Invariant Polynomials and Minimal Zero Sequences

Bryson W. Finklea

St. John's College (undergraduate)

Terri Moore

University of Washington (undergraduate)

Vadim Ponomarenko

Department of Mathematics and Statistics, San Diego State University, 5500 Campanile Drive, San Diego, CA 92182-7720
E-mail: vadim123@gmail.com

Zachary J. Turner

University of Houston (undergraduate)

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 [14] and Noether [18]. Classically, it is concerned with polynomials over $\mathbb{R}$ or $\mathbb{C}$, invariant over certain permutations of its variables. For an introduction to this subject, see any of [5, 17, 19].

Minimal zero sequences (also called minimal zero-sum sequences) have also been the subject of considerable study (for example, see [3, 9, 11, 16, 23]). They are multisets of elements from a fixed finite abelian group G,

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

subject to the restriction that the sum (according to multiplicity) must be zero in G. This forms a semigroup under the multiset sum operation. For an introduction, see one of [2, 8, 10, 12].

Our main result, Theorem 1.1, connects these two areas of mathematics. Let G be a finite abelian group, and let $\mathfrak{I}$ be the subalgebra of the polynomial ring on $|G|$ variables, that is invariant under the variable permutation induced by G. We provide a canonical representation for $\mathfrak{I}$ under which the natural set of generators are bijective with minimal zero sequences of G. Since the 1948 paper of Strom [22], which settled the case where G has rank one, only partial progress [15, 21] has been made in this area.

Theorem 1.1. *There exists a canonical set of generators of $\mathfrak{I}$ in bijective correspondence with the set of minimal zero sequences of G, where generators of degree k correspond with sequences of cardinality k.*

2. APPLICATIONS

Our result permits us to count canonical generators of $\mathfrak{I}$ more efficiently, both by degree and in total. These results, found[1] in Table 1, use minimal zero sequence counting algorithms, such as recursively finding zero-free sequences, found in [7]. We are thus able to extend the table found in [22] substantially. The total number of canonical generators for cyclic G (the rightmost column of Table 1) is extended[2] in Table 2. We can similarly report the total number of canonical generators for some groups of the form $\mathbb{Z}_m \oplus \mathbb{Z}_n$ in Table 3. Some of these are of rank one and also appear in Table 1; they are included for completeness.

The relation between these two areas has great potential for mutual benefit. For example, two conjectures of Elashvili, as stated in [13], have already been partially proved in [20] and fully proved in [24], by considering Theorem 1.1.

3. PROOF OF MAIN THEOREM

Fix finite abelian group $G = \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_k}$. We consider the polynomial ring in the variables x_g, for each $g \in G$. We let $h \in G$ act on the variables via $h : x_g \to x_{h+g}$. Let $\mathfrak{I}$ denote the subring invariant

[1] Space considerations limit the size of these tables; larger versions are available (together with the software used to generate them) up to $\mathbb{Z}_{64}$ at `http://www-rohan.sdsu.edu/~vadim/research.html`

[2] These results, through other methods, were also found by A. Elashvili and V. Tsiskaridze [6]. Their unpublished data matches ours, and equally continues to $\mathbb{Z}_{64}$.

under all $|G|$ such actions, equivalently invariant under the k actions[3] $e_1 = (-1,0,\dots,0), e_2 = (0,-1,\dots,0),\dots, e_k = (0,0,\dots,-1)$.

We will describe a degree-preserving change of variables that will preserve $\mathfrak{I}$. After this change, the group action on the original variables will act on the new, canonical, variables as scalar multiplication.

For all $m \in \mathbb{N}$, we set $\varepsilon_m = e^{\frac{2\pi\sqrt{-1}}{m}}$, where e is the usual transcendental $2.718\dots$. We will need two well-known (for example, [1] or [4]) properties.

Proposition 3.1. *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 $\sum_{k=0}^{m-1} (\varepsilon_m)^{jk} = \begin{cases} m, & \text{if } m \text{ divides } j; \\ 0, & \text{otherwise.} \end{cases}$

For $g \in G$, we use $(g)_i \in \mathbb{Z}$ to denote the projection of g onto the i^{th} coordinate (for $1 \le i \le k$). For each $h \in G$, we define new variables y_h via:

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

The inverse change of basis is given explicitly below; hence this basis change is degree-preserving.

