Invariant Polynomials and Minimal Zero Sequences

Bryson W. Finklea

St. John's University

Terri Moore

Department of Mathematics, University of Washington

Vadim Ponomarenko

Department of Mathematics, Trinity University,
One Trinity Place, San Antonio, Texas 78212-7200
E-mail: vadim@trinity.edu

Zachary J. Turner

Department of Mathematics, University of Houston

A connection is developed between polynomials invariant under abelian permutation of their variables and minimal zero sequences in a finite abelian group. This connection is exploited to count the number of minimal invariant polynomials for various abelian groups.

1. INTRODUCTION

Invariant theory has a long and beautiful history, with early work by Hilbert [9] and Noether [12]. Classically, it is concerned with with polynomials over $\mathbb{R}$ or $\mathbb{C}$, invariant over certain permutations of its variables. For an introduction to this subject, see any of [4, 11, 13].

Let G be a finite abelian group, assumed without loss to be $G = \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_k}$. We fix a polynomial P in the variables x_g, for each $g \in G$. We let $h \in G$ act on the variables via $h : x_g \to x_{h+g}$, and therefore on

Research supported in part by NSF grant 0097366.
Mathematics Subject Classification (2000): Primary 13A50, 20K01; Secondary 20M14.

P in the natural way. Our goal is to find and count P invariant under all $|G|$ such actions, and minimal in the ring of polynomials. It is enough to find minimal P invariant under the k actions[1] $e_1 = (-1, 0, \dots, 0), e_2 = (0, -1, \dots, 0), \dots, e_k = (0, 0, \dots, -1)$. This extends the work of Strom [14], who focused on the case $k = 1$.

Switching gears, we now define a minimal zero sequence in a finite abelian group G. A sequence is a multiset of elements of G. A zero sequence is a multiset whose sum is zero in G. A minimal zero sequence is a zero sequence minimal with respect to set inclusion. For example, four zero sequences in the group $\mathbb{Z}_7$ are $\{4, 3\}, \{6, 6, 2\}, \{0\}, \{4, 4, 3, 2, 1\}$. However, only the first three examples are minimal zero sequences.

Our main result connects these two questions.

THEOREM 1.1. *The number of minimal polynomials P invariant under G is equal to the number of minimal zero sequences of G.*

Minimal zero sequences of finite abelian groups have been extensively studied (for example, [2, 7, 8, 10, 15]). In [6] is described an efficient algorithm for counting minimal zero sequences for a finite abelian group. Applying this algorithm we are able to extend the table found in [14] substantially. The results are found in Table 1.[2]

Space does not permit us to include much more of this table; it is available (together with the software used to generate it) up to $\mathbb{Z}_{64}$ at `http://www.trinity.edu/vadim/research.html`
However, we can report that the rightmost column that counts the total number of minimal invariant polynomials (which ends in $974, 1494$) continues as $2135, 3913, 4038, 7936, 8247, 12967, 17476, 29162, 28065, 49609, 59358, 83420, 97243, 164967, 152548, \dots$.

Also, we can report the total number of minimal invariant polynomials for some groups of the form $\mathbb{Z}_m \oplus \mathbb{Z}_n$ in Table 2.

2. PROOF OF MAIN THEOREM

Our general approach is to change variables so that all minimal invariant polynomials under the new variables will become minimal invariant monomials. After this change, the group action on the original variables acts on the new variables as scalar multiplication. This makes it easier to identify and count the minimal invariant monomials, and gives a correspondence between minimal invariant monomials and minimal zero sequences.

[1]The actions are chosen to be the negatives of the standard basis for technical reasons, to be evident later. These elements generate G.

[2]These results, through other methods, were also found by A. Elashvili and V. Tsiskaridze [5]. Their unpublished data matches ours, and equally continues to $\mathbb{Z}_{64}$.

TABLE 1.

Number of minimal invariant polynomials, by degree.

