose that \( x' \) is a solution to Equation (42). Then

\[ B_{c,d,r}(n_0x') \equiv n_0k \left( \frac{n_0p^m}{b} \right) 1_r \equiv k \left( \frac{n}{b} \right) 1_r \pmod{n}. \]

Using Lemma 2.1 we can divide by \( n_0 \) to obtain

\[ B'_{c',d',r}(x') \equiv n_0k \left( \frac{p^m}{b} \right) 1_r \pmod{p^m}. \]

Since \( n_0 \) and \( p^m \) are relatively prime, we can multiply by \( n_0^{-1} \) to get that

\[ n_0^{-1} B'_{c',d',r}(x') \equiv n_0^{-1} \left( \frac{n_0p^m}{b} \right) 1_r \pmod{p^m} \]

Thus Equations (11) and (42) have solutions for the same set of \( k \)-values, which implies that \( \kappa(n_0p^m, p^\ell, c, d) = \kappa(p^m, p^\ell, c, d) \).

5.5 Case when \( r \) is a product of distinct primes

In Lemma 5.5 we stated that if \( r = p_1^\ell_1 p_2^\ell_2 \cdots p_j^\ell_j \) and \( M_i = M(n, p^c_i, d) \), then

\[ M(n, r, c, d) = \gcd(M_1, M_2, \ldots, M_j) = \kappa_1 \kappa_2 \ldots \kappa_j \frac{n}{b}. \]
Combining Lemmas 5.3, 5.4, and 5.5, we obtain Proposition 1.8 (which in turn implies the statements of each of the three lemmas). To prove Proposition 1.8, we will want to separately examine which power of each $p_i$ is contained in $M$ individually. To do so, the following properties will be helpful:

$$\gcd(z, \prod_{i=1}^{j} p_i^{m_i}) = \prod_{i=1}^{j} \gcd(z, p_i^{m_i})$$  (44)

$$\text{lcm}\left(\prod_{i=1}^{j} p_i^{u_i}, \prod_{i=1}^{j} p_i^{v_i}\right) = \prod_{i=1}^{j} \text{lcm}(p_i^{u_i}, p_i^{v_i}) = \prod_{i=1}^{j} p_i^{\text{max}(u_i, v_i)}$$  (45)

$$\gcd(a, b) = \gcd(a \pmod{b}, b).$$  (46)

We now prove Proposition 1.8.

**Proof.** We will prove that Proposition 1.8 follows from the definition of $a$ and the fact that $M = \gcd\left(\frac{n}{b}, a\right)$. For each $1 \leq i \leq j$, let:

$$c - d \equiv c_i p_i^{t_i} \pmod{p_i^{m_i}}$$

$$d \equiv d_i p_i^{s_i} \pmod{p_i^{m_i}}$$

$$r \equiv r_i p_i^{\mu_i} \pmod{p_i^{m_i}}$$

where $c_i, d_i, r_i$ are nonzero and relatively prime to $p_i$ and $0 \leq t_i, s_i, \mu_i \leq m_i$. Note that $\mu_i = \min(m_i, \ell_i)$ so that $b = p_i^{\mu_1} p_i^{\mu_2} \cdots p_i^{\mu_j}$. Then

$$\frac{n}{b} = \prod_{i=1}^{j} p_i^{m_i - \mu_i}.$$

Recall that

$$a = \gcd\left(c + (r - 1)d, \frac{dn}{d_1}, n\right)$$

$$= \gcd\left((c - d) + rd, \frac{dn}{d_1}, \prod_{i=1}^{j} p_i^{m_i}\right).$$

For each $1 \leq i \leq j$, let

$$a_i = \gcd\left((c - d) + rd, \frac{dn}{d_1}, p_i^{m_i}\right).$$

Note that $a_i$ must be a power of $p_i$. Then by Equation (44), $a = a_1 a_2 \cdots a_j$.

