Invariant polynomials and minimal zero sequences

Bryson W. Finklea, Terri Moore, Vadim Ponomarenko and Zachary J. Turner
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 Kruyswijk 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 \( J \) 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 \( J \) 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.

Keywords: invariant polynomials, minimal zero sequences, finite abelian group, block monoid, zero-sum.
**Theorem 1.** There exists a canonical set of generators of $\mathcal{I}$ 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 $\mathcal{I}$ more efficiently, both by degree and in total. These results, found in Table 1\(^1\), 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 $\mathcal{I}$ denote the subring that is invariant under all $|G|$ such actions, and equivalently invariant under the $k$ actions

$$e_1 = (-1, 0, \ldots, 0),$$
$$e_2 = (0, -1, \ldots, 0), \ldots,$$
$$e_k = (0, 0, \ldots, -1).$$

(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 $\mathcal{I}$. After this change, the group action on the original variables will act on the new canonical variables as scalar multiplication.

---

\(^1\)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](http://www-rohan.sdsu.edu/~vadim/research.html)

\(^2\)These 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 $\mathbb{Z}_{64}$. 
INVARIANT POLYNOMIALS AND MINIMAL ZERO SEQUENCES

<table>
<thead>
<tr>
<th>G</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
<th>15</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Z_1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Z_2</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2</td>
</tr>
<tr>
<td>Z_3</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4</td>
</tr>
<tr>
<td>Z_4</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>7</td>
</tr>
<tr>
<td>Z_5</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>15</td>
</tr>
<tr>
<td>Z_6</td>
<td>1</td>
<td>3</td>
<td>6</td>
<td>6</td>
<td>2</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>20</td>
</tr>
<tr>
<td>Z_7</td>
<td>1</td>
<td>3</td>
<td>8</td>
<td>12</td>
<td>12</td>
<td>6</td>
<td>6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>48</td>
</tr>
<tr>
<td>Z_8</td>
<td>1</td>
<td>4</td>
<td>10</td>
<td>18</td>
<td>16</td>
<td>8</td>
<td>4</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>65</td>
</tr>
<tr>
<td>Z_9</td>
<td>1</td>
<td>4</td>
<td>14</td>
<td>26</td>
<td>32</td>
<td>18</td>
<td>12</td>
<td>6</td>
<td>6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>119</td>
</tr>
<tr>
<td>Z_{10}</td>
<td>1</td>
<td>5</td>
<td>16</td>
<td>36</td>
<td>48</td>
<td>32</td>
<td>12</td>
<td>8</td>
<td>4</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>166</td>
</tr>
<tr>
<td>Z_{11}</td>
<td>1</td>
<td>5</td>
<td>20</td>
<td>50</td>
<td>82</td>
<td>70</td>
<td>50</td>
<td>30</td>
<td>20</td>
<td>10</td>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>348</td>
</tr>
<tr>
<td>Z_{12}</td>
<td>1</td>
<td>6</td>
<td>24</td>
<td>64</td>
<td>104</td>
<td>84</td>
<td>36</td>
<td>20</td>
<td>12</td>
<td>8</td>
<td>4</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td>367</td>
</tr>
<tr>
<td>Z_{13}</td>
<td>1</td>
<td>6</td>
<td>28</td>
<td>84</td>
<td>168</td>
<td>180</td>
<td>132</td>
<td>84</td>
<td>60</td>
<td>36</td>
<td>24</td>
<td>12</td>
<td>12</td>
<td></td>
<td>827</td>
<td></td>
</tr>
<tr>
<td>Z_{14}</td>
<td>1</td>
<td>7</td>
<td>32</td>
<td>104</td>
<td>216</td>
<td>242</td>
<td>162</td>
<td>96</td>
<td>42</td>
<td>30</td>
<td>12</td>
<td>6</td>
<td>6</td>
<td></td>
<td>974</td>
<td></td>
</tr>
<tr>
<td>Z_{15}</td>
<td>1</td>
<td>7</td>
<td>38</td>
<td>130</td>
<td>306</td>
<td>388</td>
<td>264</td>
<td>120</td>
<td>88</td>
<td>56</td>
<td>40</td>
<td>24</td>
<td>16</td>
<td>8</td>
<td>8</td>
<td>1494</td>
</tr>
</tbody>
</table>

Table 1. Number of canonical generators of $\mathcal{I}$, by degree.