Lemma 3.1. *For all $g \in G$ we have*

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

Proof. We substitute for y_h into the right hand side to get:

$$\tfrac{1}{|G|} \sum_{h\in G} \left(\prod_{j=1}^{k} (\varepsilon_{n_j})^{(h)_j(-(g)_j)} \right) \sum_{g'\in G} \left(\prod_{i=1}^{k} (\varepsilon_{n_i})^{(g')_i (h)_i} \right) x_{g'} =$$

$$\tfrac{1}{|G|} \sum_{g'\in G} x_{g'} \sum_{h\in G} \left(\prod_{i=1}^{k} (\varepsilon_{n_i})^{(h)_i n_i} \right) \left(\prod_{i=1}^{k} (\varepsilon_{n_i})^{(h)_i((g')_i-(g)_i)} \right) =$$

$$\tfrac{1}{|G|} \sum_{g'\in G} x_{g'} \sum_{h\in G} \left(\prod_{i=1}^{k} (\varepsilon_{n_i})^{(h)_i((g')_i-(g)_i)} \right) = \tfrac{1}{|G|} \sum_{g'\in G} x_{g'} \left\{ \begin{array}{ll} |G|, & \text{if } g = g'; \\ 0, & \text{otherwise.} \end{array} \right\}$$

In the last step, if $g = g'$, then each term in the innermost product is 1. Otherwise, for some w, we have $(g')_w - (g)_w \neq 0$. We now collect

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

the summands n_w at a time, where the w^{th} coordinate assumes all possible values and the other coordinates are fixed. We pull out the common factors and apply Proposition 3.1 to get 0. ∎

Under the canonical basis $\{y_h\}$, the k actions permuting the variables act as scalar multiplication.

Lemma 3.2. $e_j : y_h \to (\varepsilon_{n_j})^{(h)_j} y_h$.

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

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

$$= y_h(\varepsilon_{n_j})^{-(e_j)_j(h)_j} = y_h(\varepsilon_{n_j})^{(h)_j}.$$ ∎

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

Observe that, under the canonical basis, all invariant polynomials may be written as the sum of invariant monomials. Further, each invariant monomial may be written as the product of invariant monomials. Hence, there is a canonical set of generators of $\mathfrak{I}$ under the canonical basis, namely the set of irreducible invariant monomials.

Consider an irreducible monomial $\prod_{h\in G} y_h^{a_h}$. 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. Further, this must be a minimal zero sequence by the irreducibility of the generator. Conversely, every minimal zero sequence yields an irreducible monomial.

TABLE 1.

Number of canonical generators of $\mathfrak{I}$, 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.

Total number of canonical generators for $G = \mathbb{Z}_n$.

$\mathbb{Z}_1$	1	$\mathbb{Z}_{16}$	2135	$\mathbb{Z}_{31}$	280352	$\mathbb{Z}_{46}$	7581158
$\mathbb{Z}_2$	2	$\mathbb{Z}_{17}$	3913	$\mathbb{Z}_{32}$	295291	$\mathbb{Z}_{47}$	10761816
$\mathbb{Z}_3$	4	$\mathbb{Z}_{18}$	4038	$\mathbb{Z}_{33}$	405919	$\mathbb{Z}_{48}$	9772607
$\mathbb{Z}_4$	7	$\mathbb{Z}_{19}$	7936	$\mathbb{Z}_{34}$	508162	$\mathbb{Z}_{49}$	15214301
$\mathbb{Z}_5$	15	$\mathbb{Z}_{20}$	8247	$\mathbb{Z}_{35}$	674630	$\mathbb{Z}_{50}$	15826998
$\mathbb{Z}_6$	20	$\mathbb{Z}_{21}$	12967	$\mathbb{Z}_{36}$	708819	$\mathbb{Z}_{51}$	20930012
$\mathbb{Z}_7$	48	$\mathbb{Z}_{22}$	17476	$\mathbb{Z}_{37}$	1230259	$\mathbb{Z}_{52}$	23378075
$\mathbb{Z}_8$	65	$\mathbb{Z}_{23}$	29162	$\mathbb{Z}_{38}$	1325732	$\mathbb{Z}_{53}$	34502651
$\mathbb{Z}_9$	119	$\mathbb{Z}_{24}$	28065	$\mathbb{Z}_{39}$	1709230	$\mathbb{Z}_{54}$	32192586
$\mathbb{Z}_{10}$	166	$\mathbb{Z}_{25}$	49609	$\mathbb{Z}_{40}$	1868565	$\mathbb{Z}_{55}$	44961550
$\mathbb{Z}_{11}$	348	$\mathbb{Z}_{26}$	59358	$\mathbb{Z}_{41}$	3045109	$\mathbb{Z}_{56}$	47162627
$\mathbb{Z}_{12}$	367	$\mathbb{Z}_{27}$	83420	$\mathbb{Z}_{42}$	2804474	$\mathbb{Z}_{57}$	63662925
$\mathbb{Z}_{13}$	827	$\mathbb{Z}_{28}$	97243	$\mathbb{Z}_{43}$	4694718	$\mathbb{Z}_{58}$	74515122
$\mathbb{Z}_{14}$	974	$\mathbb{Z}_{29}$	164967	$\mathbb{Z}_{44}$	4695997	$\mathbb{Z}_{59}$	102060484
$\mathbb{Z}_{15}$	1494	$\mathbb{Z}_{30}$	152548	$\mathbb{Z}_{45}$	5902561	$\mathbb{Z}_{60}$	85954379

