Hilbert Functions of Finite Group Orbits: Abelian and Metacyclic Groups

A Thesis
Presented to
The Division of Mathematics and Natural Sciences
Reed College

In Partial Fulfillment
of the Requirements for the Degree
Bachelor of Arts

Scott Corry

May 2001

Approved for the Division
(Mathematics)

David Perkinson

Acknowledgements

For all the help and encouragement, and for so much more, I would like to thank:

Dave Perkinson, for being an outstanding thesis advisor. You devoted more time and energy to me than I could have hoped for, and always with a smile on your face. Thanks for your ideas, your enthusiasm, and for always making things fun.

Rao Potluri, for help with the representation theory of metacyclic groups.

Jerry Shurman, for help with the thesis, but moreover for your friendship, and for going out of your way the past three years to offer me opportunities and assistance that have enriched me immeasurably.

Madera, for all your love, support, and patience, but most of all for your laughter and your touch.

Kate, Maggie, Sammie, and Joe, for your friendship and understanding, and for making the past four years so memorable.

My parents and my sister, for all your love and support, for believing in me so fully, and for your wonderful company, thank you.

Contents

Abstract

This thesis is concerned with Hilbert functions of ideals of finite group orbits, focusing in particular on abelian and metacyclic groups. Conjecture 16 in Section 4 characterizes the Hilbert functions that arise from two-dimensional representations of certain abelian groups, and a proof of the necessity of its conditions is provided. In Section 6, Proposition 18 gives a bound for the Hilbert function of the orbit ideal of an induced representation of a metacyclic group. Proposition 21 improves this result in the two-dimensional case, providing a description of the actual Hilbert function. Conjecture 24 characterizes the three-dimensional representations that fail to achieve the bound in Proposition 18, while Proposition 25 reformulates this characterization in terms of a simple number theoretic condition.

1 Introduction

Given a system of polynomial equations $f_i(x_1, \ldots, x_n) = 0$, our instinct is to describe the solution set, i.e. the set of points $(p_1, \ldots, p_n) \in \mathbf{C}^n$ that satisfy the system of equations. But we can also reverse the situation and ask the following question: Given a subset S of $\mathbf{C}^n$, what does the set I of polynomials that vanish on S look like? This thesis is concerned with the case where S is a finite set of points. Moreover, we do not consider just any finite sets, but only those that have an underlying symmetry in their arrangement. We impose this symmetry by taking our point sets to be group orbits, and in particular, we consider abelian and metacyclic groups. Now, there are many ways to describe the set of polynomials, and we will be concerned with a very coarse one, namely the Hilbert function. Basically, the Hilbert function tells us how many polynomials of each degree vanish on S. Since S is a group orbit, it has a certain structural symmetry that we expect to find expressed in the set of polynomials I. Thus, we should be able to inspect the group to obtain information about I. In the case where we take our group to be abelian, I turns out to be a *lattice ideal*. These ideals are associated with toric varieties and integer programming, and much is known about them (cf. [1],[12]). The case of the symmetric group S_n (the group of permutations on n letters) is dealt with in [8], where the ideal I and its Hilbert function are determined via Gröbner basis methods. Finally, if the group is metacyclic, then I is actually the intersection of several lattice ideals. Thus, the part of our study that deals with abelian groups is really a description of certain lattice ideals, while the part on metacyclic groups is concerned with the behavior of lattice ideals under intersection.

The thesis is divided as follows: In Section 2 we introduce the notion of a group representation and prove some results on irreducible representations of abelian groups. We also define metacyclic groups and determine their irreducible representations. In Section 3 we introduce ideals of group orbits and define the Hilbert function which will be our main object of study. Section 4 deals with the Hilbert functions that arise from orbit ideals of two-dimensional representations of abelian groups generated by two elements. We state Conjecture 16 and show that it provides necessary conditions for a sequence of positive integers to be such a Hilbert function. In Section 5 we apply Theorem 13 (which describes the Hilbert function of abelian group orbits) to the case of cyclic groups, thereby motivating a generalization to metacyclic groups. Section 6 comprises the bulk of this thesis. In Proposition 18 we provide an upper bound for the Hilbert function of the orbit ideal of an induced representation of a metacyclic group. We then look at two-dimensional representations and formulate a description of the Hilbert function in this case (Proposition 21). Next, we consider three-dimensional representations and offer a conjecture (Conjecture 24) as to when these representations fail to achieve the bound in Proposition 18. Finally, we relate the results on metacyclic groups to the Molien series and provide a discussion of how these results might be generalized.

2 Representations of Metacyclic Groups

Let G be a finite group. A *representation* of G on a finite-dimensional complex vector space V is a homomorphism $\phi : G \to GL(V)$, from G into the group of invertible linear transformations on V. In particular, if $V = \mathbf{C}^n$, then the image of G is a group of $n \times n$ matrices. In practice, we will usually suppress reference to ϕ, instead calling V the representation, and we will simply think of G itself as acting on V. Thus instead of $\phi(g)(v)$ we will write gv to denote the image of an element of V under $\phi(g)$.

By a *subrepresentation* of V we mean a vector subspace $W \subset V$ such that W is invariant under the action of G. We say that V is *irreducible* if it contains no proper nonzero subrepresentations. This notion of irreducibility is important because of the following proposition, which can be found in any text on representation theory (e.g. [9]):

Proposition 1 (Complete Reducibility) *Any representation is a direct sum*[1] *of irreducible representations.*

This says that the irreducible representations of a group are the basic building blocks out of which all other representations of that group are constructed. Accordingly, the remainder of this section will be devoted to determining the irreducible representations of metacyclic groups, which we define momentarily. But first we will develop some results concerning irreducible representations of abelian groups. These results are necessary for our work on metacyclic groups, and will also be needed in Section 4.

[1] If V and W are representations of G, then $V \oplus W$ is a representation in the obvious way: $g(v \oplus w) = (gv) \oplus (gw)$.

Irreducible representations of abelian groups

We begin with a basic result:

Lemma 2 (Schur's Lemma) *Let V and W be irreducible representations of a finite group G. If $\phi : V \to W$ is a G-module homomorphism*[2] *then*

1. *Either ϕ is an isomorphism or $\phi = 0$;*
2. *If $V = W$, then $\phi = \lambda I$ for some $\lambda \in \mathbf{C}$.*

Proof: It is easily seen that $\ker(\phi)$ and $\mathrm{im}(\phi)$ are invariant subspaces of V and W respectively. It follows from the irreducibility of V and W that either $\ker(\phi) = 0$ and $\mathrm{im}(\phi) = W$ (in which case ϕ is an isomorphism) or $\ker(\phi) = V$ and $\mathrm{im}(\phi) = 0$ (in which case $\phi = 0$). This proves (1).

Now suppose $V = W$. Then since we are working over $\mathbf{C}$, the characteristic polynomial for ϕ has a root $\lambda \in \mathbf{C}$, which means that λ is an eigenvalue for ϕ. Thus the linear transformation $\phi - \lambda I$ has a nonzero kernel, so that by (1) we have $\phi - \lambda I = 0$. Thus $\phi = \lambda I$. □

Using this lemma we obtain the following nice result:

Proposition 3 *All irreducible representations of a finite abelian group G are one-dimensional.*

Proof: Let V be an irreducible representation of G. Now each g in G acts as a linear map on V, and since G is abelian, these maps are G-linear. Thus we may apply Schur's lemma to conclude that each g acts by some scalar multiple of the identity. But then every subspace of V is G-invariant, which implies that V is one-dimensional. □

This shows that the irreducible representations of an abelian group G are simply homomorphisms $\varphi : G \to \mathbf{C}^*$, from G into the multiplicative group of complex numbers. G is finite, so the homomorphic image $\varphi(G)$ must be a finite subgroup of the unit circle. These irreducible representations are given by the *characters* of G:

Definition 4 *If V is a representation of a finite group G, its* character *is the function $\chi_V : G \to \mathbf{C}$ given by*

$$\chi_V(g) = Tr(g|_V) \quad \forall g \in G. \tag{2.1}$$

[2] A G-module homomorphism $\rho : V \to W$ is a linear map from V to W that is G-linear: $\rho(gv) = g\rho(v)$ $\forall g \in G, v \in V$.

That is, $\chi_V(g)$ is the trace of g as a linear operator on V. Note that if $\varphi : G \to \mathbf{C}^*$ is an irreducible representation of a finite abelian group G, then $\chi_V(g) = Tr(\varphi(g)) = \varphi(g)$, so that the characters are simply the irreducible representations.

By the Fundamental Theorem of Finite Abelian Groups, every finite abelian group can be written as $G = \prod_{i=1}^{t} \mathbf{Z}/n_i\mathbf{Z}$ for some $n_i \in \mathbf{Z}$, where $n_1|n_2|\dots|n_t$. Then for each group element $a = (a_1, \dots, a_t)$, we define a character $\chi_a : \prod_{i=1}^{t} \mathbf{Z}/n_i\mathbf{Z} \to \mathbf{C}^*$ as follows:

$$\chi_a(g_1, \dots, g_t) = \prod_{j=1}^{t} \exp(2\pi i a_j g_j / n_j). \tag{2.2}$$

Thus each element of G corresponds with a character, and hence with an irreducible representation of G.

Irreducible representations of metacyclic groups

Definition 5 *A metacyclic group is a group G containing a normal cyclic subgroup A such that G/A is also cyclic.*

Perhaps the best known examples of metacyclic groups are the dihedral groups, D_{2n}. In this case the cyclic subgroup has order n, and the quotient group has order 2.

Now suppose that G is metacyclic, the cyclic subgroup $A = \langle a \rangle$ has order m, and $G/A = \langle bA \rangle$ has order s. Since A is normal, the inner automorphism of G induced by b restricts to an automorphism of A. Therefore

$$b^{-1}ab = a^r \qquad \text{for some } r \text{ such that } (r, m) = 1. \tag{2.3}$$

The fact that r is relatively prime to m is necessary for $\sigma : a^i \mapsto b^{-1}a^i b$ to be an automorphism. Let u be the order of σ. Then since the powers of σ are given by

$$\sigma^k(a) = b^{-k}ab^k = a^{r^k}, \tag{2.4}$$

we have

$$\begin{cases} r^k - 1 \not\equiv 0 \quad (m), & 1 \le k \le u-1, \\ r^u - 1 \equiv 0 \quad (m). \end{cases} \tag{2.5}$$

Since σ^s is the identity (because $b^s \in A$), it follows that $u|s$, so that $r^s - 1 \equiv 0 \quad (m)$. Letting t be the smallest non-negative integer such that $b^s = a^t$, we also find that

$$a^{rt} = (b^{-1}ab)^t = b^{-1}a^t b = b^{-1}b^s b = b^s = a^t \tag{2.6}$$

so $a^{t(r-1)} = 1$ which implies that $m|t(r-1)$.

In summary, the generators a and b of the metacyclic group G satisfy the following relations:

$$a^m = 1, \quad b^{-1}ab = a^r, \quad (r, m) = 1, \quad b^s = a^t, \quad m|t(r-1), \quad m|r^s - 1. \tag{2.7}$$

The converse is also true: given the relations above, there exists a metacyclic group G of order ms with generators a, b. To see this, simply take G to be the matrix group generated by the elements $T_1^G(a), T_1^G(b)$ defined below in (2.13) and (2.11) respectively. As we will see, this group is metacyclic, and it is easy to show that it has the correct order.

Our strategy in determining the irreducible representations of the metacyclic group G will be to first identify the irreducible representations of A (which are all one-dimensional since A is cyclic and thus abelian). Then we will use these one-dimensional representations to induce representations of the whole group G. We begin by noting that A has m non-isomorphic one-dimensional representations, one for each mth root of unity. Calling these representations T_i, they are defined as follows: $T_i(a) = \omega^i$ for each $i = 1, \ldots, m$, where ω is a primitive mth root of unity. Denote the underlying vector space for T_i by $L_i = \mathbf{C}l_i$, where we have chosen a basis l_i for each L_i. In the language of modules, T_i turns L_i into a $\mathbf{C}A$-module, where $\mathbf{C}A$ is the group algebra. We will now use each one-dimensional module L_i to construct a representation T_i^G of the whole group G.