Next recall that $M$ is the least common multiple of $a$ and $\frac{n}{b}$. We have identified a way to write $a$ is a product of powers of $p_i$ for each $1 \leq i \leq j$, and $\frac{n}{b} =$

27
\( p_1^{m_1-\mu_1} p_2^{m_2-\mu_2} \cdots p_j^{m_j-\mu_j} \) is also a product of powers of \( p_1, p_2, \ldots p_j \). Therefore, by Equation (45),

\[
M = \text{lcm} \left( a, \frac{n}{b} \right) = \text{lcm} \left( a_1a_2 \cdots a_j, p_1^{m_1-\mu_1} p_2^{m_2-\mu_2} \cdots p_j^{m_j-\mu_j} \right) = \prod_{i=1}^{j} \text{lcm}(a_i, p_i^{m_i-\mu_i}).
\]

(47)

We will next find \( a_i \), but we first need to identify \( \delta_1 \). By Equations (44) and (46), \( \delta_1 \) equals

\[
\gcd \left( c - d, \prod_{i=1}^{j} p_i^{m_i} \right) = \prod_{i=1}^{j} \gcd(c - d, p_i^{m_i}) = \prod_{i=1}^{j} \gcd(c_i p_i^{t_i}, p_i^{m_i}) = \prod_{i=1}^{j} p_i^{t_i}.
\]

Now we can evaluate \( a_i \), applying Equation (46) to obtain:

\[
a_i = \gcd \left( (c - d) + rd \pmod{p_i^{m_i}}, d \frac{n}{\delta_1} \pmod{p_i^{m_i}}, p_i^{m_i} \right).
\]

We now substitute in the values of \((c - d)\) and \(d\) modulo \( p_i^{m_i} \). Observe that \( \frac{n}{\delta_1} = p_1^{m_1-t_1} p_2^{m_2-t_2} \cdots p_j^{m_j-t_j} \), so the only factor of \( \frac{n}{\delta_1} \) that can contribute to \( a_i \) is \( p_i^{m_i-t_i} \). Therefore, we only substitute \( p_i^{m_i-t_i} \) for \( \frac{n}{\delta_1} \).

\[
a_i = \gcd \left( c_i p_i^{t_i} + d_i p_i^{s_i} r_i p_i^{t_i}, d_i p_i^{s_i} p_i^{m_i-t_i}, p_i^{m_i} \right) = \gcd \left( c_i p_i^{t_i} + r_i d_i p_i^{s_i+\mu_i}, d_i p_i^{s_i+m_i-t_i}, p_i^{m_i} \right).
\]

Now we consider three cases. If \( t_i < s_i + \mu_i \), then

\[
a_i = \gcd \left( p_i^{t_i} (c_i + r_i d_i p_i^{s_i+\mu_i-t_i}), d_i p_i^{s_i+m_i-t_i}, p_i^{m_i} \right) = p_i^{\min(t_i, s_i + m_i - t_i, m_i)} = p_i^{\min(t_i, s_i + m_i - t_i)}
\]