TABLE 3.

Total number of canonical generators 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	152548	674630
$\mathbb{Z}_6$	253	2642	19463	152548	390861	2804474
$\mathbb{Z}_7$	974	12967	97243	674630	2804474	9540473

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. Yair Caro. Remarks on a zero-sum theorem. *J. Combin. Theory Ser. A*, 76(2):315–322, 1996.
3. 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.
4. 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.
5. Igor Dolgachev. *Lectures on invariant theory*, volume 296 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 2003.
6. A. Elashvili and V. Tsiskaridze. Private Communication.
7. Bryson W. Finklea, Terri Moore, Vadim Ponomarenko, and Zachary J. Turner. On groups with excessive Davenport constant. In Preparation.
8. Weidong Gao and Alfred Geroldinger. Zero-sum problems in finite abelian groups: A survey. *Expo. Math.*, 24(4):337–369.
9. Weidong Gao and Alfred Geroldinger. On long minimal zero sequences in finite abelian groups. *Period. Math. Hungar.*, 38(3):179–211, 1999.
10. Alfred Geroldinger and Franz Halter-Koch. *Non-unique factorizations*, volume 278 of *Pure and Applied Mathematics (Boca Raton)*. Chapman & Hall/CRC, Boca Raton, FL, 2006. Algebraic, combinatorial and analytic theory.
11. Alfred Geroldinger and Rudolf Schneider. On Davenport's constant. *J. Combin. Theory Ser. A*, 61(1):147–152, 1992.
12. Franz Halter-Koch. Finitely generated monoids, finitely primary monoids, and factorization properties of integral domains. In *Factorization in integral domains (Iowa City, IA, 1996)*, volume 189 of *Lecture Notes in Pure and Appl. Math.*, pages 31–72. Dekker, New York, 1997.
13. John C. Harris and David L. Wehlau. Non-negative integer linear congruences. *Indag. Mathem.*, 17:37–44, 2006.

14. David Hilbert. Über die vollen Invariantensysteme. *Math. Ann.*, 42:313–373, 1893.

15. Hanspeter Kraft and Claudio Procesi. Classical invariant theory, a primer.

16. Marcin Mazur. A note on the growth of Davenport's constant. *Manuscripta Math.*, 74(3):229–235, 1992.

17. Mara D. Neusel and Larry Smith. *Invariant theory of finite groups*, volume 94 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2002.

18. Emmy Noether. Der Endlichkeitssatz der Invarianten endlicher Gruppen. *Math. Ann.*, 77:89–92, 1916.

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

20. Vadim Ponomarenko. Minimal zero sequences of finite cyclic groups. *Integers*, 4:A24, 6 pp. (electronic), 2004.

21. Barbara J. Schmid. Finite groups and invariant theory. In *Topics in invariant theory (Paris, 1989/1990)*, volume 1478 of *Lecture Notes in Math.*, pages 35–66. Springer, Berlin, 1991.

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

23. 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.

24. Pingzhi Yuan. On the index of minimal zero-sum sequences over finite abelian groups. To appear.