The underlying vector space for this new representation will be $\mathbf{C}G \otimes_{\mathbf{C}A} L_i$. We turn this into a $\mathbf{C}G$-module by defining the action of G:

$$g(x \otimes l_i) := (gx) \otimes l_i \qquad \forall g, x \in G. \tag{2.8}$$

Finally, T_i^G is the representation corresponding to this action. In order to get a better idea of what this representation looks like, we choose the following basis of $\mathbf{C}G \otimes_{\mathbf{C}A} L_i$: $\{1 \otimes l_i, b \otimes l_i, \ldots, b^{s-1} \otimes l_i\}$. Then

$$b(b^k \otimes l_i) = b^{k+1} \otimes l_i \qquad 0 \leq k \leq s-2, \tag{2.9}$$

$$b(b^{s-1} \otimes l_i) = b^s \otimes l_i = a^t \otimes l_i = 1 \otimes a^t l_i = 1 \otimes \omega^{it} l_i = \omega^{it}(1 \otimes l_i). \tag{2.10}$$

So the matrix of $T_i^G(b)$ with respect to the basis above is

$$T_i^G(b) = \begin{bmatrix} 0 & 0 & \dots & 0 & \omega^{it} \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 \end{bmatrix}. \tag{2.11}$$

Similarly, using the relation $b^{-k}ab^k = a^{r^k}$ we find that

$$a(b^k \otimes l_i) = b^k a^{r^k} \otimes l_i = b^k \otimes a^{r^k} l_i = b^k \otimes \omega^{ir^k} l_i = \omega^{ir^k}(b^k \otimes l_i). \tag{2.12}$$

So the matrix of $T_i^G(a)$ with respect to this basis is

$$T_i^G(a) = \begin{bmatrix} \omega^i & 0 & 0 & \dots & 0 \\ 0 & \omega^{ir} & 0 & \dots & 0 \\ 0 & 0 & \omega^{ir^2} & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & \omega^{ir^{s-1}} \end{bmatrix}. \tag{2.13}$$

We now quote several results from [5] concerning the irreducibility of these induced representations T_i^G.

Proposition 6 *T_i^G is irreducible if and only if $r^j i \not\equiv i \ (m), \quad 1 \le j \le s-1$.*

Proposition 7 *Let T_i^G and T_k^G be irreducible. Then T_i^G and T_k^G are non-isomorphic if and only if we have $r^j i \not\equiv k \ (m), \quad 1 \le j \le s-1$.*

Theorem 8 *Every irreducible matrix representation of a metacyclic group G is either one-dimensional or isomorphic to one of the induced representations T_i^G, $1 \le i \le m$, if and only if, for each i and j, $1 \le i \le m, 1 \le j \le s-1$,*

$$r^j i \equiv i \ (m) \Longrightarrow \ ri \equiv i \ (m).$$

Corollary *Suppose that G is a metacyclic group with generators a and b satisfying the relations in (2.7), and moreover that s is prime. Then all the irreducible matrix representations of G are either one-dimensional or one of the induced representations T_i^G.*

Using the concepts from the next section, we can rephrase these results as follows. Proposition 6 says that T_i^G is irreducible if and only if the orbit of i in $\mathbf{Z}/m\mathbf{Z}$ under $\langle r \rangle$

has size s. In other words, T_i^G is irreducible if and only if the diagonal elements of $T_i^G(a)$ are distinct. Similarly, Proposition 7 says that T_i^G and T_k^G are non-isomorphic if and only if $Orb_{\langle r\rangle}(i)$ and $Orb_{\langle r\rangle}(k)$ are disjoint, i.e. if and only if the diagonal elements of $T_i^G(a)$ and $T_k^G(a)$ are not the same[3]. Finally, Theorem 8 states that every irreducible representation of G is either one-dimensional or one of the T_i^G if and only if $|Orb_{\langle r\rangle}(i)| \in \{1, s\}$ for $1 \leq i \leq m$. The Corollary follows since the size of each orbit must divide s.

3 Ideals of Group Orbits

Suppose that G is a finite group and fix a representation of it on $\mathbf{C}^n$. Choosing a point $p \in \mathbf{C}^n$, we make the following definitions:

Definition 9 *The* orbit *of p under G, denoted $Orb_G(p)$, is $\{gp \mid g \in G\}$.*

Note that the orbit of p depends not only on G, but on the particular representation being used. In practice, however, we simply write $Orb(p)$, leaving the group in question and its representation to be inferred from the context.

Definition 10 *The* ideal *of Orb(p) is $\{f \in \mathbf{C}[x_1, \ldots, x_n] \mid f(Orb(p)) = 0\}$ and is denoted by $I(Orb(p))$.*

It is easy to see that the set defined in Definition 10 is in fact an ideal in the polynomial ring $\mathbf{C}[x_1, \ldots, x_n]$. The bulk of this thesis is devoted to describing the ideals of metacyclic group orbits. Of course, a complete description of the ideal would be afforded by explicitly characterizing the polynomials belonging to the ideal, or by finding a finite set of generators for the ideal. (We know that a finite generating set exists since any finitely generated polynomial ring over a field is Noetherian, and hence all ideals in a such a ring are finitely generated.) But we can obtain a coarser description of the ideal by means of the (affine) Hilbert function of the associated coordinate ring $S := \mathbf{C}[x_1, \ldots, x_n]/I$. Let $S_{\leq d} := \mathbf{C}[x_1, \ldots, x_n]_{\leq d}/I_{\leq d}$, where the subscript "$\leq d$" denotes restriction to degree at most d.

Definition 11 *The* (affine) Hilbert function *of S is the function $H : \mathbf{N} \to \mathbf{N}$ defined by*

$$H_S(d) = \dim_{\mathbf{C}} S_{\leq d} = \dim_{\mathbf{C}} \mathbf{C}[x_1, \ldots, x_n]_{\leq d} - \dim_{\mathbf{C}} I_{\leq d}. \tag{3.1}$$

[3] It is easy to see that the two orbits are either identical or disjoint.

Thus if $I = I(Orb(p))$, then the dth value of the Hilbert function defined above is the codimension in $\mathbf{C}[x_1, \ldots, x_n]_{\leq d}$ of the subspace of polynomials of degree at most d which vanish on the orbit of p. Since $\dim_{\mathbf{C}} \mathbf{C}[x_1, \ldots, x_n]_{\leq d} = \binom{n+d}{d}$, knowing the Hilbert function of S is equivalent to knowing the dimension of $I_{\leq d}$ for all $d \geq 0$. We thus often refer to H_S as the Hilbert function of I.

Proposition 12 *For all d sufficiently large, the Hilbert function of I is given by a polynomial in d (cf. [4]).*

By definition, the degree of the polynomial in Proposition 12 is the dimension of $\mathcal{V}(I)$, the affine algebraic variety[4] defined by I. Since finite group orbits are zero-dimensional algebraic varieties, the Hilbert function of the ideal of such an orbit is eventually constant. It turns out that this constant value is the number of points in the orbit (see [7]), which is just the order of the group G if we require that the action of G is faithful and choose a generic[5] point p.

4 Two-Dimensional Representations of Abelian Groups

Recall from Section 2 that every m-dimensional representation of a finite abelian group $G = \prod_{i=1}^{t} \mathbf{Z}/n_i\mathbf{Z}$ is equivalent to a representation of the form

$$g \mapsto \begin{bmatrix} \chi_{a_1}(g) & 0 & \ldots & 0 \\ 0 & \chi_{a_2}(g) & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & \chi_{a_m}(g) \end{bmatrix}$$

where $a_i = (a_{i1}, \ldots, a_{it}) \in G$ and χ_{a_i} is the character of G corresponding to the group element a_i. We have the following theorem:

Theorem 13 (Glassbrenner, Perkinson) *The Hilbert function of the ideal of the orbit of a generic point $p \in \mathbf{C}^m$ under the above representation of G is*

$$H(d) = \# \left\{ \sum_{i=1}^{m} e_i a_i \in G \,|\, e_i \geq 0 \textit{ for } i = 1, \ldots, m \textit{ and } \sum_{i=1}^{m} e_i \leq d \right\}.$$

[4] The *affine algebraic variety defined by an ideal I* is the zero set in $\mathbf{C}^n$ of the polynomials in I. Since I is finitely generated, this zero set is actually just the solution set of a finite system of polynomial equations.

[5] A point p is *generic* if the values of the Hilbert function do not vary when p is perturbed. The Hilbert function is the same for all generic points.

Furthermore, $I(Orb(p)) = \langle x^e - x^{e'} \,|\, \chi_{e\cdot a} = \chi_{e'\cdot a}\rangle$*, where* $x^e := x_1^{e_1} \dots x_m^{e_m}$ *for* $e \in \mathbf{N}^m$ *and* $a := (a_1, \dots, a_m)$*.*

This theorem is proved in [2] by looking at the ranks of certain matrices whose columns are the characters of G. In that thesis, Campbell examines the case of two-dimensional representations of finite abelian groups generated by two elements a and b. He shows that such a group can be written as $G = \mathbf{Z}/n_1\mathbf{Z} \times \mathbf{Z}/n_2\mathbf{Z}$ with $n_1|n_2$, and then gives a geometric interpretation of the Hilbert function described in Theorem 13. In effect, he provides an algorithm for constructing an L-shaped region from a given two-dimensional representation of G. This construction proceeds as follows. First define a homomorphism $\varphi : \mathbf{Z}^2 \to G$ by $\varphi(u, v) = ua + vb$. Then define an order $\prec$ on $\mathbf{Z}^2_{\geq 0}$:

$$(u, v) \prec (u', v') \iff u + v < u' + v' \text{ or } u + v = u' + v' \text{ and } v < v'. \tag{4.1}$$

Finally, define the *region* R for (G, a, b) using the following algorithm:

1. Set $R = \mathbf{Z}^2_{\geq 0}$.
2. Choose the smallest $(u, v) \in R$ (according to $\prec$) such that $\exists\, (u', v') \in R$ with $(u', v') \prec (u, v)$ and $\varphi(u, v) = \varphi(u', v')$.
3. Remove $(u + m, v + n)$ from R for all $m, n \geq 0$.
4. Repeat 2 if possible.

Campbell then proves that φ restricted to the region R thus produced is a bijection onto the group G. We illustrate this construction with the following example.

Example 14 Consider the two-dimensional representation of $\mathbf{Z}/12\mathbf{Z}$ corresponding to the generators $a = 5, b = 2$. At each point of $\mathbf{Z}^2_{\geq 0}$ we place the value of φ at that point:

0	5	10	3	8	1	6	11	4	9	2	7	0
10	3	8	1	6	11	4	9	2	7	0	5	10
8	1	6	11	4	9	2	7	0	5	10	3	8
6	11	4	9	2	7	0	5	10	3	8	1	6
4	9	2	7	0	5	10	3	8	1	6	11	4
2	7	0	5	10	3	8	1	6	11	4	9	2
0	5	10	3	8	1	6	11	4	9	2	7	0

The region R for $(\mathbf{Z}/12\mathbf{Z}, 5, 2)$ is the boxed portion above. It was produced by starting at the lower left corner (at $(0,0)$), and proceeding along successive diagonals (from $(d,0)$ to $(0,d)$ for the dth diagonal). Whenever a group element is encountered for the second time, that point is removed along with all of the points above and to the right of it. □

Definition 15 *A point $(u,v) \in \mathbf{Z}^2_{\geq 0} \backslash R$ is a* boundary point *for R, if for all $(m,n) \in \mathbf{Z}^2_{\geq 0} \backslash \{(0,0)\}$, $(u-m, v-n) \in \mathbf{Z}^2_{\geq 0} \Longrightarrow (u-m, v-n) \in R$.*

In Example 14, the boundary points are $(6,0), (2,1)$ and $(0,4)$. Campbell observes that a region has at most three boundary points[6], and that it is determined by them. Thus, the L-shape that appeared in our example was no accident: all regions are L-shaped (or rectangular, which we think of as a degenerate L).