G	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	Total
$\mathbb{Z}_1$	1															1
$\mathbb{Z}_2$	1	1														2
$\mathbb{Z}_3$	1	1	2													4
$\mathbb{Z}_4$	1	2	2	2												7
$\mathbb{Z}_5$	1	2	4	4	4											15
$\mathbb{Z}_6$	1	3	6	6	2	2										20
$\mathbb{Z}_7$	1	3	8	12	12	6	6									48
$\mathbb{Z}_8$	1	4	10	18	16	8	4	4								65
$\mathbb{Z}_9$	1	4	14	26	32	18	12	6	6							119
$\mathbb{Z}_{10}$	1	5	16	36	48	32	12	8	4	4						166
$\mathbb{Z}_{11}$	1	5	20	50	82	70	50	30	20	10	10					348
$\mathbb{Z}_{12}$	1	6	24	64	104	84	36	20	12	8	4	4				367
$\mathbb{Z}_{13}$	1	6	28	84	168	180	132	84	60	36	24	12	12			827
$\mathbb{Z}_{14}$	1	7	32	104	216	242	162	96	42	30	18	12	6	6		974
$\mathbb{Z}_{15}$	1	7	38	130	306	388	264	120	88	56	40	24	16	8	8	1494

TABLE 2.

Number of minimal invariant polynomials for $G = \mathbb{Z}_m \oplus \mathbb{Z}_n$.

	$\mathbb{Z}_2$	$\mathbb{Z}_3$	$\mathbb{Z}_4$	$\mathbb{Z}_5$	$\mathbb{Z}_6$	$\mathbb{Z}_7$
$\mathbb{Z}_2$	5	20	39	166	253	974
$\mathbb{Z}_3$	20	69	367	1494	2642	12967
$\mathbb{Z}_4$	39	367	1107	8247	19463	97243
$\mathbb{Z}_5$	166	1494	8247	31029	164967	508162
$\mathbb{Z}_6$	253	2642	19463	164967	390861	4694718
$\mathbb{Z}_7$	974	12967	97243	508162	4694718	9540473

For all $m \in \mathbb{N}$, we set $\varepsilon_m = e^{\frac{2\pi\sqrt{-1}}{m}}$, where e is the usual transcendental $2.718\ldots$. We will need two well-known (for example, [1] or [3]) properties of these constants ε_m.

Proposition 2.1. *Let ε_m be as above. Then*

1.$(\varepsilon_m)^k = 1$ if and only if m divides k.

2.Let $j \in \mathbb{Z}$. Then $\sum_{k=0}^{m-1} (\varepsilon_m)^{jk} = \begin{cases} m, & \text{if } m \text{ divides } j; \\ 0, & \text{otherwise.} \end{cases}$

Recall that $G = \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_k}$. Henceforth, for $g \in G$, we use $(g)_i \in \mathbb{Z}$ to denote the projection of g onto the i^{th} coordinate. For each $h \in G$, we define a new variable y_h, a linear combination of the x_g's, as

$$y_h = \sum_{g\in G} \left(\prod_{i=1}^{k} (\varepsilon_{n_i})^{(g)_i (h)_i} \right) x_g$$

Naturally, we can write the x_g's as linear combinations of the y_h's, as below.

Lemma 2.1. *For all $g \in G$ we have*

$$x_g = \frac{1}{|G|} \sum_{h\in G} \left(\prod_{j=1}^{k} (\varepsilon_{n_j})^{(h)_j (n_j - (g)_j)} \right) y_h$$

Proof. We substitute for y_h into the right hand side to get:
$\frac{1}{|G|} \sum_{h\in G} \left(\prod_{j=1}^{k} (\varepsilon_{n_j})^{(h)_j (n_j - (g)_j)} \right) \sum_{g'\in G} \left(\prod_{i=1}^{k} (\varepsilon_{n_i})^{(g')_i (h)_i} \right) x_{g'} =$
$\frac{1}{|G|} \sum_{g'\in G} x_{g'} \sum_{h\in G} \left(\prod_{i=1}^{k} (\varepsilon_{n_i})^{(h)_i n_i} \right) \left(\prod_{i=1}^{k} (\varepsilon_{n_i})^{(h)_i ((g')_i - (g)_i)} \right) =$
$\frac{1}{|G|} \sum_{g'\in G} x_{g'} \sum_{h\in G} \left(\prod_{i=1}^{k} (\varepsilon_{n_i})^{(h)_i ((g')_i - (g)_i)} \right) = \frac{1}{|G|} \sum_{g'\in G} x_{g'} \left\{ \begin{array}{ll} |G|, & \text{if } g = g'; \\ 0, & \text{otherwise.} \end{array} \right\}$ ∎

The main reason for this change of variables is that the k actions permuting the variables act on the new variables as scalar multiplication.

Lemma 2.2. $e_j : y_h \to (\varepsilon_{n_j})^{(h)_j} y_h$.

