

involve

a journal of mathematics

Invariant polynomials and minimal zero sequences

Bryson W. Finklea, Terri Moore,
Vadim Ponomarenko and Zachary J. Turner

 mathematical sciences publishers

2008

Vol. 1, No. 2

Invariant polynomials and minimal zero sequences

Bryson W. Finklea, Terri Moore,
Vadim Ponomarenko and Zachary J. Turner

(Communicated by Scott Chapman)

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 [1893] and Noether [1915]. Classically, it is concerned with polynomials over \mathbb{R} or \mathbb{C} that are invariant over certain permutations of their variables. For an introduction to this subject, see any of [Dolgachev 2003; Neusel and Smith 2002; Olver 1999].

Minimal zero sequences (also called minimal zero-sum sequences) have also been the subject of considerable study (for example, see [Chapman et al. 2001; Gao and Geroldinger 1999; Geroldinger and Schneider 1992; Mazur 1992; van Emde Boas and Kruswijk 1967]). They are multisets of elements from a fixed finite abelian group G 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 [Caro 1996; Gao and Geroldinger 2006; Geroldinger and Halter-Koch 2006; Halter-Koch 1997].

Our main result, Theorem 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 the $|G|$ 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 [1948], which settled the case where G has rank one, only partial progress [Kraft and Procesi 1996; Schmid 1991] has been made in this area.

MSC2000: primary 13A50, 20K01; secondary 20M14.

Keywords: invariant polynomials, minimal zero sequences, finite abelian group, block monoid, zero-sum.

Theorem 1. *There exists a canonical set of generators of \mathfrak{J} in bijective correspondence with the set of minimal zero sequences of G , where generators of degree k correspond to sequences of cardinality k .*

2. Applications

Our result permits us to count canonical generators of \mathfrak{J} more efficiently, both by degree and in total. These results, found in Table 1¹, use minimal zero sequence counting algorithms such as that found in [Finklea et al. \geq 2008] which recursively finds zero-free sequences. We are thus able to extend the table found in [Strom 1948] substantially. The total number of canonical generators for cyclic G (the rightmost column of Table 1) is extended in Table 2.² 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 [Harris and Wehlau 2006], have already been partially proved in [Ponomarenko 2004] and fully proved in [Yuan 2007], by considering Theorem 1.

3. Proof of main theorem

Fix the 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 $h : x_g \rightarrow x_{h+g}$. Let \mathfrak{J} denote the subring that is invariant under all $|G|$ such actions, and equivalently invariant under the k actions

$$\begin{aligned} e_1 &= (-1, 0, \dots, 0), \\ e_2 &= (0, -1, \dots, 0), \dots, \\ e_k &= (0, 0, \dots, -1). \end{aligned}$$

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

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

¹Space 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>

²These results, through other methods, were also found by A. Elashvili and V. Tsiskaridze [Elashvili and Tsiskaridze \geq 2008]. Their unpublished data matches ours, and equally continues to \mathbb{Z}_{64} .

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 1. Number of canonical generators of \mathfrak{J} , by degree.

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 properties (for example, see [Ahlfors 1978] or [Dav-enport 2000]).

\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 2. Total number of canonical generators for $G = \mathbb{Z}_n$.

	\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

Table 3. Total number of canonical generators for $G = \mathbb{Z}_m \oplus \mathbb{Z}_n$.

Proposition 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 $1 \leq i \leq k$). 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 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:

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

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 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 1 to get 0. \square

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

Lemma 2. $e_j : y_h \rightarrow (\varepsilon_{n_j})^{(h)_j} y_h$.

Proof. We have

$$\begin{aligned} e_j(y_h) &= \sum_{g \in G} \left(\prod_{i=1}^k (\varepsilon_{n_i})^{(g)_i (h)_i} \right) x_{g+e_j} \\ &= \sum_{(g+e_j) \in G} \left(\prod_{i=1}^k (\varepsilon_{n_i})^{(g+e_j-e_j)_i (h)_i} \right) x_{g+e_j} = \sum_{g \in G} \left(\prod_{i=1}^k (\varepsilon_{n_i})^{(g-e_j)_i (h)_i} \right) x_g \\ &= y_h (\varepsilon_{n_j})^{-(e_j)_j (h)_j} = y_h (\varepsilon_{n_j})^{(h)_j}. \quad \square \end{aligned}$$

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

Lemma 3. For constant α , $e_j : \alpha \prod_{h \in G} y_h^{a_h} \rightarrow \left((\varepsilon_{n_j})^{\sum_{h \in G} a_h (h)_j} \right) \alpha \prod_{h \in G} y_h^{a_h}$.

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.

4. Acknowledgement

The authors would like to thank the anonymous referee for some helpful references and suggestions.