Let H be the Hilbert function for the ideal of the orbit of the two-dimensional representation of G obtained from the characters χ_a and χ_b. Then the region R for (G, a, b) gives a geometric interpretation of H. Namely, the dth diagonal in R (taken from $(d,0)$ to $(0,d)$) corresponds to the linear combinations $e_1 a + e_2 b$ with $e_1 + e_2 = d$. But these are exactly the linear combinations being counted in Theorem 13. Thus $H(d)$ is the number of elements in diagonals 0 through d of R. The Hilbert function of the representation in Example 14 is then $H = 1, 3, 6, 9, 11, 12, 12, \ldots$.

The problem that we would like to solve is to give an explicit characterization of the Hilbert functions that arise from two-dimensional representations of finite abelian groups generated by two elements. Given the correspondence between Hilbert functions and regions, one would hope that the consideration of these regions would shed light upon which Hilbert functions are possible. This line of thought leads to the following conjecture.

Conjecture 16 *The Hilbert functions that arise from two-dimensional representations of finite abelian groups generated by two elements are precisely those with a first difference[7] of the form:*

$$\Delta H = 1, 2, \ldots, \overbrace{n, \ldots, n}^{c}, m_1, \ldots, m_k \tag{4.2}$$

with $n, c \geq 1$, and such that the m_i satisfy the following conditions:

[6] This fact is easily seen by a translation argument of the type described in the proof of condition 1 of Conjecture 16 below.

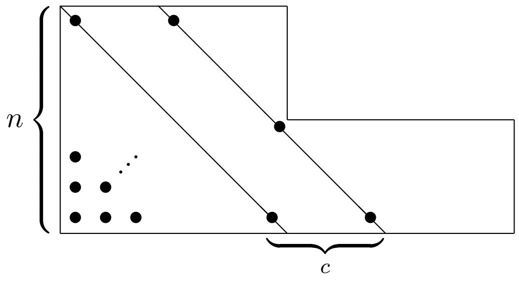
[7] $\Delta H(d) := H(d) - H(d-1)$, and we define $\Delta H(0) = 1$. Note that we only list the nonzero values of ΔH.

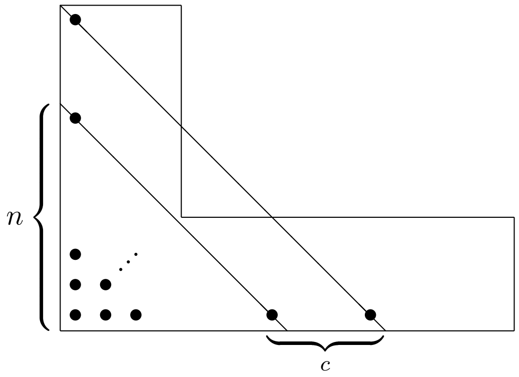
1. *$n > m_1 > m_2 > \ldots > m_k \geq 1$;*

2. *$m_k = 1$ or 2;*

3. *the first difference of the* tail sequence *$\{n, m_1, m_2, \ldots, m_k\}$ must have the form*[8] *$\{\overbrace{-1,\ldots,-1}^{p}, \overbrace{-2,\ldots,-2}^{q}, \overbrace{-1,\ldots,-1}^{r}\}$ where $p+q+r = k+1$ and $p, q, r \geq 0$.*

First of all, note that a region's L-shape immediately implies that every possible Hilbert function has a first difference of the form given in equation (4.2) with the tail sequence $n, m_1, \ldots, m_k$ decreasing (but not yet strictly decreasing). This is because $\Delta H(d)$ is the number of elements in the dth diagonal of R. It is therefore clear from consideration of the L-shapes[9] below that ΔH must increase strictly for awhile, then level off for awhile, and finally start decreasing again, eventually reaching zero. (Of course, "awhile" here may in fact be only one step, so we must include the possibility that n or c may be 1.)





[8] We include the difference $0 - m_k = -m_k$ as the last value of this first difference.

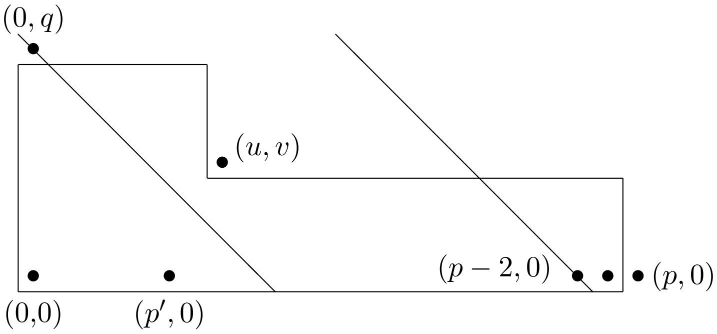
[9] These are actually the only two types of L-shapes that need be considered: either the diagonals cross the "middle" boundary point first, or they cross an "end" boundary point first. If the diagonals cross both types of boundary point at the same time, then $c = 1$, and the two diagrams coincide.

Moreover, it is clear that the tail sequence can level out at most once, and otherwise has to decrease strictly. Thus it has the form

$$n > m_1 > \cdots > m_i = m_{i+1} = \cdots = m_{i+j} > m_{i+j+1} > \cdots > m_k$$

for some $i = 1, \ldots, k$, and $j = 0, \ldots, k-i$. We say that the tail sequence has a *plateau* if $j > 0$. Now our tail sequence can only have a plateau if one leg of the corresponding L-shaped region is sufficiently longer than the other. Thus in order to prove the necessity of condition 1 in Conjecture 16, we will prove that the tail sequence has no plateau by showing that one leg of a region can't be too much longer than the other.

Proof of the necessity of condition 1: Suppose we have a region R that corresponds to a Hilbert function whose tail sequence has a plateau:



Then the diagonal through $(p-2,0)$ must not intersect the other leg. The equation of this diagonal is:

$$y = -x + p - 2. \tag{4.3}$$

Then the y-coordinate of this diagonal must be at least q at $x = u - 1$:

$$-(u-1) + p - 2 \geq q \Longrightarrow p \geq q + u + 1. \tag{4.4}$$

Thus $p > u + q$. Now since the point $(0,q)$ was removed as R was constructed, it follows that there is a point (p',q') in R such that $(p',q') \prec (0,q)$ and $\varphi(p',q') = \varphi(0,q)$. This point (p',q') must be on or under the diagonal through $(0,q)$, and in fact it must be on the lower edge of R $(q' = 0)$. For if $q' > 0$, then

$$\begin{aligned} \varphi(0,q-1) &= \varphi(0,q) - \varphi(0,-1) \quad \text{since } \varphi \text{ is a homomorphism} \\ &= \varphi(p',q') - \varphi(0,-1) \\ &= \varphi(p',q'-1). \end{aligned}$$

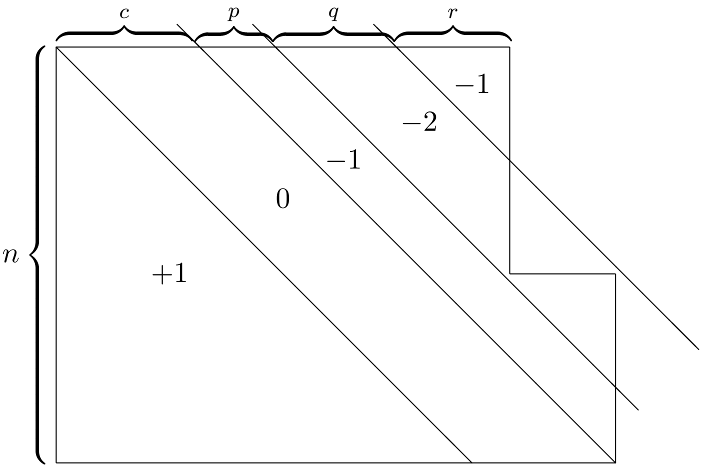
But this contradicts the fact that φ is a bijection from R onto the group, since both $(0, q-1)$ and $(p', q'-1)$ are in the region. Thus $q' = 0$. This argument can be summarized geometrically: if two points in $\mathbf{Z}^2$ are preimages under φ of the same group element, let w be the vector pointing from one to the other. Then any two elements separated by w in $\mathbf{Z}^2$ correspond to the same group element under φ. It is easy to see by this translation argument that (u, v) corresponds to the same group element as $(0, 0)$, namely the identity. Thus any two elements in R separated by a linear combination of the vectors (u, v) and $(p', -q)$ correspond to the same group element. Since R is in bijection with the group, the existence of two such elements will be a contradiction. I claim that $(u+p', 0)$ and $(0, q-v)$ are two such elements. Since $p > u + q$, and $p' \leq q$, they are both in R. Moreover:

$$\begin{aligned}(u+p', 0) - (0, q-v) &= (u+p', v-q) \\ &= (u, v) + (p', -q).\end{aligned}$$

This contradiction shows that a region cannot have one leg long enough to yield a plateau in the corresponding Hilbert function. This proves the necessity of condition 1. □

Condition 2 of Conjecture 16 is easily seen to be necessary: m_k is the number of elements in the last diagonal intersecting the region. But this last diagonal either just catches the upper right corner of one leg (in which case m_k=1), or it catches the corners of both legs (in which case $m_k = 2$).

In order to show the necessity of condition 3, examine the following generic region:



The diagonals drawn above serve to distinguish the several different *second difference regimes* of the region[10]. The number displayed in each regime is the value of $\Delta^2 H(d)$ for all d indexing diagonals in the regime (including the upper boundary diagonal of the regime). Moreover it is easy to convince yourself that these are the only possible regimes for a region (remember that condition 1 rules out a second regime with second difference 0). This establishes the necessity of condition 3.

Note that by starting in the upper right hand corner of the vertical leg, we can construct an L-shape with regimes of length p, q, r, for any choice of $p, q, r \geq 0$, as long as at least one of p, q, r is nonzero. Then since (in the notation of Conjecture 16) $p+2q+r = n$, all that is left is to choose c, and then the sequence corresponding to the constructed L-shape is determined. Thus there is a correspondence between sequences allowed by the conjecture and four-tuples of integers (p, q, r, c) where $p, q, r \geq 0$, $p+q+r = k+1 \geq 1$ and $c \geq 1$. The correspondence is not well defined if $q = 0$, however, because $(p, 0, r, c)$ yields the same sequence as $(\alpha, 0, \beta, c)$ for all $\alpha, \beta \geq 0$ such that $\alpha + \beta = p + r$. We remedy this ambiguity by always choosing the four-tuple of the form $(p, 0, 0, c)$. Thus we have a one-to-one correspondence between allowed sequences and four-tuples in $\mathcal{S}$, where

$$\mathcal{S} := \left\{(p, q, r, c) \in \mathbf{Z}^4_{\geq 0} \mid c \geq 1, p+q+r \geq 1, \text{and } r = 0 \text{ if } q = 0\right\}. \tag{4.5}$$

Given $(p, q, r, c) \in \mathcal{S}$, we know immediately what the first difference of the corresponding allowed sequence H looks like. But we would like to know the total number of points N in the orbit, i.e. the sum of the first differences of H:

$$\begin{aligned} N &= \sum_{d=0}^{\infty} \Delta H(d) = 1 + 2 + \cdots + (n-1) + cn + m_1 + m_2 + \cdots + m_k \\ &= \frac{n(n-1)}{2} + cn + (1 + \cdots + r) + [(r+2) + (r+4) + \cdots + (r+2q)] \\ &\quad + [(r+2q+1) + (r+2q+2) + \cdots + (r+2q+p-1)] \\ &= \frac{1}{2}(p+2q+r)(p+2q+r-1) + c(p+2q+r) + \frac{r(r+1)}{2} + qr \\ &\quad + q(q+1) + (p-1)(r+2q) + \frac{p(p-1)}{2} \\ &= p^2 + 3q^2 + r^2 + 4pq + 2pr + 3qr + (c-1)(p+2q+r). \end{aligned} \tag{4.6}$$

We can now reformulate our conjecture:

[10] The other type of region (where the diagonal first crosses a “middle” boundary point) yields the same second difference regimes.

Reformulation of Conjecture 16 *The Hilbert functions arising from two-dimensional faithful representations of abelian groups of order N generated by two elements correspond to the solutions $(p, q, r, c) \in \mathcal{S}$ of the polynomial equation (4.6).*

We have shown that the conjecture provides necessary conditions for an increasing (but eventually constant) sequence of positive integers to be the Hilbert function for a two-dimensional representation of an abelian group generated by two elements. In order to show sufficiency, we would like to start with a sequence $(p, q, r, c) \in \mathcal{S}$ and work backwards to find an abelian group generated by two elements whose representation has the Hilbert function (p, q, r, c). We begin with the case $q = 0$.