For all $m \in \mathbb{N}$, we set $\varepsilon_m = e^{2\pi \sqrt{-1} / m}$, where $e$ is the usual transcendental $2.718 \ldots$. We will need two well-known properties (for example, see [Ahlfors 1978] or [Davenport 2000]).

| Z_1 | Z_{16} | Z_{31} | Z_{46} | Z_2 | Z_{17} | Z_{32} | Z_{47} | Z_3 | Z_{18} | Z_{33} | Z_{48} | Z_4 | Z_{19} | Z_{34} | Z_{49} | Z_5 | Z_{20} | Z_{35} | Z_{50} | Z_6 | Z_{21} | Z_{36} | Z_{51} | Z_7 | Z_{22} | Z_{37} | Z_{52} | Z_8 | Z_{23} | Z_{38} | Z_{53} | Z_9 | Z_{24} | Z_{39} | Z_{54} | Z_{10} | Z_{25} | Z_{40} | Z_{55} | Z_{11} | Z_{26} | Z_{41} | Z_{56} | Z_{12} | Z_{27} | Z_{42} | Z_{57} | Z_{13} | Z_{28} | Z_{43} | Z_{58} | Z_{14} | Z_{29} | Z_{44} | Z_{59} | Z_{15} | Z_{30} | Z_{45} | Z_{60} |
|-----|-------|-------|-------|-----|-------|-------|-------|-----|-------|-------|-------|-----|-------|-------|-------|-----|-------|-------|-------|-----|-------|-------|-------|-----|-------|-------|-------|-----|-------|-------|-------|-----|-------|-------|-------|-----|-------|-------|-------|-----|-------|-------|-------|-----|-------|-------|-------|
| 1   | 2135  | 280352| 7581158| 2   | 3913  | 295291| 10761816| 4   | 4038  | 405919 | 9772607| 7   | 7936  | 508162 | 15214301| 15  | 8247  | 674630 | 15826998| 20  | 12967 | 708819 | 20930012| 48  | 17476 | 123059 | 23378075| 65  | 29162 | 1325732| 34502651| 119 | 28065 | 1709230| 32192586| 166 | 49609 | 1868565| 44961550| 248 | 59358 | 3045109| 47162627| 348 | 59358 | 2804474| 63662925| 74515122| 1494 | 152548| 5902561| 85954379|

Table 2. Total number of canonical generators for $G = \mathbb{Z}_n$. 
Table 3. Total number of canonical generators for $G = \mathbb{Z}_m \oplus \mathbb{Z}_n$.

<table>
<thead>
<tr>
<th>$\mathbb{Z}_2$</th>
<th>$\mathbb{Z}_3$</th>
<th>$\mathbb{Z}_4$</th>
<th>$\mathbb{Z}_5$</th>
<th>$\mathbb{Z}_6$</th>
<th>$\mathbb{Z}_7$</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>20</td>
<td>39</td>
<td>166</td>
<td>253</td>
<td>974</td>
</tr>
<tr>
<td>20</td>
<td>69</td>
<td>367</td>
<td>1494</td>
<td>2642</td>
<td>12967</td>
</tr>
<tr>
<td>39</td>
<td>367</td>
<td>1107</td>
<td>8247</td>
<td>19463</td>
<td>97243</td>
</tr>
<tr>
<td>166</td>
<td>1494</td>
<td>8247</td>
<td>31029</td>
<td>152548</td>
<td>674630</td>
</tr>
<tr>
<td>253</td>
<td>2642</td>
<td>19463</td>
<td>152548</td>
<td>390861</td>
<td>2804474</td>
</tr>
<tr>
<td>974</td>
<td>12967</td>
<td>97243</td>
<td>674630</td>
<td>2804474</td>
<td>9540473</td>
</tr>
</tbody>
</table>

Proposition 1. Let $\epsilon_m$ be as above. Then

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

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

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:

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

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

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

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

$$\frac{1}{|G|} \sum_{h \in G} \left( \prod_{j=1}^{k} (\epsilon_n)^{(h)_j} (- (g)_j) \right) \sum_{g' \in G} \left( \prod_{i=1}^{k} (\epsilon_n)^{((g')_i, -(g)_i)} \right) x_{g'} =$$

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

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 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.

Under the canonical basis $\{y_h\}$, the $k$ actions permuting the variables act as scalar multiplication.
Lemma 2. \( e_j : y_h \rightarrow (e_{n_j})^j y_h \).

Proof. We have

\[
e_j(y_h) = \sum_{g \in G} \left( \prod_{i=1}^{k} (e_{n_i})^j x_{g+e_j} \right) x_g = \sum_{(g+e_j) \in G} \left( \prod_{i=1}^{k} (e_{n_i})^j x_{g+e_j} \right) x_g = \sum_{g \in G} \left( \prod_{i=1}^{k} (e_{n_i})^j x_{g+e_j} \right) x_g = y_h(\epsilon_{n_j})^j y_h \tag{\text{□}}
\]

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

Lemma 3. For constant \( \alpha \), \( e_j : \alpha \prod_{h \in G} y_h^a h \rightarrow \left( \prod_{h \in G} (e_{n_j})^{a(h)} \right) \alpha \prod_{h \in G} y_h^a h \).

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 \( I \) 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

\[
\sum_{h \in G} a_h(h)_j \equiv 0 \quad (\text{mod } n_j)
\]

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


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