References

- [Ahlfors 1978] L. V. Ahlfors, *Complex analysis*, Third ed., McGraw-Hill Book Co., New York, 1978. An introduction to the theory of analytic functions of one complex variable, International Series in Pure and Applied Mathematics. MR 80c:30001
- [Caro 1996] Y. Caro, “Remarks on a zero-sum theorem”, *J. Combin. Theory Ser. A* **76**:2 (1996), 315–322. MR 98f:20005 Zbl 0865.20037
- [Chapman et al. 2001] S. T. Chapman, M. Freeze, and W. W. Smith, “Equivalence classes of minimal zero-sequences modulo a prime”, pp. 133–145 in *Ideal theoretic methods in commutative algebra (Columbia, MO, 1999)*, Lecture Notes in Pure and Appl. Math. **220**, Dekker, New York, 2001. MR 2002d:11020 Zbl 1003.20047
- [Davenport 2000] H. Davenport, *Multiplicative number theory*, Third ed., Graduate Texts in Mathematics **74**, Springer, New York, 2000. Revised and with a preface by Hugh L. Montgomery. MR 2001f:11001
- [Dolgachev 2003] I. Dolgachev, *Lectures on invariant theory*, London Mathematical Society Lecture Note Series **296**, Cambridge University Press, Cambridge, 2003. MR 2004g:14051 Zbl 1023.13006
- [Elashvili and Tsiskaridze \geq 2008] A. Elashvili and V. Tsiskaridze, “Private Communication”.
- [van Emde Boas and Kruyswijk 1967] P. van Emde Boas and D. Kruyswijk, “A combinatorial problem on finite Abelian groups”, *Math. Centrum Amsterdam Afd. Zuivere Wisk.* **1967**:ZW-009 (1967), 27. MR 39 #2871
- [Finklea et al. \geq 2008] B. W. Finklea, T. Moore, V. Ponomarenko, and Z. J. Turner, “On groups with excessive Davenport constant”. In Preparation.
- [Gao and Geroldinger 1999] W. Gao and A. Geroldinger, “On long minimal zero sequences in finite abelian groups”, *Period. Math. Hungar.* **38**:3 (1999), 179–211. MR 2001f:11027 Zbl 0980.11014
- [Gao and Geroldinger 2006] W. Gao and A. Geroldinger, “Zero-sum problems in finite abelian groups: a survey”, *Expo. Math.* **24**:4 (2006), 337–369. MR 2313123
- [Geroldinger and Halter-Koch 2006] A. Geroldinger and F. Halter-Koch, *Non-unique factorizations*, Pure and Applied Mathematics (Boca Raton) **278**, Chapman & Hall/CRC, Boca Raton, FL, 2006. Algebraic, combinatorial and analytic theory. MR 2006k:20001
- [Geroldinger and Schneider 1992] A. Geroldinger and R. Schneider, “On Davenport’s constant”, *J. Combin. Theory Ser. A* **61**:1 (1992), 147–152. MR 93i:20024 Zbl 0759.20008
- [Halter-Koch 1997] F. Halter-Koch, “Finitely generated monoids, finitely primary monoids, and factorization properties of integral domains”, pp. 31–72 in *Factorization in integral domains (Iowa City, IA, 1996)*, Lecture Notes in Pure and Appl. Math. **189**, Dekker, New York, 1997. MR 98h:13003 Zbl 0882.13027
- [Harris and Wehlau 2006] J. C. Harris and D. L. Wehlau, “Non-negative integer linear congruences”, *Indag. Math. (N.S.)* **17**:1 (2006), 37–44. MR 2337163
- [Hilbert 1893] D. Hilbert, “Ueber die vollen Invariantensysteme”, *Math. Ann.* **42**:3 (1893), 313–373. MR 1510781
- [Kraft and Procesi 1996] H. Kraft and C. Procesi, “Classical invariant theory, a primer”, 1996, Available at <http://www.math.unibas.ch/~kraft/Papers/KP-Primer.pdf>.
- [Mazur 1992] M. Mazur, “A note on the growth of Davenport’s constant”, *Manuscripta Math.* **74**:3 (1992), 229–235. MR 93a:20036 Zbl 0759.20009

- [Neusel and Smith 2002] M. D. Neusel and L. Smith, *Invariant theory of finite groups*, Mathematical Surveys and Monographs **94**, American Mathematical Society, Providence, RI, 2002. MR 2002k:13012
- [Noether 1915] E. Noether, “Der Endlichkeitssatz der Invarianten endlicher Gruppen”, *Math. Ann.* **77** (1915), 89–92.
- [Olver 1999] P. J. Olver, *Classical invariant theory*, London Mathematical Society Student Texts **44**, Cambridge University Press, Cambridge, 1999. MR 2001g:13009
- [Ponomarenko 2004] V. Ponomarenko, “Minimal zero sequences of finite cyclic groups”, *Integers* **4** (2004), A24, 6 pp. MR 2005m:11024
- [Schmid 1991] B. J. Schmid, “Finite groups and invariant theory”, pp. 35–66 in *Topics in invariant theory (Paris, 1989/1990)*, Lecture Notes in Math. **1478**, Springer, Berlin, 1991. MR 94c:13002
- [Strom 1948] C. W. Strom, “Complete systems of invariants of the cyclic groups of equal order and degree”, *Proc. Iowa Acad. Sci.* **55** (1948), 287–290. MR 11,413d
- [Yuan 2007] P. Yuan, “On the index of minimal zero-sum sequences over finite abelian groups”, *J. Combin. Theory Ser. A.* **114** (2007), 1545–1551.

Received: 2007-10-28 Revised: Accepted: 2007-11-01

s-tmoore9@math.unl.edu

*Department of Mathematics, University of Nebraska-Lincoln,
203 Avery Hall, Lincoln, NE 68588-0130, United States*

vadim123@gmail.com

*Department of Mathematics and Statistics, San Diego State
University, San Diego, CA 92182, United States
<http://www-rohan.sdsu.edu/~vadim>*