Given a sequence $(p, 0, 0, c)\in \mathcal{S}$, we need to find a two-dimensional representation of an abelian group of order $N = p^2 + p(c - 1)$. We claim that the representation of $\mathbf{Z}/N\mathbf{Z}$ obtained by choosing the generators $a = p$, $b = 1$ has $(p, 0, 0, c)$ as its Hilbert function. The region R for $(\mathbf{Z}/N\mathbf{Z}, 1, p)$ is a rectangle of height p and width $(p + c - 1)$:

$$\begin{array}{|cccc|}
\hline
p-1 & 2p-1 & \cdots & p^2+p(c-1)-1 \\
p-2 & 2p-2 & \cdots & p^2+p(c-1)-2 \\
\vdots & \vdots & \cdots & \vdots \\
2 & p+2 & \cdots & p^2+p(c-2)+2 \\
1 & p+1 & \cdots & p^2+p(c-2)+1 \\
0 & p & \cdots & p^2+p(c-2) \\
\hline
\end{array}$$

Thus we have

$$\Delta H = 1, 2, \ldots, \overbrace{p, \ldots, p}^{c}, p - 1, p - 2, \ldots, 1.$$

This sequence is just $(p, 0, 0, c)$.

Note that sequences in $\mathcal{S}$ have a symmetric first difference if and only if $q = 0$. Since the ideals we are concerned with have a Hilbert function with symmetric first difference if and only if they are gorenstein (cf. [6], [10]), we have shown that the sequences in $\mathcal{S}$ with $q = 0$ correspond to gorenstein ideals.

Now suppose that we are given a sequence $(p, 1, r, c) \in \mathcal{S}$. Then we are searching for a group of order

$$\begin{aligned}
N &= p^2 + r^2 + 2pr + 4p + 3r + 3 + (c - 1)(p + 2 + r) \\
&= (p + r + 2)(p + r + c + 1) - r - 1.
\end{aligned}$$

The representation of $\mathbf{Z}/N\mathbf{Z}$ obtained by choosing $a = p+r+2$, $b = 1$ yields the desired Hilbert function. This is because the region R is then the rectangle of height $(p+r+2)$

and width $(p+r+c+1)$ with a strip of width 1 and length $r+1$ removed from the right side:

$p+r+1$	$2(p+r)+3$	$\cdots$	$P+p+r+1$
$p+r$	$2(p+r)+2$	$\cdots$	$P+p+r$
$\vdots$	$\vdots$	$\cdots$	$\vdots$
p	$2p+r+2$	$\cdots$	$P+p$
$\vdots$	$\vdots$	$\cdots$	$\vdots$
1	$p+r+3$	$\cdots$	$P+1$
0	$p+r+2$	$\cdots$	P

$(P := (p+r+2)(p+r+c))$

We then have:

$$\Delta H = 1, \ldots, \overbrace{p+2+r, \ldots, p+2+r}^{c}, p+2+r-1, \ldots, 2+r, r, r-1, \ldots, 1,$$

which is $(p, 1, r, c)$.

For larger values of q, it is unclear how to construct the desired representation. Certainly not all sequences can be achieved using cyclic groups. For example, the sequence with first difference $\Delta H = 1, 2, 3, 4, 2$ (which corresponds to $(p, q, r, c) = (0, 2, 0, 1)$) cannot be obtained with $\mathbf{Z}/12\mathbf{Z}$, but it is the first difference of the Hilbert function of the representation of $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/6\mathbf{Z}$ with $(a, b) = ((0, 1), (1, 5))$.

5 Cyclic Groups

Fix an arbitrary diagonalized n-dimensional representation of $\mathbf{Z}/m\mathbf{Z}$. This representation has the form

$$g \mapsto \begin{bmatrix} \omega^{a_1 g} & 0 & \ldots & 0 \\ 0 & \omega^{a_2 g} & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & \omega^{a_n g} \end{bmatrix} \tag{5.1}$$

for some $a_i \in \{1, \ldots, m\}$, where $\omega = e^{\frac{2\pi i}{m}}$. Theorem 13 says that the dth value of the Hilbert function of the orbit ideal of this representation is the number of elements of $\mathbf{Z}/m\mathbf{Z}$ obtainable by adding together at most d of the a_i with repetition allowed. In an effort to understand what the theorem is counting and why it is true, we define an action of $\mathbf{Z}/m\mathbf{Z}$ on the polynomial ring $R := \mathbf{C}[x_1, \ldots, x_n]$.

Definition 17 *Let G be a finite group, and fix a representation of it on $\mathbf{C}^n$. We define a representation of G on $R := \mathbf{C}[x_1, \ldots, x_n]$ by composition:*

$$gF := F \circ g \quad \forall g \in G, F \in R. \tag{5.2}$$

In terms of this action, the dth value of the Hilbert function for $I(Orb_G(p))$ is the codimension in $R_{\leq d}$ of

$$\{F \in R_{\leq d} \,|\, gF(p) = 0 \quad \forall g \in G\}.$$

Let τ be the image of $1 \in \mathbf{Z}/m\mathbf{Z}$ under the representation given in (5.1). Since the action of τ on $\mathbf{C}^n$ is diagonalized, it is also diagonalized on R_1, so that x_i is an eigenvector for τ with eigenvalue ω^{a_i} for $i = 1, \ldots, n$. Define the eigenspace

$$R_{\leq d}(\omega^j) = \{F \in R_{\leq d} \,|\, \tau F = \omega^j F\}. \tag{5.3}$$

Then $R_{\leq d} = \bigoplus_{j=0}^{m-1} R_{\leq d}(\omega^j)$, and we can write any $F \in R_{\leq d}$ uniquely as $F = \sum_{j=0}^{m-1} F_j$ with $F_j \in R_{\leq d}(\omega^j)$. The condition that F vanish on the orbit of a generic point $p \in \mathbf{C}^n$ is that $0 = F(\tau^j(p)) = (\tau^j F)(p)$ for $j = 0, \ldots, m-1$. We can write these m conditions as one matrix condition:

$$\begin{bmatrix} 1 & 1 & 1 & 1 & \ldots & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \ldots & \omega^{m-1} \\ 1 & \omega^2 & (\omega^2)^2 & (\omega^2)^3 & \ldots & (\omega^2)^{m-1} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{m-1} & (\omega^{m-1})^2 & (\omega^{m-1})^3 & \ldots & (\omega^{m-1})^{m-1} \end{bmatrix} \begin{bmatrix} F_0(p) \\ F_1(p) \\ F_2(p) \\ \vdots \\ F_{m-1}(p) \end{bmatrix} = 0. \tag{5.4}$$

This is a Vandermonde matrix and is thus nonsingular. What this means is that F vanishes on the orbit of p under τ if and only if $F_j(p) = 0$ for $j = 0, \ldots, m-1$. This places one condition on each non-trivial eigenspace of $R_{\leq d}$. Since the dth value of the Hilbert function is the number of independent vanishing conditions on the polynomials of degree less than or equal to d, this analysis shows that

$$H(d) = \text{the number of nontrivial eigenspaces for } \tau \text{ in } R_{\leq d}.$$

To see how this result is just a restatement of the theorem on abelian groups, note that the eigenvalues for τ (the mth roots of unity) are in obvious one-to-one correspondence with the elements of $\mathbf{Z}/m\mathbf{Z}$. When we multiply polynomial eigenvectors together we obtain a new eigenvector with eigenvalue equal to the product of the old eigenvalues. But multiplying mth roots of unity corresponds to adding the exponents modulo m, and these exponents are simply the group elements. Thus the number of group elements obtainable by adding up to d of the a_i together with repetition allowed is the same as the number of nontrivial eigenspaces in $R_{\leq d}$. This interpretation of Theorem 13 suggests a generalization to metacyclic groups.

6 Metacyclic Groups

Suppose that we have the following presentation of a metacyclic group G:

$$G = \langle a, b \,|\, a^m = 1, b^{-1}ab = a^r, b^s = a^t \rangle, \tag{6.1}$$

where m, r, and s further satisfy the conditions in (2.7). We will begin by looking at irreducible representations. Theorem 8 says that under certain conditions (and in particular if s is prime) all the irreducible representations of G are either one-dimensional or one of the induced T_i^G given by:

$$T_i^G(a) = \begin{bmatrix} \omega^i & 0 & 0 & \dots & 0 \\ 0 & \omega^{ir} & 0 & \dots & 0 \\ 0 & 0 & \omega^{ir^2} & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & \omega^{ir^{s-1}} \end{bmatrix}, \quad T_i^G(b) = \begin{bmatrix} 0 & 0 & \dots & 0 & \omega^{it} \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 \end{bmatrix}.$$

Fix such an induced representation. Then if $p \in \mathbf{C}^s$ is a generic point, the conditions that $F \in R_{\leq d}$ vanish on the orbit of p under G are that F vanish on the orbit of $(T_i^G(b))^j(p)$ under $T_i^G(a)$ for $j = 0, \dots, s-1$. In other words, the ideal of the whole orbit is the intersection of the ideals for the s cyclic orbits. As before, the Vandermonde trick works for each of the cyclic orbits, so that the condition that $F \in R_{\leq d}$ vanish on one of the cyclic orbits places one condition on each of the non-trivial eigenspaces of $R_{\leq d}$. Putting all the cyclic orbits together, we get s conditions on each of the nontrivial eigenspaces. This analysis yields an upper bound on the Hilbert function of the orbit ideal, as shown in the following.

Proposition 18 *The Hilbert function for the orbit ideal of an induced representation T_i^G of the metacyclic group G (as presented in (6.1)) satisfies the following upper bound:*

$$H(d) \leq \sum_{\dim R_{\leq d}(\omega^j) < s} \dim R_{\leq d}(\omega^j) + \alpha s$$

where α is the number of eigenspaces for $T_i^G(a)$ of dimension greater than or equal to s in $R_{\le d}$.

Proof:

$$\begin{aligned} H(d) &= \dim R_{\le d} - \dim I_{\le d} \qquad \text{where } I \text{ is the orbit ideal} \\ &= \sum_{j=0}^{m-1} \dim R_{\le d}(\omega^j) \quad - \sum_{\dim R_{\le d}(\omega^j) \ge c_j} (\dim R_{\le d}(\omega^j) - c_j) \end{aligned}$$

where $c_j \le s$ is the number of *independent* conditions placed on $R_{\le d}(\omega^j)$. Clearly the second sum is least if $c_j = s$ for all j. In this case we have

$$\begin{aligned} H(d) &\le \sum_{j=0}^{m-1} \dim R_{\le d}(\omega^j) \quad - \sum_{\dim R_{\le d}(\omega^j) \ge s} (\dim R_{\le d}(\omega^j) - s) \\ &= \sum_{\dim R_{\le d}(\omega^j) < s} \dim R_{\le d}(\omega^j) + \alpha s. \qquad \square \end{aligned}$$

So the question is: when are the conditions obtained by concatenating all the conditions from the s cyclic orbits independent? In order to investigate this question, we first introduce some notation. For any vector $e = (e_1, \ldots, e_s) \in \mathbf{N}^s$, we define $x^e := x_1^{e_1} x_2^{e_2} \ldots x_s^{e_s}$. Each eigenspace $R_{\le d}(\omega^j)$ has a basis consisting of a finite collection of monomials. Let E_j^d be the collection of exponent vectors corresponding to these monomials. That is:

$$E_j^d = \{e \in \mathbf{N}^s \,|\, e \cdot (i, ir, ir^2, \ldots, ir^{s-1}) \equiv j \quad (m) \text{ and } \sum_{l=1}^{s} e_l \le d\}.$$

Let $\tau = T_i^G(a)$ and $\sigma = T_i^G(b)$. Then by definition, for all $e \in E_j^d$ we have $\tau x^e = \omega^j x^e$. We also have $\sigma x^e = \omega^{ite_1} x^{\hat{e}}$ where $\hat{e} = (e_2, e_3, \ldots, e_s, e_1)$. Let $\{e^k\}_{k=1}^{\gamma}$ be the degree-lexicographic enumeration of E_j^d. Then any $F \in R_{\le d}(\omega^j)$ can be written uniquely as $F = \sum_{k=1}^{\gamma} a_k x^{e^k}$. The conditions that F vanish on the G-orbit of a point $p \in \mathbf{C}^s$ are that $(\sigma^j F)(p) = 0$ for $j = 0, \ldots, s-1$. These can be expressed as the single matrix condition:

$$\begin{bmatrix} x^{e^1} & x^{e^2} & \ldots & x^{e^\gamma} \\ \omega^{ite_1^1} x^{e^{\hat{1}}} & \omega^{ite_1^2} x^{e^{\hat{2}}} & \ldots & \omega^{ite_1^\gamma} x^{e^{\hat{\gamma}}} \\ \vdots & \vdots & \ddots & \vdots \\ \omega^{it\sum_{l=1}^{s-1} e_l^1} x^{e^{\overset{\vdots}{\hat{\hat{1}}}}} & \omega^{it\sum_{l=1}^{s-1} e_l^2} x^{e^{\overset{\vdots}{\hat{\hat{2}}}}} & \ldots & \omega^{it\sum_{l=1}^{s-1} e_l^\gamma} x^{e^{\overset{\vdots}{\hat{\hat{\gamma}}}}} \end{bmatrix}_{x=p} \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_\gamma \end{bmatrix} = 0 \qquad (6.2)$$

where there are $q-1$ hats above the exponent vectors in the qth row. Denote this matrix by Σ_j^d. Then we wish to determine when Σ_j^d has full rank. The following example shows that this is not always true, i.e. the s conditions are not always independent.