Proof. We have $e_j \circ y_h = \sum_{g\in G} \left(\prod_{i=1}^{k} (\varepsilon_{n_i})^{(g)_i (h)_i} \right) x_{g+e_j} =$
$= \sum_{(g+e_j)\in G} \left(\prod_{i=1}^{k} (\varepsilon_{n_i})^{(g+e_j-e_j)_i (h)_i} \right) x_{g+e_j} = \sum_{g\in G} \left(\prod_{i=1}^{k} (\varepsilon_{n_i})^{(g-e_j)_i (h)_i} \right) x_g =$
$= y_h (\varepsilon_{n_j})^{-(e_j)_j (h)_j} = y_h (\varepsilon_{n_j})^{(h)_j}.$ ∎

An immediate consequence of the above is that $e_j : y_h^a \to (\varepsilon_{n_j})^{a(h)_j} y_h^a$. More generally, we can calculate the effect of e_j on an arbitrary monomial.

Lemma 2.3. *For constant α, $e_j : \alpha \prod_{h\in G} y_h^{a_h} \to \left((\varepsilon_{n_j})^{\sum_{h\in G} a_h (h)_j} \right) \alpha \prod_{h\in G} y_h^{a_h}$.*

Consider an invariant polynomial P in the x_g's. Apply the invertible linear change of variables to get a polynomial Q in the y_h's. We must also have Q invariant under the k actions. Furthermore, P is minimal if and only if Q is a monomial such that any nonconstant monomial properly dividing Q is not invariant.

By the previous discussion, an invariant polynomial P must correspond to a minimal monomial Q. Furthermore, since Q is invariant, we must have $\sum_{h \in G} a_h (h)_j \equiv 0 \pmod{n_j}$ for each j. Combining these j requirements, we get $\sum_{h \in G} a_h h = 0$, where 0 is the zero element in G. Therefore, we can consider the a_h as multiplicities for each element $h \in G$, and since the sum is zero we have a zero sequence. A nonconstant monomial Q' properly dividing Q would have corresponding a'_h, with $a'_h \leq a_h$ and not all equal. In that case, this Q' would correspond to a zero sequence properly contained in the previous zero sequence.

REFERENCES

1. Lars V. Ahlfors. *Complex analysis*. McGraw-Hill Book Co., New York, third edition, 1978. An introduction to the theory of analytic functions of one complex variable, International Series in Pure and Applied Mathematics.
2. Scott T. Chapman, Michael Freeze, and William W. Smith. Equivalence classes of minimal zero-sequences modulo a prime. In *Ideal theoretic methods in commutative algebra (Columbia, MO, 1999)*, volume 220 of *Lecture Notes in Pure and Appl. Math.*, pages 133–145. Dekker, New York, 2001.
3. Harold Davenport. *Multiplicative number theory*, volume 74 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2000. Revised and with a preface by Hugh L. Montgomery.
4. Igor Dolgachev. *Lectures on invariant theory*, volume 296 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 2003.
5. A. Elashvili and V. Tsiskaridze. Private Communication.
6. Bryson W. Finklea, Terri Moore, Vadim Ponomarenko, and Zachary J. Turner. On block monoid atomic structure. In Preparation.
7. Weidong Gao and Alfred Geroldinger. On long minimal zero sequences in finite abelian groups. *Period. Math. Hungar.*, 38(3):179–211, 1999.
8. Alfred Geroldinger and Rudolf Schneider. On Davenport's constant. *J. Combin. Theory Ser. A*, 61(1):147–152, 1992.
9. David Hilbert. über die vollen invariantensysteme. *Math. Annalen*, 42:313–373, 1893.
10. Marcin Mazur. A note on the growth of Davenport's constant. *Manuscripta Math.*, 74(3):229–235, 1992.
11. Mara D. Neusel and Larry Smith. *Invariant theory of finite groups*, volume 94 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2002.
12. Emmy Noether. Der enlichkeitssatz der invarianten endlicher gruppen. *Math. Annalen*, 77:89–92, 1916.

13. Peter J. Olver. *Classical invariant theory*, volume 44 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1999.

14. Carl W. Strom. Complete systems of invariants of the cyclic groups of equal order and degree. *Proc. Iowa Acad. Sci.*, 55:287–290, 1948.

15. P. van Emde Boas and D. Kruyswijk. A combinatorial problem on finite Abelian groups. *Math. Centrum Amsterdam Afd. Zuivere Wisk.*, 1967(ZW-009):27, 1967.