where we’ve used the fact that \( t_i \leq m_i \) in the last step. Therefore,

\[
\text{lcm}(a_i, p_i^{m_i-\mu_i}) = \text{lcm}(p_i^{\min(t_i, s_i + m_i - t_i)}, p_i^{m_i-\mu_i}) = p_i^{\max(m_i-\mu_i, \min(t_i, s_i + m_i - t_i))}.
\]
Next suppose that $t_i > s_i + \mu_i$. Then we have
\[
a_i = \gcd \left( p_i^{s_i + \mu_i} (c_i P_i^{t_i - s_i - \mu_i} + r_i d_i), d_i p_i^{s_i + m_i - t_i} P_i^{m_i} \right)
= p_i^{\min(s_i + \mu_i, s_i + m_i - t_i, m_i)}.
\]
Since $s_i + \mu_i < t_i \leq m_i$, we can rewrite this as follows:
\[
a_i = p_i^{\min(t_i, s_i + \mu_i, s_i + m_i - t_i)}.
\]
Then
\[
lcm(a_i, p_i^{m_i - \mu_i}) = lcm(p_i^{\min(t_i, s_i + \mu_i, s_i + m_i - t_i)}, p_i^{m_i - \mu_i})
= p_i^{\max(m_i - \mu_i, \min(t_i, s_i + \mu_i, s_i + m_i - t_i))}.
\]
Since $t_i > s_i + \mu_i$, we have $s_i + m_i - t_i < m_i - \mu_i$. Therefore,
\[
\min(t_i, s_i + \mu_i, s_i + m_i - t_i) < m_i - \mu_i
\]
and
\[
lcm(a_i, p_i^{m_i - \mu_i}) = p_i^{m_i - \mu_i} = p_i^{\max(m_i - \mu_i, \min(t_i, s_i + m_i - t_i))}
\]
If $t_i = s_i + \mu_i$, then we have:
\[
a_i = \gcd \left( p_i^{s_i - \mu_i} (c_i + r_i d_i), d_i p_i^{s_i + m_i - (s_i + \mu_i)} P_i^{m_i} \right).
\]
Note that $c_i + r_i d_i$ may contain additional powers of $p_i$, so the largest power of $t_i$ in $p_i^{s_i - \mu_i} (c_i + r_i d_i)$ is unknown. Call this power $\bigodot$ for now. Then
\[
a_i = p_i^{\min(\bigodot, m_i - \mu_i, m_i)} = p_i^{\min(\bigodot, m_i - \mu_i)}.
\]
Therefore,
\[
lcm(a_i, p_i^{m_i - \mu_i}) = lcm(p_i^{\min(\bigodot, m_i - \mu_i)}, p_i^{m_i - \mu_i})
= p_i^{\max(m_i - \mu_i, \min(\bigodot, m_i - \mu_i))}
= p_i^{m_i - \mu_i}.
\]
Because $s_i + m_i - t_i = m_i - \mu_i$, we can also write this as
\[
lcm(a_i, p_i^{m_i - \mu_i}) = p_i^{\max(m_i - \mu_i, \min(t_i, s_i + m_i - t_i))}
\]
which is identical to the expression we obtained in the other two cases.
Substituting this into Equation \[17\], we obtain
\[
M = \prod_{i=1}^{j} p_i^{\max(m_i - \mu_i, \min(t_i, s_i + m_i - t_i))}
\]
as desired. \[\square\]
6 Future Work

We have obtained two very different expressions for $S_{cochar}$ in Theorem 1.5 and Equation (29), and it currently not obvious that they always give the same number. Connecting the solutions to the inhomogenous cocharacter and coroot equations in more detail would also help us to better reconcile our formulas for $S_{cochar}$. If we better understood why they are equivalent, that might point towards a simpler formula from $S_{cochar}$. In addition to the corollaries provided in Section 3.3, there are other corollaries that we would like to obtain by knowing $S_{cochar}$. For example, we would like to describe all cases when $S_{cochar} = d_1^{r-1}d_2$.

The work in [3] which motivated this project also points to other open questions. Frechette has a function from $\mathcal{W}$ to a quantum group module of dimension $(\frac{n}{r})^{r}$ which is always injective, surjective or bijective. Knowing that $\dim \mathcal{W} = \frac{n}{r} - 1$, we could identify when each case occurs by comparing $d_1$ to $a$. It would also be illuminating to generalize our work here to all reductive groups, as this paper only describes type $A_n$ groups.

Acknowledgements

This project was partially supported by RTG grant NSF/DMS-1745638 and was supervised as part of the University of Minnesota School of Mathematics Summer 2022 REU program. The authors would like to thank their mentor Claire Frechette and TA Carolyn Stephen for their guidance throughout the project and Darij Grinberg for helpful comments. They would also like to thank cats for existing, especially Holly, PUF, Snape, Lizzy, and Mouse.

References


[5] Peter J. McNamara, Principal series representations of metaplectic groups over local fields, Multiple Dirichlet series, L-functions and automorphic