Example 19 Consider the dihedral group of order 14:

$$D_{14} = \langle \tau, \sigma \,|\, \tau^7 = \sigma^2 = 1,\, \sigma^{-1}\tau\sigma = \tau^6 \rangle. \tag{6.3}$$

We examine the irreducible induced representation $T_3^{D_{14}}$:

$$\tau \mapsto \begin{bmatrix} \omega^3 & 0 \\ 0 & \omega^4 \end{bmatrix}, \sigma \mapsto \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

What follows is a decomposition of $R_{\leq 4}$ into eigenspaces for the action of τ:

	R_0	R_1	R_2	R_3	R_4
1	1		xy		x^2y^2
ω			y^2		xy^3
ω^2				x^3	y^4
ω^3		x		x^2y	
ω^4		y		xy^2	
ω^5				y^3	x^4
ω^6			x^2		x^3y

¿From Proposition 18 we see that the following sequence is an upper bound for the Hilbert function at each step:

$$1, 3, 6, 10, 14, 14, \ldots \tag{6.4}$$

The matrices showing the action of σ on various eigenspaces are given below:

$$\Sigma_0^2 = \begin{bmatrix} 1 & xy \\ 1 & xy \end{bmatrix}, \quad \Sigma_3^3 = \begin{bmatrix} x & x^2y \\ y & xy^2 \end{bmatrix}, \quad \Sigma_4^3 = \begin{bmatrix} y & xy^2 \\ x & x^2y \end{bmatrix}.$$

All of these clearly have determinant zero. In fact, in each case the second column is just the first column multiplied by the monomial xy. □

Suppose that some submatrix of the matrix Σ_j^d in (6.2) has determinant zero. Then the columns of this submatrix are dependent in the sense that there exists a vector with polynomial components such that the dot product of this vector with each row of the submatrix is zero. It is difficult to characterize what sorts of relations can exist between the columns of the matrix, because it is unclear at the outset what monomials make up the first row. That is, we don't know what the set E_j^d looks like. As should be expected, things simplify in the 2×2 case. Accordingly, to get some purchase on this problem, we look first to the case where the quotient group $G/\langle a \rangle$ has order $s = 2$.

6.1 The two-dimensional case

Fix an induced representation T_i^G for a metacyclic group G with $s = 2$. Choose an eigenvalue ω^j for the action of τ, and let d be the least integer such that $|E_j^d| \geq 2$. Suppose that the matrix Σ_j^d corresponding to the action of σ on $R_{\leq d}(\omega^j)$ (as constructed in (6.2)) has rank less than 2. Then all the 2×2 submatrices of Σ_j^d have zero determinant, in particular the submatrix formed by taking the first two columns. This matrix has the following form:

$$M = \begin{bmatrix} x^\alpha y^\beta & x^{\alpha'} y^{\beta'} \\ \omega^{it\alpha} x^\beta y^\alpha & \omega^{it\alpha'} x^{\beta'} y^{\alpha'} \end{bmatrix}$$

where (α, β) and (α', β') are the first and second elements in the degree-lexicographic enumeration of E_j^d. We are assuming that M has zero determinant:

$$0 = \det M = \omega^{it\alpha'} x^{\alpha+\beta'} y^{\alpha'+\beta} - \omega^{it\alpha} x^{\alpha'+\beta} y^{\alpha+\beta'},$$

which yields the following two conditions:

$$\omega^{it\alpha'} = \omega^{it\alpha}$$

$$\alpha' - \alpha = \beta' - \beta =: k.$$

This shows that $x^{\alpha'} y^{\beta'} = x^k y^k x^\alpha y^\beta$. But then $x^k y^k$ must have eigenvalue 1 under τ. Recalling that $\tau x = \omega^i x$ and $\tau y = \omega^{ir} y$, we see that:

$$x^k y^k = \tau(x^k y^k) = \omega^{k(i+ir)} x^k y^k \iff ik(1+r) \equiv 0 \quad (m). \tag{6.5}$$

Also:

$$\omega^{it\alpha'} = \omega^{it\alpha} \iff \omega^{itk} = 1 \iff itk \equiv 0 \quad (m). \tag{6.6}$$

Let k be the least positive integer satisfying (6.5) and (6.6). Note that we have dependence of conditions if and only if $(xy)^k$ is the only nonconstant eigenmonomial with eigenvalue 1 of degree less than or equal to $2k$. This is because *all* 2×2 minors of the matrix Σ_j^d must be zero, and if $x^a y^b$ were another such eigenmonomial, then the 2×2 minor obtained by taking the first column and the column corresponding to $x^{\alpha+a}y^{\beta+b}$ would be nonzero. On the other hand, if $(xy)^k$ is the only nonconstant eigenmonomial for 1, then we have dependence of conditions in $R_{\leq 2k}(1)$, i.e. Σ_0^{2k} has rank 1. We summarize this discussion in the following proposition:

Proposition 20 *If G is a metacyclic group with $s = 2$ and parameters (m, r, t), then the Hilbert function of the orbit ideal of the representation T_i^G achieves the bound in Proposition 18 if and only if the following condition is satisfied:*

If k is the least positive integer solution to the congruences (6.5) and (6.6), then there are nonnegative integers a, b (not both equal to k) such that $1 \leq a + b \leq 2k$ and $i(a + br) \equiv 0 \quad (m)$.

Using Proposition 20 we can determine the actual Hilbert function for any metacyclic group G with $s = 2$. To do this, first define an equivalence relation on each eigenspace $R_{\leq d}(\omega^j)$:

$$x^\alpha y^\beta \sim x^{\alpha'} y^{\beta'} \iff x^{\alpha'} y^{\beta'} = x^k y^k x^\alpha y^\beta$$

for some integer k satisfying (6.5), (6.6). Let $\overline{E_j^d}$ denote the set of equivalence classes in E_j^d. Now Proposition 18 says that

$$H(d) \leq \sum_{j=0}^{m-1} \min\{|E_j^d|, 2\}.$$

But the discussion leading up to Proposition 20 shows that H achieves this bound unless an invariant monomial of the form $(xy)^k$ prevents it. But we can say more: in determining the number of vanishing conditions placed on $R_{\leq d}(\omega^j)$, we should treat two monomials related by such an invariant monomial as the same. That is, we should be counting the number of equivalence classes in $R_{\leq d}(\omega^j)$, *not* the number of monomials.

Proposition 21 *Let G be a metacyclic group with $s = 2$. Then the Hilbert function of the ideal of the orbit of a generic point under T_i^G is given by*

$$H(d) = \sum_{j=0}^{m-1} \min\{|\overline{E_j^d}|, 2\} \quad \forall d \geq 0. \tag{6.7}$$

Example 22 We will determine the actual Hilbert function of the representation $T_3^{D_{14}}$ considered in Example 19. First we must extend the decomposition into eigenspaces a bit further:

	R_0	R_1	R_2	R_3	R_4	R_5	R_6	R_7
1	1		xy		x^2y^2		x^6y^6	x^7, y^7
ω			y^2		xy^3	x^5	x^2y^4	x^6y
ω^2				x^3	y^4	x^4y	xy^5	x^5y^2
ω^3		x		x^2y		x^3y^2	y^6	x^4y^3
ω^4		y		xy^2		x^2y^3	x^6	x^3y^4
ω^5				y^3	x^4	xy^4	x^5y	x^2y^5
ω^6			x^2		x^3y	y^5	x^4y^2	xy^6

Now Proposition 21 tells us to determine $H(d)$ by counting monomials in $R_{\leq d}$ modulo factors of the form $(xy)^k$, since any integer k satisfies (6.5) and (6.6). Clearly every equivalence class has a unique representative of the form x^q or y^q. Thus to determine the Hilbert function, we only need to count how the powers of x and y appear. Inspection of the decomposition above reveals that they appear two at a time, so the Hilbert function is:

$$H = 1, 3, 5, 7, 9, 11, 13, 14, 14, \ldots \quad \square$$

6.2 The three-dimensional case

In this section we consider three-dimensional induced representations T_i^G of metacyclic groups with $t = 0$:

$$G = \langle a, b \,|\, a^m = 1, b^3 = 1, b^{-1}ab = a^r \rangle.$$

Of course, $r^3 \equiv 1 \quad (m)$ and $(r, m) = 1$. The condition that $t = 0$ means that these groups are semi-direct products. A computer search was conducted using CoCoA (cf. [3]) in the range

$$3 \leq m \leq 15$$
$$1 \leq r \leq m - 1$$
$$1 \leq i \leq m - 1$$

to find representations whose Hilbert functions do not achieve the bound presented in Proposition 18. We will refer to such representations as *nonstandard*. The search resulted in a list of nonstandard cases for $m = 7, 13, 14$. After sorting this list into isomorphism classes (where by Theorem 7 two representations are isomorphic for given m, r if their exponent sets $\{i, ir, ir^2\}$ are the same mod m), we are left[11] with two nonstandard representations for $m = 7$, four for $m = 13$, and two for $m = 14$. We work out one of the nonstandard representations for $m = 7$ in detail.

Example 23 Consider the representation T_1^G of the metacyclic group G indexed by parameters $(m, s, r, t) = (7, 3, 2, 0)$. Using CoCoA, we find that the Hilbert function is

$$H = 1, 4, 10, 19, 21, 21, \ldots \tag{6.8}$$

We have:

$$\tau := T_1^G(a) = \begin{bmatrix} \omega & 0 & 0 \\ 0 & \omega^2 & 0 \\ 0 & 0 & \omega^4 \end{bmatrix}, \quad \sigma := T_1^G(b) = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}.$$

A decomposition of $R_{\leq 3}$ into eigenspaces for τ is as follows:

	R_0	R_1	R_2	R_3
1	1			xyz
ω		x	z^2	y^2z
ω^2		y	x^2	xz^2
ω^3			xy	x^3, yz^2
ω^4		z	y^2	x^2y
ω^5			xz	xy^2, z^3
ω^6			yz	x^2z, y^3

Then Proposition 18 gives the following sequence as a bound for H:

$$1, 4, 10, 20, 21, 21, \ldots$$

Comparison with (6.8) shows that this representation is nonstandard. We would like to determine the cause of the decreased Hilbert function.

The matrices Σ_j^d (as in (6.2)) have full rank for $1 \leq j \leq 6, 1 \leq d \leq 3$. For example:

$$\Sigma_1^3 = \begin{bmatrix} x & z^2 & y^2z \\ y & x^2 & z^2x \\ z & y^2 & x^2y \end{bmatrix} \quad \text{and} \quad \det \Sigma_1^3 = x^5y + y^5z + z^5x - 3x^2y^2z^2.$$

[11] Notice that the representation indexed by the parameters (m, r, i) is isomorphic to the representation indexed by (m, r^2, i).

But Σ_0^3 has rank 1:

$$\Sigma_0^3 = \begin{bmatrix} 1 & xyz \\ 1 & xyz \\ 1 & xyz \end{bmatrix}.$$

Thus the vanishing conditions imposed by the action of σ yield only one condition on $R_{\leq 3}(1)$, which has dimension 2. So while we expected to obtain no polynomials in $R_{\leq 3}(1)$ vanishing on $Orb(p)$, we do in fact get one, namely:

$$xyz - p_1p_2p_3.$$

This unexpected cubic polynomial causes $H(3)$ to decrease by one. □

The other nonstandard representation with $m = 7$ is T_3^G for the same group G as in the previous example. The situation is the same: the first nonconstant monomial eigenvector for τ with eigenvector 1 is xyz, and all other such eigenvectors have degree at least four. When we let the quotient group of order three impose its conditions on the eigenspace $R_{\leq 3}(1)$, we get only one condition

$$Axyz + B = 0,$$

and thereby the expected value of $H(3)$ decreases by one. Notice that this situation will always result in a nonstandard representation. The question is then whether a representation can be nonstandard for any other reason.

In fact, this situation can occur even if xyz does not have eigenvalue 1, provided that $(xyz)^k$ does for some k. The condition that $(xyz)^k$ is an eigenvector with eigenvalue 1 is equivalent to the condition that $ik(1 + r + r^2) \equiv 0 \quad (m)$. Solving this congruence (with $k = 1$) for $m = 7, 13, 14$ yields precisely the r and i-values produced in the computer search.

The values $m = 3, r = 1$ also solve the congruence. So why doesn't the metacyclic group $(m, s, r, t) = (3, 3, 1, 0)$ have a nonstandard representation? Inspection of the representations T_i^G for this group reveals that while xyz is an eigenvector with eigenvalue 1, so is every monomial of degree 3. This gives enough monomials so that Σ_0^3 has full rank. Evidently, we need to include in our condition the fact that $(xyz)^k$ must be at most the second nonconstant eigenvector. This is because a single additional monomial eigenvector with degree $\leq 3k$ isn't enough to make the conditions independent:

$$\det \begin{bmatrix} 1 & x^e & (xyz)^k \\ 1 & x^{\hat{e}} & (xyz)^k \\ 1 & x^{\hat{\hat{e}}} & (xyz)^k \end{bmatrix} = 0.$$

This leads us to the following conjecture:

Conjecture 24 *The only nonstandard induced representations of metacyclic groups with $s = 3, t = 0$ correspond to m, r, and i-values such that if k is the least positive integer with $a = b = c = k$ a solution to the congruence*

$$i(a + br + cr^2) \equiv 0 \pmod{m},$$

then there is at most one other solution with $1 \leq a + b + c \leq 3k$, and $a, b, c \geq 0$.

Note that this generalizes the two-dimensional result stated in Proposition 20.

A C-program was written to find all such (m, r, i)-values for $m \leq 100$, and they are listed along with their associated k-values in Appendix A. Using CoCoA we have checked that these account for all nonstandard representations with $m \leq 71$.

The condition in Conjecture 24 can be recast in a particularly simple form:

Proposition 25 *Fix a positive integer m. Then the following two statements are equivalent:*

1. *There exist positive integers r, i satisfying $1 \leq r, i < m; (r, m) = 1; r^3 \equiv 1 \pmod{m}$, such that if k is the least positive integer with $a = b = c = k$ a solution to the congruence*
$$i(a + br + cr^2) \equiv 0 \pmod{m}, \tag{6.9}$$
then there is at most one other solution with $1 \leq a + b + c \leq 3k$, and $a, b, c \geq 0$.

2. *m is divisible by a prime congruent to 1 mod 3.*

Proof: Suppose that (m, r, i) satisfies (1). Then I claim that $(m', r, 1)$ also satisfies (1), where $m' = \frac{m}{(i,m)}$. This is because the solutions to (6.9) are the same in both cases. As a partial converse, it is also true that if $(m, r, 1)$ satisfies (1), then so does (m, r, i) for any i relatively prime to m. Using these facts, it will be sufficient to consider representations with $i = 1$.

We begin by taking m to be a prime power p^e. There are three cases: $p = 3$; $p \equiv 2 \pmod{3}$; $p \equiv 1 \pmod{3}$. First suppose that $p \equiv 2 \pmod{3}$. Then the multiplicative group $(\mathbf{Z}/p^e\mathbf{Z})^*$ has order

$$\varphi(p^e) = p^{e-1}(p-1)$$

which is not divisible by 3. By Lagrange's Theorem, $(\mathbf{Z}/p^e\mathbf{Z})^*$ has no subgroup of order 3, so that the only choice for r is 1. Then we must determine the least k such that $3k \equiv 0 \pmod{p^e}$. Clearly $k = p^e$, which means that there are many solutions a, b, c. For instance $a = p^e, b = c = 0$, and $a = b = 0, c = p^e$ both work. Thus (1) does not hold.

Now suppose that $p = 3$. Then $(\mathbf{Z}/3^e\mathbf{Z})^*$ has order

$$\varphi(3^e) = 2 \cdot 3^{e-1}.$$

Thus if $e = 1$ then there is no subgroup of order 3, and we must have $r = 1$. A before, there are many solutions, so (1) does not hold. If $e > 1$, then since $(\mathbf{Z}/3^e\mathbf{Z})^*$ is cyclic, there is a unique subgroup of order 3. Let ζ be a generator for this subgroup (i.e. a nontrivial cube root of unity), so that $r \in \{1, \zeta, \zeta^2\}$. If $r = 1$ then we are looking for the least k such that $3k \equiv 0 \pmod{3^e}$, so $k = 3^{e-1}$. In this case there are lots of solutions a, b, c so (1) does not hold. Finally, suppose that $r = \zeta$ (the analysis for $r = \zeta^2$ is identical). Then we must determine the least k such that

$$k(1 + \zeta + \zeta^2) \equiv 0 \pmod{3^e}. \tag{6.10}$$

But the cube roots of 1 in $(\mathbf{Z}/3^e\mathbf{Z})^*$ are $(1 + 3^{e-1}q)$ for $q = 0, 1, 2$. Taking $\zeta = (1+3^{e-1})$, $\zeta^2 = (1+2\cdot 3^{e-1})$, we find that (6.10) becomes

$$k(1 + 1 + 3^{e-1} + 1 + 2 \cdot 3^{e-1}) = 3k(1 + 3^{e-1}) \equiv 0 \pmod{3^e},$$

which implies that $k = 3^{e-1}$. Now we need nonnegative a, b, c with $1 \leq a+b+c \leq 3k = 3^e$ such that

$$a + b(1 + 3^{e-1}) + c(1 + 2 \cdot 3^{e-1}) = a + b + c + (b + 2c) \cdot 3^{e-1} \equiv 0 \pmod{3^e}.$$

$a = 2 \cdot 3^{e-1}, b = 0, c = 3^{e-1}$ and $a = 2 \cdot 3^{e-1}, b = 3^{e-1}, c = 0$ work, so (1) does not hold. This completes the analysis for $p = 3$.

Now suppose $p \equiv 1 \pmod{3}$. In this case $(\mathbf{Z}/p^e\mathbf{Z})^*$ is cyclic of order

$$\varphi(p^e) = p^{e-1}(p-1)$$

which is a multiple of 3. Thus there is a unique cyclic subgroup of order 3, so that $r \in \{1, \zeta, \zeta^2\}$. If $r = 1$, then as we have seen several times now, there are many solutions and (1) does not hold. So suppose $r = \zeta$. Then we are looking for the least k such that

$$k(1 + \zeta + \zeta^2) \equiv 0 \pmod{p^e}.$$

Since $(1 - \zeta)(1 + \zeta + \zeta^2) = \zeta^3 - 1 \equiv 0 \pmod{p^e}$, it follows that if $1 - \zeta \not\equiv 0 \pmod{p}$, then $(1 + \zeta + \zeta^2) \equiv 0 \pmod{p^e}$. So suppose that $\zeta = 1 + p^f n$, where $p \not| n$ and $0 \leq f \leq e - 1$. We wish to show that $f = 0$. Now

$$\begin{aligned} & \zeta^3 = (1 + p^f n)^3 = 1 + 3p^f n + 3p^{2f} n^2 + p^{3f} n^3 \equiv 1 \pmod{p^e} \\ \iff & 3p^f n + 3p^{2f} n^2 + p^{3f} n^3 \equiv 0 \pmod{p^e} \\ \iff & 3n + 3p^f n^2 + p^{2f} n^3 \equiv 0 \pmod{p^{e-f}}. \end{aligned}$$

If $f > 0$, then we must have $p | 3n$, which is a contradiction. Thus $f = 0$, and $(1 + \zeta + \zeta^2) \equiv 0 \pmod{p^e}$. But then $k = 1$, and we are looking for nonnegative a, b, c such that $1 \leq a + b + c \leq 3$ and

$$a + b\zeta + c\zeta^2 = (a - c) + (b - c)\zeta \equiv 0 \pmod{p^e},$$

(where we have used the fact that $\zeta^2 \equiv -1 - \zeta \pmod{p^e}$). Since ζ is invertible mod p^e, we must have either $a = b = c = 1$ or a, b, c distinct. We are looking for another solution besides the former case, so assume that they are distinct. This means that they are 0,1,2 in some order. The following table lists the possibilities along with the associated values of ζ and ζ^3:

a	b	c	ζ	ζ^3
0	1	2	-2	-8
0	2	1	1	1
1	0	2	$-\frac{1}{2}$	$-\frac{1}{8}$
1	2	0	$-\frac{1}{2}$	$-\frac{1}{8}$
2	0	1	1	1
2	1	0	-2	-8

Since $\zeta^3 \equiv 1 \pmod{p^e}$, the only possible solutions are the second and fifth rows. But these yield $\zeta = 1$, which is untrue since ζ is a nontrivial cube root of unity. Thus there are no solutions and (1) holds.

Thus far we have shown that (1) and (2) are equivalent for $m = p^e$ a prime power.

Now suppose that $m = 3^e p_1^{e_1} \cdots p_n^{e_n} q_1^{f_1} \cdots q_l^{f_l}$, where $p_i \equiv 1 \quad (3)$ and $q_i \equiv 2 \quad (3)$. By the Chinese Remainder Theorem (see [11]) we have the following isomorphism:

$$(\mathbf{Z}/m\mathbf{Z})^* \simeq (\mathbf{Z}/3^e\mathbf{Z})^* \times (\mathbf{Z}/p_1^{e_1}\mathbf{Z})^* \times \cdots \times (\mathbf{Z}/p_n^{e_n}\mathbf{Z})^* \times (\mathbf{Z}/q_1^{f_1}\mathbf{Z})^* \times \cdots \times (\mathbf{Z}/q_l^{f_l}\mathbf{Z})^*.$$

Now each of the first $n+1$ factors has a unique subgroup of order 3 (assuming $e > 1$), while none of the other factors have any elements of order 3. Thus, there are 3^{n+1} elements (3^n if $e = 0, 1$) of order dividing 3 in $\mathbf{Z}/m\mathbf{Z}^*$, and these are the possible r-values. Note that if $r = 1$ then $k = m$ or $\frac{m}{3}$, and as before there are many solutions so (1) does not hold. So assume that $r \neq 1$. Then if $n = 0$ (i.e. if m is not divisible by a prime congruent to 1 mod 3), then the only possible r-values correspond to elements of the form $(\zeta, 1, \ldots, 1)$ under the isomorphism above, where ζ is a nontrivial cube root of unity mod 3^e. For ζ to be nontrivial we must have $e > 1$. Then we are looking for the least k such that

$$k(1 + \zeta + \zeta^2, 3, \ldots, 3) \equiv 0 \quad (3^e, q_1^{f_1}, \ldots, q_l^{f_l}),$$

where the congruence is taken componentwise. The previous analysis in terms of prime powers shows that $k = 3^{e-1} q_1^{f_1} \ldots q_l^{f_l}$. Then $a = 2{\cdot}3^{e-1} q_1^{f_1} \ldots q_l^{f_l}, b = 0, c = 3^{e-1} q_1^{f_1} \ldots q_l^{f_l}$ and $a = 2 \cdot 3^{e-1} q_1^{f_1} \ldots q_l^{f_l}, b = 3^{e-1} q_1^{f_1} \ldots q_l^{f_l}, c = 0$ are solutions, so (1) does not hold.

Finally, suppose that $n \geq 1$. Then let r be the element of $(\mathbf{Z}/m\mathbf{Z})^*$ corresponding to $(1, \zeta, 1, \ldots, 1)$. That is, we have chosen 1 for each component except the component corresponding to $p_1^{e_1}$ where we have chosen a nontrivial cube root ζ. Furthermore, set $i = 3^{e-1} p_2^{e_1} \cdots p_n^{e_n} q_1^{f_1} \cdots q_l^{f_l}$. Then

$$ik(3, 1 + \zeta + \zeta^2, 3, \ldots, 3) \equiv 0 \quad (3^e, p_1^{e_1}, \ldots, q_l^{f_l})$$

implies that $k = 1$. Then we are looking for nonnegative a, b, c such that $1 \leq a+b+c \leq 3$ and

$$i(a + b + c, a + b\zeta + c\zeta^2, a + b + c, \ldots, a + b + c) \equiv 0 \quad (3^e, p_1^{e_1}, \ldots, q_l^{f_l}).$$

But this reduces to the same problem we had before, namely

$$a + b\zeta + c\zeta^2 \equiv 0 \quad (p^e)$$

where a, b, c must be distinct. We have seen that there are no solutions, so that (1) holds. This completes the proof of the equivalence of (1) and (2). □

If we are only interested in which values of m have metacyclic groups with nonstandard representations, then we can reformulate Conjecture 24 in a particularly pleasing form:

Reformulation of Conjecture 24: *Let m be a positive integer. Then the following two conditions are equivalent:*

1. *There exists a nonstandard induced representation of a metacyclic group G whose normal cyclic subgroup A has order m.*
2. *m is divisible by a prime congruent to 1 mod 3.*

6.3 Invariants and the Molien series

It is interesting to observe that Conjecture 24 (as well as Proposition 20) relates nonstandard representations to the existence of invariant polynomials. The conjecture states that we will have a nonstandard representation precisely when $(xyz)^k$ is invariant for k small enough so that at most one other nonconstant monomial of equal or lesser degree also is invariant. To determine whether we have such a case, we must investigate the equation $ar^2 + br + c \equiv 0 \quad (m)$. But another way to compute the number of invariants of each degree is by the Molien series. In fact, the Molien series is just a machine for counting solutions to our equation.

The Molien series of G, denoted Φ_G, is the ordinary power series generating function for the sequence $\{d_j\}_{j=0}^{\infty}$, where d_j is the dimension of the vector space of degree j polynomial invariants for G. A formula in terms of the group elements is as follows (see [12]):

$$\Phi_G(z) = \frac{1}{|G|} \sum_{g \in G} \frac{1}{\det(id - zg)}.$$

Now $G = \{A_j, B_j, C_j \mid j = 0, \ldots, m-1\}$ where

$$A_j = \begin{bmatrix} \omega^{ij} & 0 & 0 \\ 0 & \omega^{ijr} & 0 \\ 0 & 0 & \omega^{ijr^2} \end{bmatrix}, B_j = \begin{bmatrix} 0 & 0 & \omega^{ijr^2} \\ \omega^{ij} & 0 & 0 \\ 0 & \omega^{ijr} & 0 \end{bmatrix}, C_j = \begin{bmatrix} 0 & \omega^{ijr} & 0 \\ 0 & 0 & \omega^{ijr^2} \\ \omega^{ij} & 0 & 0 \end{bmatrix}.$$

We compute the determinants:

$$\begin{aligned} \det(id - zA_j) &= (1 - z\omega^{ij})(1 - z\omega^{ijr})(1 - z\omega^{ijr^2}) \\ \det(id - zB_j) &= 1 - z^3\omega^{ij(1+r+r^2)} \\ \det(id - zC_j) &= 1 - z^3\omega^{ij(1+r+r^2)}. \end{aligned}$$

Then the Molien series is:

$$\begin{aligned}\Phi_G(z) &= \frac{1}{3m}\sum_{j=0}^{m-1}\left[\frac{1}{(1-z\omega^{ij})(1-z\omega^{ijr})(1-z\omega^{ijr^2})}+\frac{2}{1-z^3\omega^{ij(1+r+r^2)}}\right]\\ &= \frac{1}{3m}\sum_{j=0}^{m-1}[(1+z\omega^{ij}+z^2\omega^{2ij}+\ldots)(1+z\omega^{ijr}+z^2\omega^{2ijr}+\ldots)\times\\ &\qquad (1+z\omega^{ijr^2}+z^2\omega^{2ijr^2}+\ldots)+2(1+z^3\omega^{ij(1+r+r^2)}+z^6\omega^{2ij(1+r+r^2)}+\ldots)].\end{aligned}$$

Since we are summing over j, the only terms that survive are those with exponent zero mod m. Evidently the last infinite series in this sum tells whether $(xyz)^k$ is invariant. The other part of the sum counts solutions to $ar^2+br+c\equiv 0 \quad (m)$.

6.4 A more general scenario

The question may arise as to why the eigenspace for 1 is so important in the identification of nonstandard representations. We have seen explicitly in two dimensions that the possibility of nonstandardness depends upon the existence of a certain type of eigenvector with eigenvalue 1, i.e. a certain type of invariant. Moreover, computer data suggests that the same is true in three dimensions. In the three-dimensional case, the cause of the decreased Hilbert function is that we have at least 2 eigenmonomials invariant under the action of $\langle\sigma\rangle$, with at most one other eigenmonomial in the same eigenspace of the same or lesser degree. (Recall that σ is the generator for the cyclic quotient group.) Since the constant polynomial 1 is always an eigenvector with eigenvalue 1, we need only one more eigenvector for this eigenspace. But we need two for the other eigenspaces. This provides an intuitive explanation for why the eigenspace for 1 is so important here: it is simply easier for our scenario to arise because we already start out with an invariant.

But the scenario we have been discussing is really only the lowest order manifestation of a more general problem. That is, it may happen that for some eigenspace $R_{\leq d}(\omega^j)$, some of the exponent vectors in E_j^d have the property that the least common multiple of the size of their orbits under $\langle\sigma\rangle$ properly divides s. If this subcollection of E_j^d is large enough, then the value of the Hilbert function will be reduced. We have been discussing the case in which the lcm is 1. In fact, when s is prime, no other situation can occur since the lcm must divide s. However, if $s=4$, for instance, then a scenario may arise in which the least common multiple is 2. The following example provides an illustration of this more general scenario.

Example 26 Consider the metacyclic group G with parameters $(m, s, r, t) = (5, 4, 3, 0)$. We examine the representation T_2^G:

$$\tau := T_2^G(a) = \begin{bmatrix} \omega^2 & 0 & 0 & 0 \\ 0 & \omega & 0 & 0 \\ 0 & 0 & \omega^3 & 0 \\ 0 & 0 & 0 & \omega^4 \end{bmatrix}, \quad \sigma := T_2^G(b) = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}. \tag{6.11}$$

(Here $\omega = e^{\frac{2\pi i}{5}}$.) We decompose $R_{\leq 3}$ into eigenspaces for τ:

	R_0	R_1	R_2	R_3
1	1		xz, yt	x^2y, xt^2, y^2z, z^2t
ω		y	xt, z^2	x^3, xyz, y^2t, zt^2
ω^2		x	y^2, zt	x^2z, xyt, yz^2, t^3
ω^3		z	xy, t^2	x^2t, xz^2, y^3, yzt
ω^4		t	x^2, yz	xy^2, xzt, yt^2, z^3

Proposition 18 says that the Hilbert function is bounded by the sequence:

$$1, 5, 15, 20, 20 \ldots \tag{6.12}$$

But notice that $E_0^2 = \{(0,0,0,0), (1,0,1,0), (0,1,0,1)\}$, and each of these exponent vectors has order dividing 2 under σ. Thus, instead of obtaining four conditions for a polynomial in $R_{\leq 2}(1)$ to vanish on the orbit of $p \in \mathbf{C}^4$ (which would overdetermine the system since there are only three monomials), we only get two:

$$\begin{aligned} \sigma^0, \sigma^2 : &\quad A + Bp_1p_3 + Cp_2p_4 = 0 \\ \sigma^1, \sigma^3 : &\quad A + Bp_2p_4 + Cp_1p_3 = 0 \end{aligned}$$

So there exists a single solution to the system, which decreases the Hilbert function by 1. Indeed, using CoCoA, we find that the actual Hilbert function of this representation is:

$$H = 1, 5, 14, 20, 20 \ldots \quad \Box$$

A Appendix

The following is a list of all nonstandard induced representations (up to isomorphism) of metacyclic groups G with $s = 3, t = 0, m \leq 100$, and satisfying the condition in Conjecture 24. The 3-tuple of numbers in each entry gives the parameters (m, r, i) of the group representation, while k is the least positive integer solution to the congruence $ik(1 + r + r^2) \equiv 0 \quad (m)$.

(7,2,1) k=1
(7,2,3) k=1

(13,3,1) k=1
(13,3,2) k=1
(13,3,4) k=1
(13,3,7) k=1

(14,9,2) k=1
(14,9,6) k=1

(19,7,1) k=1
(19,7,2) k=1
(19,7,4) k=1
(19,7,5) k=1
(19,7,8) k=1
(19,7,10) k=1

(21,4,1) k=1
(21,4,2) k=1
(21,4,3) k=1
(21,4,5) k=1
(21,4,9) k=1
(21,4,10) k=1

(26,3,1) k=2
(26,3,2) k=1
(26,3,4) k=1
(26,3,5) k=2
(26,3,7) k=2
(26,3,8) k=1
(26,3,14) k=1
(26,3,17) k=2

(28,9,4) k=1
(28,9,12) k=1

(31,5,1) k=1
(31,5,2) k=1
(31,5,3) k=1
(31,5,4) k=1
(31,5,6) k=1
(31,5,8) k=1
(31,5,11) k=1
(31,5,12) k=1
(31,5,16) k=1
(31,5,17) k=1

(35,11,5) k=1
(35,11,15) k=1

(37,10,1) k=1
(37,10,2) k=1
(37,10,3) k=1
(37,10,5) k=1
(37,10,6) k=1
(37,10,7) k=1
(37,10,9) k=1
(37,10,11) k=1
(37,10,14) k=1
(37,10,17) k=1
(37,10,18) k=1
(37,10,21) k=1

(38,7,1) k=2
(38,7,2) k=1
(38,7,3) k=2
(38,7,4) k=1
(38,7,5) k=2
(38,7,8) k=1
(38,7,9) k=2
(38,7,10) k=1
(38,7,13) k=2
(38,7,16) k=1
(38,7,20) k=1
(38,7,27) k=2

(39,16,1) k=1
(39,16,2) k=1
(39,16,3) k=1
(39,16,4) k=1
(39,16,6) k=1
(39,16,7) k=1
(39,16,8) k=1
(39,16,12) k=1
(39,16,14) k=1
(39,16,17) k=1
(39,16,19) k=1
(39,16,21) k=1

(42,25,2) k=1
(42,25,4) k=1
(42,25,6) k=1
(42,25,10) k=1
(42,25,18) k=1
(42,25,20) k=1

(43,6,1) k=1
(43,6,2) k=1
(43,6,3) k=1
(43,6,4) k=1
(43,6,5) k=1
(43,6,7) k=1
(43,6,9) k=1
(43,6,10) k=1
(43,6,13) k=1
(43,6,14) k=1
(43,6,19) k=1
(43,6,20) k=1
(43,6,21) k=1
(43,6,26) k=1

(49,18,1) k=1
(49,18,2) k=1
(49,18,3) k=1
(49,18,4) k=1
(49,18,6) k=1
(49,18,7) k=1
(49,18,8) k=1
(49,18,9) k=1
(49,18,12) k=1
(49,18,13) k=1
(49,18,16) k=1
(49,18,19) k=1
(49,18,21) k=1
(49,18,24) k=1
(49,18,26) k=1
(49,18,29) k=1

(52,9,2) k=2
(52,9,4) k=1
(52,9,8) k=1
(52,9,10) k=2
(52,9,14) k=2
(52,9,16) k=1
(52,9,28) k=1
(52,9,34) k=2

(56,9,8) k=1
(56,9,24) k=1

(57,7,1) k=1
(57,7,2) k=1
(57,7,3) k=1
(57,7,4) k=1
(57,7,5) k=1
(57,7,6) k=1
(57,7,8) k=1
(57,7,10) k=1
(57,7,11) k=1

(57,7,12) k=1
(57,7,15) k=1
(57,7,16) k=1
(57,7,22) k=1
(57,7,23) k=1
(57,7,24) k=1
(57,7,29) k=1
(57,7,30) k=1
(57,7,31) k=1

(61,13,1) k=1
(61,13,2) k=1
(61,13,3) k=1
(61,13,4) k=1
(61,13,6) k=1
(61,13,7) k=1
(61,13,8) k=1
(61,13,9) k=1
(61,13,11) k=1
(61,13,12) k=1
(61,13,14) k=1
(61,13,16) k=1
(61,13,18) k=1
(61,13,22) k=1
(61,13,23) k=1
(61,13,27) k=1
(61,13,28) k=1
(61,13,31) k=1
(61,13,32) k=1
(61,13,36) k=1

(62,5,1) k=2
(62,5,2) k=1
(62,5,3) k=2
(62,5,4) k=1
(62,5,6) k=1
(62,5,7) k=2
(62,5,8) k=1
(62,5,9) k=2
(62,5,11) k=2
(62,5,12) k=1
(62,5,16) k=1
(62,5,17) k=2
(62,5,19) k=2
(62,5,21) k=2
(62,5,22) k=1
(62,5,24) k=1
(62,5,32) k=1
(62,5,34) k=1
(62,5,37) k=2
(62,5,47) k=2

(63,4,1) k=3
(63,4,2) k=3
(63,4,3) k=1
(63,4,5) k=3
(63,4,6) k=1
(63,4,9) k=1
(63,4,10) k=3
(63,4,11) k=3
(63,4,13) k=3
(63,4,15) k=1
(63,4,22) k=3
(63,4,23) k=3
(63,4,26) k=3
(63,4,27) k=1
(63,4,30) k=1
(63,4,31) k=3
(63,4,43) k=3
(63,4,47) k=3

(65,16,5) k=1
(65,16,10) k=1
(65,16,20) k=1
(65,16,35) k=1

(67,29,1) k=1
(67,29,2) k=1
(67,29,3) k=1
(67,29,4) k=1
(67,29,5) k=1
(67,29,6) k=1
(67,29,8) k=1
(67,29,9) k=1
(67,29,10) k=1
(67,29,12) k=1
(67,29,15) k=1
(67,29,16) k=1
(67,29,17) k=1
(67,29,18) k=1
(67,29,23) k=1
(67,29,25) k=1
(67,29,27) k=1
(67,29,30) k=1
(67,29,32) k=1
(67,29,34) k=1
(67,29,36) k=1
(67,29,41) k=1

(70,11,10) k=1
(70,11,30) k=1

(73,8,1) k=1
(73,8,2) k=1
(73,8,3) k=1
(73,8,4) k=1
(73,8,5) k=1
(73,8,6) k=1
(73,8,7) k=1
(73,8,9) k=1
(73,8,11) k=1
(73,8,12) k=1
(73,8,13) k=1
(73,8,14) k=1
(73,8,17) k=1
(73,8,18) k=1
(73,8,21) k=1
(73,8,25) k=1
(73,8,26) k=1
(73,8,27) k=1
(73,8,33) k=1
(73,8,34) k=1
(73,8,35) k=1
(73,8,36) k=1
(73,8,42) k=1
(73,8,43) k=1

(74,47,1) k=2
(74,47,2) k=1
(74,47,3) k=2
(74,47,4) k=1
(74,47,5) k=2
(74,47,6) k=1
(74,47,7) k=2
(74,47,9) k=2
(74,47,10) k=1
(74,47,11) k=2
(74,47,12) k=1
(74,47,14) k=1
(74,47,15) k=2
(74,47,17) k=2
(74,47,18) k=1
(74,47,21) k=2
(74,47,22) k=1
(74,47,23) k=2
(74,47,28) k=1
(74,47,29) k=2
(74,47,34) k=1
(74,47,36) k=1
(74,47,42) k=1
(74,47,55) k=2

(76,45,2) k=2
(76,45,4) k=1
(76,45,6) k=2
(76,45,8) k=1
(76,45,10) k=2
(76,45,16) k=1
(76,45,18) k=2
(76,45,20) k=1
(76,45,26) k=2
(76,45,32) k=1
(76,45,40) k=1
(76,45,54) k=2

(77,23,11) k=1
(77,23,33) k=1

(78,55,1) k=2
(78,55,2) k=1
(78,55,3) k=2
(78,55,4) k=1
(78,55,5) k=2
(78,55,6) k=1
(78,55,7) k=2
(78,55,8) k=1
(78,55,11) k=2
(78,55,12) k=1
(78,55,14) k=1
(78,55,15) k=2
(78,55,16) k=1
(78,55,17) k=2
(78,55,19) k=2
(78,55,21) k=2
(78,55,24) k=1
(78,55,25) k=2
(78,55,28) k=1
(78,55,29) k=2
(78,55,34) k=1
(78,55,38) k=1
(78,55,42) k=1
(78,55,51) k=2

(79,23,1) k=1
(79,23,2) k=1

(79,23,3) k=1
(79,23,4) k=1
(79,23,5) k=1
(79,23,6) k=1
(79,23,8) k=1
(79,23,9) k=1
(79,23,10) k=1
(79,23,11) k=1
(79,23,12) k=1
(79,23,15) k=1
(79,23,17) k=1
(79,23,18) k=1
(79,23,20) k=1
(79,23,22) k=1
(79,23,24) k=1
(79,23,27) k=1
(79,23,30) k=1
(79,23,33) k=1
(79,23,34) k=1
(79,23,37) k=1
(79,23,40) k=1
(79,23,41) k=1
(79,23,44) k=1
(79,23,47) k=1

(84,25,4) k=1
(84,25,8) k=1
(84,25,12) k=1
(84,25,20) k=1
(84,25,36) k=1
(84,25,40) k=1

(86,49,1) k=2
(86,49,2) k=1
(86,49,3) k=2
(86,49,4) k=1
(86,49,5) k=2
(86,49,6) k=1
(86,49,7) k=2
(86,49,8) k=1
(86,49,9) k=2
(86,49,10) k=1
(86,49,13) k=2
(86,49,14) k=1
(86,49,15) k=2
(86,49,17) k=2
(86,49,18) k=1
(86,49,19) k=2
(86,49,20) k=1
(86,49,21) k=2
(86,49,26) k=1
(86,49,27) k=2
(86,49,28) k=1
(86,49,29) k=2
(86,49,31) k=2
(86,49,38) k=1
(86,49,40) k=1
(86,49,42) k=1
(86,49,52) k=1
(86,49,63) k=2

(91,9,1) k=1
(91,9,2) k=1
(91,9,3) k=1
(91,9,4) k=1
(91,9,5) k=1
(91,9,6) k=1
(91,9,7) k=1
(91,9,8) k=1
(91,9,10) k=1
(91,9,12) k=1
(91,9,13) k=1
(91,9,14) k=1
(91,9,15) k=1
(91,9,16) k=1
(91,9,19) k=1
(91,9,20) k=1
(91,9,23) k=1
(91,9,24) k=1
(91,9,28) k=1
(91,9,29) k=1
(91,9,30) k=1
(91,9,37) k=1
(91,9,38) k=1
(91,9,39) k=1
(91,9,40) k=1
(91,9,46) k=1
(91,9,47) k=1
(91,9,48) k=1
(91,9,49) k=1
(91,9,57) k=1

(93,25,1) k=1
(93,25,2) k=1
(93,25,3) k=1
(93,25,4) k=1
(93,25,5) k=1
(93,25,6) k=1
(93,25,8) k=1
(93,25,9) k=1
(93,25,10) k=1
(93,25,11) k=1
(93,25,12) k=1
(93,25,13) k=1
(93,25,16) k=1
(93,25,17) k=1
(93,25,18) k=1
(93,25,20) k=1
(93,25,22) k=1
(93,25,24) k=1
(93,25,26) k=1
(93,25,29) k=1
(93,25,33) k=1
(93,25,36) k=1
(93,25,37) k=1
(93,25,40) k=1
(93,25,43) k=1
(93,25,44) k=1
(93,25,47) k=1
(93,25,48) k=1
(93,25,51) k=1
(93,25,55) k=1

(95,11,5) k=1
(95,11,10) k=1
(95,11,20) k=1
(95,11,25) k=1
(95,11,40) k=1
(95,11,50) k=1

(97,35,1) k=1
(97,35,2) k=1
(97,35,3) k=1
(97,35,4) k=1
(97,35,5) k=1
(97,35,6) k=1
(97,35,7) k=1
(97,35,9) k=1
(97,35,10) k=1
(97,35,11) k=1
(97,35,12) k=1
(97,35,13) k=1
(97,35,15) k=1
(97,35,18) k=1
(97,35,19) k=1
(97,35,20) k=1
(97,35,22) k=1
(97,35,23) k=1
(97,35,26) k=1
(97,35,27) k=1
(97,35,30) k=1
(97,35,33) k=1
(97,35,36) k=1
(97,35,38) k=1
(97,35,41) k=1
(97,35,44) k=1
(97,35,46) k=1
(97,35,47) k=1
(97,35,49) k=1
(97,35,52) k=1
(97,35,55) k=1
(97,35,60) k=1

(98,67,1) k=2
(98,67,2) k=1
(98,67,3) k=2
(98,67,4) k=1
(98,67,6) k=1
(98,67,8) k=1
(98,67,9) k=2
(98,67,11) k=2
(98,67,12) k=1
(98,67,13) k=2
(98,67,14) k=1
(98,67,16) k=1
(98,67,17) k=2
(98,67,18) k=1
(98,67,19) k=2
(98,67,23) k=2
(98,67,24) k=1
(98,67,26) k=1
(98,67,27) k=2
(98,67,29) k=2
(98,67,32) k=1
(98,67,33) k=2
(98,67,38) k=1
(98,67,39) k=2
(98,67,42) k=1
(98,67,48) k=1
(98,67,52) k=1
(98,67,57) k=2
(98,67,58) k=1
(98,67,73) k=2

References

[1] Bayer D., B. Sturmfels, Cellular resolutions of monomial modules. *J. Reine Angew. Math.*, 502:123-140, 1998.

[2] Campbell, J., *Hilbert Function of Abelian Group Orbits.* Reed College Thesis, 1999.

[3] Capani, L.R.A., G. Niesi. *CoCoA*. Available via anonymous ftp from: cocoa.dima.unige.it. a system for doing Computations in Commutative Algebra.

[4] Cox, D., J. Little, and D. O'Shea, *Ideals, Varieties and Algorithms.* New York: Springer-Verlag, 1992.

[5] Curtis, C. and I. Reiner, *Representation Theory of Finite Groups and Associative Algebras.* New York: InterScience, 1962.

[6] Davis, E.D., A.V. Geramita, and F. Orecchia. Gorenstein algebras and the Cayley-Bacharach theorem. *Proc. Amer. Math. Soc.*, 93(4):593-597, 1985.

[7] Eisenbud, D., *Commutative Algebra—with a View Toward Algebraic Geometry.* New York: Springer-Verlag, 1995.

[8] Fesler, C., *The Hilbert Function of the Permutahedron.* Reed College Thesis, 1996.

[9] Fulton, W. and J. Harris, *Representation Theory—A First Course.* New York: Springer-Verlag, 1991.

[10] Geramita, A.V., M. Kreuzer, and L. Robbiano. Cayley-bacharach schemes and their canonical modules. *Trans. Amer. Math. Soc.*, 339(1):163-189, 1993.

[11] Ireland, K. and M. Rosen, *A Classical Introduction to Modern Number Theory—2nd Edition.* New York: Springer-Verlag, 1990.

[12] Sturmfels, B., *Algorithms in Invariant Theory.* New York: Springer-Verlag, 1993.